THE CYBER SECURITY GOVERNANCE BY INTERNAL AUDIT IN THE TURKISH BANKING SECTOR

DOCTORATE THESIS

MUSTAFA HAKAN SALDI

ESKİŞEHİR 2022

THE CYBER SECURITY GOVERNANCE BY INTERNAL AUDIT IN THE TURKISH BANKING SECTOR

Mustafa Hakan SALDI

DOCTORATE THESIS

Management Department

Advisor: Prof. Dr. Seval Selimoğlu

Eskişehir

Anadolu University

Institute of Social Sciences

May 2022

JÜRİ VE ENSTİTÜ ONAYI

ABSTRACT

THE CYBER SECURITY GOVERNANCE BY INTERNAL AUDIT IN THE TURKISH BANKING SECTOR

Mustafa Hakan SALDI

Management Department

Anadolu University, Institute of Social Sciences, May 2022

Advisor: Prof. Dr. Seval Selimoğlu

This study is designed to frame the functions of internal auditors in cyber security governance through the Delphi technique to collect the qualitative data from panelists who are selected from the Turkish banking sector, legislators, and academic environment. The goal of the study is to observe the processes in cyber security management which are interacted with internal auditors' operations in information technology audits by proposing predictive solutions for industry experts and academicians. In the first part of the study, the terms of internal audit, internal control, risk management, cyber security, governance, and cyber risk are examined conceptually. Then, in the second part, the interaction of internal audit functions with cyber security governance, risk, and compliance variables are investigated. In the research plan section, which covers the third part of the study, the exploratory sequential mixed methods research design is applied to organize the route to be followed in the practice of the study. In this context, firstly, the qualitative part is operated by using open-ended questions through semi-structured interviews as the first round of Delphi, and then the quantitative stage is processed by applying questionnaires for the second and third rounds of the Delphi. As a result, authorization is decided as the most critical component in cyber security governance for risk controls, and blockchain technology is recommended to automate and improve the continuous monitoring of cyberspace for secure encryption.

Key Words: Internal audit, Cyber Security, Governance, Delphi technique

ÖZET

TÜRK BANKACILIK SEKTÖRÜNDE İÇ DENETİM YOLUYLA SİBER GÜVENLİK YÖNETİŞİMİ

Mustafa Hakan SALDI

İşletme Anabilim Dalı

Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü, Mayıs 2022

Danışman: Prof. Dr. Seval SELİMOĞLU

Bu çalışma iç denetçilerin siber güvenlik yönetişimindeki fonksiyonlarını, Türk bankacılık sektöründen, yasa düzenleyicilerden ve akademik çevreden seçilen panelistlerden delphi tekniği ile elde edilen kalitatif veriler doğrultusunda çerçevelemek için tasarlanmıştır. Çalışmanın amacı iç denetçilerin bilgi teknolojileri kontrollerindeki operasyonları ile etkileşim halinde olan siber güvenlik yönetimi süreçlerini gözlemleyerek sektör uzmanlarına ve akademisyenlere geleceğe yönelik çözümler sunmaktır. Çalışmanın, birinci kısmında iç denetim, iç kontrol, risk yönetimi, siber güvenlik, yönetişim ve siber risk terimleri kavramsal açıdan incelenmiştir. Ardından, ikinci bölümde, iç denetim fonksiyonlarının siber güvenlik yönetişimi, risk ve uyumluluk değişkenleri ile etkileşimi sorgulanmıştır. Çalışmanın üçüncü kısmını kapsayan araştırma planı bölümünde ise keşifsel sıralı karma yöntemler araştırma tasarımı, çalışmanın pratiğe dönüştürülmesinde izlenecek rotayı organize etmek için uygulanmıştır. Bu bağlamda, birincil olarak, çalışmanın nitel bölümü kapsamında delphi tekniğinin ilk kısmı, hazırlanan açık uçlu soruların yarı yapılandırılmış görüşmeler doğrultusunda kullanılmasıyla gerçekleştirilmiştir, akabinde ise çalışmanın nicel kısmı anketlerin delphi yönteminin ikinci ve üçüncü kısımlarında kullanılmasıyla gerçekleştirilmiştir. Sonuç olarak, yetkilendirme siber güvenlik yönetişimindeki risk kontrolleri için en kritik parça olarak tanımlanarak, blok zincir teknolojisi güvenli şifreleme açısından siber uzaydaki faaliyetlerin sürekli izleme yöntemlerinin otomatikleştirilmesi ve iyileştirilmesi için önerilmiştir.

Anahtar Sözcükler: İç denetim, Siber güvenlik, Yönetişim, Delphi tekniği

ACKNOWLEDGMENTS

I present my regards to my esteemed advisor Prof. Dr. Seval Selimoğlu who continuously supports and guides me in conducting this doctorate thesis research study. Also, I particularly state my thankfulness to each of the thesis committee members, Prof. Dr. Gülsün Meriç Kurubacak who encourages me as my co-advisor with her efforts in practicing the method of this research and Assoc. Prof. Dr. Buket Karatop for her invaluable knowledge and contribution. Correspondingly, I indicate my thanks to all respected participants one by one for their acceptance to attend the research study with their precious time. Likewise, I express my glory to my family for their endless support.

16 May 2022

STATEMENT OF COMPLIANCE WITH ETHICAL PRINCIPLES AND RULES

I hereby truthfully declare that this thesis is an original work prepared by me; that I have behaved in accordance with scientific ethical principles and rules throughout the stages of preparation, data collection, analysis and presentation of my work; that I have cited the sources of all the data and information that could be obtained within the scope of this study, and included these sources in the reference section; and that this study has been scanned for plagiarism with "scientific plagiarism detection program" used by Anadolu University, and that "it does not have any plagiarism" whatsoever. I also declare that, if a case contrary to my declaration is detected in my work at any time, I hereby express my consent to all ethical and legal consequences that are involved.

Mustafa Hakan SALDI

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND DEFINITIONS

3LoD	:	Three Lines of Defense
5G	:	Fifth Generation Mobile Networks
5LoA	:	Five Lines of Assurance
APO	:	Align, Plan and Organize
ASQ	:	American Society for Quality
ATM	:	Automated Teller Machine
BAI	:	Bank Administration Institute
BMIS	:	Business Model for Information Security
BRSA	:	Banking Regulation and Supervision Agency
BS	:	British Standard
CAE	:	Chief Audit Executive
CBOK	:	Common Body of Knowledge
CCDCOE	:	Cooperative Cyber Defence Centre of Excellence
CCI	:	Cyber Capability Index
CEH	:	Certified Ethical Hacker
CEO	:	Chief Executive Officer
CERT	:	Computer Emergency Response Team
CG	:	Computer Graphics
CIA	:	Confidentiality, Integrity and Availability
CICA	:	Canadian Institute of Chartered Accountants
CII	:	Cyber Intent Index
CIO	:	Chief Information Officer
CIRT	:	Computer Incident Response Team
CISA	:	Certified Information Systems Auditor
CISO	:	Chief Information Security Officer
CMB	:	Capital Markets Board of Turkey
CML	:	Capital Markets Law

CMM	:	Capacity Maturity Model
COBIT	:	Control Objectives for Information and Related Technology
CoCo	:	Criteria of Control
COSO Commission	:	Committe of Sponsoring Organizations of the Treadway
CRO	:	Chief Risk Officer
CRSA	:	Control Risk Self-Assessment
CSIRT	:	Computer Security Incident Response Team
CSO	:	Chief Strategy Officers
CTI	:	Cyber Threat Intelligence
CTO	:	Chief Technology Officers
DDoS	:	Distributed Denial of Service
DLP	:	Data Loss Prevention
DPA	:	Data Protection Act
ECIIA	:	European Confederation of Institutes of Internal Audit
ENISA	:	European Union Agency for Network and Information Security
ERM	:	Enterprise Risk Management
EY	:	Ernst&Young
FERMA	:	Federation of European Risk Management Associations
FIPS PUB	:	Federal Information Processing Standards Publications
FIPS	:	Federal Information Processing Standards
FISMA	:	Federal Information Security Management Act
GAO	:	General Accounting Office
GCI	:	Global Cyber Security Index
GEIT	:	Governance of Enterprise Information Technology
GRC	:	Governance, Risk and Compliance
HM Treasury	:	Her Majesty's Treasury
HR	:	Human Resources
ICCP	:	Institute for the Certification of Computer Professionals
ICT	:	Information and Communication Technology

IDS : Intrusion Detection System

IEC : International Electrotechnical Commission

IGRM : Information Governance Reference Model

IIA : The Institute of Internal Auditors

IPS : Intrusion Prevention System

IPSEC : Internet Protocol Security

IRGC : International Risk Governance Council

IS : Information Systems

ISACA : Information Systems Audit and Control Association

ISAE : International Standards on Assurance Engagements

ISMS : Information Security Management System

ISO/IEC : International Organization for Standardization and International Electrotechnical Commission

ISO : International Organization for Standardization

ISSO : Information Systems Security Officer

IT : Information Technology

ITGI : Information Technology Governance Institute

ITIL : Information Technology Infrastructure Library

ITU : International Telecommunication Union

KPI : Key Performance Indicators

KPMG : Klynveld Peat Marwick Goerdeler

MCDA : Multi Criteria Decision Analysis

NAS : National Academies of Sciences

NASCAT : National Association of Shareholder&Consumer Attorneys

NATO : North Atlantic Treaty Organization

NCPI : National Cyber Power Index

NII : National Information Infrastructure

NIST CSF : National Institute of Standards and Technology Cyber Security Framework

NIST : National Institute of Standards and Technology

OECD	:	Organisation for Economic Cooperation and Development
OMB	:	Office of Management and Budget
OSCP	:	Offensive Security Certified Professional
OTP	:	One Time Password
OWASP	:	Open Web Application Security Project
PCAOB	:	Public Company Accounting Oversight Board
PCI DSS	:	Payment Card Industry Data Security Standards
PDLP	:	Personal Data Protection Law
PMBOK	:	Project Management Body of Knowledge
PMI	:	Project Management Institute
PwC	:	PricewaterhouseCoopers
RBIA	:	Risk Based Internal Auditing
RPA	:	Robotic Process Automation
SaaS	:	Software as a Service
SAI	:	Standards Australia International
SANS	:	SysAdmin, Audit, Network and Security
SCADA	:	Supervisory Control and Data Acquisition Systems
SCB	:	Shell Control Box
SEC	:	Securities and Exchange Commission
SHA	:	Secure Hash Algorithm
SIEM	:	Security Information and Event Management
SOC	:	Service Organization Controls
SOx	:	Sarbanes Oxley Act
SOX	:	Sarbanes-Oxley Act
SSID	:	Service Set Identifier
SWIFT	:	Society for Worldwide Interbank Financial Telecommunication
TCP/IP	:	Transmission Control Protocol/Internet Protocol
TOGAF	:	The Open Group Architecture Framework
U.K.DTI	:	United Kingdom Department of Trade and Industry

U.S.	:	United States
VOIP	:	Voice Over Internet Protocol
VPN	:	Virtual Private Network
WWW	:	World Wide Web

INTRODUCTION

The effects of technological developments are being undeniably perceived and observed in business flows and models of the organizations. Especially, financial industries which cover banking, insurance, and capital investment enterprises have been transforming their information and communication systems with algorithmic-based structures, tools, hardware, and software to quickly respond the customer needs through resilient and robust technological infrastructure. In such kinds of service sectors, the organizations have to deal with huge amounts of data that hold strategic importance and can be considered as sensitive assets that reflect the goodwill of a company. Therefore, specifically, the implementation of suitable cyber security systems into the banks is necessary to gain customer loyalty and commitment by providing the confidentiality, integrity, and availability of information assets with testifying the validity of audit and control activities. Particularly, internal audit which has precise functions in operational, financial, and managerial examinations in organizational processes, has also responsibilities in cyber security systems as verification of internal controls and risk management activities through the analyses of compliance-related problems and governance issues. In the global environment, the risk culture of industries has been being shifted with the exponential growth and avalanche improvements in technology according to the innovations which are coming along with robotics, retail automation, artificial intelligence, machine learning, virtual reality, wireless networks, cloud computing, fifth-generation mobile systems, Internet of Things (IoT), blockchain and quantum computing. Therefore, the concerns are turning around the privacy and security of personal and corporate data which are gathered, recorded, kept, processed, flowed, accessed, and transferred by these IT systems. In summary, intolerable situations, which arise in the technology space, have been affecting the information security infrastructure, perception, and governance models of enterprises can be considered as cyber risk. In this context, escalating importance to safeguard the critical assets from cyber risks come to the fore with the reassessment of cyber security governance mechanisms. So, the new terms come up and reconstruct the conventional approaches in corporate governance structures from the internal audit perspective. In this sense, the role of internal audit has been being modified to new developments and standards in both macro and micro-frame by considering cyber risks into consideration. Precisely, the enterprises must adapt to these transformations by organizing their cyber security governance patterns through the

supportive role of internal audit. Concerning to mentioned reasons, this Ph.D. thesis study is produced in terms of aiming to deeply investigate the role of internal audit on cyber security governance in the Turkish banking sector by applying the Delphi technique. Thus, this thesis study is designed to discover the role of internal audit in cyber security governance by focusing on the Turkish Banking Sector. The research study will be based on both the theoretical framework of the subject and will be backed by the application of the Delphi technique which is selected as a scientific methodology to gather qualitative data from bank managers, experts, and academicians.

1. CONCEPTUAL FRAMEWORK WITH THE DEFINITIONS OF FUNDAMENTAL TERMS

The international finance mechanisms have been confronting with cyber risks since the computerized structures have been dominating conventional financial transactions due to the emerging technical improvements. Therefore, banks, which have a critical significance level because their businesses are heavily based on sensitive clients' data and intangible assets as a result of the nature of the banking industry, are being affected by varying cyber-attacks and threats. Especially, the principles which serve as a corporate structure can be designed and established via adequate cyber risk management approaches, strategies, governance frameworks, and continuous improvement of organizational culture and learning. Also, the corporate management principles can provide the organizations to step in a dynamic activity for the reconsideration of their cyber security systems, strategies, and frameworks to be prepared for both the external and internal attack surface. Thus, the first part of the thesis study is outlined to present the theoretical and fundamental pattern of the subject in terms of defining and perceiving the basic terms in audit, control, and cyberspace, before going into the deep research of international cyber security policies, frameworks, Turkish banking sector and it's interaction with internal audit and cyber security governance aspects.

1.1. Audit

In general, every enterprise operates businesses to be sustainable in a competitive environment by reaching corporate goals and performance objectives. As a result of the operations, enterprises need to record, monitor, and improve their activities by refreshing their organizational cultures dynamically. Therefore, the top managements execute this

loop of systematical detection process by integrating audit as a way of following the overall performance of enterprises. Briefly, a holistic, independent, and science-based examination of the organizational activities which include finance, human resources, production, marketing, and technology are performed by the efforts of qualified experts is defined as audit (Kumar & Sharma, 2013, p. 2).

The audit is defined in the records of ISO 19011:2018, as a set of organized, independent, reported, and documented cycles to provide audit statements that testify to the objective evaluations through the identification of which audit criteria are met. An audit operation can be classified as process, product, and system according to the type of activity. Also, the kind of audit can be categorized as internal or external corresponding to the relationship between associates. Likewise, audits can be sorted according to their goals as function audit which is performed for a particular division or activity, and management audit which is executed for administrative concerns such as evaluations of specific performance fields or effectiveness. As mentioned above, an audit activity can be defined as internal or external due to the association of contributors such as the type of audit can be called internal if the audit operations are being performed by the organization's employees and department. On the flip side, an audit can be classified as external if the audit activities are being operated by outside agents. In other words, internal audits are discussed as first-party examinations, whereas external audits can be considered as second-party or third-party. First-party audits are executed through the auditors who are put into service by the organization to assess the strengths and weaknesses of business processes versus the legal framework and authorized external standards. Second-party audits are implemented to a supplier by an external customer or by an employed organization on account of the customer. Second-party audits are performed with extra formal approaches which can affect the purchasing decision of customers in contrast to the first-party audits. The third-party audits are done by an independent audit firm that is free from conflict of interest and result after reviews with endorsement, registration, certification, license authorization, award, citation, charge, or penalty. Enterprises that are sustaining their businesses in high-risk classes must be confirmed by third-party audit organizations to show their compliance level to international standards such as ISO 9001, ISO 14001, ISO 22000, or ISO 27000. Also, audits have goals beyond examining the compliance matter cases and parameters which can be considered as the objectives for

adding value and providing continuous improvement in organizations to focus on performance metrics (ASQ, 2021).

In practice, after an organization specifies the requirements in audit services for which approaches will be applied to business functions, the chief audit executive (CAE) is assigned for the utilization of professional audit standards. However, internal audit is explained as a professional discipline based on sophisticated standards, there are diversified ways in carrying out the internal audit services inside the enterprises. But, this does not mean that every person without education or training may perform the audit profession. Relatively, diversities in approaches and applications of internal audit services provide resiliency, versatility, and adaptability in organizations. For example, Performance Standard 2100 clarifies the internal audit function as assessing and supporting the enhancement of governance, risk management, and control activities by implementing systematic and disciplined ways and techniques. Differently, Performance Standard 2120.A1 enlightens the activity of internal audit as evaluation of risks which are relevant to the governance structures, business processes, and information systems by taking into account the trustworthiness and integrity of fiscal and operational information, effectiveness and efficiency of operations, security of assets, compliance with principles and legislative framework. Therefore, professional standards set the epistemic guidelines for internal audit services, despite they do not have a specific role in the development of a methodology or practice. Feasibly, the final method of internal audit activity in an organization is formed by the combination of elements as the operating sector, business type and objectives, product and service segmentation, values, and intellectual capital. Conceptually, another notion of internal audit role in enterprises is stood on risk-based systems to provide validity in assurance function besides the direct consulting service and support for installation of risk management structures in organizations. In essence, a predesign is needed to follow risk-based systems audit in enterprises at the first step. Therefore, the internal audit activities and services necessitate policies for outlining the systems of organizations by preventive approaches to describe deficiencies and misconducts in the first place on the part of risk-based systems methods. After the designation of major risks, the measurements and assessments of specific controls which shape the principle view of risk management strategies are taken into account for evaluating the capability of control processes. Additionally, the compliance tests are applied to inspect control systems in organizations for ensuring the accuracy of the audit

results. Just in case, if there are still inadmissible residual risks inside an organization, reexamination of control systems are operated and reporting mechanism will be stepped in. In terms of completing the follow-up audit activities, the role of CAE is defined in Performance Standard 2060 as reporting to the board and senior management about the objective, authority, responsibility, and achievements in performance goals of internal audit events according to predisposed routes and plans. As well, reporting parts should cover risk and control cases referring to the fraudulent issues and governance breakdowns for adequate acknowledgment of managements in enterprises. The criteria of processing the risk-based systems audit in organizations are remarked in Figure 1 as a conceptual model (Pickett, 2011, pp. 203, 204, 205).

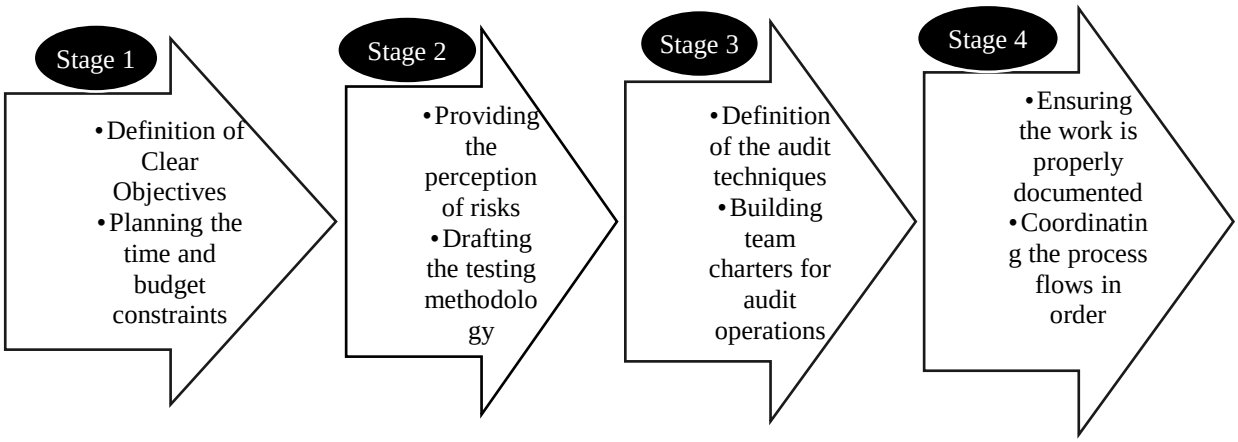


Figure 1.1. *Risk-Based Systems Audit Flowing Diagram (Pickett, 2011, p. 206)*

In the first step of the risk-based systems audit approach, it is necessary to define the objectives clearly for measuring the organizational achievements according to actual outputs. Next, the planning part of the limitations as time, cost, and budget are activated for providing a continuous review of operations in each stage by audit authorities. Variables in the voice of the customer should be analyzed thoroughly for ensuring a total understanding of the enterprise risks which have impacts on the achievements of organizational goals. By the application of the tryouts, after assessment and compliance testing methods, the change over the function of the process flow for the next stage is performed. From the technical point of view, structural outlining, flow-charting, cross-examinations, control self-evaluating, numerical and statistical sampling methods are

carried out for assessing the functioning of the audit services. The problematic cases, deficiencies, flaws, and breakdowns should be considered with team charters by alternating ideas for analytical and sustainable solutions through feedback systems. The formal documentation mechanisms provide that all the activities in an audit service are entirely cataloged and recorded for the assessment of quality standards and procedures which are the core roles of audit teams and managers. Finally, the coordination and interaction of processes in a flowing diagram of risk-based systems audit approach must be transformed into practice systematically for succeeding the sufficiency and effectiveness of risk management and governance mechanisms in enterprises (Pickett, 2011, pp. 206, 207).

Feasibly, organizational functioning can be simulated as a complete business model with a sequence of processes that encloses functions of workflows in the financing, marketing, production, human resources, information technology, sales, and marketing to visualize and streamline the operations in audit and control systems (Pickett, 2011, p. 207).

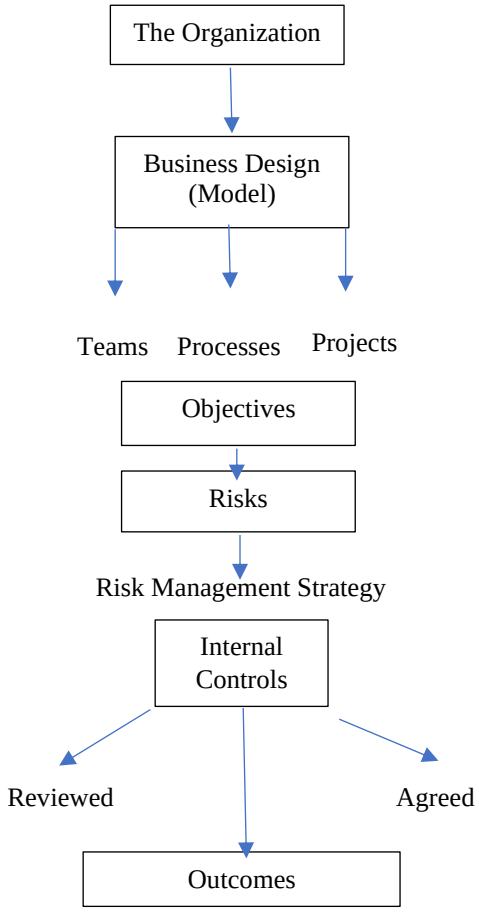


Figure 1.2. *Risk-Based Systems Auditing Process (Pickett, 2011, p. 207)*

Conceptually, an organization is harmonized with three elements as teams, processes, and projects through setting objectives and risk management strategies for review in depth by internal audit in all respects of the organization according to the risk-based systems auditing process model. In practice, there is no possibility to ensure outright neutrality in organizations however, in such kind of system, both evaluations of the feedback mechanism and measurement of the deviations between expected and actual outcomes for impartial assessment of achievement levels in objectives can be operated by audit functions. (Pickett, 2011)

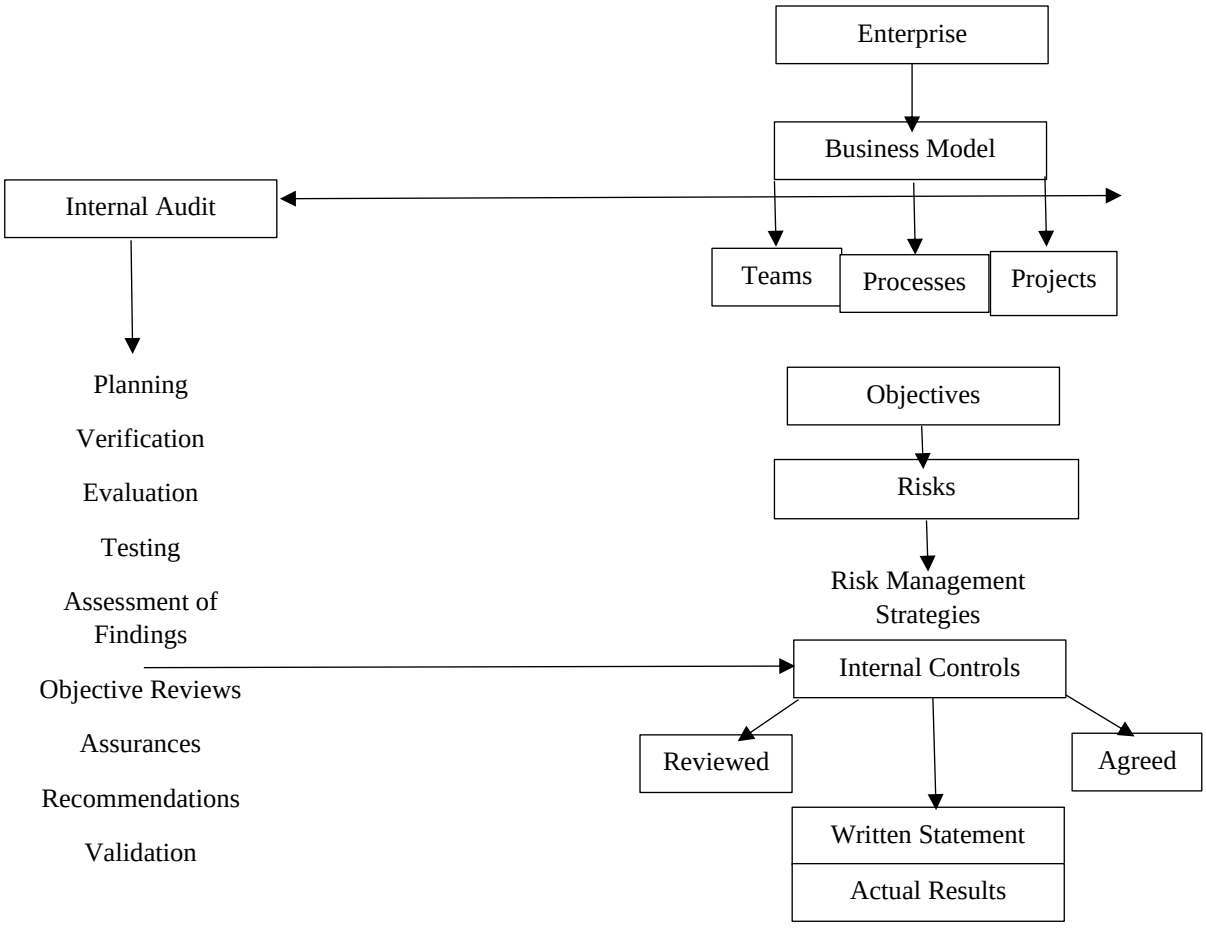


Figure 1.3. *Risk-Based Systems Auditing Process (Improved with Internal Audit Functions) (Pickett, 2011)*

Technically, the compound of business objectives, control mechanisms, and risks is established into organizations by control risk self-assessment (CRSA) methodology for enhancement of risk management approaches and practices all through the enterprises.

As such, this technique can be performed by all levels of management and audit teams. In this way, chief audit executives (CAE) can compile a complete system from the aspects of both audit processes and corporate objectives of enterprises. Also, this tool not only provides a risk management strategy by proposing a self-assessment cycle but also interacts with internal control for lean to focus on predetermined underlying risks in the organizations. In essence, authorizing the project teams to consider their risk management approaches and strategies can promote awareness of the key risks through organizational agility and resiliency for making realistic decisions and actions. CRSA technique supports the interactions between the operational activities which are conducted by project teams and managerial processes which are coordinated by executives and auditors. In addition, the acceptance of the consulting role for assisting the establishment of CRSA into organizations by the Institute of Internal Auditors demonstrates the expertise points of internal audit. Following a similar logic, the synergy is created by the interactions of the CRSA participants, project, and audit teams for increasing value-added activities via internal audit processes that can provide the symmetrical dispersal of responsibilities all over an organization. The framework of Practice Advisory 2120.1 is proposed by IIA emphasizes extraction points of internal audit role in overall mechanism as describing the self-assessment activities' effectiveness of management by examinations, regular testing of control and monitoring procedures with scanning the validity of information used in audit functions. Naturally, CRSA practices can be integrated into organizations with alternative ways for simplification of the multidimensional consistency by adopting techniques that are appropriate to organizational culture as part of intellectual capital. This approach provides one of the benefits for organizations as clarification of the connection between risk planning, analyzing, controlling, assessing, monitoring, and performance management activities for achievement of effective governance by utilizing risk management strategies in all parts of organizations. In practice, interpretation of the self-control assessment processes in organizations can be applied as workshops by setting team cases or group meetings through carrying out survey studies or questionnaires which are called the applications of business risk management philosophy. Also, statistical methods can be implemented for the measurement and inspection of self-control assessment outcomes by using representative samples from stakeholders, management, or project teams. To perform mentioned tools, techniques, and approaches in business risk management strategies, primarily the board of directors hands over the responsibility

to the corporate planning officer for the construction of the link between risk management and performance objectives in organizations. Therefore, organizations can take precautions for the key specific risks, if the system design of the control self-assessment model is supported by a chief risk officer who is supported by board management and also responsible for planning operations through meticulous monitoring of audit and risk management teams too (Pickett, 2011).

Fundamentally, corporate governance practices are needed to risk controlling processes through diagnosing business risks with the formal explanations of how they are being managed. Indeed, performing risk management operations is the core and pivotal role of internal control. Also, the administrative functions depend on the identification and execution of risks are operated under the full responsibility of the board of directors and in this context, the role of internal audit takes place as ensuring that business risks are being adequately managed to reach organizational goals. The effectiveness and efficiency of internal audit activities can be improved with the settlement of its functions as pillars of corporate governance into risk management frameworks of enterprises. Risk-based internal auditing (RBIA) is linked with all-around risk management structures of organizations due to the IIA's definition. Provision of assurance that risk management activities are being functioned effectively and properly in accordance with risk perceptions of organizations through assessing the risk appetite and tolerance variables is the major mission of RBIA. Therefore, the risk management frameworks of enterprises should be constructed robustly to structure effective internal controls for accomplishing the support of internal audits in corporate governance practices. There are challenges such as monitoring improvements versus annual plans which are being altered relative to variations in the business environment and setting organizational objectives with assessing the performance targets of employees to implement RBIA in comparison with traditional auditing methods. In reality, the design of risk management frameworks and functioning levels of them covering the effectiveness of internal controls with the categorization of risks and convenient reporting are the fields of internal audit's focal points for assuring the board managements (Chartered Institute of Internal Auditors, 2014).

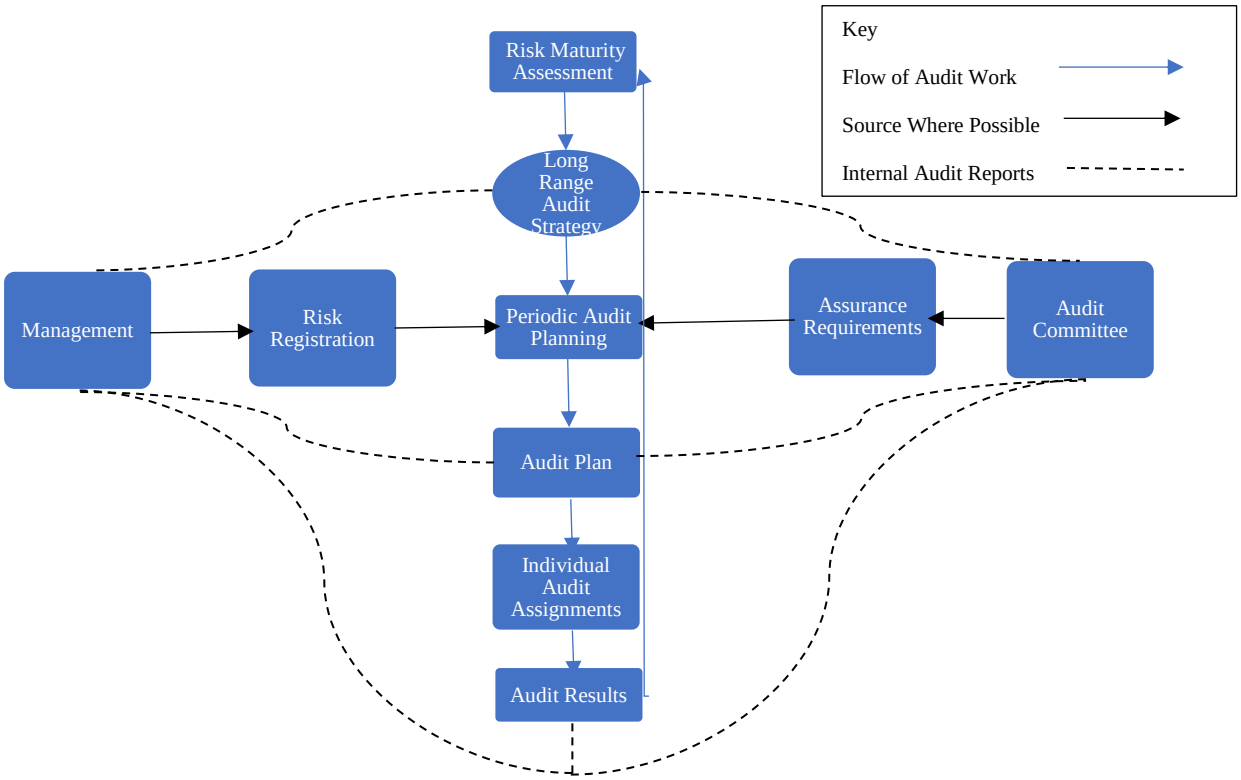


Figure 1.4. *RBIA Implementation Stages (Chartered Institute of Internal Auditors, 2014)*

In essence, risk-adjusted internal audit systems propose models for scanning how internal controls optimize risks to admissible levels. Therefore, the inspection of internal control structures is framed by the board managements through evaluating, testing, and monitoring the achievement level of business objectives are performed and assisted by internal audit with systematic approaches and practices. Methodically, risk-based internal audit systems provide the measurements for how the capability of internal control processes is adequate to tolerance and appetite levels of risks to understand organizational culture and resilience for uncertain cases. In this context, the risk maturity level of organizations can be defined through the problematics as how risks can be measured and how the measurements can be scaled and utilized with the full responsibility of the board management and support of internal audit functions. Correspondingly, the role of internal audit focuses on thoughts and notions for the assessments of adequacy level of the risks are being handled in proper with the organizational risk culture which indicates the viewpoint of board management and employees in terms of perceiving and tolerating risks (Griffiths, 2006).

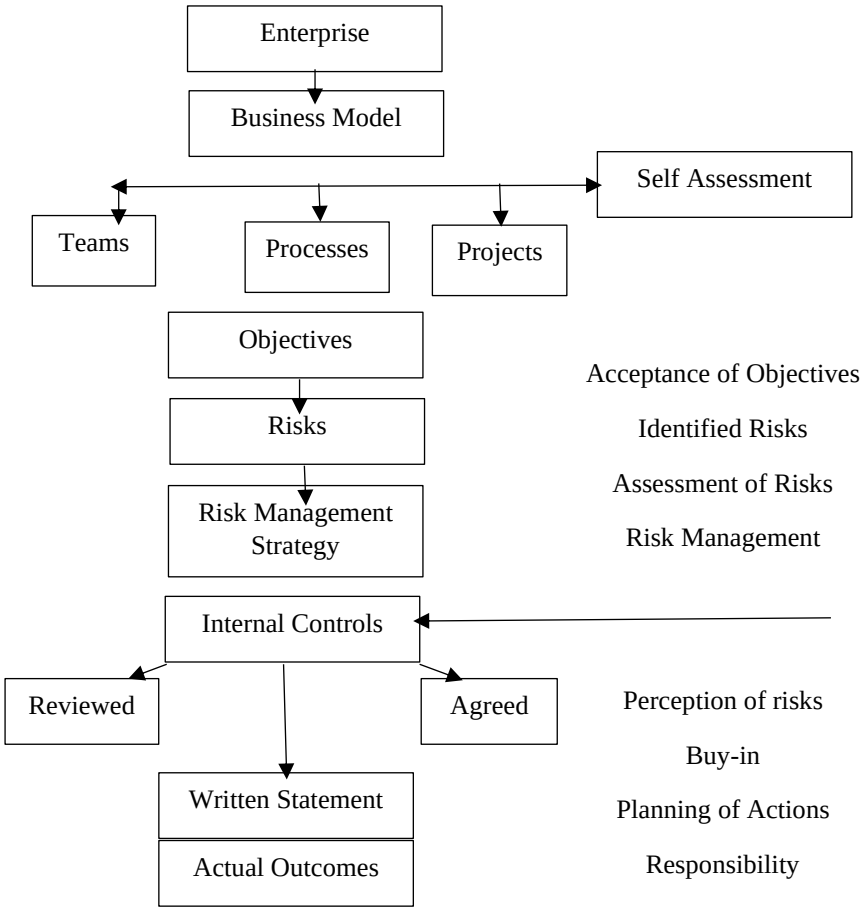


Figure 1.5. *Risk-Based Systems Auditing Process (Improved with Self Assessment Functions) (Pickett, 2011)*

Performance Standard 2201 of IIA advises about planning discussions for internal auditors to consider the objectives of each activity in business functions by which of them are capable of controlling their performance, the significant risks which affect the operations with an acceptable tolerance, the competence and effectiveness of risk management techniques and tools in comparison with commonly recognized control models, the cost and benefits of making advancements for the risk management and control mechanisms of business activities (Pickett, 2011).

Applicatively, the hybridization of audit objectivity and self-assessment processes which have a key role in evaluating and testing the information and knowledge within the organizations can develop an integrated approach. In this way, the risk management activities can be assessed by internal audit services to provide an objective and autonomous review of risk control systems. Also, the combination of both internal audit and self-assessment operations can improve the organizational integrity through the

formations of the multifaceted cross relations between each part of the business management model (Pickett, 2011). In summary, as a nature of the business environment, the internal audit role fits in supportive activities for recognition of risks and guiding on controls through ensuring that the objectivity of internal auditors is not affected and they don't get a direct role in managing risks (Griffiths, 2006).

The operations such as crime, bribery, nepotism, demoralization, profiteering, malfeasance, extortion, misappropriation, and money laundering are explained in terms of fraudulent acts inside the organizations. The legal definition of fraud varies due to the countries, sectors, businesses, and organization types, but commonly deceptive behaviors and practices are providing a personal advantage for self benefits with the creation of losses or damages for the other employees can be defined as fraudulent activities in organizations. 2006 Fraud Act of United Kingdom was outlined for attracting notice to escalating risks in fraud acts as deceitful representation, disclosure of sensitive information and misconduct of responsibility and constituting up to date proposals, articles, and practices. The role of management and internal auditors differentiate precisely between each other to execute fraud prevention and detection activities in organizations. In essence, managements have responsibilities for the establishment and sustainment of effective control systems with acceptable costs in organizations. Assessments and tests are conducted by internal audit activities through the assistance of control mechanisms are installed by managements to improve the possibility of taking precautions against fraud activities (Pickett, 2011).

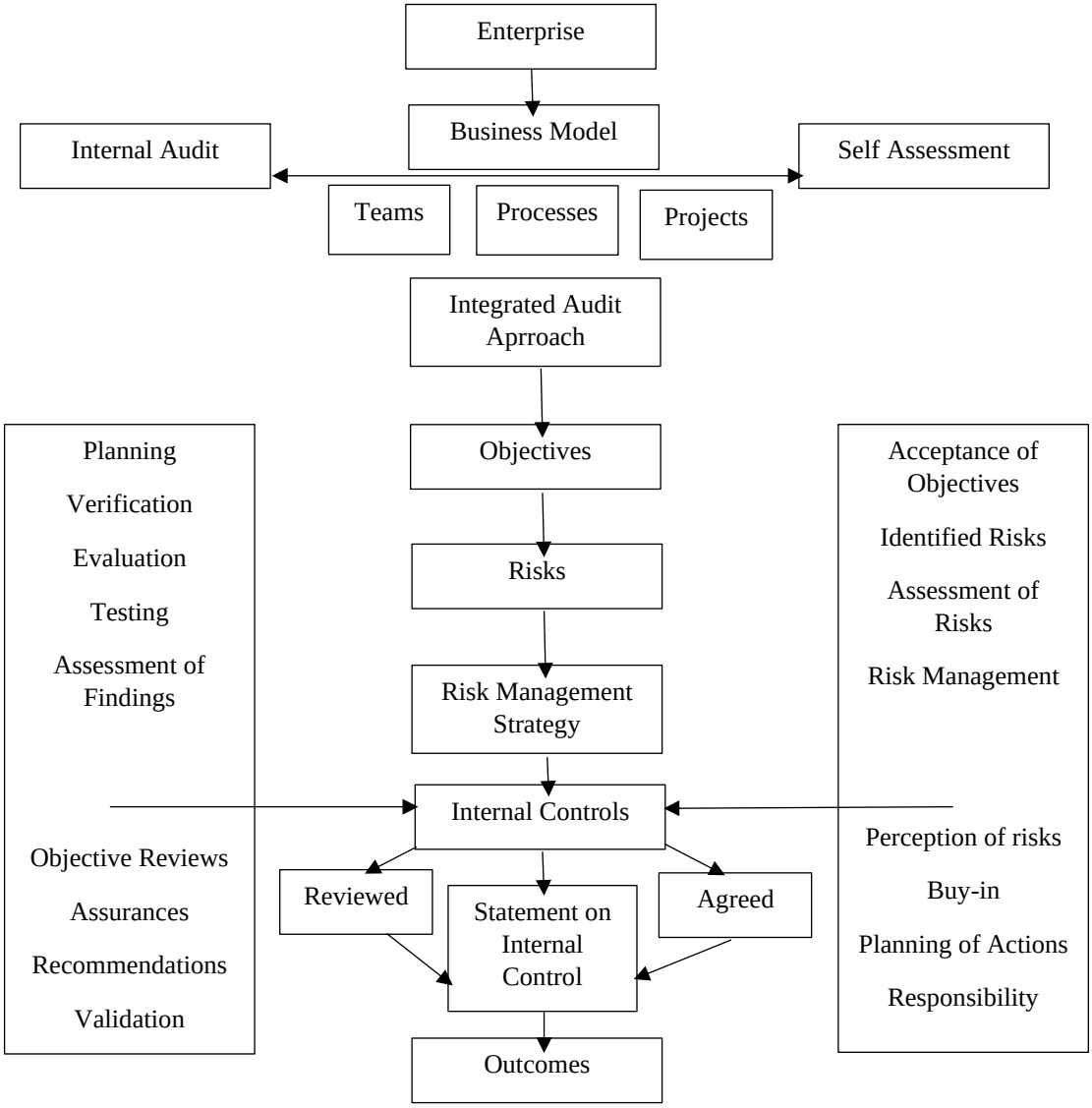


Figure 1.6. *Risk-Based Systems Auditing Process (Integrated Model) (Pickett, 2011)*

1.2. Internal Audit

Fundamentally, audit operations are classified as internal and external audits. According to the polite definition of the Institute for Internal Auditors, assisting processes as the consulting activity, which involves designing a systematic, disciplined approach to both assess and enhance the efficiency and effectiveness of risk management and governance mechanism based on an independent and objective manner is performed by the employees of an organization can be described as internal audit. On the other hand, an external audit differs from an internal audit because, there is a separate corporation that serves externally to provide audit operations for an organization (Gantz, 2014).

Particularly, the main basis of internal audit processes is to support organizations for reaching their objectives by enhancing their effectiveness of risk measurement, assessment, and control units by providing organized, disciplined techniques and mindsets. In similar, the internal audit role covers improving and reviewing the governance mechanisms in risk management systems of enterprises by contributing to value-added activities. Differently, internal audit processes are operated and executed by the employees of an organization internally. Therefore, the functions of internal audit are provided by taking the assistance of people from the inside of the organization. Additionally, internal audit operations have to be performed objectively to serve as an independent service. If this objectivity and independence of internal audit functions can not be ensured, the operating mechanism of the processes will be flawed from beginning to final. In fundamental, the consultative role of internal audit in enterprises supports the assuring of risk management in consistent with organizational plans and objectives. As well, the internal audit activities should be described certainly with a team charter, funding plan, and senior-level manager for provision of organizational awareness. Inherently, internal audit functions should be built on the voice of the customers according to the needs of enterprises for value creation in governance models. In common, continuous improvement philosophy in organizational management must be integrated into all levels of functions in the role of internal audit. The items of value chain mechanism in internal audit processes are designed to support the enterprises for reaching their corporate objectives through governance, internal control, and compliant risk management methods. Naturally, this mechanism requires professionalism with a clear understanding of principles and standards for satisfying the quality metrics and specifications of industries and enterprises. Thus, the functions of internal audit should be operated methodically in a disciplined and systematic manner. Particularly, principles, standards, guidelines, and policies should be planned, organized, and formed by the chief audit executive for instructing the internal auditors due to the Performance Standard 2040 of the Institute of Internal Auditors. Necessarily, the assessment of corporate governance, organizational management, and internal control processes is the uppermost task of internal audit for taking into account the reliability of operations. In practice, the evaluation formations should be executed neutrally and professionally in view of objective observations and specific pieces of information. Potentially, the measurement of effectiveness according to the level of attainment for corporate objectives demonstrates

the performance feedbacks of business functions in relation to the internal audit role. In long term, the control systems in enterprises are the indicator of efficiency and utility metrics which are analyzed and discussed by internal auditors. Therefore, the link between risk management, internal control, and governance is improved and reviewed by the internal audit processes. In summary, the vision, mission, plans, objectives, and activities in an enterprise should be fit together with a clear definition of risk appetite and risk tolerance degrees by taking the guidance of internal audit operations (Pickett, 2011).

Fundamentally, the core items of the internal audit role are obtainment of trustworthiness and integrity of operational and financial information for providing steady improvement in efficiency and effectiveness of organizational processes in compliance with standards, rules, and legislative framework by ensuring the uppermost protection of assets. In detail, identification, measurement, classification, reporting, and monitoring of the information assets are performed with the assistance of internal audit functions for the provision of governance mechanisms through the development of value creation activities in accordance with corporate objectives, principles, policies, and legal frame. Normally, the basic authority of internal audit processes in enterprises is the investigation of fraudulence in all operations of organizations to provide safeguard of assets with full responsibility for the integrity and reliability of operational, financial, cognitive, and technological systems. Therefore, in current conditions, the conventional approaches locked up to check the results of accounting and financial records are outdated in the practice of internal audit operations. As well, the educational role of internal audit in enterprises is undeniable for the assessment of the organizational culture and risk perception according to the parameters of both qualitative and quantitative variables with human conduct. The role of internal audit consists of the review of information technology systems for ensuring confidentiality, integrity, and availability of data sets, software, hardware, tools, and technical equipment with taking the support of internal control and risk management methods (Pickett, 2011).

1.3. Internal Control

Enterprises should implement control mechanisms internally to look over their organizational environment for attaining their achievable corporate objectives by examining and preventing misfortunes, risks, damages, and losses. In essence, the need for internal control processes causes businesses to comply with the legislation framework

by optimizing the inherent control environment of organizations. From this standpoint of view, the installation of corporate governance models to enterprises is dependent on the principles and policies of risk management techniques in internal control systems. Synchronistically, risk assessment operations are tested and performed by internal auditors consistently with internal control frameworks to eliminate misconceptions and conflicts for presenting effective interaction with the empowerment of governing body. The components of internal control structure in organizations are sources, operations, processes, business functions, task units, employees, and culture arranged and considered with holistic approaches in parallel with organizational plans and objectives (Pickett, 2011).

Risk management processes are functioned by internal controls with responding strategies through avoiding or also known as terminating, transferring, and tolerating the risks. In essence, internal control frameworks are based on the measuring systems of risks which are established by determining the risk appetite and tolerance levels of organizations. Therefore, the risk measurements should be identified before effective internal control structures are integrated into the organizations' risk management strategies in order to optimize the risks relative to accepted levels that are settled by the board of directors. In essence, the pivotal objective of internal controls is performing risk management activities in parallel with the role of RBIA which has functions as reacting to individual risks through assessment, monitoring, and reporting processes to acknowledge the board managements. In this sense, the functions of RBIA do not cover the audit operations of risks directly, however, their core missions are related to detecting the risk management activities which are operated by internal controls (Chartered Institute of Internal Auditors, 2014).

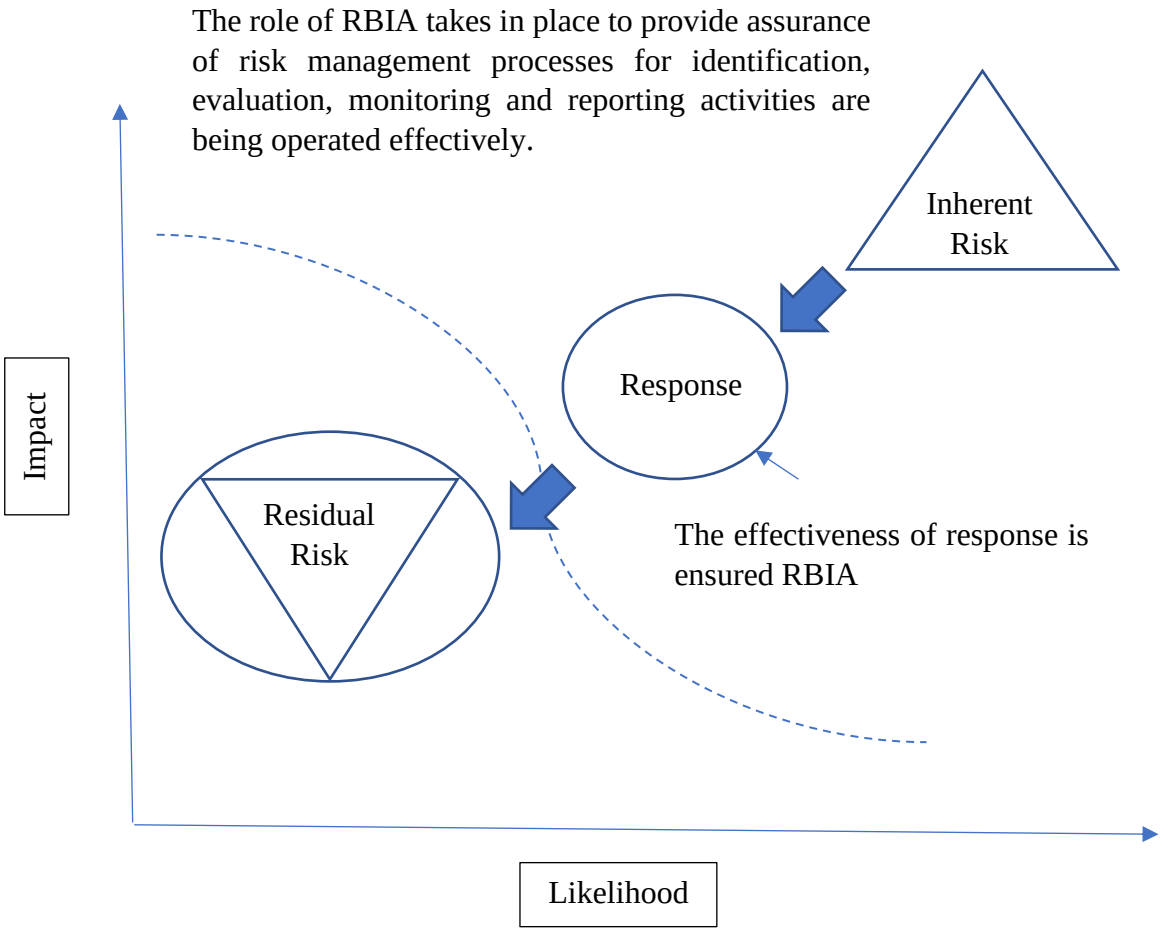


Figure 1.7. *Representation of Assurance Provided by RBIA (Chartered Institute of Internal Auditors, 2014)*

As a matter of fact, the internal control embodies processes that are implemented under the full responsibility of board management through taking the guidance of internal audit for providing sensible assurance relative to the accomplishments of business objectives concerning risk management, governance, and compliance. The basis of internal control frameworks is structured on three classes of objectives which are covered by operations, reporting, and compliance processes in terms of performing how the internal controls in organizations are being laid out, put into action and conducted feasibly for reasonable risk management practices. Operational objectives to reach performance goals include the protection of organizational assets in opposition to risks and losses. Reporting objectives are incorporated by parameters of accuracy, timeliness, and transparency metrics which are framed by organizational policies, authorized standard setters and legislators refer to financial and operational activities through the support of information systems. The objectives, which pertain to compliance criteria for adhering to legal frameworks, are shaped by organizational culture and governing bodies to catalyze

internal control activities. In practice, there are five combined parts that internal control involves as control environment, risk assessment, control activities, information, and communication as well as monitoring activities (COSO, 2013).

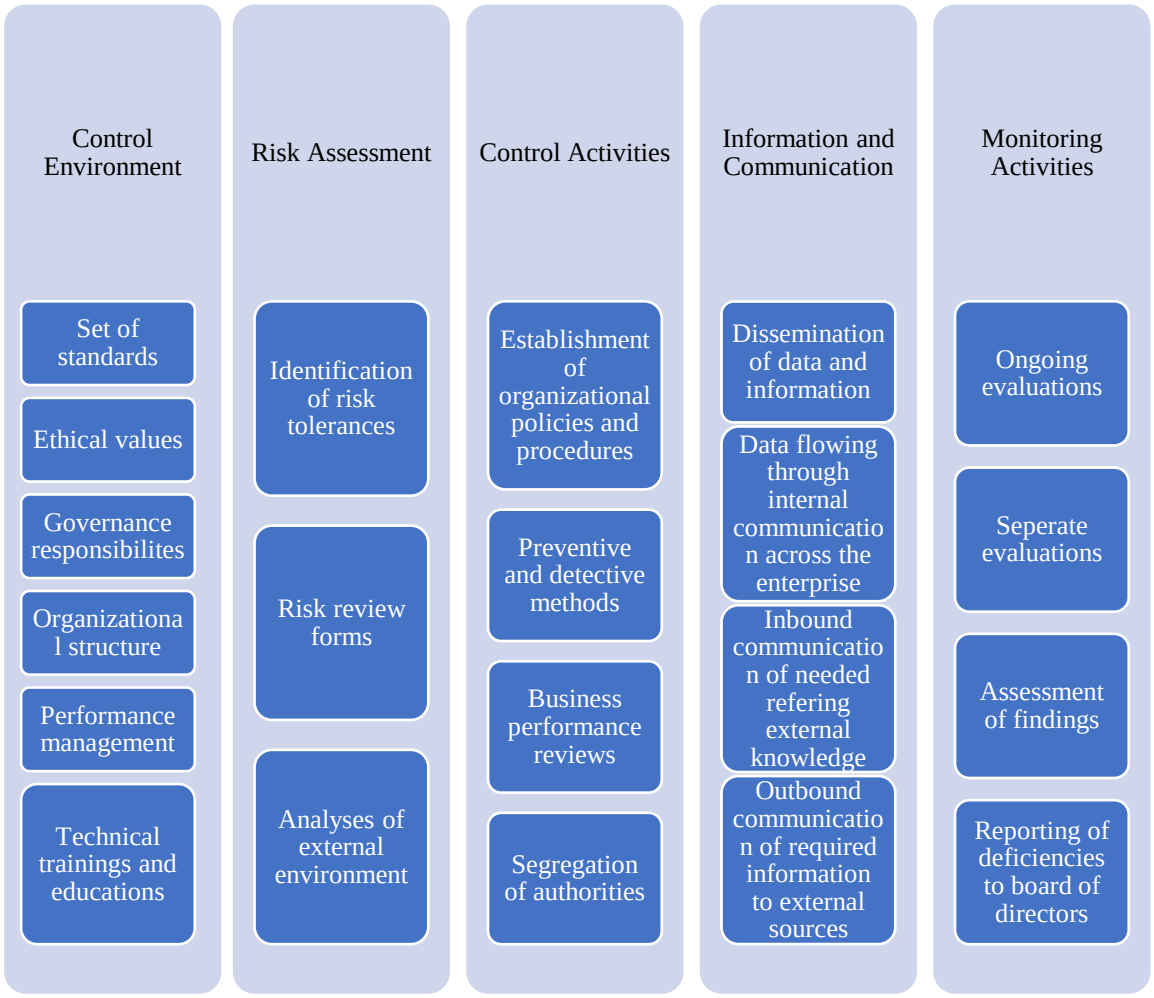


Figure 1.8. *The Items of Internal Control (COSO, 2013)*

The internal control framework covers five components are mentioned through entirely seventeen principles that indicate fundamental notions for the effectuation of internal control with the practices in operations, reporting, and compliance processes. Control environment principles can be stated as;

- The commitment to integrity and ethical values must be provided in the organizations.
- The board of directors manifests autonomy from management and practices for checking over the development and performance of internal control.

- The establishment of frameworks and reporting systems through adequate authorities and responsibilities for tracking business objectives must be provided by management.
- Qualified staff in adjustment with business objectives should be retained, improved, and attracted by policies and practices for providing organizational commitment in enterprises.
- Organizations hand over the liability to the experts who are responsible for internal controls in the achievement of business objectives.

Risk Assessment principles can be explained as;

- The organizational objectives must be specified clearly for enabling the determination and evaluation of risks on achievable goals.
- Identification of risks across the enterprise must be performed by the organization through analyses as essential for understanding how the risks should be handled.
- Consideration of the probable fraud events in assessment operations of risks related to the accomplishment of business objectives must be executed by the organization.
- Identification and assessment of both internal and external changing conditions, which can affect the internal control systems, should be operated by the organization.

The principles of control activities can be illustrated as;

- Control activities that add a contribution to the moderation of risks must be framed and improved by the organization.
- The establishment and development of control activities must be supported by technology to expedite the achievement of organizational goals.
- Deployment of control activities should be performed through taking policies in for the definitions of expected risk scores and procedures that support putting policies to work.

The principles of information and communication can be represented as;

- The provision and generation of relevant information from both internal and external sources should be functioned to assist the internal control activities.

- Provision of internal communication must be performed for flowing the information across the organization involving objectives and responsibilities of internal controls to support the business activities.
- External communication which covers the information transferring processes between the organization and outside enterprises must be operated in order to understand the voice of customers.

The principles of monitoring activities can be depicted as;

- Periodical and continuous evaluations for verification must be performed to examine whether the items of internal controls are in process and being executed effectively.
- The considerations of defects and insufficiencies in internal controls must be operated by the board of directors and senior-level management with timely approaches through taking proactive and corrective actions if needed (COSO, 2013).

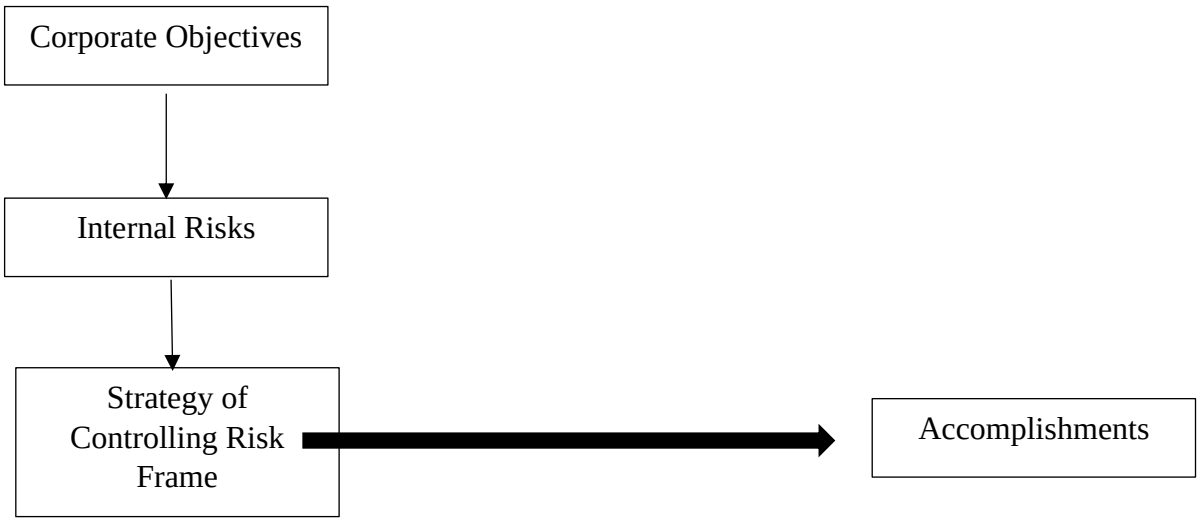


Figure 1.9. *Control Model 1 (Pickett, 2011)*

The Institute of Internal Auditors (IIA) is a professional association that proposes applicative models for evaluating the ethical status, integrity, reliability, managerial structures, policies, placement of authorities, and responsibilities of employees fit with their competencies within the controlling environment of enterprises. Similarly, the business functions in enterprises are operated through a planning and organizing style of the managements to achieve the corporate objectives by governing the inherent risks

economically, efficiently, and effectively with control strategies. In parallel with organizational goals, the internal control framework embodies principles, rules, policies, standards, moral attitudes, and management approaches to ensure the full protection of assets from fraudulent acts, cheating, damages, and losses by the provision of compliance with the legal environment. In practice, internal control systems of enterprises are installed by board management via setting reasonable guidelines and providing assurance for operating complete mechanisms in harmony. The efficient functioning of internal control mechanisms is under the authority and responsibility of board managements for assurance of organizations run on their operations to accomplish short term plans and long term goals in accordance with the code of ethics and laws (Pickett, 2011).

IIA frames Performance Standard 2130 to form the role of internal auditors in internal control mechanisms as assisting the enterprises in keeping the optimal control of the inherent business environment with the assessment of their efficiency and effectiveness through the way of continuous improvement. The supportive role of internal audit processes in the internal control framework distinguishes it from the activities of board management. Particularly, the advisory task of internal audit for the managements in enterprises is to inspect whether the controlling operations are coordinated efficiently and effectively in equilibrium or not with corporate objectives and legislations. Performance Standard 2130.A1 of IIA comes up with four major duties of internal audit activity for assessment of the internal control functionings in risk management, corporate governance, and information systems as providing the reliability and integrity of operational and fiscal data, improving the efficiency and effectiveness of business processes, full covering of enterprise assets and ensuring the compliance between controlling operations with the legal environment. The involvement of consulting activities of internal auditors for the control framework is arranged by constraints and red lines. Therefore, the variables and parameters are set according to inherent risks, business objectives, and strategies in control systems. Qualitatively, moral attitude, ethics, standards, and organizational culture are the other determinants which have indirect effects on the internal audit role in the internal risk control structure. In summary, the engagement of internal audit functions into risk control strategies is measured by the performance metrics of enterprises which are observed in efficiency, effectiveness, employee motivation, and satisfaction with ongoing manner. Also, the control mechanisms for managing inherent risks should be optimized by the guidance of internal

audit, for example, excessive control can cause much bureaucracy and reduction of organizational performance due to the stagnant workflows and oppositely the weak control can bring forth the deterioration of awareness in efforts for achievements of organizational goals. Naturally, the attributes of control systems are framed and affected by the organizational culture which can be either hierarchical or flexible. In essence, management boards are fully responsible for the incorporation of both cultural aspects and governance parts of organizations for the achievement of control objectives in harmony with business functions and activities for ongoing improvement in efficiency and effectiveness. In practice, the managements of enterprises need the consulting role of internal audit for controlling inherent risks to reduce entropy which is described as a tendency for decomposition in the performance of control mechanisms. Therefore, periodic reviews and assessments of internal control systems are required for the provision of organizational discipline and resiliency. Briefly, the unsteady nature of the controlling environment is optimized by the collaboration of internal auditors, internal controllers, and the board of directors (Pickett, 2011).

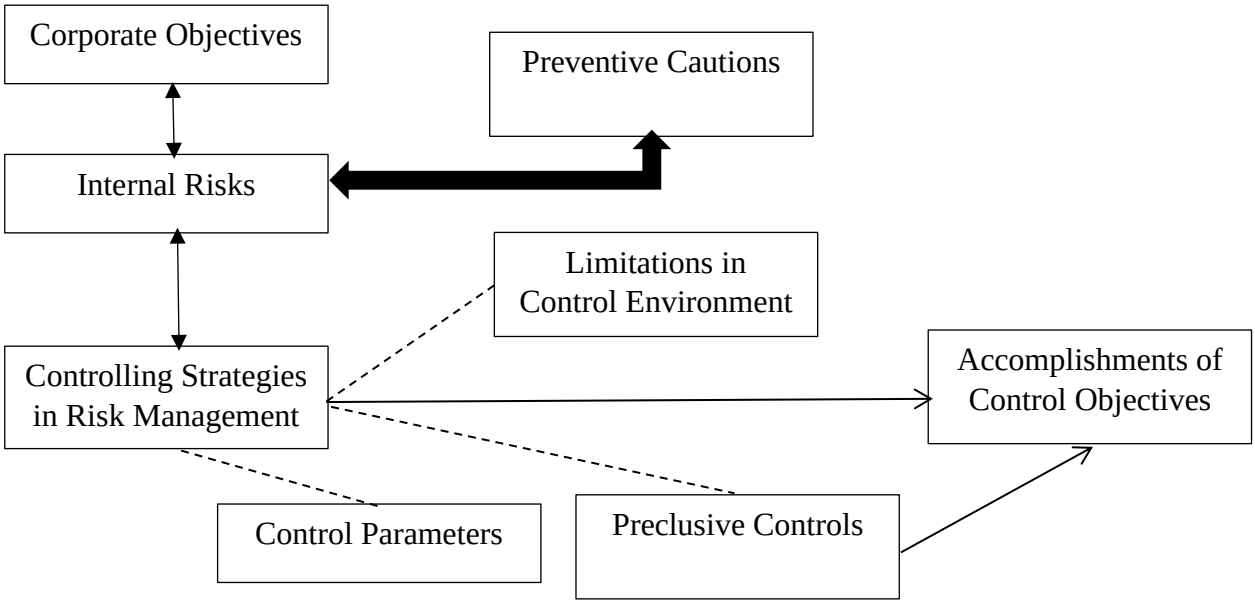


Figure 1.10. *Control Model 2 (Pickett, 2011)*

Mainly, all the corporations have to protect their assets from risks that stem from unexpected events, frauds, defects, and wastes which cause inefficient processes and as a result unsatisfied customer portfolios. Therefore, internal control is based on ensuring relevant information is gathered from valid and reliable sources to monitor the risk

management structure of an organization. This process is operated in a controlled environment which can be defined as an enterprise in a micro base by observing, measuring, and analyzing inherent risks by taking assistance of information and communication technology as well in today's business conditions (Trenerry, 1999).

1.3.1. Risk

Epistemologically, the risicare term was used in Italian which means dare or attempt as a derivation of the conceptual term of risk. From this point of view, risk corresponds to decision-making and preferences instead of chance or fate. Particularly, the success factors in businesses and industries are linked with the risk-taking approaches by controlling unpredictable cases. The description of Her Majesty's Treasury (HM Treasury) conceptualizes risks as results of uncertainties in a frame through assessment and synthesis of impacts and probabilities of unexpected events. Similarly, the risk is explained as the ambiguity of the events which can have effects on the accomplishments of objectives according to the Glossary of Institute of Internal Auditors. Therefore, from the standpoint of internal audit, the cases which cause deviations on achievements of organizational goals and objectives as come out with unexpected outcomes can be considered as risks. As follows, in theory, the likelihood and output of an event are taken into account to gauge risk. So, the risk measurement parameters indicate the uncertainty level of events through scales in a defined time range by assuming the information in hand related to cases is secure and reliable (Pickett, 2011).

In general, the types of risk can be classified as economic, social, political, biological, and technological in a macro environment. From the viewpoint of information and technology, International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) defines risk as the synthesis of possible occurrence and outcome of a case. Equivalently, the risk is perceived as unexpected results of events, in fact, it can be both negative and positive. Therefore, deviations and variations from the expected consequences illustrate the measurement of risk (ISACA, 2012).

The tendency for modernization and civilization to industrial activities as production, transportation, marketing, financing, exchanging, and supplying processes are required controlling functions of information technology and communication systems

because of the multiplex interactions in international business. Correspondingly, the escalation rate of complexities in controlling the industrial systems has been gaining momentum since information systems have been integrated into facilities and business functions. In this context, risks depending on cyber security have been emerged to affect critical infrastructures, industrial automation mechanisms, or supervisory control and data acquisition systems (SCADA). In practice, wholly safeguarding of SCADA systems can be unattainable because of the surrounding factors which are respected to international legislations, governmental policies, industry standards, and organizational culture. However, the identification, analyses, and assessments of risks or unexpected events which can have impacts on the functioning processes of SCADA systems should be performed for reducing their effects to tolerable levels (Radvanovsky & Brodsky, 2016).

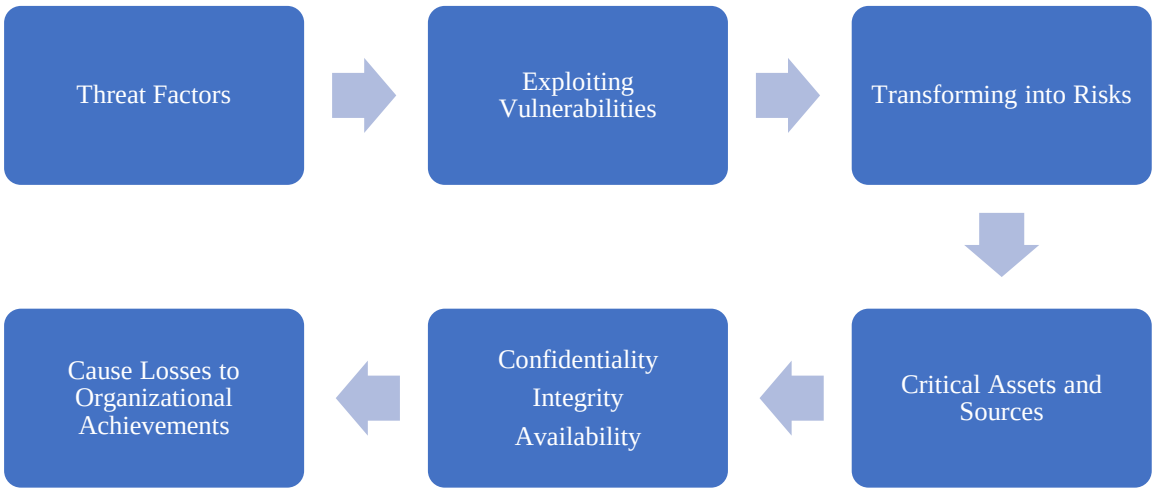


Figure 1.11. *Risk Conversion Cycle*

From the standpoint of asset protection and security, the major parts of understanding risks can be discussed by determination of mission and vision to perceive which business fields an organization is struggling for further improvement through the definitions of resource classes and their asset valuations with the consideration of threat factors and vulnerability causes which can reduce the efficiency and effectiveness of the business functions for desired products or services that will be delivered to customers. In principle, the definition of risk can vary according to the sector and organizational departments. For example, according to financial associations, discussions of risks are dependent on the variables of the macroeconomic environment and fiscal statements of organizations. Factually, due to the methodical description of the Infrastructure Protection

and International Security graduate program of Carleton University, the risk is perceived as in terms of damages that arise from threat factors that exploit vulnerabilities which lead to losses of confidentiality, integrity, and availability in critical assets and sources (Radvanovsky & Brodsky, 2016).

1.3.2. Risk appetite and tolerance

Risk perception is a variable which depends on critical factors like risk appetite and tolerance. Enterprises set organizational goals before they initiate their business operations by venturing their capital and critical assets. Therefore, the amount of risks that organizations have to accept before they attempt their activities is defined as risk appetite. Similarly, risk tolerance shows the admissible variability for reaching an objective. Correspondingly, the acceptable deviation that an enterprise considered before getting risks for pursuing organizational goals can be confirmed as a risk tolerance level (ISACA, 2009).

Within the context of COSO definition, risk appetite can be stated as the amount of risk which an enterprise is responsible to take for achieving organizational objectives, mission, and vision. Two primary problematics are considered while identifying the risk appetite of an enterprise as what amount of losses the organization is willing to accept for chasing return and how much capacity the organization has for absorbing losses. Also, risk appetite varies according to the industry and organizational culture of enterprises. The risk appetite of an organization can be measured by taking into account of frequency and magnitude metrics of risks (ISACA, 2009).

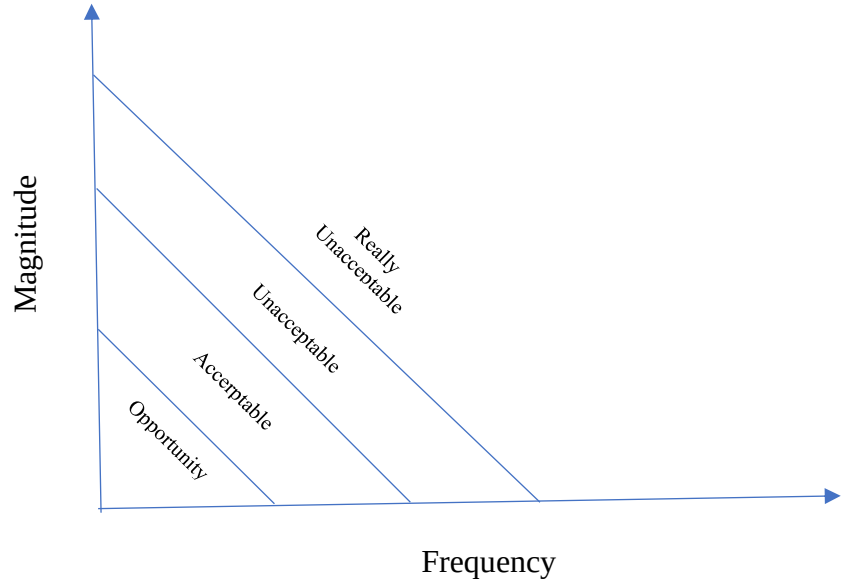


Figure 1.12. *Risk Map that Indicates Risk Appetite Bands (ISACA, 2009)*

Risk map indicates the areas which are segmented as an opportunity, acceptable, unacceptable, and really unacceptable for effective internal controls to take action if a risk has over acceptable impacts on an organization according to the magnitude and frequency levels of the risk. As a nature of diversifications between enterprises that depend on their risk culture, there are no universally approved standards for risk appetite, so this indicator ranges among the organizations.

From the aspect of information systems security, relative to the definition of the National Institute of Standards and Technology (NIST), protection frameworks of confidentiality, integrity, and availability or also known as the CIA triad of critical assets and sources such as hardware, software, embedded computer programs or firmware, data, knowledge, and communication routes are the indicators of how the organizations are understanding and measuring risky events. Primarily, the policies and approaches in the safeguarding of crucial assets can be observed and analyzed for recognition of risk limitations of an organization in terms of confidential data will be disclosed in what ways and to which authorities to explore how the controlling of management information systems is being performed (Stallings, 2017). Within this context, the valuation of information assets depends on both quantitative and qualitative assessments to measure how the organization will be affected if there are possible adversaries which jeopardize the confidentiality of critical info. Accordingly, the E-Government Act of 2002 (Public Law 107-347) was legislated for emphasizing the critical importance of information and

communication technology security, and as well Federal Information Security Management Act of 2002 (FISMA) was warranted to task NIST for building standards and guidelines in order to get awareness for the protection of information systems. Correspondingly, Federal Information Processing Standards Publications 199 (FIPS PUB 199) were established by NIST in favor of framing the minimum requirements of information systems security for managerial, operational, and technical controls. As a matter of fact, the threshold values of risk appetite and tolerance limits, which refer to information and communication systems, can be measured by taking into account the standards which were recommended by NIST in FIPS PUB 199. In essence, the main objective of this publication's establishment is to categorize the information according to the types of info such as private, medical, proprietary, financial, and sensitive which are classified by organizational principles and policies in accordance with the legislative framework (U.S. Department of Commerce, 2004).

Also, the information assets can be categorized according to their fiscal values with defining the cost effects of adversaries to the organizations. In practice, data types of an organization can be arranged in classes relative to their values as low or also known as public, internal or also known as medium, confidential or also known as sensitive or high, very high and restricted otherwise known as top secret or critical (UcedaVelez & Morana, 2015).

Table 1.1. *Risk Mapping According to Asset Values of Information* **(UcedaVelez & Morana, 2015)**

Heat Map of Information Systems Security Risk(Threat Likelihood*Vulnerability Exposure*Asset Value)	**Likelihood of Threat**	Low			Medium			High		
	Ease of Exploitation	Low	Medium	High	Low	Medium	High	Low	Medium	High
Asset Value	Low(Public)	0	1	2	1	2	3	2	3	4
	Medium(Internal)	1	2	3	2	3	4	3	4	5
	High(Confidential)	2	3	4	3	4	5	4	5	6
	Very High	3	4	5	4	5	6	5	6	7
	Critical(Restricted)	4	5	6	5	6	7	6	7	8

X =Risk	Low Risk	Medium Risk	High Risk
	0≤X≤2	3≤X≤5	6≤X≤8

In addition, observing the risk appetite and tolerance levels of an organization to discover the elements of internal controls also assists to perceive the resilience capability of information systems. The resilience capacity of organizations refers to cyber security

can be defined through how much time is needed for convergence of the information systems performance to the optimal and acceptable levels when unexpected events emerge. The resilience potential of an organization shows the coping ability of information systems when an adversary attack happens and preventive methods can not be enabled to mitigate risk as well. According to the definition of the National Academies of Science (NAS), resilience can be described as a system's capability for adapting to adverse circumstances by providing optimal recovery responses to reach the standard efficiency levels with regenerating adequate performance. In practice, the resiliency assessments of information systems can be performed with searching for the rate of speed that shows how quick the recovery is provided.

1.3.3. Risk culture

The origin of considerations in risk culture was emerged because of fiscal scandals in the United Kingdom and the United States which have important effects on the global economy and markets in the 1990s and 2000s. Accordingly, the macro impacts of these kinds of events have shaped the framework of the risk culture concept in enterprises by two directions defined as top-down and bottom-up manner. The main goal of each way is to engage with audit operations holistically. Especially, the strategic, middle, and operational parts of managements in organizations have to set the risk tolerances and appetites with interacting each other to reach the corporate objectives by structuring risk culture framework in line with internal control and internal audit. This process starts from the board of directors by appointing the responsibilities and authorities of employees for respecting the main components of the risk culture frame in accordance with corporate governance according to the top-down approach. In practice, the reviews and controls of performance feedbacks are the basic missions of the inverse approach was mentioned above as bottom-up. Therefore, the system should be designed in both two directions to effectively consolidate internal audit and control operations with the framework of risk culture and governance (Carretta, Fiordelisi, & Schwizer, 2017).

Correspondingly, organizational policies in security management of the cyber environment frame and catalyze the development of behavioral awareness and codes of ethics across the business functions among the employees for keeping safety precautions of information systems in line. Therefore, understanding the organizational policies of enterprises in cyber security systems through the discussions of how those policies can

harmonize with security practices in information systems is essential for the dissemination of cyber risk culture and awareness within the enterprises. Also, security measurements with technical control infrastructures can be supported effectively by setting organizational policies for building cyber security sense among the employees. Pre system development phase of protective activities in response to cyber threats is formed due to the security policies by classifying assets and distribution of responsibilities to the system administrators and experts for an efficient reporting mechanism when the information systems encounter unexpected cases. Also, the security policies of an organization due to the cyber environment should be combined with the industry standards. Data protection standards in the payment card sector in the United States can be shown as an example for this case. In essence, the security policies, that cover both organizational strategies and technical level practices, have common objectives for the prevention and elimination of not only accidental cases but also intentional acts which cause cyber threat factors. Natural catastrophes such as earthquakes, flooding, fires, lightning, thunderstorms, tornados, hurricanes, typhoons, and tsunamis can cause threat factors and transform into risks for entire parts of enterprises including information technology systems as well. Business functions in enterprises are coordinated and sustained by electronic mail mechanisms, voice over internet protocol communication systems, and electronic data interchange structures through information centers and servers with equipment and hardware such as computers and mobile devices to provide processing and administration of organizational activities by employees. Therefore, disaster recovery plans should be implemented to the security policies of organizations to ensure business continuity in worst-case scenarios through simulations, modeling approaches, practices, and testings. Fundamentally, information and communication systems cover computerized structures, hardware, operating systems, software, data warehouses, file directory systems, and network mechanisms. Also, those components of information technology systems should be protected primarily by precautions and policies because of their strategic and sensitive values for the sustainability of business functions in organizations. For example, data server rooms must be secured by climate control units through the backup of power supply with periodical maintenance, or sensitive data are kept in digital warehouses should be restored in alternative hard drives. Most importantly, critical business processes inside the organizations can not tolerate any breakdowns or outages, so the enterprises take

advantage of multi-synchronized data centers to overcome unexpected events. Enterprises generate and derive an extensive scale of data and information in their daily activities and if there are any losses or corruption in these assets, the business functions can be deteriorated and the reputations of firms will be jeopardized with extra costs and reduction of sales. So, in summary, emergency plans of organizations should be designed to ensure the full protection of their critical data assets through backup applications and restoration methods for providing maximum resiliency in information systems (United States Government, 2021).

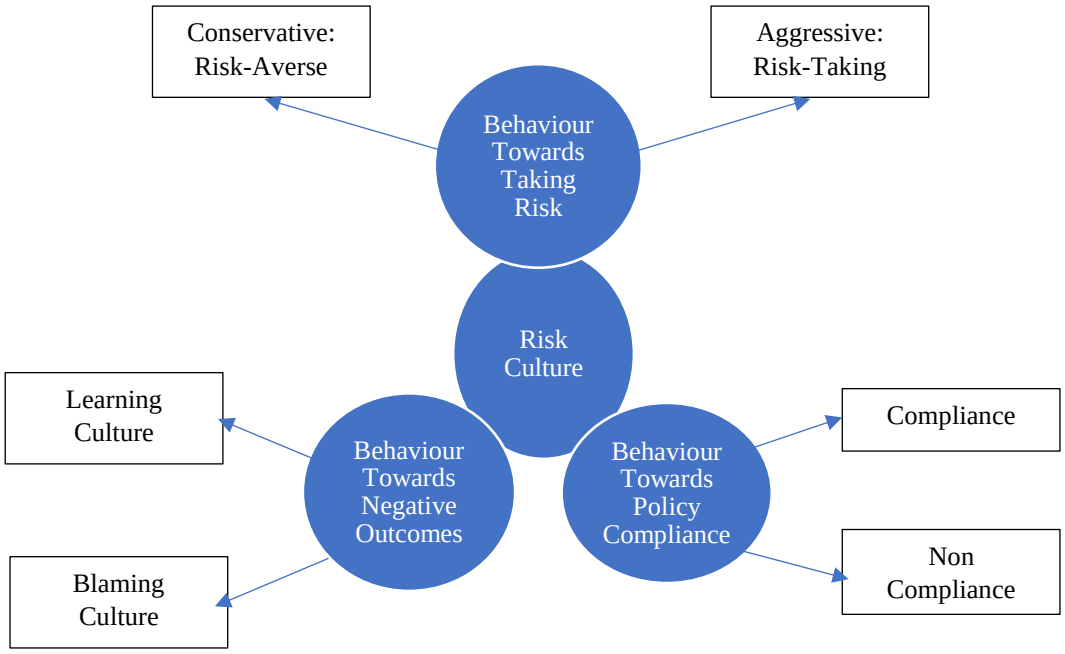


Figure 1.13. *Items of Risk Culture (ISACA, 2009)*

In essence, risk management activities and methodologies provide enterprises for adapting to unsteady conditions in terms of taking acceptable level risks. Similarly, a risk culture with feasible practices can assist how to understand risks and be aware of them through framing adequate behaviors for effective risk management and internal control. Due to the diagram of ISACA, risk culture contains three fundamental elements as behavior towards taking the risks, following policy, and negative outcomes. First, behaviors about risk-taking demonstrate how much risk an enterprise can absorb and what kind of risks it is willing to take. Second, behaviors related to policies show which scale employees are complying with organizational principles. Third, behaviors refer to negative results that display how an enterprise copes with losses or missed opportunities

by learning from the mistakes by trying to adjust and improve or blaming each other without exploring the root causes of the failures (ISACA, 2009).

1.3.4. Enterprise risk management

Organizations systematically have to cope with risks that threaten their critical assets in both internal and external frames. In accordance, without having a risk management outline it is not feasible to identify and control the uncertain conditions. Therefore, a sense of enterprise risk management was developed in the 1990s to focus on the diagnosis, assessment, and control of corporate risks. Also, this continuous process was supported by the Committee of Sponsoring Organizations of the Treadway Commission and the Sarbanes Oxley Act as the integrated framework (Olson & Wu, 2015).

Rapid technological developments in recent years demonstrate that encountered risks in information systems can not be totally avoided, but could be declined with a proactive manner by applying the risk management cycle which was offered by Kliem and Ludin (1998). This process involves the identification, analysis, control, and reporting stages of corporate risks to overcome ambiguous conditions. Particularly, interviewing with executive management and information technology experts by applying qualitative techniques such as Delphi, brainstorming, and system failure is a probable way to identify risks related to technology (Olson & Wu, 2015).

As well, the control systems within the organizations are designed to shield the unexpected and unacceptable risks with providing the compliance of legal and regulatory bodies and legislative framework. Therefore, the internal control mechanisms have to be fit with not only the enterprise risk management strategies for effective governance in business processes but also the legal environment for satisfying the international standards and complying with laws adequately (Pickett, 2011).

In essence, risk management processes in enterprises have to be dynamic and adaptive as a result of varying conditions in the nature of the business environment, because the risks which are encountered with uncertain events can not be totally controlled, so the organizations should implement flexible and robust systems to provide a maximum return with minimum losses. The alignments of organizational processes and roles should be in harmony with risk management strategies for the improvement of the resiliency and agility of business activities in a predetermined recovery period when

enterprises incur uncertain events and risks. Naturally, the cycle of risk and control chain in enterprises necessitates operable and efficient mechanisms for rendering the multidimensional communication between organizational processes and employees (Pickett, 2011).

The risk policies should be defined and arranged to provide complete awareness in organizational activities to fully control and manage the risks in enterprises. The frame of risk policies encompasses not only the protocols but also the workforces by enclosing the roles with stipulated diagrams to indicate the coordinators, risk managers, controllers, auditors, and activators through the sponsoring of board management. In practice, the efforts in risk management are coordinated under the responsibility of the Chief Risk Officer (CRO) who drives the activities proactively by both forming dynamic strategies for risk policies and providing their integration into daily operations. In common sense, the person who has the responsibility as CRO should meet the requirements of the task unit as;

- Providing the adaptation of the board's mission and vision philosophy into the risk management systems
- Supporting the establishment of risk policies into the operations
- Obtainment of education and seminars to improve organizational culture and awareness
- Installation of risk management practices all over the organization with convenient techniques and tools
- Assuring for prompt reaction to changing business conditions and new types of risks with ongoing approaches
- Setting up reporting mechanisms for assisting the board management to review internal control activities
- Searching continuously for up to the minute technologies to develop optimal information and communication systems within the organization (Pickett, 2011)

Due to the roles of CROs and experts in teams, the risk policies are designed for providing synergic governance models through connection mechanisms between the business activities and employees in enterprise risk management. First, the definition of risks and statement of the mission is considered for the effective interrelation between the board management and employees for integrating risk management strategies into the

enterprises. The parameters of risk appetite and tolerance for the understanding of an organization's approach to acts of risk-taking or preventing are determined in respect of risk policies. Also, in terms of risk policy, the authorities and responsibilities of internal and external audit experts are described in detail for risk-based assessment, reporting, and monitoring systems to demonstrate an organization's resistance level to risks objectively and independently by taking the guidance of corporate governance codes. Concisely, risk policy includes a clear, compact, and lean framework of the organizations' approaches, techniques, actions, and positionings of risk management strategies through the definite message of board management. Particularly, the practices of risk strategies highlight and mentor how to put the policies into force and catalyze their activities in enterprises. In essence, the risk management policy covers the outlining of governance structures in relation to board management, the comprehension of policies to express the requirements for legislations with the benefits of composing the risk management strategies, framing the risk tolerances, appetites, and threshold ranges for providing organizational perception with awareness of risks and ensuring the applicability of policies by setting and presenting the organizational duties to the experts (Pickett, 2011).

In practice, enterprise risk management (ERM) is accommodated through the enlargement of risk management strategies and approaches within the organizations. In essence, there are five key activities for determinants of ERM in projects from the aspect of internal audit which are described as settling a surveillance system, prescribing a common framework for corporate code of conducts and ethics, marking business processes and risks, installing organizational goals and assessing the proficiency of risk management applications. In order to reach an overall audit structure, the practices of ERM models are enriched with performance measurement systems by the addition of strategy and key performance indicators (KPI) besides of objective which is the major factor in risk management. Therefore, risk management approaches are advanced with performance measurement applications in the part of strategic planning processes for activation of ERM models in organizations (Pickett, 2011).

1.4. Corporate Governance

Primitive formations of corporations were occurred in the early history of the Roman Empire in order to coordinate cities, territories, and educational institutions. The main goal of these corporate bodies was to assist the construction of rules for organizing

colonies and states. Later on, corporations' role transformed into acting as merchandising establishments in the early period of the sixteenth century. In the current state, ownership structures are based on two main types of corporations as private and public enterprises. Two forms of business existences differ from each other according to jurisdictions, stakeholder attitudes, governance methods, and the cultural atmosphere of countries (Shailer, 2018).

Conceptually, the grassroots of governance came on the scene as the controlling and management methods of organizations were initially described by Sir Adrian Cadbury. Inherently, organizations have common goals are defined as the accomplishment of business objectives and performance targets established by board managements. Nonetheless, the organizations have to operate their business functions adequately with referring principles standards, rules, legal and policy frameworks to measure and assess the performance in a planned and defined structure. Therefore, the organizations require governance codes and policy frames for ensuring integrity, openness, and accountability in business functions with providing a balance between performance and conformance (Pickett, 2011).

The coordination of operations, processes, frameworks, and systems in harmony with controlling and management activities which have major roles in business continuity for value creation and distribution to stakeholders is defined as corporate governance. Extensively, corporate governance as a term covers the liabilities and strategies of enterprises relative to the principles and practices of governmental organizations, legislative bodies, sectoral associations, special interest groups, shareholders, suppliers, and customers through the adaptation of internal business functioning systems and contributors by taking into account the risk and performance management structures, directors, managers, and employees. Feasibly, there are two leading corporate governance models which are taken in place as principal-agent and pluralist approaches by the board managements of organizations. From the point of principal-agent aspect or also known as Anglo American model, shareholders delegate their authority to management for controlling business operations and taking decisions for investments. In such this model, managers can be considered as agents who have full accountability to execute and coordinate business functions on behalf of shareholders who can be discussed as principals. However, this mindset may cause issues like conflict of interests which can be observed when agencies do not take actions entirely consistent with the principal's

interests. From the point of pluralist and also known as the multistakeholder or European model the interaction and governance between shareholders and business functions of corporations are provided with multilateral manners as stakeholders who can be defined as shareowners, creditors, employees, staff members, suppliers, purchasers, and formal institutions can both affect and be affected from corporations' operations and management approaches. In regards, corporate governance practices are expressed from the aspect of the pluralist model through the recognition of the shareholders and employees as the main owners of enterprises relative to directors and managers. Also, there is a frame of mind to classify the multistakeholder model as preferable due to ethical norms because of the commitment level to corporate social responsibility and citizenship values in comparison with the principal-agent perspective (Shailer, 2018).

As well as to above mentioned major corporate governance models, stewardship theory was proposed that corporate governance structures can be designed in respect to the ethics aspect which formulates the responsibility of managers and employees for ensuring the effective control and utility of organizational resources in operating of corporate assets. The affiliation of the pluralist model with stewardship liabilities includes extensive series of interests to mechanize the corporate governance mentality through the value criteria of social responsibility and organizational commitment compare to Anglo American type. Besides these approaches, resource dependency theory was systematized for focusing on the board managements' roles to manage the organization's internal sources and external requirements effectively. In addition to these methodologies, transaction cost and political theories were designed to understand the macro factors which cover legislative, economical, and political aspects of the corporate governance practices with the combination of organizational activities are enclosed in the micro environment (Abdullah & Valentine, 2009).

Briefly, the theoretical models of corporate governance are mentioned above have the common goal to synthesize ethical and moral codes of organizational behavior with operational and managerial activities for providing continuous improvement of value creation and sharing to stakeholders as well as customers. In essence, the segregation of right and wrong attitudes in enterprises is defined by business ethics through corporate culture and the management which are framed by employees, intellectual capital, shareholders, and board of directors. Therefore, the proposed corporate governance models, which are harmonized with ethical and normative values, formulate and architect

the composition of employees, management board, independent audit commissions, and the role of senior administrations. Correspondingly, the transformation of corporate governance methodologies into practices is broadly dependent on collective relationships rather than process-adapted approaches in actual business conditions. In detail, critical parts of the large-scale external environment such as regulatory, social, political, cultural, economic, and technological concepts and perceptions have impacts on internal activities and corporate governance applications of enterprises. Hence, the operational and managerial dynamics of enterprises are interacted by internal and external business environment events and developments as strategic partnerships between firms, mergers, and acquisitions, startups, and innovations in information and communication technology. As well, the scandals, corruption, and fraudulent acts are observed in cases as the fall down of Enron and the collapse of Lehman Brothers have effects on corporate governance practices of organizations (Abdullah & Valentine, 2009).

However, the proposed theoretical framework of corporate governance models have also weaknesses in the definition of complexities in dynamic and changing business circumstances. Especially, the enhancement of the critical significance of data and information assets relative to technological developments adds up novel inquiries and assumptions for the philosophies in order to modify corporate governance models in the theoretical framework.

1.4.1. Common body of knowledge

In explanation, the Common Body of Knowledge (CBOK) expresses the minimal level of competency for an expert to perform effectively in the internal audit profession. Internal audit experts steadily engage in fields where they can achieve particular and professional skills through improving their knowledge. Correspondingly, the effects of sectoral developments and technological shifts transform the expected proficiencies and knowledge which are gained from industry-specific legislative environment involve an extensive range of subjects for both general and individual practices in enterprises. Also, this situation causes common problems for internal auditors as in which field they must have professional skills and what knowledge they need to have and develop. Foremost internal audit expertise fields had been introduced by accustomed auditors, before the years of information and communication technology which involves internet and web services were prevailed. Nevertheless, in essence, the least possible set of internal audit

knowledge essentials couldn’t have been recognized through a precise frame since the concept of the audit was presented as practice. In that matter, there has been no certainly adapted CBOK for the specialists of the internal audit profession. In this context, the absence of a clear CBOK was pointed out by Willliam G. Bishop had been performing as president of IIA between 1992 and 2004, for the experts who practice internal audit processes. Accordingly, in respect to the efforts of Bishop, the research studies were launched by IIA for the need of a clearly framed CBOK. Basically, a minimum level of competency required for performing effectively in a profession is defined as the common body of knowledge (CBOK). For example, a CBOK was published by Bank Administration Institute (BAI) for risk management professionals who are serving in the banking industry. As a matter of fact that risk management is discussed as a critical area requiring a broad scale of knowledge through the need for a CBOK to describe proficiencies and expectations for banking specialists who concentrate on this field. Correspondingly, in place of covering all the info concerns that an internal audit professional is needed to be viewed as an expert in this career, the focal point of CBOK is to define the minimal knowledge required for any professional in this discipline to serve effectively. Although, the initiation of CBOK refers to internal audit is feasible for creation of awareness in professional sufficiencies for practicing, the concerns of funding and taking interest to this subject cause problematics that internal auditors suffer. Also, there are different issues relative to the information technology and its expertise fields because of the agilely varying nature of the digital environment. For instance, an IT-based CBOK was established by the attempt of the Institute for the Certification of Computer Professionals (ICCP) to develop its own professional set of knowledge, but the framework couldn’t be entirely launched as a result of IT processes are moving more rapidly than any professional or team is able to define and document (Moeller, Brink's Modern Internal Auditing: A Common Body of Knowledge, 2016).

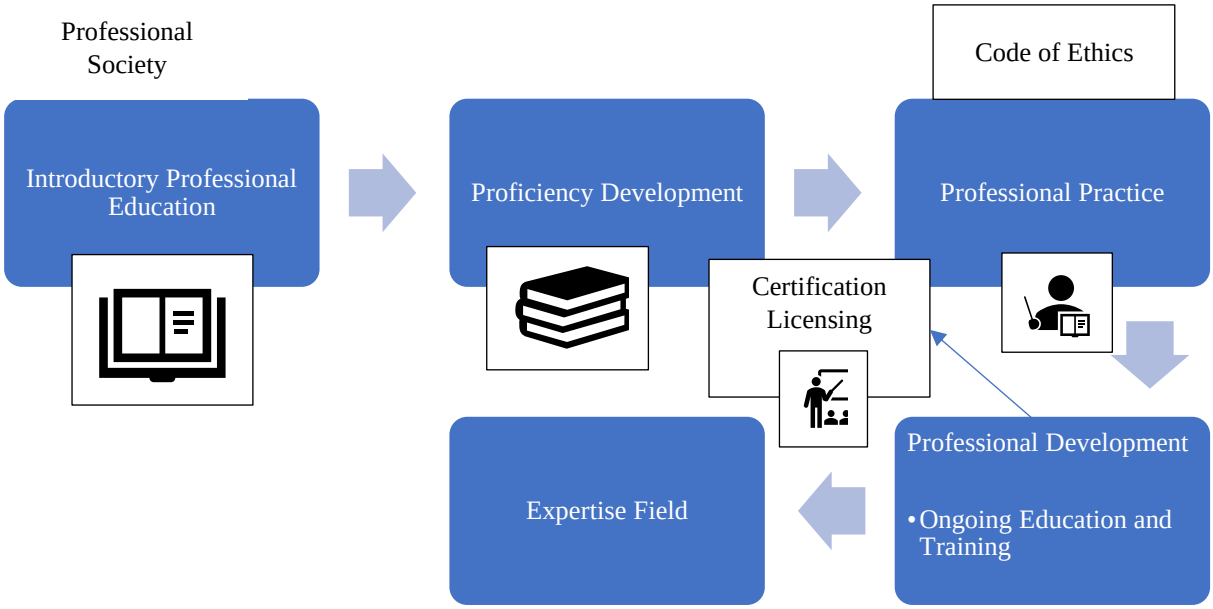


Figure 1.14. *Stages of Acquiring Profession as Infrastructural Level (Ford & Gibbs, 1996)*

The formations of CBOK documentation diversify relative to what profession an institution targets to develop in which minimal knowledge they need to frame either by general outlines or detailed explanations. For an instance, the Project Management Body of Knowledge (PMBOK) has been established by Project Management Institue (PMI) to define a required set of information for the professionals who are planning to continue their careers as project managers. This example of CBOK that PMI has been publishing describes all required parts of project management processes as inputs, methods, tools, and outputs as well as how to link this set of knowledge with business applications. In this context, a set of professional knowledge with general management discipline and an understanding of practices are needed to improve internal audit capabilities. Progressively, the role of internal audit as a profession has been derived from assisting accounting operations with computative verifications in terms of evaluating internal controls. Fundamentally, competency as a term covers the information, qualifications and behavioral skills are required for performing effectively in an authorized role. To make sense of this assertion, a comprehensive schema for the internal audit profession was established by IIA to demonstrate how basic competencies refer to each other.

Figure 1.15. *The IIA Global Internal Audit Competency Framework (Rose, 2015, p. 5)*

Epistemologically, according to Confucius who is a Chinese philosopher, people who aim to acquire true knowledge should identify what they know and don't know. In this context, professional ethics has the maximum score in all of the core competencies due to the international practitioner survey of CBOK which was carried out by researchers of IIA in 2015 to provide self-assessment to internal auditors relative to their key abilities and personality skills (Rose, 2015, pp. 9, 10).

In essence, both personal and technical skills are needed to enhance a sustainable career in the internal audit profession for contributing to value-added activities and assurance of risk management functions. Purposeful talent development plans are required for achieving additional improvement in industry-specific capabilities. In practice, the functions of internal audit are kept up with not only daily operations are performed by technical abilities but also strategic thinking is established through critical reasoning or known as the analytical understanding of social relations via personal skills (Rose, 2016, p. 1).

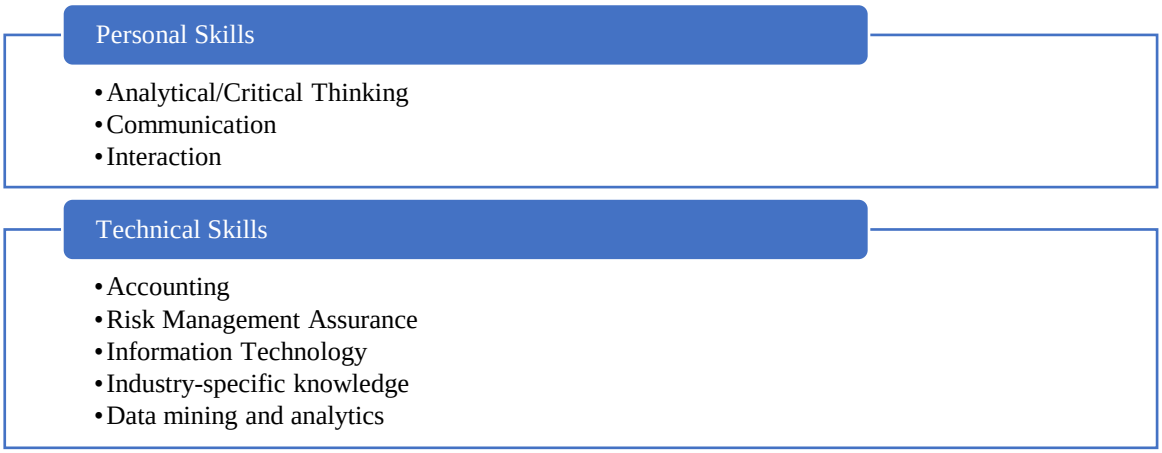


Figure 1.16. *Seven Skills Which Chief Audit Executives Want (Rose, 2016, p. 2)*

According to the findings of the Global Practitioner Survey of CBOK 2015 which is the greatest open-ended study of internal auditors worldwide, analytical thinking and communication surmounted the other five skills when the chief audit executives (CAEs) had been questioned to decide on the major five competencies while hiring and building in their internal audit crew. By reason of the survey results can be determined as analytical thinking and communication are shown as personal skills which gather every other part of the competency set of an internal auditor to realize audit practices (Rose, 2016, p. 2).

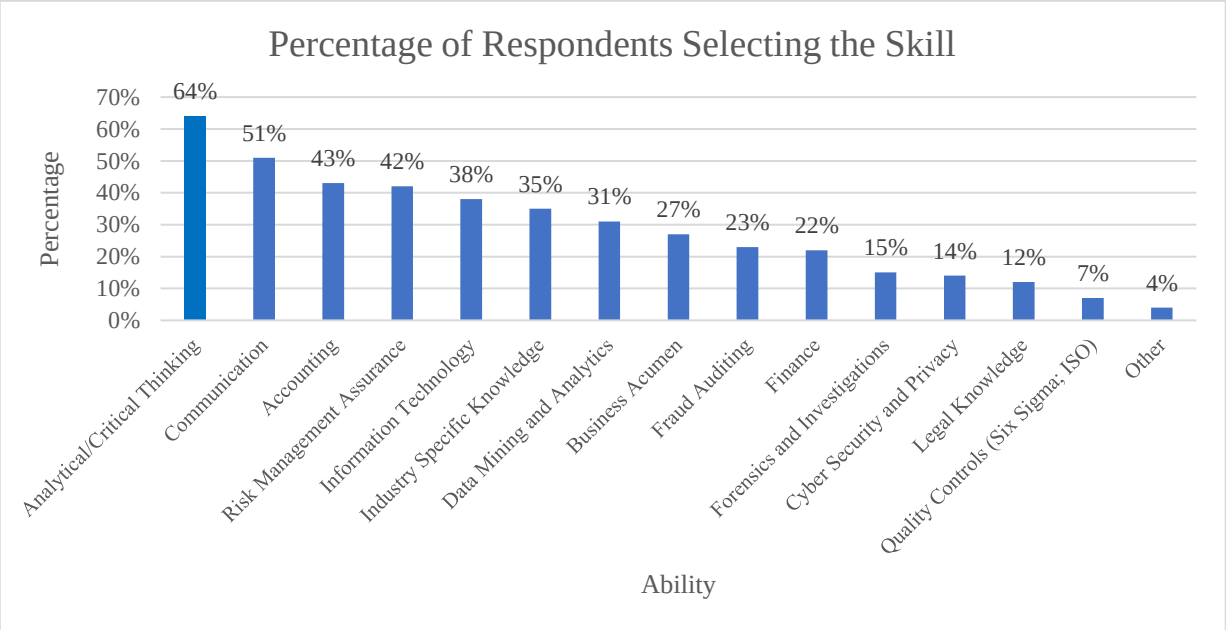


Figure 1.17. *Which Skills CAEs are Searching For While Recruiting or Building The Most In Their Internal Audit Department? (n=3,304) (Rose, 2016, p. 3)*

Technical skills are covered by major five components are shown in the graph as accounting competencies for how to assess financial reporting controls, risk management assurance for how to function risk-based audit with providing continuous improvement, and information technology capabilities to evaluate business and IT processes through performing audit role, industry-specific knowledge for providing assurance, strategic reviews, and consultative services, data mining and analytics for simplifying the functioning processes of efficiency and effectiveness assessments of audit operations (Rose, 2016, p. 2).

1.4.2. Committee of sponsoring organizations (COSO)

In 1985, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) was established to promote the pointers as opposed to the corruption in fiscal reportings of both private and public enterprises for auditors. In consideration of this, COSO has an advisory role on the internal control frameworks of enterprises for fulfilling the financial reporting obligations by constructing risk management models (Tipton & Krause, 2007).

In 1992, a framework was organized to provide the elements and principles of an effective mechanism for internal control operations in enterprises defined as the Committee of Sponsoring Organisations. Initially, it was not covered with formal standards and legal procedures, then it was modified to risk assessment operations for internal controls of external auditors which were accepted as one of the key factors for Sarbanes-Oxley Act (SOX) compliance. But, this set of rules shows some weaknesses in reflecting the technological shift in industries since it was first designed. As a result, this management tool was enriched with up-to-date approaches, information technology management, and governance in May 2013 (Moeller, 2014).

The items of internal control are formed by risk assessment, reporting, and monitoring functions. Following a similar logic, the control of information technology operations is executed by the guidance of COSO through the items of the internal control frame for reaching the root causes of problematic situations. Integrally, the role of internal audit steps in scheduled reviewing of abnormalities is identified in internal control items. Most commonly, the multi-dimensional approach of the COSO internal control framework is used with three-axis as x, y, and z for profiling the relationships in organizations (Moeller, 2014, p. 107).

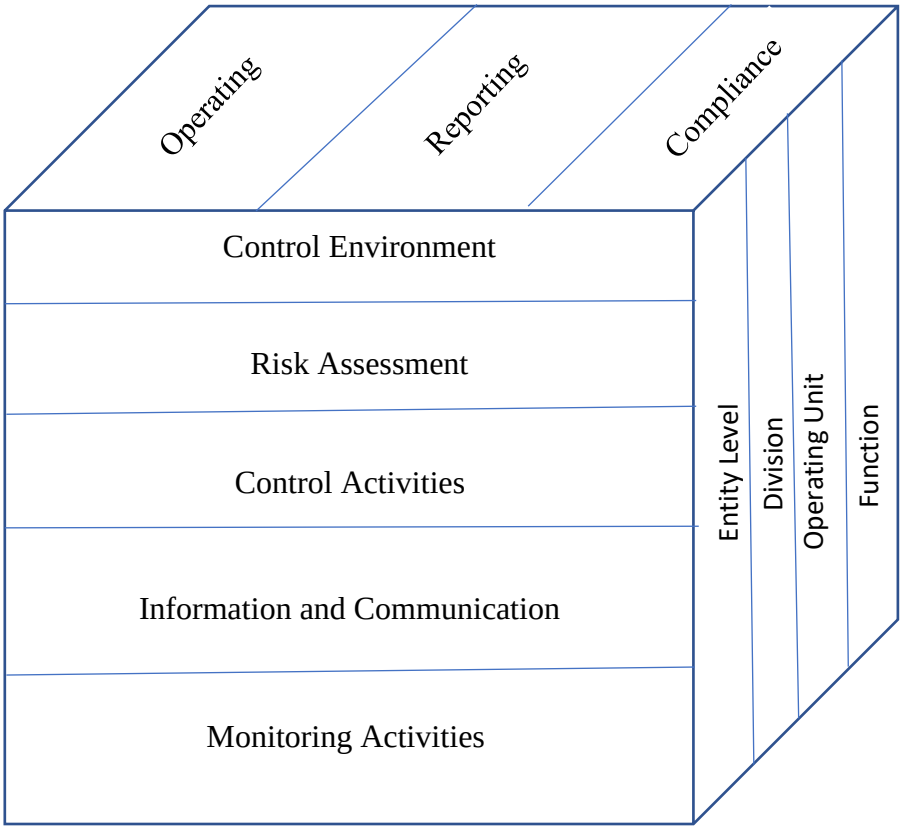


Figure 1.18. *COSO Internal Control-Integrated Framework Principles (COSO, 2013)*

Entirely seventeen principles, which are established into the framework, are mentioned through details in the stage of internal control, for reaching maximal effectiveness in internal control processes which have interactions between each other.

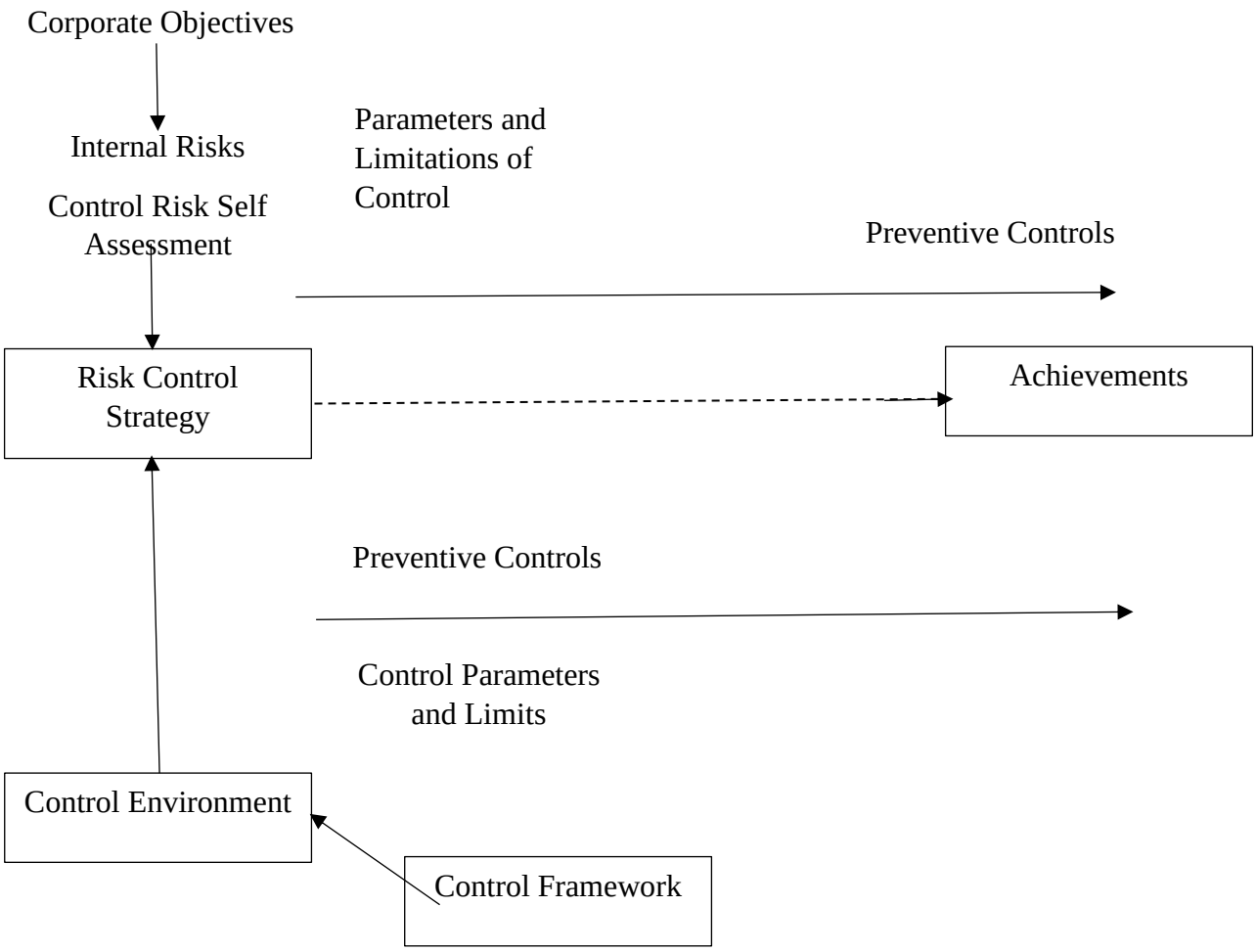


Figure 1.19. *Control Model 3 (Pickett, 2011, p. 104)*

The role of internal audit, which is related to quality metrics, is described in the performance standards of IIA and ISACA for the professional practices. Mainly, six performance standards are considered under the part of managing internal audit activity which is coded under 2000 series with subtitles that are denoted as 2010 refers to planning that is framed by 2010.A1 is named as annual risk assessment and 2010.C1 is termed as acceptance of consulting engagements, as well as 2020 pertains to communication and approval, 2030 relates to resource management, 2040 addresses to policies and procedures, 2050 belongs to coordination and 2060 connects with reporting to senior management and the board of directors. Internal Audit activities must be controlled effectively by CAEs to ensure that these activities are adding value to the organization (Moeller, 2010, p. 69). Particularly, risk-based plans must be developed by CAEs for the determination of the primary concerns of the internal audit role and precisely showing

that these priorities are consistent with organizational objectives. The establishment of risk-based plans is executed by the board of directors and senior management by taking the guidance of the CAE to understand what the organization's major goals, strategies, and risk management approaches are. In practice, the adjustments and reviews of risk-based plans should be conducted by CAE in terms of reacting to alterations in the enterprise's risks, policies, processes, systems, performance, and controls (Zain, 2019, p. 10).

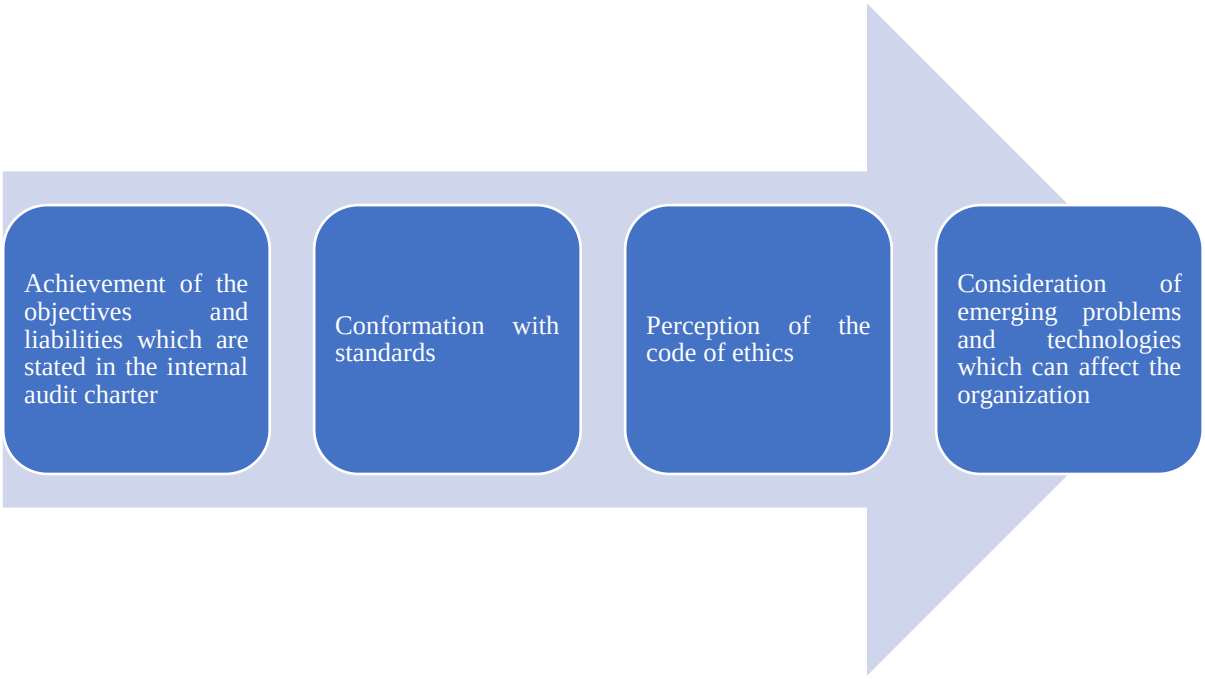


Figure 1.20. *Value Added Effective Internal Audit Activity Management*

Feasibly, enterprises require a formally defined framework for internal control systems, and IIA Performance Standard 2120.A4 forms a set of organizational guidelines for the auditors to actualize the assessments of control activities. Also, these criteria provide the enhancement of the control framework within the organizations by taking the assist of the COSO control model which contains monitoring, communication, information, risk evaluations, control activities, and environment. In essence, the basis of this model is a controlled environment that shapes the types of management's doctrines and thoughts for business activities, assignments of task roles, authorities, and responsibilities in line with behavioral norms, competence, and ethical perception of employees. In the second level, risk assessment of the control environment is needed for the identification of prior and related risks with the approaches of how the risks will be

managed which have impacts on predetermined achievable corporate objectives. Principles, procedures, policies, quality standards, and duty classifications are designed for the stipulation of management's philosophy with the guidance of internal audit functions to ensure the steady performance improvement of enterprise and protection of organizational assets in control activities. Information and communication systems provide required data in organizations for employees to carry out their tasks, authorities, and responsibilities in a defined time range. Generated data from both internal and external sources is provided for business flows cross-functionally through the information and communication mechanisms as down, up, and across in organizations for decision making, governance, and reporting. Holistically, the data generation, storage, and processing systems should be executed in harmony with management's philosophy, expectations, and corporate objectives with a clear definition of task units, organizational roles, and responsibilities in the control environment within the organization. Further, the enterprises need to have effective interaction with exterior customers such as regulators, suppliers, subcontractors, and vendors for a complete governance mechanism. Necessarily, monitoring infrastructure is designed in coordination with enterprise data management, internal audit, and control systems in business utilities. Therefore, inherent monitoring mechanisms are responsible for the evaluation of the overall performance quality in organizations by taking the support of information and communication systems for the isolation of ineffective activities as a core responsibility to sustain and detect the consistency with organizational culture, goals, plans, and policies. Briefly, the proposed model of COSO is the dynamic and applicable guideline that embodies the methodologies, approaches, and practices for how board managements express their assessments of internal control activities at the corporate level. There are five leading questions in the frame of COSO for enterprises (Pickett, 2011, pp. 104, 105, 106, 107, 108).

- Does the enterprise have the valid principles to control the business functions?
- Does the enterprise perceive the risks which can halt the controlling activities within the organization?
- Does the enterprise integrate convenient control processes for drawing attention to the risks in the business environment?

- Does the enterprise have the capability for monitoring how the business activities are being controlled?
- Does the enterprise have an optimal mechanism for controlling strategy of data flow and interaction is being driven with bottom-up and top-down approaches in business flows?

All these five key questions are respectively defined due to the control model of COSO through the items which are explained as control environment, risk assessment, control activities, monitoring, information, and communication systems. Subsequently, the assessment of the quality level of answers to these inquiries partly shows the accomplishment degree of control objectives inside the organization (Pickett, 2011, p. 108).

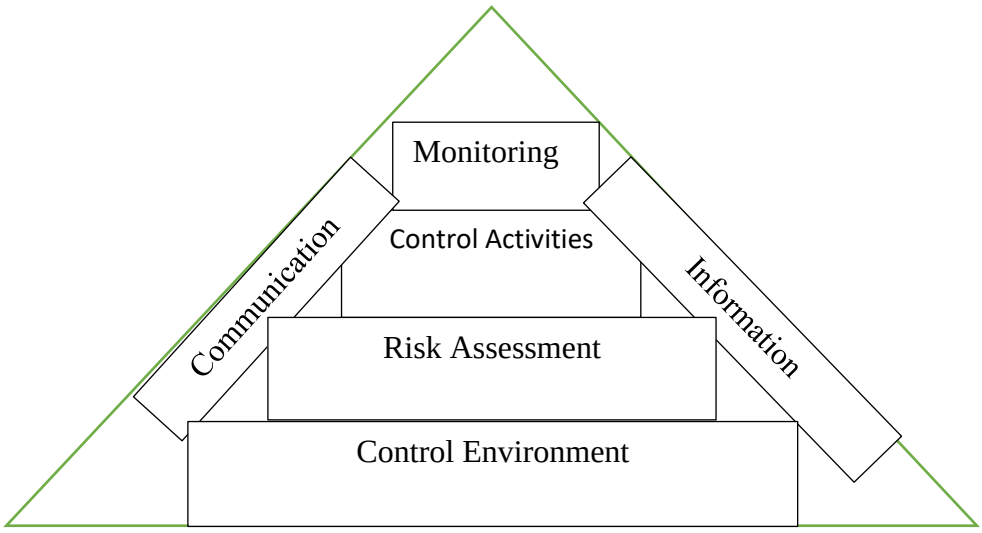


Figure 1.21. *The Control Model of COSO (Pickett, 2011, p. 105)*

Factually, the COSO mindset pays attention not only to the financial reports or fiscal cases but also to the values, assets, and complete mechanisms in the functioning of enterprises. In order to develop this framework, the Canadian Institute of Chartered Accountants (CICA) established criteria of control (CoCo) implementation to combine every single item of the business environment for evaluating the interrelations between each other, because control factors should be reviewed in the whole structure which contains behaviors, beliefs, attitudes and ethical values of employees with principles, standards, policies, governance and compliance systems. In essence, two major functions of control mechanisms are remarked as determination and alleviation of risks in CoCo. First, according to the instructions of CoCo, assessments of control activities'

effectiveness should be coordinated under the authority and responsibility of the chief executive officer with a complete manner that covers all parts of the organization. Second, the assessments must embrace the reporting outputs for the board management and the assessment cycle should be observed, analyzed, and detected regularly to provide ongoing improvement (Pickett, 2011).

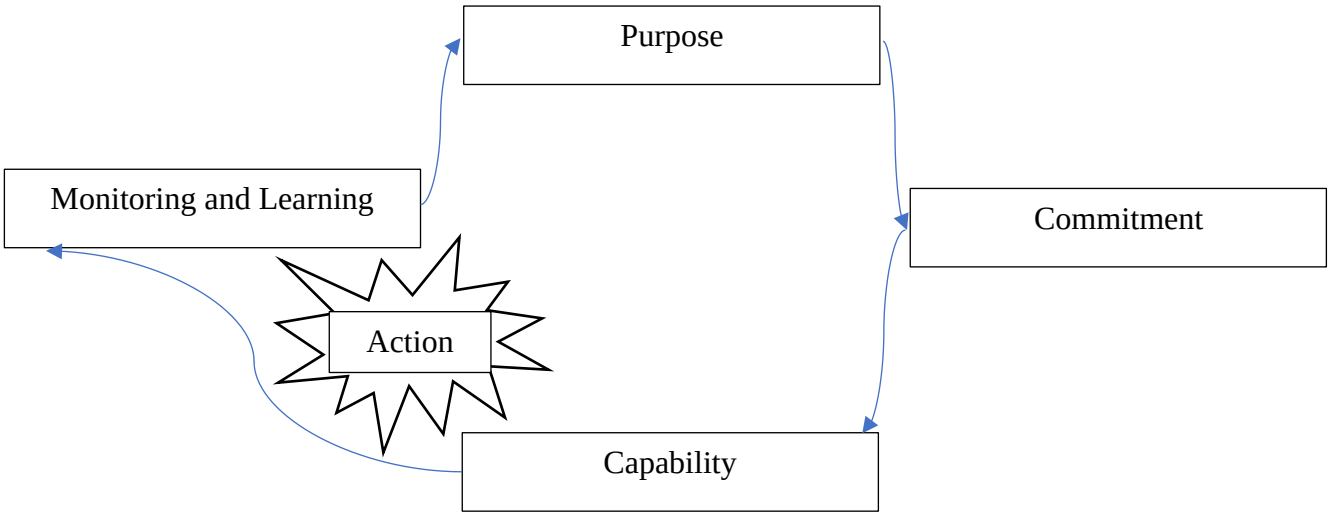


Figure 1.22. *The Model of CoCo (Pickett, 2011, p. 110)*

The criteria of the control model initiate with a clear and precise definition of the purpose statement which is the outcome of corporate objectives, strategic goals, mission, vision, plans, policies, performance metrics, and targets. Therefore, setting objectives for the future direction of the organizational activities in control environment provides the driving force for the performance of employees. As well, the relationship between control and performance parameters designates how an organization gauges and manages the effectiveness and efficiency of business functions. The characteristics and values of enterprises form, affect and obtain the commitment and motivation of employees inside the organizations. Especially, the enterprises need to structure their qualitative and intangible assets to fit with control systems to attract the attention of employees for both ensuring mutual trust and feeling themselves as parts of the organization's culture. After the clear definition of corporate objectives and implementation of organizational awareness for loyalness of employees, the knowledge, skill sets, tools, equipment, wisdom, information, and communication systems are needed for the execution of controlling function. Therefore, the efforts in control activities are sourced and supported

by the capability of processes and employees with taking into account their sufficiencies, competencies, experiences, and behaviors through fair and objective policies and mechanisms to be able for assessing risks and securing the control systems. Furthermore, capability should be supported and guided by education, conferences, seminars and technical training for the integration of continuous improvement approaches into organizations. Later on, these conditions are being accomplished the action part of the model will be activated for the assurance of business activities are being controlled within the organization. The final process of the cycle is monitoring both the internal and external environment by learning from the cases and observations in harmony with controlling functions systematically. Elaborately, the criteria of the control model propose monitoring mechanisms for performance feedback of employees, the effectiveness of business processes, and reconsideration of information and communication systems in accordance with governance norms of enterprises (Pickett, 2011, p. 109).

1.4.3. Sarbanes Oxley Act

The protection of investors adversely to the defrauding, unfair, makeup, and tricky actions in fiscal statements are required because of financial scandals such as Enron Corporation and WorldCom which had impacts on the reliability of investing environment around the globe. Therefore, in response to prevent these actions Sarbanes-Oxley Act (SOX) was put into force also known as accounting reforms for the protection of investors' rights by the United States (U.S.) Congress on July 30, 2002, with the main goal of detecting and blocking the financial frauds in statements (Vay, 2006, p. 1).

The authorization of revisions, which assists in recovering the financial statement reporting and acknowledgments, was established by SOX to minimize the unethical attitudes and illegal acts in accounting practices. Also, the internal control functions over the financial reporting systems were enhanced by SOX with the settlement of modified standards and punishments to mitigate deceitful activities in recording and disclosure of accounting information for improving the reliability and accuracy of financial statements in compliance with international frameworks. Affirmatively, the interaction and collaboration between the board of directors, managers, and auditors were intensified through new principles and procedures in financial reporting and internal control (Defond, 2005, pp. 5-30).

The guidelines and regulations were enacted by SOX have a role in internal control mechanisms for measuring and assessing the effectiveness and efficiency of financial reporting structures through auditing the reliability and accuracy of the information on fiscal statements (Koehn & DelVecchio, 2006, pp. 14-19). Especially, the main role of internal auditors had been altered to ensure how the internal controls are being efficiently functioned in accordance with outputs of financial tables are generated from information systems with taking in place the external audit for validation of the data that is shown in fiscal reports based on investment and business decisions of board management. Therefore, the confidentiality, integrity, and availability of data must be called into query through information systems in harmony with internal audit functions, if internal control activities are not being performed in compliance with guidelines that were established by SOX. In addition, the standpoint of the Sarbanes Oxley Act emphasizes the critical role of professional qualifications and abilities of auditors to promote objectivity for the evaluation of internal control processes through using their independent judgments. Similarly, in current business conditions, the concerns of internal controls over fiscal reports are related to information technology governance beside corporate governance. In essence, settling guidelines and standards for effective governance practices, which embodies entire organizational activities, is a critical factor for shareholders to rely on enterprises. Sarbanes Oxley Act was passed for countering the fraud cases in financial operations and management activities to reconstruct the confidence of investors in public markets of the United States which were also influenced by deteriorations of corporate governance practices as side effects of fiscal manipulations in enterprises. Furthermore, information technology governance methodologies and practices were affected by SOX because of the modifications in requirements which depend on internal controls. Benchmarking of activities related to managing risks, accomplishing compliance, and governing standards for continuous improvement were activated and catalyzed after SOX to frame both corporate and information technology governances for providing effective relations in the international business environment between nations and enterprises. For instance, Australian Standard for Information Technology Governance AS8015 was issued by Standards Australia International (SAI) in the matter of organizing information systems relative to corporate governance for supporting the consulting activities of information technology audit. In this context, the guidelines of SOX cover accountabilities of enterprise managements for internal controls in sections 302 and 404.

The chief financial officers or the personnel staff who perform related functions should authorize the responsibilities of corporate management to effectively outline and retain internal control processes according to section 302. In essence, the requirements of section 302 were constructed to cover the company managements' role in internal controls with not only financial reporting function but also adapting procedures and frameworks for controlling processes. Correspondingly, two elements of internal controls were marked in section 404 as the responsibility of enterprise and certified public accounting firms. Internal control reports are encompassed by remarks to sustain and develop adequate controlling principles and frameworks to validate financial statements through the accountability of corporate managers. Categorically, the assessments of managements for the adequacy of internal controls over financial reports through establishing and periodically monitoring the guidelines should be evaluated by external auditors with reviewing the affirmations of disclosed results on financial reports. Therefore, authorized auditors' mission is to make assessments of the discussions on the internal control reports which are prepared under the responsibility of enterprise management. Additional regulations and procedures were issued by the Securities and Exchange Commission (SEC) and Public Company Accounting Oversight Board (PCAOB) for clarification of SOX through taking the support of the private sector. In this context, internal control efforts of enterprises were enhanced through in-depth guidelines which were established by SEC and PCAOB to supplement the framework of SOX. In the current business environment, the financial reporting processes are being conducted by the involvement of information technology systems. In particular, the effects of SOX can be observed on information technology governance as well as internal control over financial reporting to review risk management and compliance parts of corporate governance (Cuong, 2007, pp. 1-5).

1.5. Cyber Security

From the beginning, security as a term puts in all kinds of systems in the life cycles of organizational activities to ensure the business continuity of enterprises. Deductively, from the standpoint of nations, industries, and enterprises, the official experts in system management have the responsibility to provide safe conditions through security policies with protection planning to support the sustainability of economic and business activities.

Fundamentally, assuring the confidentiality, integrity, and availability of assets concerning cyberspace is described as cyber security (Ryder & Madhavan, 2019, p. 2). The security side of cyberspace accompanies with the need for a defensive mechanism to enforce the cyber attacks. In other words, the main purpose of security systems in cyberspace is to ensure the safety of assets from both physical and digital damage. Therefore, cyber security term covers the precautions, resilience, and robustness of a system to the cyber threats and vulnerabilities. In relation to this statement, the main objectives of cyber security are defined as inhibiting cyber attacks, minimizing vulnerabilities and damages with optimizing the recovery time according to the United States Cyber Space Strategy documents (Westby, 2004, pp. 2-3).

According to etymology, cyber security expression had found a place in the nineteen sixties. In these years, communication security term was pervasive, then over the 1970s, when the computers seem, the concept of computer security came out. Later on within the 1980s, threats such as Morris Worm and Cuckoo's Egg showed that the computers connected in a network were the main targets of malicious attacks. The intervention of both network communications and computers was realized in such these events and so, a sense of information security impressed (Kesetovic & Putnik, 2013, p. 217).

Due to the cyber risk concerns of the industries and enterprises, the applicative methodologies for security structures in information systems have been developed and adapted to counteract the adversary types which are sophisticated, well-sourced, motivated, and covered in advanced persistent threats have strategic targets to extract data from critical infrastructures of nations and organizations for malicious intentions. For example, to diagnose and prohibit cyber intrusion attacks, a framework is designed by Lockheed Martin as the unit of the intelligence-based defensive systems which is called cyber kill chain. This model proposes a process through sequential activities for the identification of which phases cyber-attacks should achieve according to reach their objectives. In practice, the chain of intrusion activities is broken by cyber security cautions and preventive actions through stopping adversaries at any step of the model. The killer chain model is fundamentally structured on the principles due to the definition of the defender's objective via perceiving the intruder's acts and provision of intelligence through the perception of adversary type with detecting the complete success of attackers that is dependent on the proceeding of steps in cyber killer chain model from one to six

then reaching the final phase. Correspondingly, the stages of the cyber killer model are respectively classified as reconnaissance, weaponization, delivery, exploitation, installation, command with control, and actions on objectives. From the start of the model as a reconnaissance step, according to the adversary side, the planning of the intrusion activities is constructed by attackers who conduct researches to get which targets will make them possible to accomplish their intentions. This stage covers activities such as gathering email addresses, identifying employees by using social media networks and discovering network servers. From the defenders' side, identification of recon can provide to reveal the purposes of the adversaries after the fact. The methods for discovering the intrusion acts in the reconnaissance stage are collecting visitor logs from websites that were visited in history for controlling and alerting, working with web administrators collectively to take advantage of browser analytics, developing detection applications for browsing conducts particular for reconnaissance and arranging defense systems around unique technologies and employees whose main objectives are detection of recon activities. The preparation and organization activities of the adversary attempt are discussed in the weaponization phase of the model. In this stage, the weaponizers who have the capability to operate in house, public or private channels are coordinated by attackers through the selection of decoy documentations for delivering to the victims with file-based exploits. After that, selection of embedded backdoor, relevant command and control infrastructure with labeling the mission of operation through implanting specific identification code into the malware is systematized. Later on, the weaponization phase of the attackers' side finalizes through command with the compiler of the backdoor by weaponizing the payload. From the defender side of this phase, the probability of malware identification by detecting is relatively low when an adversary happens in real-time and because of this reason, the defenders figure out the issue by analyzing the malware prototypes. Also, the methods to defend the system in the weaponization stage of the cyber-killer chain model are lined up as analyzing entire malware types, building detection mechanisms by searching for new scenarios and payloads because they can be used as toolkits of attackers, scrutinizing the time frames such when malware was invented and used, accumulating relevant data and folders for future analyses, discovering which weaponizer artifacts are taking place in common with advanced persistent threats campaigns through exploring that they are extensively deployed or intentionally held. Malicious emails, malwares on universal services buses, social media accounts, and

websites are covered with watering hole attacks are transmitted by adversaries to the targets such as data and web servers for launching the intrusion acts, according to the third step of the model which is called delivery. Inversely, blocking of such kind of intrusion attempts is stepped in delivery stage with measuring the effectiveness of the defending systems as searching for the ratio between realized and blocked adversaries. Exploitation for vulnerabilities in server-based systems, software, hardware, or human conduct is aimed to achieve through malicious emails and links with exploit codes as zero-day for access to the victims in the fourth phase of the model. When victims open attachments of those emails and links, the exploit codes will be activated and injected into the systems. Technical training and coding educations with email testing for enterprise staff, web developers, and users to enhance organizational awareness, scanning the information systems for vulnerability detection through penetration testings and executions of shellcodes, auditing digital processes legislatively to discover the root causes of exploit attempts are the methods which defenders apply to counteract the adversaries in this stage. The fifth step of the model is called installation for intending establishment of beachheads in systems and in order to achieve this goal the backdoors are placed in an information technology environment through installing web shells on web servers and adding autorun keys into services to keep access with victims for a planned time period by adversaries. Implementation of host intrusion and prevention systems through endpoint tools for observing, detecting, recording, and logging operations of installation paths and extraordinary folder generations are operated and executed by defenders to get compiling stages of malwares for blocking and inhibiting the adversary attacks. According to the sixth stage of the model which is named as command and control (C2), the victims are exploited remotely through command channels like web, domain name systems, and email protocols which are initiated by the malwares for the objective of enabling adversaries. If commands can not be released by attackers, this phase is the last opportunity relative to defenders for cutting off the C2 channels in terms of preventing the effects of adversaries, Auditing C2 channels with malware analyses, solidification of networks by reinforcing network nodes, adjusting systems for blocking of C2 protocols on web proxies, prohibition of hosts by applying domain name services sinkholing technique when the system requests for trying to connect with undesired malicious domains and attending researches for exploring new attack types in C2 channels. The occurrence probability of intruder acts purely depends

on who is on the system and using such devices as keyboard or mouse. If the adversaries reach the seventh stage of the model which is defined as actions on objectives to accomplish their missions. Therefore, if the attackers can leap over the first six stages of the model, interruption of information systems through collecting and overwriting of user data and credentials for undermining cyber security and technology infrastructure is fulfilled with a possibility above the level of critical threshold. From the defenders' side, the impacts of adversary events are assessed by the engagement of management with updated plans and simulations of such activities which have damages to the information system environment. In summary, the cyber killer chain model which is established and developed by Lockheed Martin supports the cyber security systems of organizations in the identification of intrusion scenarios and patterns through agile and resilient defending mechanisms for adapting the information technology infrastructure to the upcoming adversaries (Lockheed Martin Corporation, 2015).

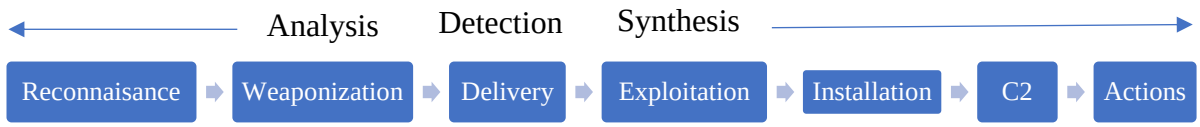


Figure 1.23. *Earlier Phase Detection (Hutchins, Cloppert, & Amin, 2012)*

Global Cyber Security Index (GCI) which is a compound indicator was established in 2007 by International Telecommunication Union (ITU) for evaluating the adherence of 193 ITU affiliate countries to cyber security standards according to five pillars as legal, technical, organizational, capacity building, and cooperation to enhance awareness in cyber security. The main purpose of ITU by launching GCI is to develop governmental strategies for implementing a universal culture through sharing of data and information across industries to promote organizational culture and awareness in enterprises. In essence, the computational model of GCI is based on 25 designators clustered in five sub-indexes to measure the improvements in the commitment of cyber security in nations through motivating them to promote their rates by recommending strategies and

applications relative to identified weaknesses. Correspondingly, legal pointers which consist of measurements are based on the frameworks relative to cybercrime and security regulations of legitimate institutions. Computer Incident Response Team (CIRT), Computer Emergency Response Team (CERT), and Computer Security Incident Response Team (CSIRT) are the organizations that provide measurements are based on the framework for technical standards to diagnose, safeguard, counter and control cyber risks through advancements of cyber security practices. The measurements are depending on coordination between institutions that build policies and governance models to design and integrate the strategies related to cyber security covered by organizational metrics. Capacity building indicator covers the measurements formed on the presence of accredited professionals, research and development initiatives, technical training, and educational programs to encourage the understanding of technology and cyber risks for improving appropriate principles, regulations, policies, and strategies for nations. The indicator in terms of measuring the cooperation metrics is based on intelligence and sharing of information related to cyber threats and risks through attack scenarios with how to react, mitigate and defend. Those five stated fields are combined in GCI by industry experts for proposing a feasible assessment of cyber security culture at the national level. In practice, political, economical, and social organizations should cooperate with each other at the international level because dialogue and coordination improve the governance structures for entire applications of cyber security. As a nature of cyberspace, threats and risks have global impacts and emerged independently from national borders or industrial specifics (ITU, 2018).

1.5.1. Cyberspace

Etymologically, the breakthrough of cyber as a term was initially proposed by Norbert Wiener with the usage of expression in cybernetics. Then, in 1982, a short fiction was created by William Gibson with the name of Burning Chrome for gathering attention to computer-generated virtual reality (Fourkas, 2002, p. 424). Later on, William Gibson coined the definite concept of cyberspace which has become popular since this term had been mentioned at first in Neuromancer’s novel of himself (Mehan, 2008, p. 25). Linguistically, cyberspace was consisted of two words as a compound noun phrase like cyber was derived from Greek terminology which expresses kybernetes in similar with the meanings of the pilot, governor, and ruler as well space was originated from the

French word which means basically area, field or complicatedly extension of three dimensions. The origin of the cyber term also refers to cyborg which defines a human-machine integration that can be designed and provided through the connection of human and technological environment. The developments in information and communication technology (ICT) started up the discovery of the World Wide Web (WWW) in 1989 which provides access and exploration through utilizing graphical user interfaces, nodes of network structure, and connections that cover a set of data, visuals, and multimedia elements. Then in the 1990s, users and researchers tended to concentrate on Internet while they are speaking of cyberspace. Particularly, the innovations in cybernated and mobile systems provided the independence of the digital market environment as well as hardware, software, and virtual reality platforms through the enhancement of network and communication processes are related to the Internet for public and private enterprises in both service and production industries (Fourkas, 2002). Furthermore, the critical value of information-based systems exponentially has grown since 1995 when the deployment of the National Information Infrastructure (NII) was accelerated by the United States Government with the principal objective of developing a national policy framework to encourage new technologies through a legislative environment to be competitive in international trade activities. In this way, the unreal and imaginative demonstration of cyberspace as a matrix in the novels of William Gibson transformed from science fiction to reality.

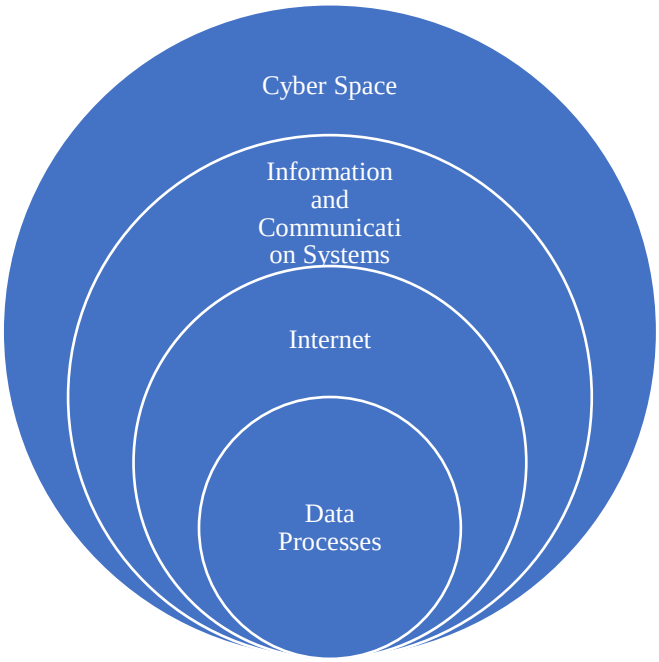


Figure 1.24. *Diagram Representation of Sets in Cyber Space*

In a short definition, virtual environment refers to the communication networks, electronic connections, and frame of data warehouses and interactions in a digital platform such as software and operating systems is called cyberspace. Fictionally, cyberspace plays a role as a universal set which covers both virtual environment and interaction with users. Therefore, this field involves both technical parts and personal factors to take care of. As an example, the network connection between a person and computer or phone line between two people's calls can be depictions of cyberspace. As a matter of fact, cyberspace does not involve the computer or phone on the desk but encloses the entire communication platform. In this case, cyberspace is not defined as a tangible place that a person can touch or feel physically (Giacomello, 2014, p. 2). Contextually, cyberspace pertains to the artificial, simulated, and virtual environment through the access of computerized systems to provide human beings for interacting with each other with controlling and processing of the data. Therefore, a virtual domain which is called cyberspace can be created with communication lines and network links in where digital data and connections are enabled to move in desired direction and speed. Then as well, cyberspace includes digitally connected databases, servers, and centers for recording and transmitting knowledge. Also, online mail systems and teleconference connections are being functioned in cyberspace as a subset of the Internet which provides communication networks between multi-users in different locations. On the other hand, asset allocation and industrial activities such as financial transactions, supply chain processes, exchange operations, and commercial interaction between nations and organizations are being performed in cyberspace through information and communication systems. Furthermore, the navigation mechanisms are being structured in cyberspace through modeling of three-dimensional mapping with augmented reality for geographical positioning (Fourkas, 2002, p. 426).

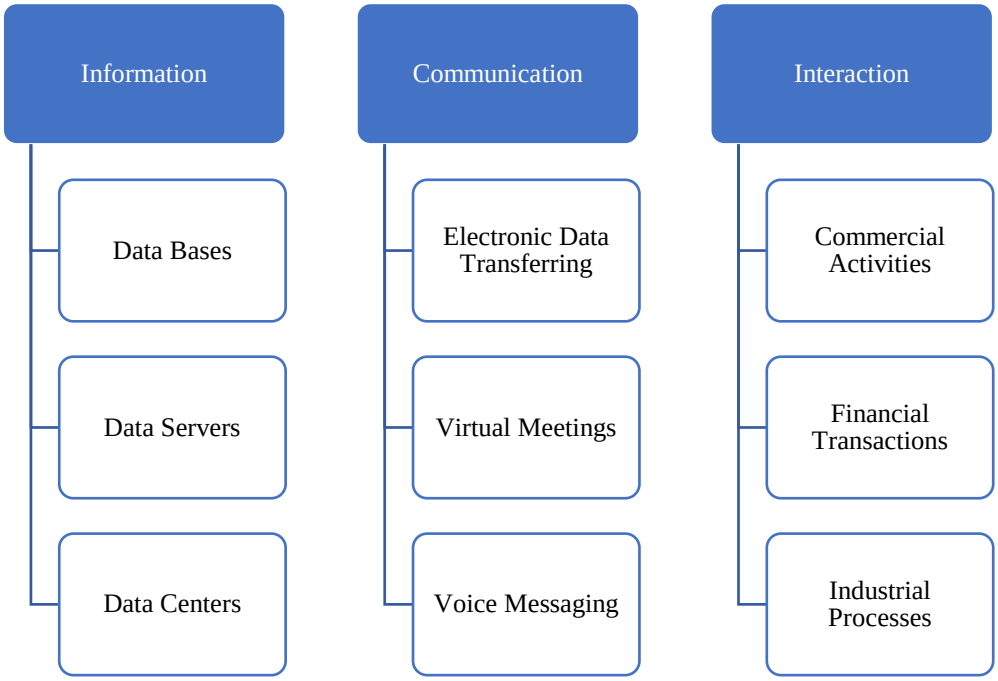


Figure 1.25. *Virtual Environment Parts with Their Functions*

The Modeling of cyberspace is an applicative subject since computer technology had been emerged which theoreticians have been focusing on to propose new methodologies and tools for practitioners. For example, according to the studies of scientists and engineers of the University of Tokyo and Canon Incorporation in 1998, a method was proposed in order to demonstrate how to build a cyberspace with a significant level of reality by combining the models which were derived from randomized standpoints that show images in actual domain with computer graphics (CG) approach (Katayama, et al., 1998). In this context, the adaptation processes to cyberspace are provided by having the capability of algorithmic and reasonable thinking which is needed for commanding information systems through encoding and programming knowledge as a computer language. Correspondingly, the tendency in transitions of societal interests, legislative frameworks, and business scenarios in global dynamics has been moving to a sustainably interacted renovated culture which is emerged and is reflected in the artificial environments that can be described as subsets of cyberspace. Particularly, cyberspace has come into existence through multidimensional chaotic domains with a high range of flexibility which cancels out basic geometry as the nature of the imaginary structure of virtual environments are independent of laws of physics such as the basic motion rule of Newton. Consequently, cyberspace is different from the existing tangible place can be

determined by fundamental principles of coordinate planes through calculating the distance between two different points or locations. The amount of range between two separate positions in cyberspace can be measured by searching for how long time is needed for moving from one Web site to another one or downloading a program. Thus, cyberspace can be perceived as an artificial platform that provides accelerated interaction between network topologies with disregarding the geographical distances between places as the minds of human beings can go into these electronic interfaces, but their physical body parts can not (Fourkas, 2002).

1.5.2. Cyber threat, vulnerability, and risk

In general, the term of threat can be shown as an event or action which initiates loss, hurt, deficit, or harm to businesses. Cyber threats can be described as cases that emerge in the digital environment that have adverse impacts on the profitability of enterprises. But, the harmful effects of cyber threats may influence both intangible and tangible assets such as data warehouses, connection mechanisms of internet technology, computing devices, or industrial control systems. Also, it involves complexity to perceive the topology of cyber threats and because of this reason, the common classification of these events is not precise according to scholars. However, commonly, in organizations, the threats in cyberspace fall into two classes as basic technical errors like system defects which may happen unintentionally having damage on operational level functions of businesses, and malicious acts which have direct negative effects on all levels of enterprises' operations such as finance, marketing, production, human resource and information technology (Progrebna & Skilton, 2019).

In practice, sorting of threats in cyberspace obtains benefits for the enterprises to both reduce their costs and increase their focus on main targets. Categorization of threats is supported by verified visuals, maps, and schedules that can stimulate the perception of management for utilizing the constraints in cyber security. Feasibly, the varieties of cyber threats can be matched by their detailed descriptions and severity levels according to which assets they plan to affect for getting attraction and awareness of the organization. For instance, a cyber threat can be classified as a hacktivist act having a high degree of severity through its basics of existence to increase political tension in a nation, region or company (Schreider, Building Effective Cybersecurity Programs: A Security Manager's Handbook, 2017).

Primarily, vulnerability is an indicator which demonstrates weak points of an object, system, or organization. Theoretically, in cyberspace, the vulnerability of a system can be discussed with probabilities as a measurement of consequences after a threat emerged. In other words, cyber vulnerability shows the possibility of an enterprise having blanks in its digital system, causing cyber risk when it coincides with the cyber threats at the same time and platform. In assumption, the vulnerability level of an organization to cyber threats can be computed by discussing all the potential ways for getting access to data, an object, or an asset. However, this scenario is not feasible in fact, because of human conduct and uncertain conditions in cyberspace. Therefore, in many cases, it may not be possible to forecast when a vulnerability and cyber threat meet with each other (Progrebna & Skilton, 2019).

Algebraically, cyber risk is defined as the multiplication of occurrence probability and impact of harmful events on the critical assets in cyberspace. Although, in the first step a cyber threat and vulnerability should emerge which causes a cyber risk. Therefore, the description of cyber risk is the demonstration of coincidence possibility in the same time and space of both the cyber threat and vulnerability. In other words, a cyber threat and vulnerability must come into existence in the same platform synchronistically before discussing a cyber risk. Consequently, cyber risk is varied with not only the severity of the cyber threat's impact and emergence probability but also the asset's critical value and vulnerability level which are affected (Progrebna & Skilton, 2019).

In practice, risk assessments of cyberspace are undertaken on the operational side of the information technology department. However, the operational part of this process is not just sufficient and should be coordinated by senior management which has direct responsibility to guide for setting a consistent cyber risk profile as a backbone of cyber security mechanism. Commonly, the key indicators while establishing a risk profile of an enterprise according to the vulnerabilities and cyber threats are defined by the classification of critical assets and information technology systems. Correspondingly, simulating, testing, and monitoring the damage or loss of confidentiality, integrity, and availability of critical assets are expected fundamental functions of internal audit in cyber security (Wilson, Gaidosch, Adelmann, & Morozova, 2019).

Conceptually, the critical term signals the importance level of an object to show how much risk is to lose. For instance, if a system or an asset will be damaged or stolen how the impact will cost the entire mechanism. Axiomatically, the critical asset is

described as the values of enterprises that have so vital importance in comparison with others. Therefore, the destruction of critical assets in enterprises causes huge costs and losses. Taking into account, first, the risk profiles of organizations are designed according to their operating sectors play role in their critical asset classification. Following a similar logic, cyber security precautions for the critical assets are planned by getting the supportive role of the information technology department to ensure their safety with the maximum degree (Lopez, Setola, & Wolthusen, 2011).

1.5.3. Cybercrime and warfare

The grassroots factors of risks in cyberspace are based on cyber threats and vulnerabilities of organizational functionings and culture. Relevant to the organizational weaknesses, the consequences of the cyber risks affect the critical assets of enterprises both tangibly and intangibly with unexpected costs. So, the criminal part of cyberspace emerges if there is an intentional attack to hurt an enterprise's physical and intellectual values. Viruses, worms, trojans, spamming, denial service assaults, ransomware, identity forging, and data theft are the most known crime types in cyberspace. In this frame, the legal environment of cyberspace is dynamically taking steps for protecting and regulating the enterprises due to cybercrimes around the globe. Therefore, the set of rules, conducts, and ethics in cyber security governance is not remaining stable because of the variations in cybercrime types and concerns (Jain, 2005).

Table 1.2. *Cost of Cybercrime across Industries in the Globe (Accenture Security, 2019, p. 12)*

Average Annual Cost of Cybercrime by Industry(US$Millions)		
Industry	2017	2018
Banking	16.55	18.37
Utilities	15.11	17.84
Software	14.46	16.04
Automotive	10.70	15.78
Insurance	12.93	15.76
High Tech	12.90	14.69
Capital Markets	10.56	13.92
Energy	13.21	13.77
US Federal	10.41	13.74
Consumer Goods	8.09	11.91
Health	12.86	11.82
Retail	9.04	11.43

Life Sciences	5.87	10.91
Communications and Media	7.55	9.21
Travel	4.61	8.15
Public Sector	6.58	7.91

Terrorists can use cyberspace as a battlefield by undertaking a range of attack types for making propaganda, brainwashing via radicalizing societies for raising their funds through planning and communicating with each other as legal associations. The main purpose of those kinds of attacks is to inflict damage to public and private enterprises' reputations and market worth through deteriorating strategic infrastructures and critical assets (Trim & Yang-Im, 2014, p. 141).

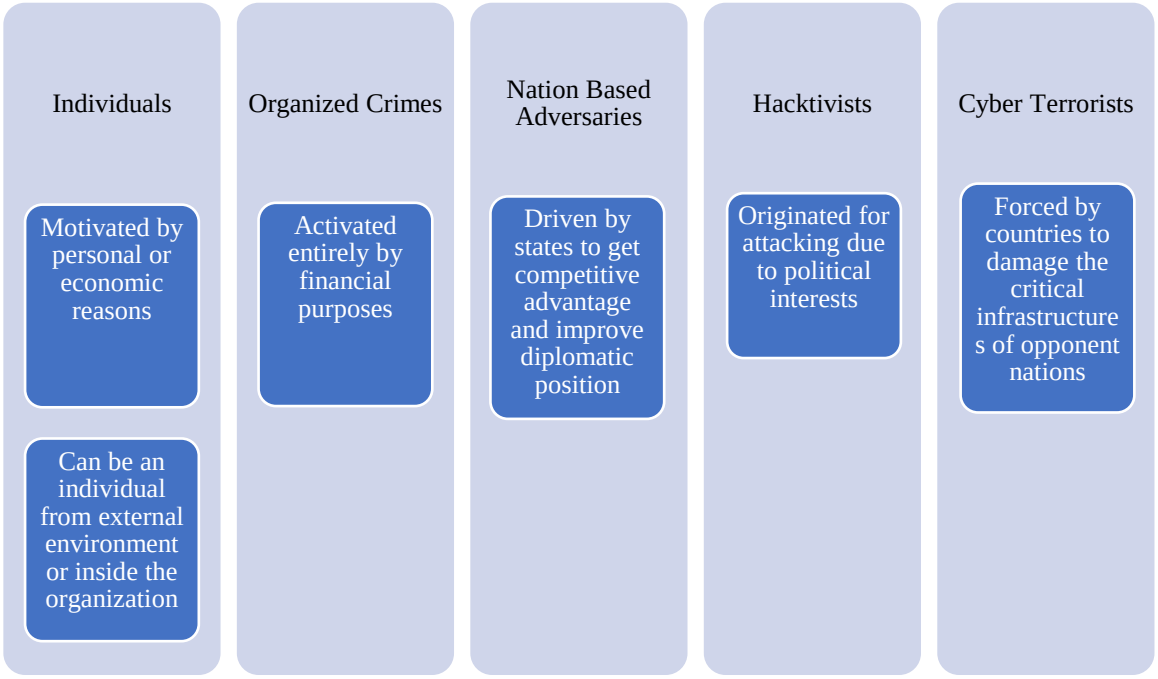


Figure 1.26. *General Classification of Cyber Attackers (KPMG, 2018, p. 22)*

European Union Agency for Network and Information Security (ENISA) is an association which provides data and recommendations to member countries, industries, and individuals for the development of information security expertise in the European region. Correspondingly, top cyber threats were described as malware, web-based attacks, web application attacks, phishing, denial of service, spam, botnets, data breaches, insider threats, physical manipulation, damage, theft, loss, information leakage, identity theft, cryptojacking, ransomware and cyber espionage in ENISA Threat Landscape Report for the 2018 year. Also, according to the executive summary of this report, the tactics and

purposes of the organizations which trigger the cyber attacks are named as cybercriminals have been switching relative to the progress in financial and technological events such as blockchain, digital economy and currencies, crypto mining and fifth-generation mobile networks (5G). Particularly, the modifications of cyber security systems concerning to the emerging attack types in cyberspace are planned and reinforced by defensive structures of the enterprises' information and communication systems through updated and refreshed techniques and tools as threat agent profiling and cyber threat intelligence (CTI) mechanisms for determination of criminal acts. Also, the investments of nations and enterprises to intellectual capital for building teams that involve cyber security professionals to improve their skills and motivations by setting and arranging technical training and education are indicators of demand to increase awareness of risk assessment qualifications in internal audit and control processes. In addition, technical staff is the previous symbol of organizations that has competencies for designing automatic tools and methods to ensure the immunology of cyber resiliency in enterprises are taking place when cyber attacks occur. Relative to the limited workforce in the cyber security field, the competition in industries and enterprises also affects the retention of employees who have advanced technical qualifications in organizations. Therefore, government incentives are needed to keep the companies' cyber security activities fresh through policies that will encourage the stakeholders for investing to construct the organizational culture by architecting the capabilities of labor capital according to new trends in cyberspace. Equivalently, specifications of cyber defense systems have been replenishing through these developments and cases, as well as existing frameworks and approaches in cyber security governance require revisions for adaptation of organizations' data protection perceptions to both international standards and national policies (European Union Agency for Cybersecurity, 2018).

In short, the emerging state of conflicts between nations or opponents result as damages, costs, and losses of critical assets in cyberspace are called cyber warfare (Kesetovic & Putnik, 2013, p. 219). In practice, cyberspace is discussed relatively as a new field for both offensive and defensive mechanisms and strategies, has contradictions because of its unclear nature. Historically, in recent times, World War One, World War Two, and Gulf War can be considered as major wars that have common points in which the enemies know each other precisely without a doubt. However, the definition of the adversaries is not possible certainly in cyberspace because of the variabilities and new

attack types. Therefore, the warfare tools, techniques, and tactics are evolving momentarily according to the developments in cyberspace for security experts and strategists. In current conditions, information technology security infrastructure investments are getting attraction increasingly because of their importance and changing perception of warfare due to cyberspace. In the macro environment, particularly, it is a way of strategy for nations that have weaknesses in conventional army forces investing in warfare tools in cyberspace for offsetting their disadvantages. For instance, the return on investment of software, which can be used both offensively and defensively in asymmetric combat, is cost-effective in comparison with a gun or tank (Geers, 2011, pp. 97, 98).

1.5.4. Cyber security management

Enterprises are interacting with their suppliers, business partners, sub-contractors, and final customers by following quality metrics and technical specifications in managerial frameworks. Similarly, cyber security operations are coordinated by strategic management levels according to principles, procedures, and policies which are formed due to both internal and external conditions. Roughly, the management framework of cyber security contains the control charters, task units of operational staff, and emergency plans for cyber attacks and breaches. However, it involves complexity to outline and implement an optimal set of rules and standards because of the relatively uncertain and unforeseeable nature of cyber threats. Comparably, the guidance of internal audit functions to these standards should be dynamic and adaptable for encountering the unpredictable nature of cyber risks. Therefore, cyber security management framework processes must be set to agile and robust systems that involve not only human wisdom but also technical tools and software packages rather than rule-oriented mechanistic and rigid approaches. In summary, preparing, investigating, responding, and transforming the cycle of the principles, policies, and standards should be based on resilient and intelligent guidance of internal audit (ISACA, 2013).

Enterprises need to re-engineer their architecture of information technology by securing their processing operations in the cyber environment. Mainly, cyber security functions cover advanced technical subjects such as access administration, encryption, encoding, firewalls, the protection of data, cloud and network systems. Technically, the layout, connection, and synchronization of all control mechanisms in identity and data access processes are the prior tasks defined in engineering functions of cyber security.

Also, engineers and experts who have authority in cyber security operations are responsible to operate and execute network zones by detecting threats and attacks. In addition, they have to guide and mentor the strategic part of management by both controlling the measurements of cyber security operations and Configuring future solutions. On the other hand, the persons, who involve in the security part of cyberspace, have to follow and perceive the standards by brainstorming collectively with the board of directors (Schreider, Building Effective Cybersecurity Programs: A Security Manager's Handbook, 2017, pp. 15, 16).

In general, the engineering operations in cyber security processes are executed in a framework according to the principles of the International Organization for Standards and the National Institute of Standards and Technology (NIST). Then, the formulation of responsibility and authority flowing diagrams are created (Reuvid, 2016, p. 7). In summary, technical, operational, functional, and strategical duties in the cyber security framework are nominated to the employees who need to understand and improve the three lines of the defense mechanism of cyber risk management processes.

Despite, having technical talent is necessary for a cyber security expert, it is as much as important to have business intellectuality and soft skills because of the metaphysical nature of cyberspace. Thus, integrally, perceiving the cultural aspects of the organizations according to their sectors, customer portfolios, enterprise risks, management types, data potential and classes, technology equipment and applications, governance structures, task units, the definition of workforce roles, performance indicators, and ethics mechanisms are the guiding principles of information technology security staff. In the past few years, operators in organizations were another form of information technology engineers who have been functioning in the cyber security field whose main tasks are installing software versus viruses, integrating firewalls, and setting detection systems as opposed to the intruders. However, this mind of business is becoming to change because of the developing technology policies and standards through moral attitudes according to the human conduct in cyberspace. Hence, the adjustments between organizational goals and cyber security challenges should fit together with the value creation activities in information technology through business visions (Tipton & Krause, 2007, pp. 11, 12, 13). Essentially, processes in cyber security development programs are predominantly dependent on labor who has active involvement to risk assessment reviews with open-minded approaches by taking into account the up-to-date types of crimes and legislations

in cyberspace. Therefore, qualitatively, the workforce has to operate their jobs enthusiastically in a cyber security environment by not only controlling the internal conditions but also following and adapting to the external events. The maturity degree of organizations in cyber security management systems can be driven by current and future projects, funding policies of strategic level management, investments, returns, authorities, responsibilities, standardized metrics, efforts, and processes via analyzing, reporting, monitoring, and tracking as the items of continuous improvement. In one sense, the role of information technology security teams is showing a tendency to progress their relational, business, and leadership abilities besides their technical knowledge and talents. From this standpoint of view, the United States General Accounting Office report in the year two thousand four presented that chief information security officers have major efforts to struggle with the obstacles in performing change and interactions. The managerial perspective of cyber security covers not only technical jargon but also business terms such as earnings, return on investments, liabilities, losses, and costs. Therefore, the officers in the cyber security environment should propose solutions both technically and organizationally, to provide effective communication, link, and interaction between top-down and bottom-up mechanisms on the management side. Naturally, information technology experts have an analytical understanding of the cases dealing in computer terminology, the common sense of publications in the cyber security field emphasized this situation as a focal point to show the lack of mindset for the voice of customers both internally and externally (Tipton & Krause, 2007, p. 11).

From the standpoint of audit, one of the elements of structural management in cyberspace is the monitoring mechanism to continuously detect the system which includes technological processes as electronic data transferring mechanisms, network accesses, antivirus, and service operations are on the way and running. Fundamentally, actively and reactively monitoring systems are in common for applications of audit to control system management approaches in the cyber environment. Correspondingly, in enterprises, active monitoring mechanisms can be framed as logging files, electronic mail alerts, text commands, and pager requests to vigorously control the up-down and running status of business functions through providing system experts for identification of problems and unexpected cases with proactive approaches in the cyber environment. On the other hand, reactively monitoring can be considered as a passive controlling mechanism to ensure that the active monitoring system is functioning normally. Also,

both of the two monitoring mechanisms should complement each other for operating and coordinating the audit activities effectively in organizations. If those two methods of monitoring are executed in harmony, the system management strategies in cyberspace can be applied with an interactive manner. In practice, actively monitoring systems in a cyber environment allows the system administrators for classification of the cases according to their critical level to proactively act when things are going to be wrong, supplementally passive monitoring mechanisms provide verification of system operations and if there is an issue or problem, the corrective actions are put in place for transforming the performance of information technology processes to acceptable and normal levels. Thus, cyber risk management infrastructures of enterprises should cover scenario plans and research methodologies with technical tools through efficient monitoring systems for detecting the verification of internal control operations with adaptive strategies to both internal and external threat factors and emerging risk criteria (Trim & Yang-Im, 2014, p. 143).

In essence, the enterprises have to ensure continuity of their critical business activities in the most worst scenarios as well as information technology context. According to European Union Agency for Cyber Security (ENISA), the business continuity degree of enterprises is explained by recovering the ability of critical organizational activities through sequential operations and processes with implemented managerial strategies which keep the critical business functions in line when unexpected events that affect the capability of vital business functions take place. Therefore, a clear definition of emergency plans through risk management policies and strategies is needed to provide sustainability of organizational activities with control models and systems for recovering the operations of information systems in a determined time scale. Also, this process should be supported by impact analyses of cases which cause risky situations for computerized systems to obtain data-oriented control models in risk management strategies of information systems. Naturally, the organizational staff and managers must be regularly trained and educated with simulation practices and scenarios to enhance organizational awareness and culture for both internal and external threat factors which raise cyber risks. Correspondingly, the installation of steering committees can be effective to execute, review, and test the business continuity strategies and plans for threat factors as insiders, hackers, and natural disasters which impact the cyber security processes in organizations (Trim & Yang-Im, 2014, pp. 60, 70).

Especially, the interaction and connection of international business activities between nations and enterprises around the globe are coordinated and detected in digital algorithmic platforms and computerized systems through technical equipment, networks, hardware, and software which involve discrete technological complexity relative to other parts of business functions. Therefore, from a micro perspective, the core qualifications which are required for cyber security professionals should be discussed by human resources, information technology, business development, and strategic management departments of organizations. Also, in the macro aspect, the international associations and national governments must propose and establish guidelines and policies to encourage and improve the cyber security experts' technical capabilities through observations and reviews of actual and real-time cases (Trim & Yang-Im, 2014, p. 143). The past intrusion cases in cyberspace are representing that education and technical training minimize the ability of criminal acts and maximize the awareness of organizations. Enterprises should train their employees for balancing the two sides of the equation in cyber security by reducing the technical faults that appeared because of the human factor. Practically, avoidance of all cracks in cyberspace is not possible, however, the reduction of these cases can be provided by taking preventive actions. Building an Information Technology Awareness and Training Program of NIST SP 800-50 keynotes the importance of cyber security education and awareness for building requisite abilities and talents. Also, the constitution of an organizational awareness for cyber security is not as same as technical training according to NIST SP 800-50. Mainly, awareness is related to the recognition of cyber security worries, responsibilities, and authorities of employees. Feasibly, the consciousness of cyber security in enterprises can be developed by using visuals, periodical reporting, and schedules (Mehan, 2008, pp. 198, 199, 200).

In practice, the implementation of an efficient educational training program to improve organizational learning, culture, and awareness starts with planning and definitions of goals. Therefore, an understanding of governance climate and cyber security atmosphere is needed previously for reaching the objectives of orientation. Particularly, the education program should motivate all levels of employees through setting an environment and ambiance with training tools, curriculum, and content. Also, it is as much as important to examine the functioning of the orientation program continuously by gathering feedback and attendance of employees (Mehan, 2008, p. 201).

1.6. Information Technology Audit

In essence, the operations are being transformed by the shifts and developments in the technological industry in which auditors involve. Especially, communication and data transferring activities affect the recording, processing, and monitoring mechanism of both financial and accounting statements like other business functions. Also, enterprises need to improve their internal control structures through big data management and audit standards (Pathak, 2005, p. 36).

Internal audit processes in the digital space are being set to strategic, management, and operational level functions in organizations. Also, both risk mitigation and value creation of the information technology department are being provided and enhanced by the applications of digitalized systems and processes. In addition, differently from the conventional operational, financial, and accounting inspections, information technology audits cover each of the business functions, which involve not only high technical expertise but also governance skills (Grembergen & Haes, 2007, pp. 2, 4).

The anatomy of an information system is formed by technological tools, equipment, hardware, operating systems, software, users, and workstations. Technically, the parts of this structure can cause attack surfaces if there are vulnerabilities in the system life cycle of the organizations for threat factors such as weak passwords, leaving programs open on monitoring screens, or giving permission to unauthorized people for accessing configuration software as well. Additionally, the grassroots of the attack surfaces can be explained by the network system cases as leaving portals open to unauthorized services which can be recovered through firewalls, breaches in software architectures which can be fixed by software patches, and human conduct issues such as malicious behaviors, ethical problems or social engineering which can be defeated via arranging educations and technical training to users for promoting organizational culture and awareness. Primarily, restraining the forbidden entry to information systems is the main task of audit operations for ensuring the confidentiality of data assets. The confidentiality of information assets displays the secrecy of data in cyberspace. On the other hand, the second duty of audit is integrity to prove the information systems in an enterprise can be controlled and executed from just a formally defined authority. Also, the enterprises need to serve the information for their permitted users when it is requested due to the operational viewpoint and this task of audit is defined as availability. According to the information security side of the situation, safeguarding the data assets from hazardous

events and taking proactive precautions are the main target objectives of the availability obligation of audit operations (Penuel & Statler, 2013, p. 218).

Performance Standard 2120.A1 of IIA points out the role of internal audit as making assessments of vulnerabilities that cause risks concerning the governance mechanisms, operations, information, and communication networks of organizations. The key target of the assessments is defined as obtaining the reliability and integrity of organizational data and information by taking into account the effectiveness and efficiency of business activities through providing the protection of assets in accordance with principles, regulations, and legislation. Performance Standard 2110.A2 clarifies that the assessment processes of information technology governance of the enterprises should be operated by internal audit services for investigation of whether governance practices of information systems are sustaining and reinforcing the strategies and goals of organizations. Meantime, the auditors of information systems have a particular role in ensuring the reliability and integrity of organizational information is described in Practice Advisory 2130.A1-22 because deficiencies in the safeguarding of the private data and information of customers and suppliers can both cause economic losses and damage the brand reputations of enterprises as a result of lowering the confidence of consumers and employees to the organizations. The determinants of privacy diversify relative to the cultural perception, political climate, and legislatorial structure of the nations in which the businesses are sustaining their activities. In essence, risks come up with the factors of information privacy covering both physiological and intellectual deterioration of personality rights and dissolution of confidentiality as a leak of personal data. Also, personal data and information are related to specific characteristics that contain factual and intuitive elements like names, location addresses, identification numerals, parental relations, employee records, performance scores, reviews, disciplinary punishments, salary, and educational status of each specified individual. The governance and risk management systems of organizations must be propped up with optimized control processes through effective methodologies for safeguarding personal data and information which is the key function of audit operations. Mitigation of the predominant risks can be provided with proper control processes through establishing convenient methods and tools, in case the board managements are strategical parts of organizations have ultimate accountability for business risk management activities, objectively identify, classify and frame those risks. Also, installation of the optimal framework for the

effective execution of business activities in organizations and implementation of this framework by ongoing monitoring are the supportive roles of board management in order to assist audit operations. Well-organized governance mechanisms and risk management structures can be reinforced by internal audit activities through evaluations of risks that are identified relative to the privacy objectives of organizations by board management for detecting the competency of control systems to temper the risks to tolerable levels. Also, the role of the internal audit covers the assessments of the entire privacy framework by advising appropriately for optimal risk management practices. According to the profoundly technical and juridical nature of privacy matter-related risks, the internal audit activities require relevant proficiency and awareness for controlling the assessments of risks and privacy frameworks of organizations. Weak information security systems raise risks referring to fraud acts, failures, and mismanagement with disobedience to data protection laws resulting in the displeasure of customer confidence, breaches in safeguarding mechanisms, and reputation loss of enterprises (Pickett, 2011, pp. 217, 218).

Occupational risk classes are defined by the Association of Certified Fraud Examiners in terms of fraudulent acts in information systems as deceptive financial reporting covers the unapproved entrance to accounting applications and nullification of system controls, misuse of tangible assets by showing false inventory or invoices through information technology systems and misappropriation of intangible assets like patents, licenses, copyrighted materials, business applications, client or supplier lists as leaking sensitive data for deceitful purposes (The Institute of Internal Auditors (IIA), The American Insitute of Certified Public Accountants (AICPA), Association of Certified Fraud Examiners (ACFE), 2007, p. 28). Information systems risk fields are classified by IIA in Information Technology Briefing Note Three as piracy of customized data, eavesdropping, system penetration, misconduct of Internet Access, denial of service attacks, viruses, and bluffing (Pickett, 2011, p. 218).

In the current business environment, sustainable development of enterprises is substantially driven by the information technology systems in computerized network platforms and the role of audit is transforming as a matter of fact. Also, the uncertain conditions of investing in control systems relative to conceptual risk management models cause unacceptable costs and failures that inhibit the audit activities to minor levels. Thus, for the elimination of this kind of conflict, the role of audit in information technology systems initiates with the assistance of board management while business objectives are

getting ready to provide the effective interaction between organizational goals and information systems. Intrinsically, the internal auditor role in organizations is modernizing relevant to the developments in information systems, so, in practice, the link between business activities and information technology mechanisms should be recognized as prior responsibility by revised functions of internal audit for facilitation of the business objectives setting and achievement stages. Methodically, information technology auditors focus on risks are causing by inputs, processes, and outputs of computerized mechanisms by taking support of a theoretical system model. On the other hand, the operational auditors have accountability for paying attention to control systems by taking into account the accomplishments of business objectives as well. Essentially, both of the audit approaches should be functioned and be coordinated synchronistically by providing interaction between each of them with corroborative and communicative ways. Not only scientific but also applicative techniques are required in control tests of information systems because findings of audit operations should be supported by tangible and precise arguments. Fundamentally, the objectivity and independence of internal audit operations can not be provided by purely auditing around the computers through depending on management to accommodate full testing of information systems. Correspondingly, the audit knowledge of the control systems in information technology can not be promoted by this kind of conventional approach, so in current business conditions, the internal audit functions in information systems are deriving trajectory to computing skills like using parallel simulation and interrogation software for providing audit samples to analyze and testing the accurateness of control documentations. Therefore, the auditors can incorporate assessments of system controls through software for extracting the data from file management mechanisms relative to findings. In essence, in the digital era, the new look internal auditors should build a tier of integrity in every function of business among operational, financial, and information experts, because of this fact auditors must have active roles in computerized systems like other parts of organizations to ensure audit targets are achieved. Hence, information technology competencies are needed for internal auditors to identify and test system controls without just relying on information system departments. The types of control systems and their assessments implemented by management and auditors in information technology have differences relative to operational and financial departments of organizations because of the sophisticated nature of computerized systems. Therefore, IIA Standard 1210.A3

clarifies the matter of computing capabilities of the internal auditors as having proficiency in major information technology risks and controls by applying technology-based audit methods and tools to achieve the objectives. Nonetheless, the internal auditors whose main responsibility is not information technology audit, don't need to have advanced computing abilities and expertise. The periodic assessments of information technology security tools and practices are processed by internal auditors through control systems and safeguards with updating mechanisms along with continuous improvement approaches. Fraudulent intentions in information technology activities, corruption, espionage, sabotage, vandalistic acts, and natural catastrophes can cut down the network systems and destruct the databases of enterprises. Axiomatically, primary business objectives of managements are ensuring sustainable development of organizational activities with the satisfaction of stakeholders according to not only earnings but also social responsibility elements and controlling risks to get maximum return with minimizing damages. Therefore, organizations need to detect their security controls by considering the convenience and effectiveness of business practices through risk analyses which provide the determination of sensitive assets and threats to them. In this way, the standards for information security management were established with BS 7799 as a consequence of demand from sector, government and trade organizations to build a common information security structure. Briefly, the conformation of BS 7799 is an element of taking into account the relevant security controls in the primary stage enhanced with continuous monitoring and advancements to secure the controls to be effective and convenient. In other words, the matter related to which principles are proper for perceiving risks and their damages. The risk perception states which assets are in jeopardy according to threats with likelihoods and effects to vulnerabilities and breaches in information security systems. BS 7799 was established for the safeguarding of the confidentiality, integrity, and availability of information assets by integrating security control standards and systems into the organizations. Major functions of BS 7799 for information security management mechanisms in organizations are to implement plannings for business sustainability, system access controls, system development and maintenance, physical and environmental security, compliance, personal security, responsibilities and training, risk assessment, organizational, computer, and network system management, asset classification and control with security policies. Asset classification and control mechanisms in organizations are executed by figuring on

occurrence probabilities and impacts of threats with a combination of sensitiveness and vulnerabilities of data security systems. Furthermore, the BS 7799 proposes that audit specifications and processes should be thoughtfully organized and planned for activities of operational systems in information technology to offset risks in business activities. Also, the audit requirements must be admitted by convenient management approaches with steady monitoring and systematic documentation mechanisms through the distribution of security roles with information security training to dynamically provide the conformance of risk control processes with the international security policies and legal framework of data protection (Pickett, 2011, pp. 219, 220, 221).

1.6.1. Cyber security governance

Strategically, enterprises have a diverse mission, vision, objectives, and management forms to meet their profitability targets and customer satisfaction. Similarly, governance, and compliance with risk perception in information security systems are verified according to the industry and executive types of the enterprises. However, the cyber security governance framework covers the status, responsibilities, and authority of information security experts by setting policies, procedures, and plans to periodically assess the risk of information assets with an overview of the consequences of reports. It is not just enough to implement these steps into the corporate culture, besides, organizations should install a culture of cyber security governance to behave the protection mechanisms of data assets as a dynamic, flexible, and agile systematic cycle. In essence, organizations should support their cyber security governance formations by creating internal audit mechanisms to integrate best practices of industrial standards complying with externally based information technology policies and procedures. Particularly, this situation can be perceived as a kind of commitment to outside-centered cyber security cautions. If an organizational perspective can be constructed as an organic structure both to provide the governance of cyber security operations internally and adapt to the external conditions will ensure continuous value-added composition. However, these processes involve complexity and need to be supported by the interrelations of senior, middle and operational level staff by not only reviewing the internal business environment but also the outside developments. Therefore, cyber security governance patterns of enterprises should be installed on a robust and elastic culture for adapting to the rapidly changing conditions considered as standards, policies, and regulations.

Briefly, organizations must take into account the effectiveness, efficiency, and validity of their cyber risk management systems by editing both internal audit and governance perceptions (Trim & Yang-Im, 2014, p. 180).

Organizations should establish a set of codes, laws, standards, ethics, and morals for affiliation to international frontiers in cyberspace. In essence, International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and Internet Protocol Security (IPsec) are the associations that have the responsibility for framing the guidelines relevant to operational, managerial, and security standards in the protocol for the creation of cyberculture in enterprises. Link points of devices in an organization are designated as interface standards in the security of the protocol. Also, the quality specifications and operational instructions are defined by these unions for effectively organized cyber security systems in enterprises. Theoretically, the assumption behind the application of guidelines in organizations is for the establishment of cyber security functionality. Familiarly, the enterprises need to set their cyber security framework in compliance with standards by deploying their principles and policies through applicable approaches to reflect a precise view of assurance in data confidentiality, integrity, and availability (Mehan, 2008, p. 104).

The metrics for an organization are satisfying its' both internal and external obligations in a cyber security environment can be gauged by compliance parameters. In recent years, the legal frame which covers laws, regulations, and rules for cyber security is expanding according to the innovations and developments in cyberspace. Also, the industries are being affected by these modifications both publicly and privately. In practice, the compliance mechanism is complex and costly for the enterprises because of its' unstable structure as a result of mobile cyberspace conditions. Therefore, organizations should construct their cyber security governance systems based on compliance with the legal environment in order to get adequate performance scores of audit tests. In addition, setting a manageable and applicable compliance authority is not a one-time episode. So, the processes in the compliance mechanism should be continuously systematized and reviewed through collaborative approaches with information officers. Applicatively, the improvements in compliance posture according to the cyber security environment must be detected by reporting and monitoring with both quantitative and qualitative scales. The static approaches in cyber security systems can not offer cost-effective functions for compliance with international standards. Therefore,

dynamic processes must be implemented into the backbone of the cyber security framework through the definitive role of laws, rules, and standards with the assistance of governance and information technology functions (Mehan, 2008, pp. 212, 213).

Vulnerable security systems in the cyber environment can cause loss of brand image and decline of market worth in enterprises, so the governance mechanisms in information technology require policies that cover stakeholders, board of directors, middle management, and front line personnel with all parts of the organization are included. Affirmatively, the main intention of governance methods in the cyber security field is to implement convenient operations for managing risks in cyberspace and investments into information technology by serving the eyesight of functionality in processes to the senior management with providing an effective interaction between the employees and security culture in the cyber environment (Tipton & Krause, 2007, p. 16).

Hypothetically, the governance term delivers a close interaction between legislative frameworks and business dynamics for providing compatibility between governmental norms and societal organizations. Particularly, transforming the international standards and governmental rules into practices in organizations depends on control risk self-assessment systems (CRSA) by taking the support of authorities as board management, auditors, and controllers. The submission and enaction of the legislative frameworks cover experimental efforts and innovations for fulfilling not only the bureaucratic procedures but also the interrelations with formal committees which have an active role in making regulations about information systems security. Analogously, the protection systems of data and informatics in enterprises should be designed in harmony with macro scale as international, governmental, and sectoral conditions by continuously assessing and adapting the microelements like organizational culture, awareness, learning, and control (Kooiman, 1993, pp. 94, 96, 97).

In practice, the policies are designed to arrange corporate governance mechanisms and recovery strategies must be harmonized with cyber security governance through information technology standards, definitions of roles, and organizational hierarchy for providing resiliency in business activities. According to the top-down approach, a risk manager is assigned who has roles in layout and integration of adequate security policies and strategies which should be fitted with organizational culture due to effectively control cyber risks with reporting of internal control systems performance to stakeholders for providing an overall view of enterprise risk management approaches and applications.

Also, the risk manager should collaborate with the information technology manager through effective reporting and monitoring mechanisms for the review of cyber risks. Human resource management policies and practices in terms of structuring the cyber security perception and governance systems must be set with the involvement of the risk manager to diffuse the cyber risk culture all over the organization. In essence, after formulating the risks management techniques and structuring the organization model through the installation of teams and managers the applications of those should be integrated into the organization for delivering the effectiveness of the business activities to stakeholders. Fundamentally, the implementation of three indicators of effectiveness as performance, conformance, and corporate responsibility into organizations through enterprise governance models provides efficient adaptation to uncertainties that cause risky conditions. In practice, performance management systems measure and present how the business functions are creating value for the sustainability of enterprise activities. Industrial standards, legislations, and regulatory codes are followed and implemented by strategic level management parts of the organizations to ensure the adaptation of enterprise governance systems with conformance accountability. In order to harmonize the interaction between performance and conformance metrics, corporate governance systems should be formed through organizational culture with risk management and internal control practices as monitoring and assessment activities by taking the support of board management. In detail, the corporate responsibility of management acts as a universal set which covers the cultural dimension of organizations, optimization of risky conditions and their impacts by taking strategic decisions, promoting motivation levels of employees, and improving the productivity rates of business functions. In relation to information technology and communication systems, the management units of enterprises should understand and check on the cyber environment continuously for which threats are emerging and cause cyber risks for organizations to support the employees with proper awareness education and programs for establishing security perception in business, control, and audit activities. With a basic explanation, corporate governance embodies coordinated activities and processes which formulate systems and their designs to control risks for supporting the improvement of organizational performance in line with legislative infrastructure to accomplish business continuity through value creation for employees and stakeholders. In this aspect, the key responsibility of corporate governance systems is to check and determine the compliance level and quality of organizations with

technical standards and regulations according to the industrial, national, regional, and international scale. Similarly, the compliance status of organizations related to cyber security should be controlled and audited in periodical time frames for evaluation of how the information systems are functioning conveniently with the legal environment which covers rules, industrial and technical standards for structuring frameworks and standardizations of critical business processes in enterprises' information technology systems. Therefore, from the starting point, organizations need to form plans through risk identifications, measurements, and assessments for demonstrating the compliance insufficiencies and states of their cyber security infrastructure to the governing bodies and regulators. As a result, the gaps between an organization's information system processes due to the cyber security matters and regulatory aspects must be reviewed through internal audits and controls to idealize governance approaches that are applied for catalyzing the business flows and coordination of employees. As well as having competencies to provide compliance accountabilities relative to codes of conduct in the legal framework, the strategic management philosophy concerning cyber security should be integrated into the business activities to consider how and in which ways the enterprises are ensuring privacy and protection of customer data. Conceptually, the applicative methodologies in cyber security governance cover technological equipment, hardware, software, databases, understanding, and knowledge capability of the organizations together with risk management techniques and tools. Also, personal staff has to pay extra attention to cyber security concerns as well as their business functions to disseminate organizational awareness into all activities of enterprises. As an example, a former employee who was working for Ex-Softbank Corporation was under scrutiny for engaging in espionage through a leak of custody information to Russian agents (Japan Times, 2020). Therefore, the behaviors of employees in organizations according to security reasons should be analyzed and investigated periodically by applying in-depth interviews, scenarios, and simulation models with the support of awareness programs, education, and pieces of training to keep the health of organizational psychology up for reducing those kinds of acts. In assumption, the interoperabilities of audit activities and cyber security governance structures can be enhanced by the support of internal control mechanisms such as identification of specific tasks, critical activities, and sensitive assets all over the organizations. After this process, threat factors that can turn into cyber risks are defined with their occurrence probabilities and impacts through matching with

vulnerable parts of organizations to measure the robustness and recovery time of information systems. By this analytical approach, the three dimensions of cyber security as governance, internal audit, and control are harmonized in order to improve the effectiveness and efficiency of business functions in enterprises by ensuring the optimum security of information assets in compliance with regulatory bodies. Furthermore, scientific methodologies such as statistical process control, fuzzy logic, machine learning, and artificial intelligence can be adapted to organizations for the determination of threat factors and unexpected cases in real-time to eliminate and reduce the cost of cyber attacks by taking proactive actions. Correspondingly, monitoring competencies of organizations can be improved through those scientific approaches to audit and control data accesses, discrete and linked databases for manifesting how the interchange mechanisms of information flow in organizations are functioning (Trim & Yang-Im, 2014, pp. 128, 129, 133, 134, 137).

Implementation of strategies in terms of cyber security governance can be provided and developed in enterprises by building effective interaction between board managements and representatives who have responsibilities for setting principles, industrial standards, rules, and codes of conduct. In essence, the resiliency and robustness of cyber security processes depend on how the senior management is concerned about intellectual property and sensitive data for the entire protection of organizations' critical business activities and assets. However, organizational understanding of cyber criminals and attacks is not solely enough for promoting effective cyber security governance systems, therefore the individuals in public, governments, and enterprises, as well as associations which have accountability for framing the set of rules according to emerging cyber threats and risks must function in harmony and coordination. Particularly, cyber threats which target networks and communication systems bring to the fore problematic cases that can affect international business activities and relations between nations and organizations because of the interdependency in the social, cultural, economic, and political environment. Hence, collectivity between governments, organizations, and institutions should be improved to ensure adequate compliance in cyberspace for robust governance in cyber security structures with a global view. In addition, the occurrence possibility of cyber attacks is not predictable because of the incompetencies of detection systems and chaotic nature of cyberspace conditions, as well as cyber threats can emerge from any part of the universe at any time frame, so risk culture and awareness must be

built in all around the globe through the powerful cooperation between countries and governments with information sharing when unexpected cases come up. Bearing in mind that, the key parts of cyber security governance can be prescribed as strategy, culture, and awareness which point to qualitative parameters of organizations. As well, tolerance and appetite levels are considered as quantitative variables which indicate the numerical measurement of enterprises' risk perception. Correspondingly, enterprise risk management methods are installed on those elements with the support of technical security tools, intelligence detection mechanisms, and continuous monitoring systems to determine threat factors and their impacts on organizational vulnerabilities. Especially, internal control of risk management activities relative to cyber security is structured on an enterprise value system, business industry frame, international standards, regulations, and policies via examinations of internal and external risk criteria with priority matrixes and reconsideration of risk treatments. In addition, execution of internal audit and control processes to strengthen the cyber security governance must be afforded by the participation of managers, specialists, and policy counselors with bringing cyber threats, human and technical factors into the equation through holistic methodologies and strategies (Trim & Yang-Im, 2014, pp. 141, 142, 143).

1.6.2. Information technology governance standards

Theoretically, the main goal of governance is to arrange the formalization and clarification of decision mechanisms through ethical rights. As same as in theory, information technology managements need to provide a set of standards for framing behaviors and controlling operations. Fundamentally, these processes layout investments in information technology and discuss the prior requirements to optimize the expected returns with continuous improvement approaches. Also, they have supportive roles in defining the cash flows to information technology, executing threats, reviewing performance, and satisfying the demands through the voice of clients. Corporate and risk culture, leadership approaches, perception of ethics, technological tools, and strategies are the primary indicators while observing an enterprise's governance standards in information technology. Briefly, the elimination of confusion by clarifying the central roles and authorities in information technology functions are the prior tasks of governance which are based on standards in enterprises (Selig, 2008, p. 21).

The description of governance according to Information Technology Governance Institute (ITGI) demonstrates that cyber security governance must be evaluated as a component of information technology governance. Through this logic, the management board should be acknowledged regarding cases, solutions, and proposals in the cyber security environment for assisting them to set the principles, procedures, policies, plans, blueprints, and cultural structure about risk management methods, authorities, responsibilities, and reengineering functions to perform change management and assurance mechanisms of internal and external audit processes, investments for the effectiveness of governance practices. Therefore, the role of management according to ITGI covers the provision of governance in implementations and adoptions of quality measurements, specifications, procedures, and standards by examinations of vulnerabilities and defaulted processes with constructing a life cycle for system advancements supported via educational training and orientations for raising organizational awareness (Tipton & Krause, 2007, p. 16).

Systematically, an inspection of information technology structures comes up with suggestions for ensuring secrecy, integrality, and presence of assets in cyber security control operations for continuous improvement and value creation. Essentially, the cycle of these processes is defined by combined frameworks that have a common level of agreement in audit aspects. Committee of Sponsoring Organizations of the Treadway Commission (COSO), Information Technology Infrastructure Library (ITIL), Control Objectives for Information and Related Technology (COBIT), International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC) are the organizations which have major and central authority for guidelines and practices accepted by governing bodies of enterprises (Tipton & Krause, 2007, pp. 17, 18, 19).

From the standpoint of Turkey, the information technology structure of enterprises should be in line with regional compliance requirements as well as internationally approved guidelines and frameworks. Banking Regulation and Supervision Agency, Central Bank of Republic of Turkey, Capital Markets Board of Turkey, Revenue Administration Presidency, Banks Association of Turkey, Ministry of Treasury & Finance, Information Systems Legislation for Insurance Industry, Ministry of Commerce Information Systems Legislation, Information and Communication Technologies Authority, Public Oversight Accounting and Auditing Standards Authority, Sarbanes Oxley Act, International Financial Reporting Standards, Capability Maturity Model Integration, Control

Objectives for Information Technologies, International Organization for Standardization (ISO20000, ISO22301, ISO27001, ISO31000, ISO38500), Information Technology Infrastructure Library, The Open Group Architecture Framework (TOGAF), Assurance Audit Standards 3000 and 3402, International Standards on Assurance Engagements 3000 and 3402 (ISAE 3402), Service Organization Controls (SOC-1-2-3) are both nationally and internationally legitimate authorized institutions and frameworks for audit services of governance and compliance matters in industries and enterprises. Framing and developing governance, risk management, and compliance structures to satisfy the requirements of legitimate bodies for improving the efficiency of information technology systems must be supported and guided by internal audit and control mechanisms (PWC Turkey, 2019).

1.6.3. Big data

In the last three decades, the developments in computer and internet technology alter the way of recording, keeping, and processing data. Paper base documentation and hardcopy of reports are being shifted to digitally operated data as shown by graphs, schedules, and indicators. Traditional software, relational databases, and spreadsheets are being transformed into agile mechanisms for multiple machines. The innovations such as cloud computing, the internet of things, or blockchain show that big data should be secured and controlled in cyberspace because of the escalating risk potential (Savaş & Deng, 2017, p. 9).

Technically, the vast size of data clusters spans diversified data types and interactions. The synthesis and analysis of the large size of data sets have advantages for auditors to search for relationships between root causes and outputs. Classifying, modifying and processing of extensive bulk of data sets automatically increase the effectiveness and efficiency of internal audit operations (Cascarino, 2017, p. 159). As a result, internal audit approaches of such multiple dimensions and big data to comply with the standards in information technology structures must be adapted to cyber security governance systems.

Particularly, in current conditions, the data protection regulations and methods are attracting the attention of both public and private enterprises. The governmental and international authorities are establishing new standards, rules, and laws to enforce the companies for the safeguarding of personal data has critical importance for nations,

societies, economies, and international relations. Therefore, the role of information systems in enterprises is not only keeping personal data records but also ensuring the security of the data assets. Also, steering of audit and control systems in information technology is supported with the governance of data protection due to the international, governmental, and organizational relations and interactions beside legislation framework. Notably, nations and governments began to legislate data protection and privacy rules to regulate the information systems in organizations, specifically for digitally held assets on computers and communication networks since the beginning of the nineteen seventies. Also, the developments in the arts and disciplines of regulation have been provided by the favorably escalating importance of data protection with the creation of new fields for research and development in both academic literature and practice. Correspondingly, the configuration of codes, guidelines, and standards have been shaped by the efforts of the Organization for Economic Cooperation and Development (OECD) and the Council of Europe for the establishment of performable frameworks into states and organizations. The main reasons of such these acts are for the obtainment of adequacy, relevancy, and entireness of the data assets by taking into account the security status relative to the sensitivity level of data. In essence, the principles have been authorized and endorsed by official foundations for the intention of building safeguarded international business conditions to provide the entire protection of data flows across borders. Adjunctly, the applicability of the principles is both dependent on regulatory associations and leadership approaches of board managements in corporations that are accountable for the implementation of frameworks. The principles and policies are implemented by the independent, objective, and judicial bodies, raising the awareness and consciousness in acts and efforts of data users and processors as well. Therefore, the dissemination of the legislative practices in enterprises provides not only enforcement of laws but also the governance of data security from an extensive perspective. The conducts of laws differ across countries and industries according to their economic level, social status, political and governmental structure. However, the enactment of the principles in the international business climate has the primary objective of installing a common language to regulate the data protection applications in organizations. For instance, Data Protection Act (DPA) was come into effect by Britain in nineteen eighty-four for the security of data held on computers by requiring the types, purposes, origins, and recipients named as data classifications (Kooiman, 1993, pp. 89, 90, 91).

Inevitably, in the competitive business environment, enterprises have to deal with big data for doing market researches, understanding correlations, and gathering general statistical inferences. Despite this, the variations of big data sets frequently cause troublesome cases while recording, warehousing, and processing. Also, it is another issue to control the data environment securely in a complete manner. Therefore, organizations should integrate enterprise data management systems into their operations and policies. Particularly, from the technical point of view, matching up the operational key risk indicators with data assets supports the information systems security of enterprises to prevent future events as data loss, deterioration, and theft (Abawajy, Choo, Islam, Xu, & Atiquzzaman, 2018, p. 158).

2. THE INTERACTION BETWEEN INTERNAL AUDIT, CONTROL, AND CYBER SECURITY GOVERNANCE

At the outset, processes, procedures, human beings, products, services, suppliers, customers, tools, and technical equipment are all the pivot parts of the organizations which structure and perform cyber security. In real-life cases, these major elements are not isolated from each other as well as they interact both as dependent variables. Correspondingly, a management system, which consists of all of the interconnected and reacting parts of the organizations for the establishment of corporate objectives, policies, and processes, is required assessments by the independent and trustworthy officials for controlling how the adequate processes have been utilized or employees are trained, equipped and organized. Similarly, information security systems should be overseen through evaluations which involve proof of concept by the accumulations and analyses of factual data and evidence in terms of assuring that the controls are being objectively performed in compliance with standards and legislation (Gallotti, Cottafavi, & Ramacciotti, 2019, p. 17).

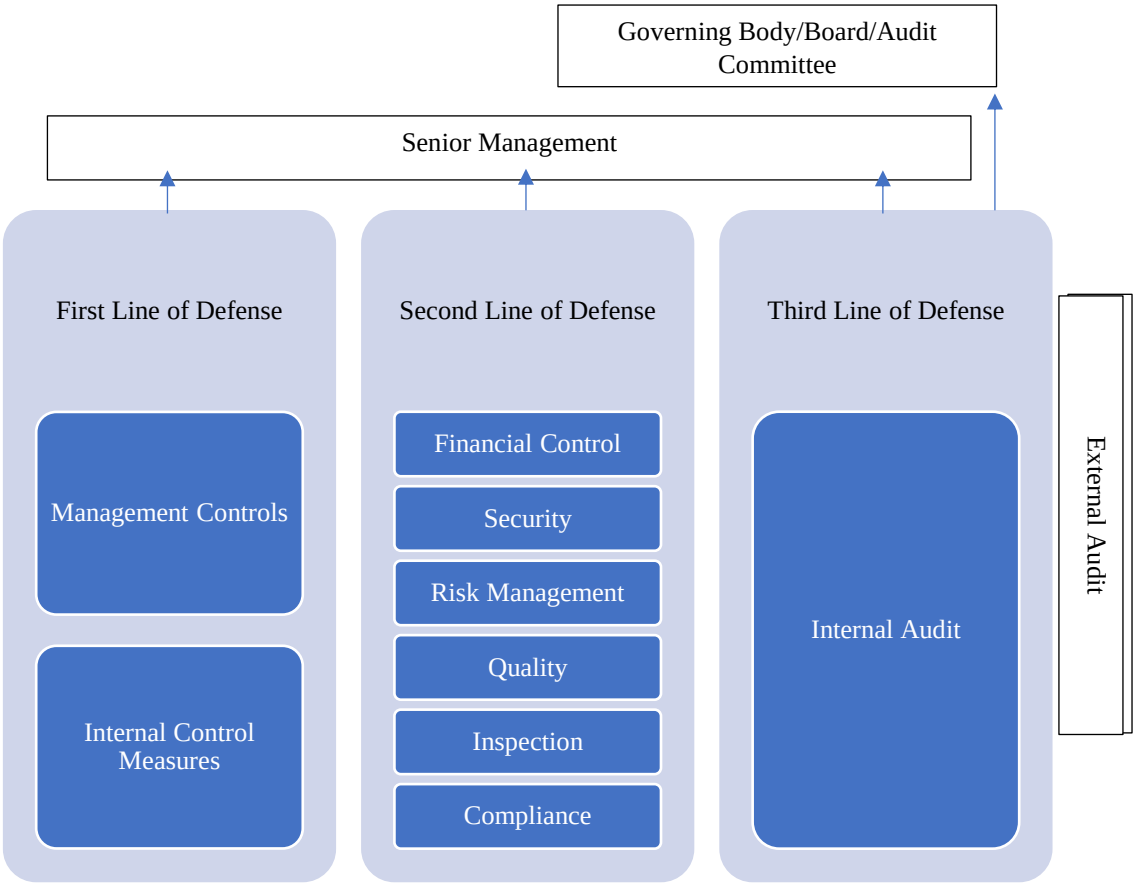


Figure 2.1. *Three Lines of Defense Model (3LoD) for Improving Governance by Using Internal Audit (Stevens, 2015, p. 12)*

The Three Lines of Defense Model of the European Confederation of Institutes of Internal Audit (ECIIA) and Federation of European Risk Management Associations (FERMA) can be summarized as;

- The operational management of organizations is responsible to control, evaluate and minimize risks in the first line of defense.
- Supporting and monitoring the risk management implementations and assisting the risk officers in reporting risk-associated information throughout the organization are performed under the cover of the second line.
- The internal audit role, which is performed with a risk-based methodology, is to ensure the board of directors that how the organization is managing inside risks that involve all parts of risk management frameworks, is defined in the third line.

Therefore, the assurance of governance effectiveness, risk management, and internal controls are provided by the internal audit function with the approach as the first and second lines are fulfilling their objectives (Leech & Hanlon, 2016, pp. 337, 338).

However, there are contrary arguments to the 3 LoD model as the recognition and active participation of board management and general manager can not be ensured effectively in risk governance processes. This approach doesn't sufficiently support the risk management activities to encourage the organization for taking risks strategically and adding value. In addition, the risk definition of ISO 31000, which is the impact of vagueness on the accomplishment of objectives, is not reinforced by this framework. Furthermore, the role of the first line is limited to only having responsibility for risk and control which must be enhanced by evaluating and reporting on the situation of residual risk to the board management. In the same way, the function of the second line is not clearly determined which should be established as assisting the first line for improving their activities in the assessments and reporting on the residual risk status of the organization. As well, the role of the third line, which is also known as internal audit activity is not entirely defined, should be advanced with assessing and reporting for the effectiveness of the risk management system that covers the assurance and consistency for the conditions of residual risk. Therefore, the Five Lines of Assurance (5LoA) model is developed with frontiers such as the board of directors, internal audit, c level managers, specialist units, and work units to mainly support the elevation of functions of the general manager and board of directors in risk control and governance processes. The overall responsibility of board management in this framework is to ensure that the risk management processes are functioning effectively and the other four parts of the system are supporting the risk control activities according to the organization's risk culture. Also, the role of the board is accountable for making the assessments of residual risk levels through the discussions of organizational objectives and performance metrics. The role of internal audit is to assure on-time information, which depends on risk management processes and the validity of reportings that state the status of residual risk is related to value addition, independently of to board of directors (Leech & Hanlon, 2016, pp. 8, 9, 10).

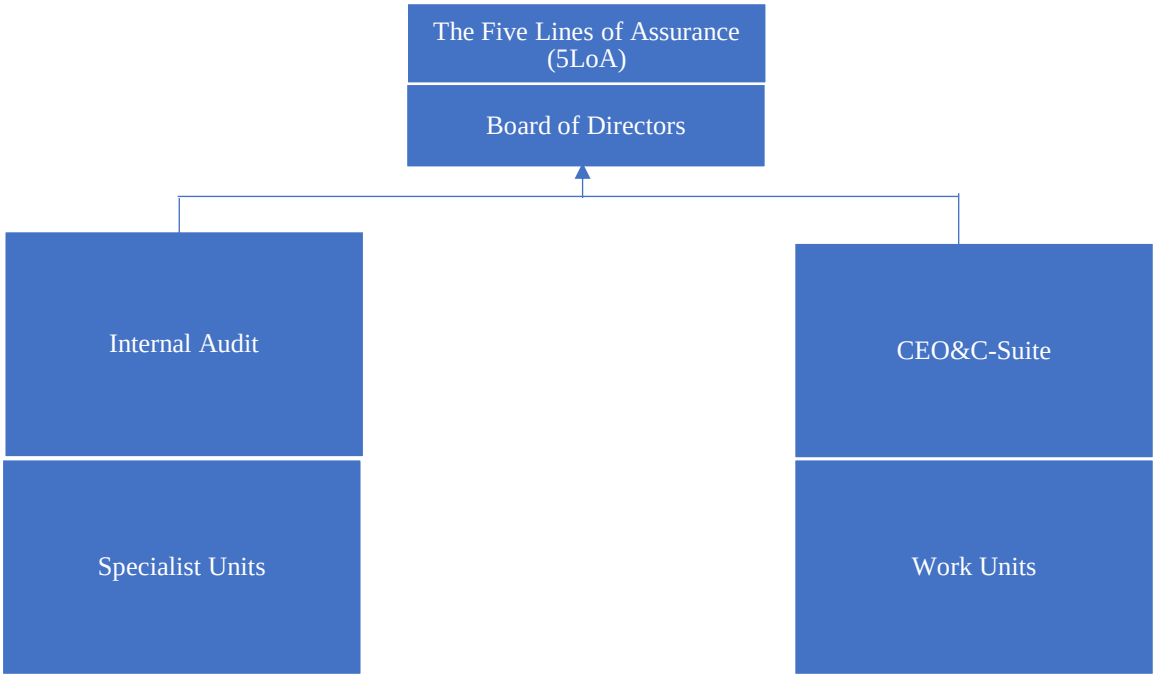


Figure 2.2. *5LoA Model for Risk Governance (Leech & Hanlon, 2016, p. 10)*

5LoA approach can support the organizations in terms of effectively managing cyber security risks through providing risk governance because the board of directors and CEO must be accepted as major participants not just as pure and simple endpoints of reports in this model. Especially, the CEO and work units have a responsibility to ensure valid consolidated reportings which depend on residual risk conditions related to value addition and upholding business objectives that can be affected by vulnerabilities and cyber threats (Antonucci, 2017, p. 16).

Initially, business continuity and development of enterprises are being supported by IT structures which include software utilization and hardware equipment to build infrastructural parts of interconnection architecture for data transferring. Also, the IT part of enterprises has not just a complementary role in business functions and as well it is essential for sustaining information flow to keep relations going across the organization. Accordingly, the dynamic interaction between IT functioning and business processes is required to understand both the mechanism in securing data flows and organizational operations for internal auditors. In similar with the internal controls framework of COSO as a standardized tool has been concealed by SOx which proposes guidelines and performance metrics to measure and evaluate primarily accounting processes for internal audit since the 1990s, CobiT was first established in 1996 for a control structure that

covers predominantly IT processes beside business operations because of the specific needs of information systems oriented auditors who review internal controls refer to IT. In connection with the mentioned reasons, IT-related assets and their functions in business activities have key importance, and safeguarding of IT relevant sources and processes have been considered under the main responsibility of enterprise management in today's business environment. Therefore, information and data-connected processes with their controls should be needed to understand by users, IT auditors, and management to support the value-added activities. Elemental CobiT framework must be perceived by both IT and internal auditors with having an essential level of knowledge, regardless of carrying out it for reviews of internal controls. In addition, to applying the internal controls framework of COSO, having an understanding of CobiT can assist the internal auditor to analytically perceive the information security risks and IT control role in enterprises. On the other hand, IT governance should be discussed as a key element of CobiT for strategic adjustments on risk and performance indicators while performing enterprise management (Moeller, IT Audit, Control, and Security, 2010, p. 30).

Correspondingly, the internal audit role in cyber security governance should be analyzed from the point of value aspect in order to understand why and how cyber risk management is related to internal control and its review. With that in mind, the applicative researches, which focus on the value creation function of internal audit, can provide an edge for recognizing how the code of ethics is being installed and revised.

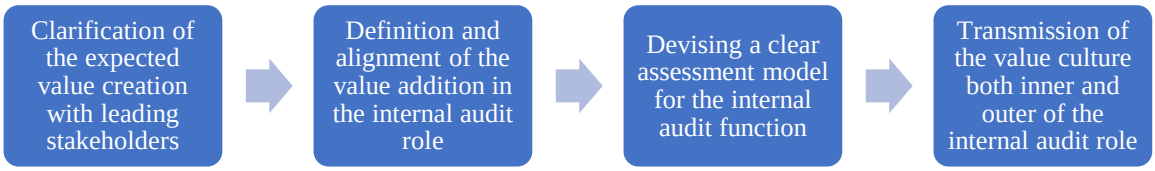


Figure 2.3. *Achievement Process of Value Additional Activities of Internal Audit (Eulerich & Lenz, 2020, p. 7)*

Fundamentally, the main goal of the audit cabinets is to guide the enterprises as a doctor or a dentist due to the major and emerging risks for framing the adequate risk management approaches, models, and tools to implement a working order internal control system. So, in general, how the definition of the value-added activities and measurement of their performance is executed by using which metrics are the common complexities for the internal audit function. Accordingly, the internal audit role can be distinguished

as GRC partner, entrusted advisor, and value rider. The function as a GRC collaborator provides assurance support of overarching the elements of organizational roles. The trusted consultant role covers not only offering recommendations but also struggling with organizational resistance for change management. The organizational biases and traditional frontiers can be broken by the support of the value-driving role of the internal audit through contributing to the enterprise what really matters as coping with just not the as usual issues, also the lesser-known subjects and deep complexities (Eulerich & Lenz, 2020, p. 14).

Table 2.1. *Responsible, Accountable, Consulted, and Informed (RACI) Role of Audit in Cyber Security (ISACA, 2020)*

Count of Audit				
Audit	**Objective**	**Practice II**	**Practice_Name**	**Total**
Accountable	**MEA03**	MEA03.02	Optimize response to external requirements.	1
	MEA04	MEA04.01	Ensure that assurance providers are independent and qualified.	1
		MEA04.02	Develop risk-based planning of assurance initiatives.	1
		MEA04.03	Determine the objectives of the assurance initiative.	1
		MEA04.04	Define the scope of the assurance initiative.	1
		MEA04.05	Define the work program for the assurance initiative.	1
		MEA04.06	Execute the assurance initiative, focusing on design effectiveness.	1
		MEA04.07	Execute the assurance initiative, focusing on operating effectiveness.	1
		MEA04.08	Report and follow up on the assurance initiative.	1
Accountable Total				**9**
Responsible	**MEA03**	MEA03.01	Identify external compliance requirements.	1
	MEA04	MEA04.09	Follow up on recommendations and actions.	1
Responsible Total				**2**
Grand Total				**11**

Effectively, a cyber security structure, which can be used as one size fits all approach, may not be certainly defined for the enterprises both in assignments of organizational roles and in designs of governance models because organizations may involve differences due to their specific industries and corporate cultures. In connection with this statement, the organizations which sustain their businesses in strategic and critical sectors such as defense, finance, transportation, or research and development may be much more sensitive to cyber risks. However, no matter which cyber security governance model is being adopted in an organization, the basal concern of IT security is to assure the confidentiality, integrity, and availability (CIA) triad of sensitive assets. Therefore, in general, the reporting mechanism is performed such as the chief information officer (CIO) or the particular responsible for IT processes in the enterprise is informed by the information systems security officer (ISSO) or chief information security officer (CISO) (Tipton & Krause, 2007).

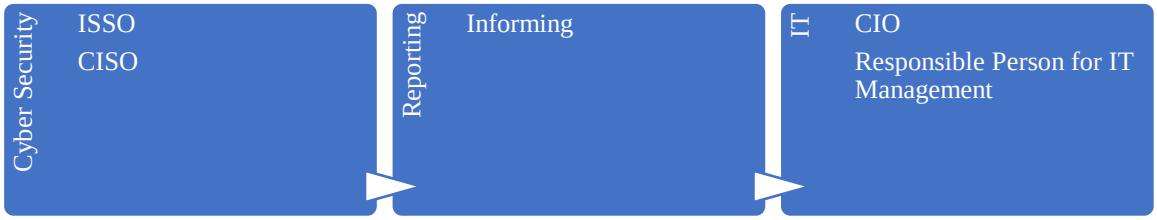


Figure 2.4. *General Reporting Paradigm in Cyber Security Governance*

As a result, this demonstration proves that cybersecurity-related cases are being considered by a multitude of enterprises as just an IT challenge rather than a central organizational issue.

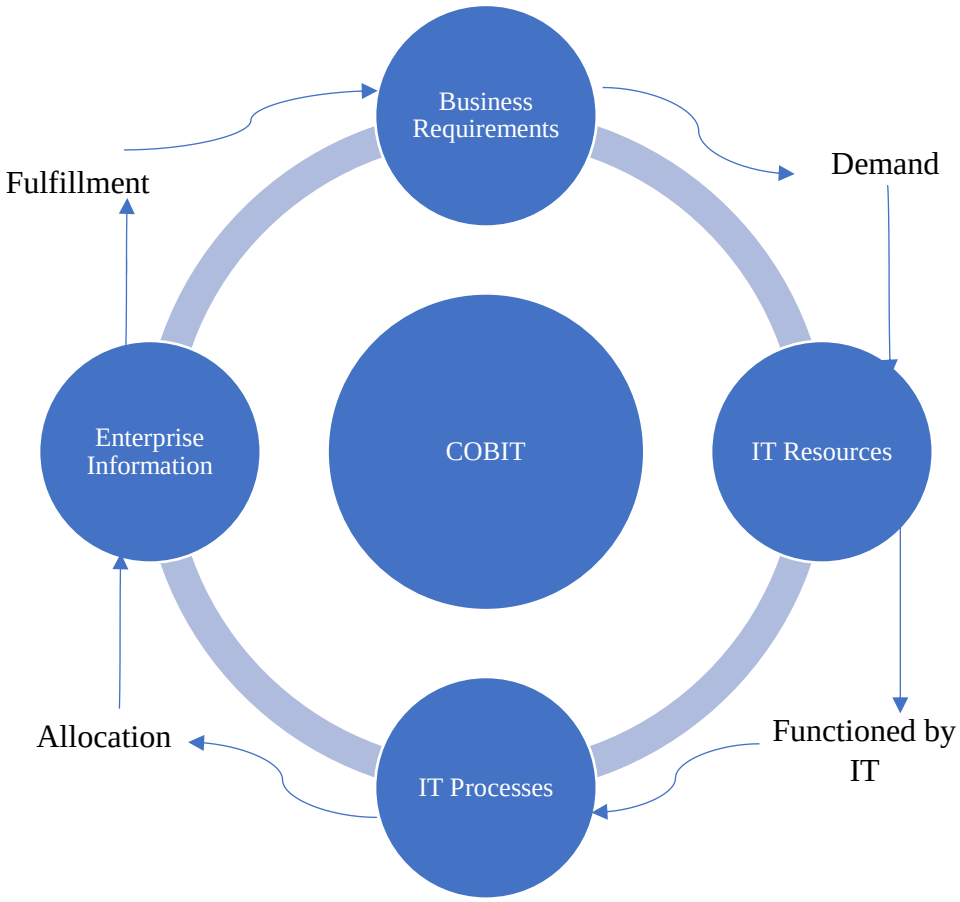


Figure 2.5. *Fundamental COBIT Principles (Moeller, IT Audit, Control, and Security, 2010)*

Accordingly, the main problem is such that there are lots of disputes about which set of principles, codes of conduct, standards, rules, and legislation must be followed and complied with to adequately ensure the CIA triad of IT processes and data protection from the viewpoint of internal audit, control, and cyber security governance as the parts of an entire system. The security of information and communication systems in cyberspace is primarily dependent on missions of control-oriented cyber security as providing full protection of data assets while performing business sustainability with the support of organizational governance. In detail, the perfect assurance of IT systems may not be feasible for all the time in every part of the enterprise. Therefore, organizational governance is needed to assist in the settlement of a basis to prescribe how the cyber security activities and objectives must be designed, developed, and organized through down-to-earth applications. In essence, governance provides systematical control for

coordinating the assurance of business continuity in enterprises. Accordingly, cyber security functions must be ensured both physically and digitally for preserving the whole system in a wider framework. In practice, there are complexities in assuring perfect protection of cyber assets because information can be retained both intangibly as dynamic forms in electronic systems and tangibly as written statements or visible physical objects (Kohnke, Shoemaker, & Sigler, 2016, pp. 6, 7).

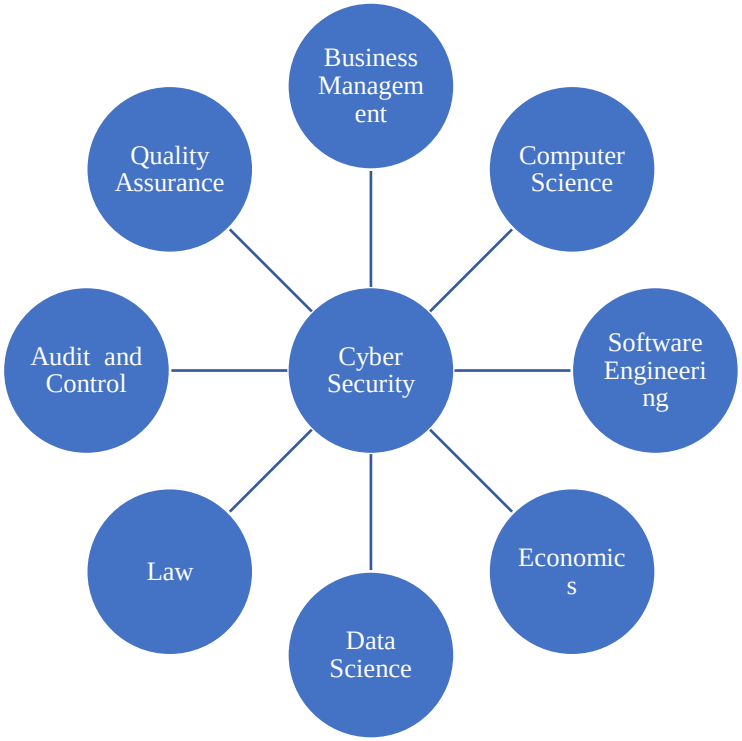


Figure 2.6. *Related Disciplines with Cyber Security (Kohnke, Shoemaker, & Sigler, 2016, p. 7)*

In general, cyber security covers multiple disciplines which assure setting, operating, analyzing, assessing, and testing of computerized systems protection adverse to cyber risks. Particularly, there are further questionable cases from the point of human conduct, ethics, law, organizational policy, economics, and risk management as to how to identify the importance and fiscal worth of cyber security functions in an enterprise and which requirements must be fulfilled for determining the expenses of safeguarding virtually stored, processed and transmitted assets in computerized and network systems. Correspondingly, the effects of threats in cyberspace are costly and unpredictable for businesses as a consequence of complications in building trustworthy, compatible, and multi-faceted protection systems for IT functions. In addition, the dynamic nature of cyberspace that has been quickly changing with the derivations of emerging technology

is making it difficult to adapt security systems to new types of risks (Kohnke, Shoemaker, & Sigler, 2016, pp. 8, 9, 10).

The report of high-risk areas which was established by the General Accounting Office (GAO) of Unites States (U.S.) in March 2019 demonstrates energy, transportation, communication, and financial industries are accepted as critical infrastructures and their operations are essentially relying on IT systems. Four serious challenges have been identified refer to build an effective cyber security system as first installing an extensive cyber security policy framework with operating it efficiently by controls, second providing optimal security to federal systems and their information assets, third safeguarding the critical infrastructures in cyberspace and fourth ensuring the protection of sensitive data's privacy. Particularly, ten strategic actions were determined for governing bodies need to take in order to conduct with mentioned four factors (United States Government Accountability Office, 2019, p. 51).

Settlement of overall cyber security strategy	• Developing a comprehensive plan for cyber security infrastructure • Mitigation of supply chain risks with a global manner • Focusing on the management of cyber security labor force • Assuring the protection of emerging technologies as artificial intelligence and Internet of Things
Making safe the federal systems and information	• Improving utilization of government scale cyber security initiatives • Observing weaknesses in federal agency information systems security programs • Stregthening the federal actions to cyber attacks and incidents
Protection of cyber critical infrastructure	• Enhancing the role of federal agencies for protecting the critical infrastructure as electricty grids and telecommunication networks
Safeguarding of sensitive data's privacy	• Improving federal efforts for protection of sensitive data's privacy • Providing the controls of the collection and ownership of data through ensuring that appropriate information is gathered with concession

Figure 2.7. *Ten Critical Responses Needed to Emphasize Four Major Cyber Security Challenges (United States Government Accountability Office, 2019, p. 53)*

In essence, the report of GAO enlightened that the security of computerized systems and networks can not be driven completely by just technical and engineering manners, because seventy-one percent of cyber attacks are dependent on human behavior. Therefore, the protection of information and communication systems is required realistic approaches that must be supported by an all-inclusive framework that takes into account governance-based control and audit processes for attainable practices. Accordingly, the framework mentioned should be strategically effective not only in orientation but also for application to reinforce all kinds of cyber-attacks which can be emerged both electronically and behaviourally (Kohnke, Shoemaker, & Sigler, 2016, p. 10).

From the viewpoint of Turkey, the services, which can not be provided on account of any reason, cause loss of life, large-scale damages to the economy, deterioration of public activities, and vulnerabilities in domestic security systems, are accepted as critical according to National Cyber Security Strategy. Similarly, the CIA triad of public services is provided by IT products that are recognized as critical assets. As well, critical infrastructures are defined in such industries as electronics and communication, energy and water systems, banking and finance, strategic public services, and transportation relative to the executive order of the Cyber Security Committee which was confirmed on 20 June 2013 (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016, p. 8).

2.1. International Policy Frameworks for Cyber Security

Policies are fundamental and critical tools that demonstrate the stance of governments on societies' perception to provide optimal security in the critical infrastructures of nations through frameworks and guidance for the foundation of both public and private enterprises. Accordingly, the major purpose of policies for every nation around the globe is to arrange the legislative environment for eliminating confusing cases, turmoils, and violent behaviors. Correspondingly, policies that have been being carried out for conventional information security goals were designed to safeguard the CIA triad of data may not be sufficient anymore if organizations are not being managed just by self-contained strategies. Therefore, classic information protection approaches should not be confused by cyber security frameworks because of the chaotic nature of cyber-space as each of the nations, industries or enterprises can be the target of cyber attacks. As a result,

cyber security structures comprehensively refer to protecting the information and communication technology systems through processes that are based on functions of prevention, detection, and reaction for resisting malicious acts. In essence, the policies and programs which are stood on cyber security frameworks cover risk management and intelligence systems for responding to incidents and attack vectors according to resiliency metrics with information transmitting. Because of the mentioned reasons installing a cyber security policy structure for an organization is required a clear definition of how the protection of information systems and data assets is being performed to support guidelines relative to reaching business objectives in compliance with the legal aspect. Correspondingly, information is processed data that has sense and value for organizations' business continuity. Therefore, information assets show the meaningful resources of an enterprise which have strategic importance and can be evaluated with fiscal terms to consider in risk management practices. For example, financial reports, brand image, firm reputation, employee documents, customer records, and intellectual ownership are such kinds of information assets that must be protected by rules and legislation (Santos, 2018, pp. 6, 7, 8, 9, 10).

In parallel with mentioned statements in the previous paragraph, information security is defined as the protection of the CIA trinity due to the ISO/IEC 27000. In short, confidentiality is linked with privacy which provides the control of the information systems by ensuring access to authorized personnel with maintaining the secrecy of knowledge. Furthermore, integrity is related to the precision and entirety of information as well as availability refers to the accessibility and usability of data. These three characteristics include the conventional aspect of information security. Aside from these attributes, the items such as authenticity, completeness, and non-repudiation can be applied to enhance security mechanisms (Gallotti, Cottafavi, & Ramacciotti, 2019, pp. 9, 10, 11, 12).

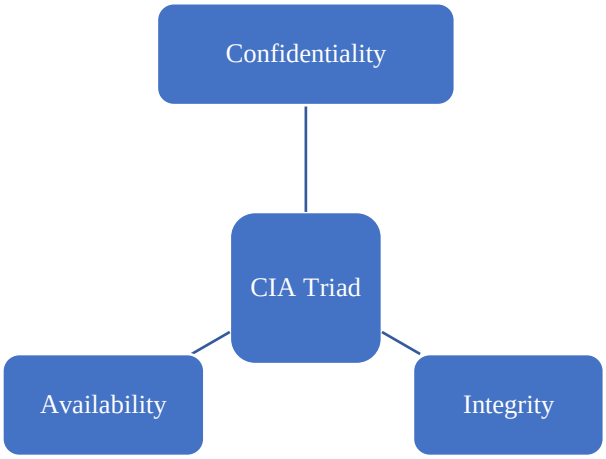


Figure 2.8. *CIA Triad (Santos, 2018, p. 380)*

Adaptation of widespread cyber security frameworks is necessary within the context of building standards for policy deployment to practice the audit and control functions in IT processes. Likewise, associations that formulate standards for organizations to take them as reference for settlement of the audit and governance-based control framework of IT operations, have guidelines for enterprises as a common body of knowledge like the Information Security Management System (ISMS) of International Organization for Standardization (ISO), Federal Information Processing Standards (FIPS) of National Institute for Standards and Technology (NIST) and Control Objectives for IT (COBIT) Model of Information System Audit and Control Association (ISACA) (IT Governance Institute, 2007, p. 7).

As well, fundamentally, multiple structures have been designed for reinforcing audit functions which are synthesized with the controls of IT security. The design phase of a cyber security program can be supported by the guidelines are proposed and established for the essentials of internal controls with the resources are provided through COSO, ITIL, COBIT, and ISO 17799/BS7799 as mentioned before (Hernandez, 2007, p. 17).

First, COSO had been established in 1985 to assist the National Commission in providing recommendations to auditors in case of reviewing and preventing fraudulent acts in financial reporting operations. As mentioned previously, the internal control model of COSO covers five core fields as control environment, risk assessment, control activities, information and communication, and monitoring, which can be endorsed as a

framework for organizations to comply with Sarbanes-Oxley Section 404 (Hernandez, 2007, p. 17).

ITIL had been developed between 1889 and 1992 as 44 books were printed by the Stationery Office of the British Government to recover management of services in information technology. The viewpoint of these publications is to integrate the applications for leading operational activities like transformation, event control, allocation of resources, and monetary management to assist the administration of services in an information technology framework. Especially, the primary purpose of ITIL's resources is to identify how internal controls can be put into action for the services of IT departments in the enterprises. In practice, the results of implementations according to the achievement levels of the standards have a direct linkage to the support of management who has full responsibility to provide ongoing processes via planning and phased approaches (Tipton & Krause, 2007, p. 17).

The COBIT framework was settled by IT Governance Institute for examining an organization's adequacy level refers to control objectives by considering the norms of effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability to accomplish business goals. Correspondingly, the COBIT model outlines four domains to provide proper governance in IT security which will be discussed deeply in the next phase. Briefly, COBIT affords a complete system for IT controls appropriate to the business requirements of enterprises (Hernandez, 2007, p. 18).

The framework of BS 7799/ISO 17799 can be implemented as a substructure intending to develop security management policies and their practices for effective cyber security processes within the organizations. The development period of ISO 17799 will be shown in the next stages of the study. Concisely, the modified ISO 17799 framework was consisted of the following matters as information security policy, organizing information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development, and maintenance, information security incident management, business continuity management and compliance for establishing a guidebook according to implement information security management systems for auditing. Also, the ISO/IEC series for code of practices to provide security objectives were amended respectively in the years 2005 and 2007. In 2007, the framework was renumerated as ISO/IEC 27002. Later on, this framework was improved with security

controls for cloud computing and services as the standards of ISO/IEC 27017 (Hernandez, 2007, p. 19).

2.1.1. Control objectives for information and related technology (COBIT) framework

COBIT is the publication of the Information Technology Governance Institute which covers control objectives with 34 items at the high level. The main purpose of this framework is to check on seven metrics such as confidentiality, integrity, availability, efficiency, effectiveness, reliability, and compliance for accomplishing the business objectives by continuously detecting the related guidelines. Controlling the components of the information technology environment which are consisted of human beings, tools, equipment, data, and formations provides competitive advantages for enterprises. Therefore, the objectives of COBIT offer major cognitive policies and applications for eliminating the confusion and fuzziness in the understanding of the information technology culture of enterprises (Tipton & Krause, 2007, p. 17).

At first, the framework of CobiT cube displays all the parts of enterprises not only as tangible assets to control facilities, plants, equipment, machinery, application software and systems, information technology, and data assets but also as intangible assets for structuring cyber security culture. In detail, the management and control of information technology sources are clustered as applications, information, infrastructure, and employees according to the COBIT cube. Therefore, the evaluations of controls in information technology systems cover both manual and automated user systems with procedures for processing info assets which include variables as inputs, outputs, and transformed data as process and system cycles to provide business continuity. Also, the control activity assessments of infrastructural items in information technology systems consist of tools, hardware, system software, operating systems, data servers, network structures, and workspaces for hosting them. In addition, consideration of information technology services contains a qualified labor force that has key functions in planning, monitoring, and supporting controls. In essence, the CobiT cube states the deep relationships between three dimensions as internal control, information technology governance, and sources (Moeller, IT Audit, Control, and Security, 2010, p. 31).

On the other hand, domains, processes, and activities are discussed as major information technology processes which are layered by the CobiT cube too. Information

technology activities that match up with organizational roles are defined through four particular domain fields as planning and enterprise, acquisition and implementation, delivery and support, monitoring, and evaluation to activate governance frameworks. First, enterprise business objectives are assisted and strengthened by planning functions that cover the methods and tactics to allow feasible applications for IT operations. The strategic vision of IT must be transmitted all around the organization with missions of IT for which business objectives are being tried to be achieved. IT services require reengineering and maintenance activities of current systems to identify problems for developing and acquiring solutions with implementation and integration of them into the business processes. The delivery of necessary services which include both system applications and infrastructural tools is covered by the domain area for providing the utility of data and controls. The evaluations of external and internal audit systems which involve adequate controls and monitoring processes are performed in domains as well (Moeller, IT Audit, Control, and Security, 2010, p. 32).

Table 2.2. *A Sample for the Consolidation of ISO 31000:2009 and COBIT 5 GEIT Principles (Antonucci, 2017, p. 24)*

<table>
<tr><td rowspan="2"></td><td colspan="5">The Principles of COBIT 5 GEIT</td></tr>
<tr><td>Meeting Stakeholder Needs</td><td>Covering Enterprise end-to-end</td><td>Applying a Single Integrated Framework</td><td>Enabling a Holistic Approach</td><td>Separating Governance from Management</td></tr>
<tr><td rowspan="4">ISO 31000 Risk Management Standards</td><td>Risk management is recognizable and comprehensive.</td><td>Risk management adds and continuously improves the value.</td><td rowspan="4">Risk management is structured for timely responses to cyber threats and vulnerabilities.</td><td>Risk management is an entire part of all business activities.</td><td rowspan="4">Continuous improvement of the organization is supported by risk management.</td></tr>
<tr><td rowspan="3">Risk Management is effective, recursive, and responsive to changing conditions.</td><td>Risk management is systematized.</td><td>Human and cultural factors are taken into account by risk management processes.</td></tr>
<tr><td rowspan="2">Uncertain events are observed and analyzed through risk management processes.</td><td>Risk management is accepted as an essential part of decision-making.</td></tr>
<tr><td>Risk management is established on all available information.</td></tr>
</table>

Similarly, international principles have a role in guiding the plans and strategies of cyber security infrastructure which support the assessments of decision-making processes of risk controls to assist the practices of expected behaviors and code of ethics in all around the enterprises. For example, the standards of ISO 31000:2009 can reinforce an organization’s cyber security governance as a risk management framework which can be

integrated into the five principles of COBIT 5 Governance of Enterprise Information Technology (GEIT). Explanatorily, the expectations of stakeholders due to the management of cyber risks and the practices of regulations and obligations for building risk culture can be aligned through the combination of ISO 31000:2009 international risk management framework and COBIT 5 GEIT principles which are taken place by the organization in terms of securing the critical and sensitive data that is logged on, put into storage, processed and transmitted in business activities (Antonucci, 2017, p. 25).

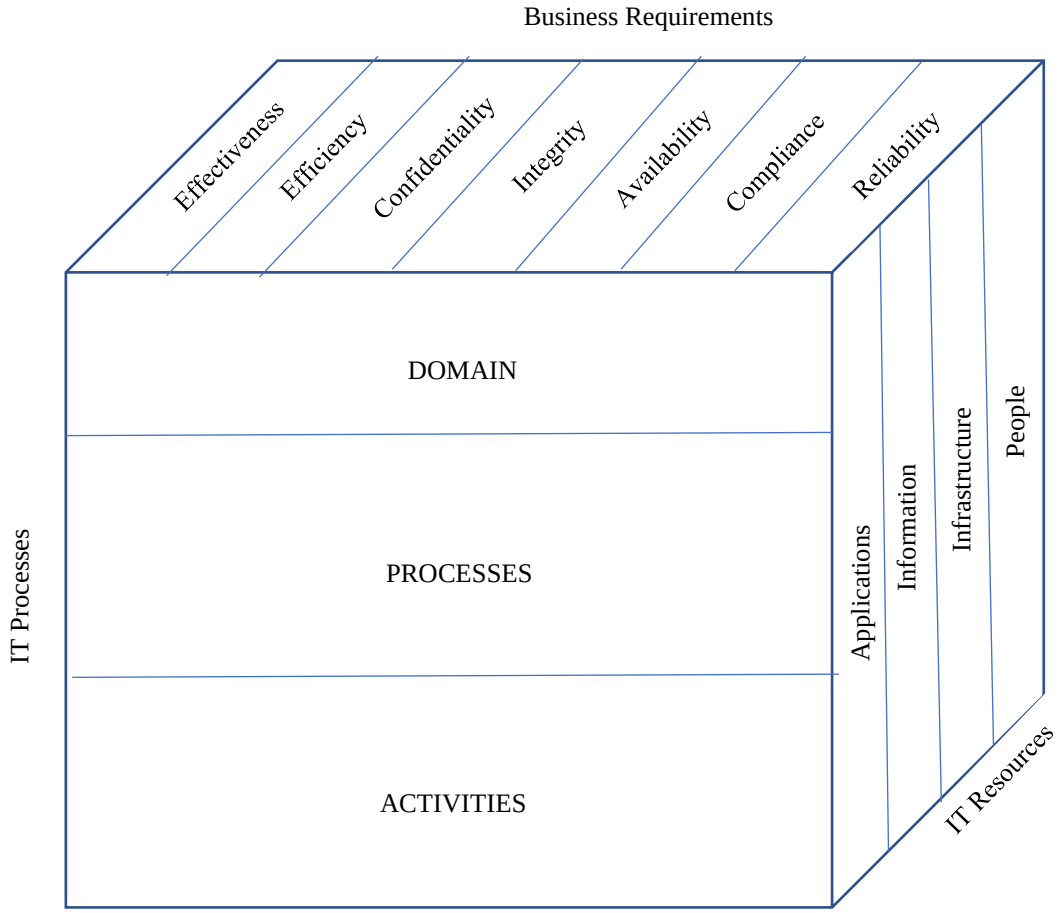


Figure 2.9. *CobiT Cube (Moeller, IT Audit, Control, and Security, 2010, p. 30)*

In essence, CobiT includes standards for safeguarding and controlling information technology and systems which are envisioned for the auditors, controllers, and management parts to assist the business activities in enterprises. The overall framework of organizational principles, policies, and norms is designed for ensuring that the business objectives will be met and risky events will be controlled proactively. In addition to a general overview, control objectives involve detailed procedures for predefined task units and roles of employees in information technology management. To attain control

objectives, the configuration of interrelations and cross functions of business processes should be optimized with value-added adjustments by information technology governance schemas elaborately. Essentially, the governance formations and practices in enterprise risk management must be harmonized with information technology activities for efficient use of resources and obtainment of interoperability in the compound information technology processes. An independent auditor is assigned by an audit board to look after their plans and consequences of reviews for standardization of regular risk assessment activities in controlling risks and preventing flaws. Naturally, information technology governance processes should be driven with precise objectives through the requirements of enterprises according to their industries, customer portfolios, and organizational culture (Pickett, 2011, p. 111).

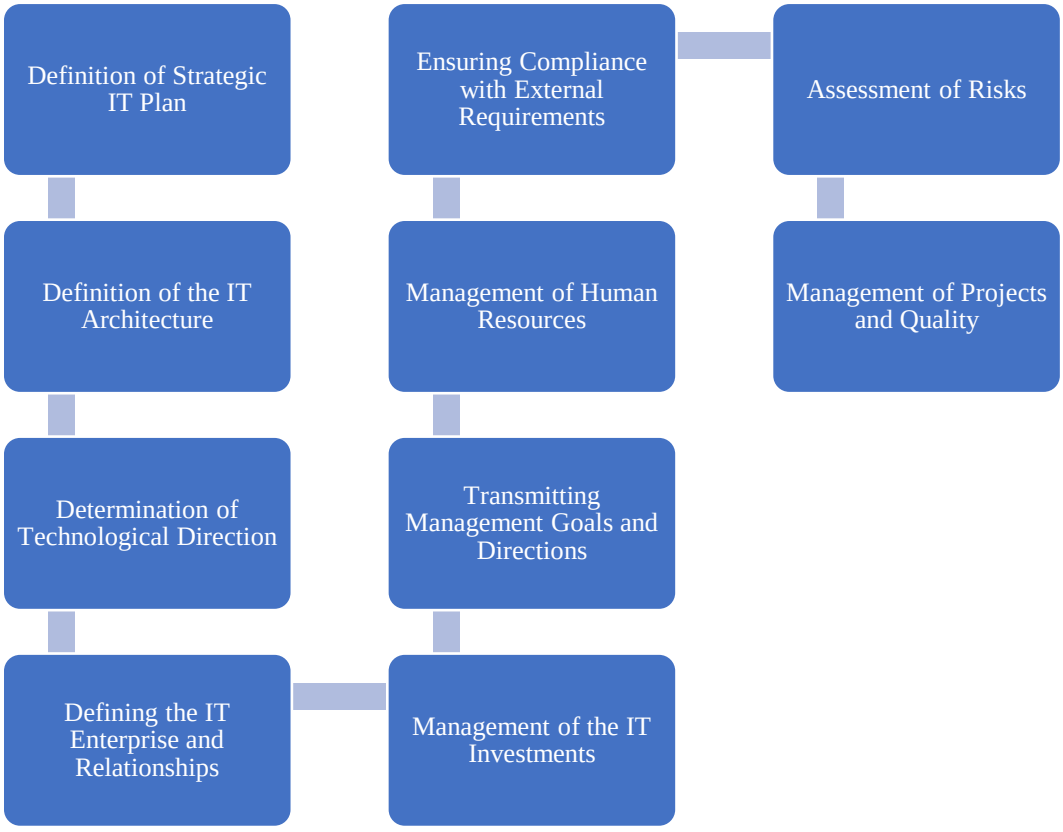


Figure 2.10. *Systems Development Life Cycle (SDLC) for COBIT Implementation and Quality Assurance in IT (Moeller, IT Audit, Control, and Security, 2010, p. 32)*

SDLC stages illustrate the complete mechanism for where utilizations will be designed, established, performed, and replaced within a period for sustaining business development processes. Likewise, business requirements are accepted as one of the

dimensions in the CobiT model which covers process criteria components as effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability. In practice, entire IT systems, processes, and resources must be considered refer to these seven metrics. Correspondingly, the CobiT cube introduces a capable route for understanding the cross interactions between IT resources, processes, and business requirements as well as the COSO cube for internal controls and enterprise risk framework. To sustain and improve business processes and flows that are significantly dependent on IT processes and resources, enterprises need to have IT auditors for inspection and perception of internal controls (Moeller, IT Audit, Control, and Security, 2010, p. 158).

2.1.2. International organization for standardization (ISO)

The interdisciplinary nature of information technology doesn't just contain operable functions of security frameworks, as well it covers the efficient leadership approaches and perception of essentiality for the safeguarding of assets in cyberspace. As a result, enterprises need to have a fundamental structure defined as standards for their security applications in information technology. According to this objective, the United Kingdom Department of Trade and Industry (U.K.DTI) established a code of conduct for the security management in information technology by taking the assistance of organizations in 1993 and later on 1995 modified as British Standard 7799 (BS 7799). These standards were reexamined in 1999 for inserting the approval and authorization items as the second phase of BS 7799. Also, BS 7799's first phase was converted to International Organization for Standardization 17799 (ISO 17799) and presented like ISO 17799:2000 as the pioneer of the standards in security management of information systems internationally on the part of both the International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO) (Tipton & Krause, 2007, p. 17). ISO was established for framing standards that assist the progress of international trade activities in 1947. Similarly, International Electrotechnical Commission (IEC) had been organized with the goal of conducting standards for all kinds of electronic technologies in Geneva, Switzerland as same as ISO, but before ISO in 1906. ISO/IEC 27002 standard explains the proposed code of practices to design information security management systems in terms of 12 security objectives, 39 security practices, and 135 security controls for structuring the assets' protection frame of enterprises. In practice, the system cycle of

security framework to tone up the safeguarding objectives can be outlined by adjusting the input variables of security controls which are the items of ISO/IEC 27002 standard. The input values are received from functional operating fields of the business environment which are measured by taking into account the parameters that have effects on security controls due to the analyses of auditors and controllers. Correspondingly, the cyber security policies of an organization demonstrate what requirements are determined to support the security posture. Also, policies refer to information security management which are configurated to define the acceptable level of behavioral guidelines to describe how an enterprise is planning to educate its employees, and security assessments are being applied for the safeguarding of its critical assets (Raggad, 2010, pp. 492, 500, 504).

ISO 27000 ISMS standards aid the organizations to control the security of information-related assets as financial data, intellectual property rights(IRP), and third-party knowledge which are consigned by their clients through systematic approaches for framing the protection mechanisms and making objective and independent assessments (ISO, 2018). The compliance of organizations with the ISO 27000 is critically significant from the point of providing the CIA triad of customer data. So, the ISO 27000 Family of Standards which was developed by the International Organization of Standardization and was approved by the International Electrotechnical Commission (IEC), has come to be the up to the date step to ensure efficient information security management (ISO, 2018).

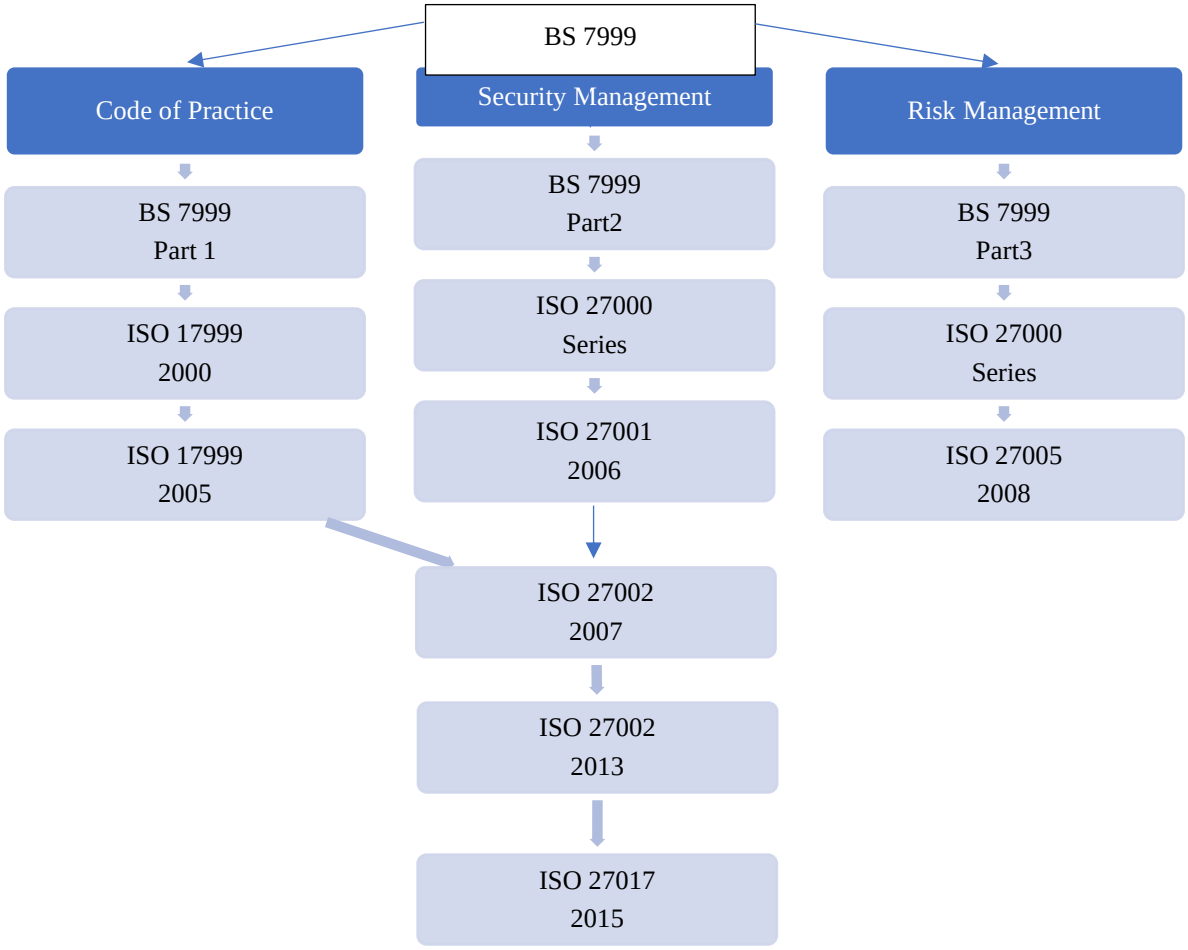


Figure 2.11. *The Development of BS 7799 (Raggad, 2010, p. 493)*

The security posture of an organization is being operated through such a systematical transformation by using the outputs of security controls as inputs for the security practices and outputs of security practices are performed as inputs for the security objectives. An applicable information security strategy frame should be derived from the participation and support of management. Therefore, ISO/IEC 27002 proposes that management parts of organizations must form and cultivate their information security policy structure to activate their strategies. Also, as a result of effective documentation of security policy mechanisms, the applications of information security strategies will be efficiently applied in the information security management systems. ISO/IEC 27002 defines two security controls which are classified as information security documents and review of the security policy in terms of satisfying the information security policy requirements. The security stance of an organization can be evaluated by system managers and internal auditors by observing the information security policy structure. If an organization's current cyber security policies comply with ISO/IEC 27002, the

security posture is accepted. Although, if there are inadequacies in an organization for satisfying the specifications of the processes which are defined as information security and asset management, human resources management, physical and environmental security, communications and operations management, access control, system acquisition, development and maintenance, information security incident management, business continuity management and compliance, the current security stance of the organization is not conformed relative to ISO/IEC 27002. Therefore, in such kinds cases, the security controls are needed to reassess by upper management for providing further improvements in security posture with both proactive and corrective actions (Raggad, 2010, pp. 500, 501, 523).

Table 2.3. *ISO 27002 Rulebase System Cycle of Cyber Security Frame Function for Business Continuity and Compliance (Raggad, 2010, pp. 521, 522)*

<table>
<tr><td colspan="3">Rule Base: IF:a.11.1.1-a.11.1.5 THEN:b.11.1; IF: b.11.1 Then:c11;</td></tr>
<tr><td>a Concepts: Security Controls</td><td>b Concepts: Security Practices</td><td>c Concept: Security Objective</td></tr>
<tr><td>a.11.1 Including Information Security in the Business Continuity Management Process</td><td rowspan="5">b.11.1 Information Security Aspects of Business Continuity Management</td><td rowspan="5">c11. Business Continuity Management</td></tr>
<tr><td>a.11.1.2 Business Continuity and Risk Assessment</td></tr>
<tr><td>a.11.1.3 Developing and Implementing Continuity Plans Including Information Security</td></tr>
<tr><td>a.11.1.4 Business Continuity Planning Framework</td></tr>
<tr><td>a.11.1.5 Testing, Maintaining and Reassessing Business Continuity Plans</td></tr>
<tr><td colspan="3">Rule Base: IF: a.12.1.1-a.12.1.6 THEN: b.12.1; IF: a.12.2.1-a.12.2.2 THEN: b.12.2; IF: a.12.3.1 THEN: b.12.3; IF: b.12.1-b.12.3 THEN: c12;</td></tr>
<tr><td>a Concepts: Security Controls</td><td>b Concepts: Security Practices</td><td>c Concepts: Security Objectives</td></tr>
<tr><td>a.12.1.1 Identification of Applicable Legislation</td><td rowspan="6">b.12.1 Compliance with Legal Requirements</td><td rowspan="6">Compliance</td></tr>
<tr><td>a.12.1.2 Intellectual Property Rights (IPR)</td></tr>
<tr><td>a.12.1.3 Protection of Organizational Records</td></tr>
<tr><td>a.12.1.4 Data Protection and Privacy of Personal Information</td></tr>
<tr><td>a.12.1.5 Prevention of Misuse of Information Processing Facilities</td></tr>
<tr><td>a.12.1.6 Regulation of Cryptographic Controls</td></tr>
</table>

a.12.2.1 Compliance with Security Policies and Standards	b.12.2. Compliance with Security Policies and Standards, and Technical Compliance	
a.12.2.2 Technical Compliance Checking		
a.12.3.1 Information Systems Audit Controls	b.12.3 Information Systems Audit Considerations	

Furthermore, the system performance of the cyber security structure of organizations can be measured and assessed through a hierarchy that is shown as if and then rule-based method to control how the organizations' cyber security activities are being operated and managed in compliance with guidelines in ISO/IEC 27002. As an example, in the figure, business continuity and compliance are shown as security objectives to define specifications for which requirements an organization must satisfy to follow the instructions of ISO/IEC 27002 (Raggad, 2010, p. 523).

2.1.3. National institute of standards and technology (NIST) configuration

The cyber security structure of NIST proposes a set of standards for organizations to design their governance mechanisms for controlling the policies which are being worked in processes of risk management operations to overcome the threats and incidents. The main objective of the NIST framework which was established refers to cyber security, is to support the protection systems in critical infrastructures of the United States. However, these guidelines are being followed and taken up as references by enterprises that have strategic cyber security plans to integrate basic aspects of audit, control, and governance methods into risk management applications. In practice, the policies, principles, and standards which are developed to assist the organizations' controlling activities can be framed with governance systems. Within the context of improving a framework for critical infrastructure, the categories and their subclasses are defined through matching with their functions and descriptive references as industrial standards (National Institute of Standards and Technology (NIST), 2018, p. 5).

Also, the framework is not just limited to the U.S. and can be adapted by corporations, enterprises, and different countries. In May 2017, federal agencies were directed by executive order 13800 of the U.S. government for adopting the NIST cyber security framework into their risk management systems by providing the assessment reports to the Secretary of Homeland Security and Director of the Office of Management and Budget (OMB). In essence, this framework presents a common terminology to perceive and evaluate cyber risks for management and shareholders. Additionally, the

NIST structure can assist the enterprises in favor of mitigating cyber risks as a tool that can be used for designing cyber security policy frameworks and developing organizational culture. The framework can be utilized to improve the validity of risk management processes of cyber security mechanisms as well. Likewise, NIST cyber security framework (CSF) is being updated through continuous improvement approaches concerning the emerging cyber threats and attack types. As expected, the specific requirements of organizations vary relative to their sector, size, and business objectives in the direction of providing cyber security entirely and effectively. Organizations can implement the NIST CSF for managing cyber risks with a cost-effective approach through maximizing return on investment refers to ensure the CIA triad of critical assets. Internal and external communication and data transferring systems of organizations can be optimized by the implementation of NIST CSF into their cyber security structures through the usage of it as a common language. Correspondingly, compliance requirements of organizations are related to the regulatory environment can be achieved by carrying out NIST CSF in terms of ensuring the adequateness of cyber security policy frameworks. In practice, this framework has a comparatively uncomplicated formation that covers three key items are defined as core, profiles, and implementation tiers. The core of the framework provides a systematic plan for how the organizations can manage cyber risks through outlining the main outcomes of putting NIST CSF into action with four major parts are described as functions, categories, subcategories, and informative references (Calder, 2018).

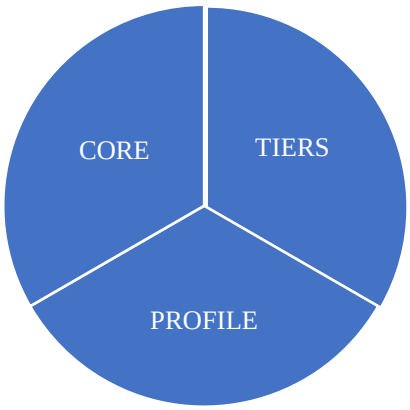


Figure 2.12. *NIST CSF Components (NIST, 2020)*

The framework core covers five functions which are represented as identify, protect, detect, respond and recover. These functions can be applied to not only internal controls in cyber security but also risk management processes all around an organization. Also, the functions which are described in the table enable communication between departments and employees to provide them with how to interpret cyber risks across the organization. In addition, each function is segmented into categories and every single category is divided into subcategories In practice, the framework core is developed to be intuitive and can be considered as a translation phase which transforms the taxonomy of cyber security terms into a basic language that could be perceived by all of the employees in an organization (NIST, 2020).

Table 2.4. *Framework Core (National Institute of Standards and Technology (NIST), 2018, p. 23)*

	Function	**Category**	**Category Unique Identifier**	**Function Unique Identifier**
Which processes and assets need protection?	Identify	Asset Management	ID.AM	ID
		Business Environment	ID.BE	
		Governance	ID.GV	
		Risk Assessment	ID.RA	
		Risk Management Strategy	ID.RM	
		Supply Chain Risk Management	ID.SC	
Which safeguards are available?	Protect	Identity Management & Access Control	PR.AC	PR
		Awareness and Training	PR.AT	
		Data Security	PR.DS	
		Information Protection Processes & Procedures	PR.IP	
		Maintenance	PR.MA	
		Protective Technology	PR.PT	
Which techniques can identify incidents?	Detect	Anomalies and Events	DE.AE	DE
		Security Continuous Monitoring	DE.CM	
		Detection Processes	DE.DP	
Which techniques can contain impacts of incidents?	Respond	Response Planning	RS.RP	RS
		Communication	RS.CO	
		Analysis	RS.AN	
		Mitigation	RS.MI	
		Improvements	RS.IM	
Which techniques can restore capabilities?	Recover	Recovery Planning	RC.RP	RC
		Improvements	RC.IM	

		Communications	RC.CO	

In addition, the functions have a backbone role as supporting the framework core for organizing the parts of cyber security in a systematic way. Cyber risk management decisions can be assisted by enabling the core functions to provide a comprehensive security program. Particularly, in connection with the thesis subject, the identification function of the core framework can be used for describing the cyber security policies inside the organizations to characterize applicable governance programs in compliance with the legislative environment relative to their risk management qualifications. Correspondingly, the protection function of the core framework can be implemented to ensure the validity and robustness of cyber security systems consistently with organizational culture. Also, the detection role of the structure can be associated with the establishment of organizational culture to develop awareness for risky events and behaviors which are related to cyber security concerns through continually monitoring systems to verify the effectiveness of safety of both cyber and physical assets. Similarly, regarding the thesis motive, the response function covers the coordination of communication between management, law enforcement agencies, internal and external stakeholders. Finally, the recovery activity provides the fulfillment of planning processes with ensuring the internal and external communications are being complemented which have a supplementary function on regaining the optimal performance of IT systems that are affected by cyber security risks and incidents (NIST, 2018).

The implementation tiers can be utilized to demonstrate the attributes of the organizations' cyber risk management applications. So, the level of cyber security examinations is provided by implementation tiers through the risk management processes are set in place for controlling their impacts and targets. The tiers range from partial which is also known as Tier 1 to adaptive which is also described as Tier 4 can be utilized for describing the degree of accuracy of how well decision-taking techniques are being performed in cyber security risk management. Likewise, each of the tiers can be implemented as a reference while organizations are determining their risk appetite and tolerance levels to moderate the effects of cyber risks to acceptable ranges. Feasibly, the cover of this framework layer is performed via three stages as a risk management process, an integrated risk management program, and external participation. The capability and

replicability parameters can be evaluated in risk management processes for penetrating cyber security structure and an integrated risk management program can be used to expand the decision making approaches in terms of supporting strategy development plans of cyber security practices (National Institute of Standards and Technology (NIST), 2018, pp. 8, 9, 10, 11).

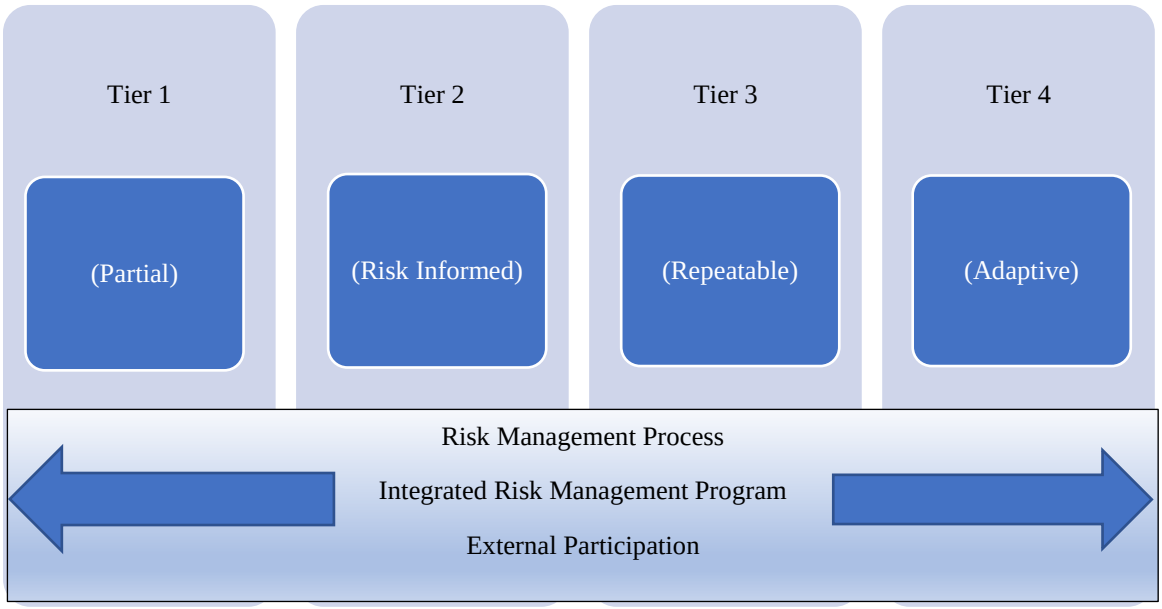


Figure 2.13. *NIST CSF Implementation Tiers (NIST, 2020)*

The framework profile is the configuration of the functions, categories, and subcategories with the risk perception, business necessities, and sources of the organizations. In essence, the profile facilitates organizations in terms of enacting a guideline to reflect risk priorities that are adequately adjusted with regulatory requirements, industry specifics, and business objectives for preventing and minimizing the effects of cyber risks. Also, the profile can be applied for defining the current state of the cyber security structure of the organizations to show them a roadmap that allows flexibility in usage for the desired safeguarding posture that they seek to reach. In consequence, a comparison of actual and targeted statuses can be explored by using a framework profile. Additionally, action plans can be developed to mitigate and close the gap between two conditions by enabling a profile that provides risk-based approaches for measuring the sources needed and supporting to reduce of overhead costs (National Institute of Standards and Technology (NIST), 2018, p. 11). The align, plan and organize (APO) process is required for any bunch of security controls and is referred to by every type of information security framework and standard (Greene, 2015, p. 1).

Table 2.5. *Representative Template of How to Implement NIST CSF into Organizations as a Matrix*

Function	Category	Subcategory	Informative References	Priority	Gaps	Budget	Proactive Action	Corrective Action
Identify	Risk Assessment	ID.RA-1(Vulnerabilities of assets are diagnosed and documented)	CIS CSC 4, COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02, ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12, ISO/IEC 27001:2013 A.12.6.1, A.18.2.3, NIST SP800-53 Rev.4 CA-2, CA-7, CA-8, RA-3, SA-5, SA-11, SI-2, SI-4, SI5	Very High	Negligible	X	Unrequired	Unrequired
Identify	Governance	ID.GV-3(Legislative requirements relative to cyber security involving privacy and civil autonomy commitments, are understood and managed)	CIS C.SC 19, COBIT 5 BAI02.01, MEA03.01, MEA03.04, ISA 62443-2-1:2009 4.4.3.7, ISO/IEC 27001:2013 A.18.1.1 A.18.1.2, A.18.1.3, A.18.1.4 A.18.1.5, NIST SP 800-53 Rev.4-1	Moderate	Urgent	Y	Regulatory environment conditions can be reviewed regularly and awareness trainings can be organized	Current organizational policies can be updated
Protect	Data Security	PR.DS-5(Protections counter to data leaks are carried out)	CIS CSC 1, COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02, ISA 62443-3-3:2013 SR 5.2, ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4	Severe	Tolerable	Z	Data leakages can be prevented and eliminated by the usage of emerging technologies such as artificial intelligence	The losses of organizations can be evaluated and forecasting models can be proposed to gauge the damages
Detect	Security Continuous Monitoring	DE.CM-4(Malicious codes are detected)	CIS CSC 4, 7, 8, 12, COBIT 5 DSS05.01, ISA 62443-2-1:2009 4.3.4.3.8, ISA 62443-3-3:2013 SR 3.2, ISO/IEC 27001:2013 A.12.2.1, NIST SP 800-53 Rev.4 SI-3, SI-8	High	Small	T	The detection criteria can be expanded due to the emerging types of threats depending on case-control studies	System performance resiliency can be measured and improved with the aid of using the systems which are affected by malicious codes to find main reasons
Respond	Communication	RS.CO-3(Information is participated consistently along response plans)	CIS CSC 19, COBIT 5 DSS03.04, ISA 62443-2-1:2009 4.3.4.5.2, ISO/IEC 27001:2013 A.16.1.2, Clause 7.4, Clause 16.1.2, NIST SP 800-53 Rev.4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4	Low	Steep	P	Inbound and outbound communications can be controlled by the applications of automation such as SCADA	Unrequired

Recover	Improvements	RS.IM-2(Response strategies are refreshed)	COBIT 5 BAI01.13, DSS04.08, ISO/IEC 27001:2013 A.16.1.6, Clause 10, NIST SP 800-53 Rev, 4 CP-2, IR-4, IR-8	Neglectable	Very Small	M	Unrequired	Unrequired

Briefly, NIST CSF can be used for establishing a systematic methodology and common language to complement the risk management programs in cyber security practices of enterprises along three pillars were mentioned in this stage as core, implementation tiers, and profile which provide a comprehensible and wide range applicable roadmaps.

2.2. National Cyber Security Policy Framework of Turkey

At first, Turkey is the second nation of the North Atlantic Treaty Organization (NATO) according to the number of military personnel data in 2019 which was stated as 435,000 after the U.S. which had 1.34 million troops. Briefly, NATO was established in 1949 in terms of figuring out the conflicts in peaceful ways as the member countries will consist of each other's defense in the event of an attack (North Atlantic Treaty Organization (NATO), 2020). Also, the Cooperative Cyber Defence Centre of Excellence (CCDCOE) was formed as an expansion of NATO through 22 sponsoring nations which include Turkey and 3 contributing participants on 14 May 2008 for drawing attention to the investigation, research, coaching, education, and exercises to enhance regular defending of critical infrastructures, IT and military systems of the promoting countries by the simulations of cyber threats, attacks, and incidents. Therefore, the information which was expressed above, represents that Turkey can be considered as one of the major nations of NATO with both having second military size due to the staff number and being a sponsoring country of CCDCOE. Furthermore, these metrics can be evaluated as extra pieces of evidence for how and to which degree Turkey is assessing its position in the globe due to the protection of tangible and intangible resources (Cooperative Cyber Defence Centre of Excellence (CCDCOE)). The usage of information and communication technologies (ICTs) has been expanding to multiple aspects of life in Turkey which is respected as an emerging country status through the applications of electronic and digital platforms in both public and private sectors. Particularly, critical infrastructures such as energy and water supply, health care, transportation, communication, and financial services have been supported and controlled by ICTs in

order to increase the efficiency and productivity of public and private companies for providing contributions to the living standards of customers and residents. Hereby, the protection of ICTs has been becoming one of the major subjects for the nation to prevent and reduce the impacts of cyber attacks by ensuring the baseline security of sectors that have critical roles in the country's development. However, the unsymmetrical nature of cyber surface makes it difficult to define which forces are subsidizing and organizing the cyberattacks for what reasons (Republic of Turkey Ministry of Transport Maritime Affairs and Communications, 2016, pp. 3, 4).

The decision, which was made by the Board of Ministers in favor of executing, steering, and coordinating the National Cyber Security activities, was published and validated in 28447 numbered official journal on the date of 20 October 2012. According to this judgment, National Cyber Security Council was established under the authority of the Transportation Navy and Communication Ministry to develop plans, policies, and strategies for entire public enterprises and agencies to ensure the optimal countrywide cyber security structure. Also, this decision context was legalized through the Additional Regulation 1 which was attached to both 5809 numbered Electronic Communication Law that was dated 5 November 2008 and 6518 numbered law which was published on 6 February 2017. As a result, new missions which refer to cyber security were added to the responsibilities of Information Technologies and Communication Organization by the 5809 numbered Electronic Communication Law which was expanded with additional clauses. Likewise, the tasks of the Cyber Security Council were put in an order with 5809 counted law. Therefore, Cyber Security Board was developed to provide the coordination, application, and conformation of standards, principles, procedures, reports, programs, plans, and precautions which are defined and designed by state agencies and utilities concerning cyber security as stated in Additional Regulation 1 of 5809 numbered law. The functions of the Cyber Security Board were stated as;

- To approve relative to the policies, strategies, and action plans which are related to cyber security by taking decisions for effective practices of those nationwide
- To determine the proposals which are regarding to define critical infrastructure
- To identify the corporations and associations which are excluded from either all or some of the judgments that are related to cyber security
- To perform other duties (Bilgi Teknolojileri ve İletişim Kurumu, 2012)

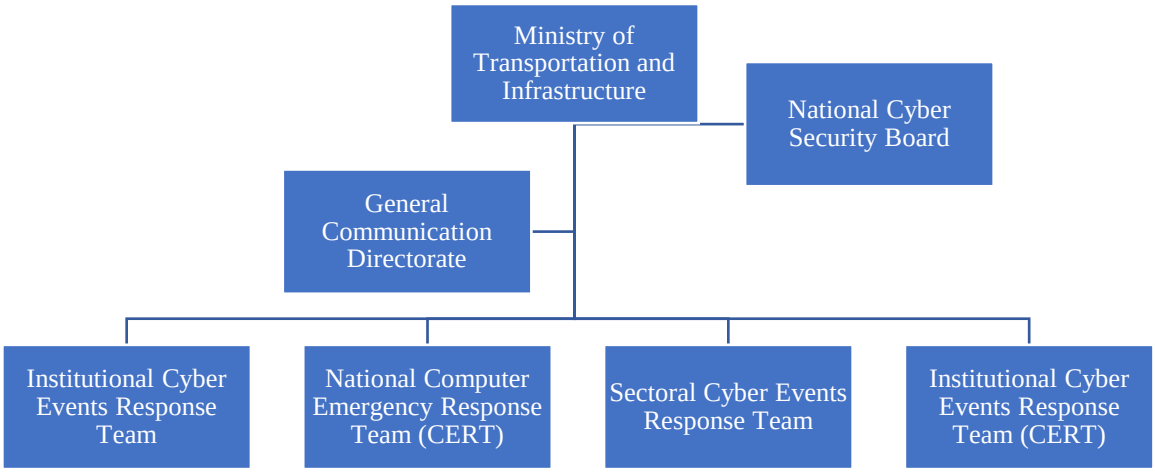


Figure 2.14. *National Cyber Security Organizational Hierarchy (T.C. Ulaştırma ve Altyapı Bakanlığı, 2016)*

The National Cyber Security Strategy and Action Plan were launched to function as a guideline for every state, legal organization, and official including the time- period between 2016 and 2019 years by National Cyber Security Board. The main objective of the National Cyber Security Strategy and Action Plan which was published for the time range between 2016 and 2019 is to establish a national cyber security framework for describing and adjusting the sensible and applicable policies by implementing the practices of this system. Cyber security is considered an integral component of national security infrastructure to be achieved through all political and technical actions for assuring the protection of entire national tangible and intangible resources and assets in cyberspace by the Strategy and Action Plan. In essence, the strategy falls apart into three elements (Republic of Turkey Ministry of Transport Maritime Affairs and Communications, 2016);

- The full protection of the CIA triad and privacy of each data and their transactions with the systems in the IT domain which cover total national cyberspace should be ensured through the compliance of plans, programs, methods, principles, and standards which are designed and published by the Ministry;
- The investigation of emerging cyber-attacks and crimes should be supported through the determination of cyber security actions which are relative to the impact and likelihood of cyber threats for keeping the IT systems and data security under control with optimal threshold values and resiliency performance

by guiding the governing bodies and lawmakers to arrange regulations and standards according to new cases in cyberspace;

- The reasonable actions which should be taken in terms of safeguarding the critical infrastructure must be based on the fundamentals of producing, developing, and using national cyber security software, hardware, tools, and services at the maximum level (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2012).

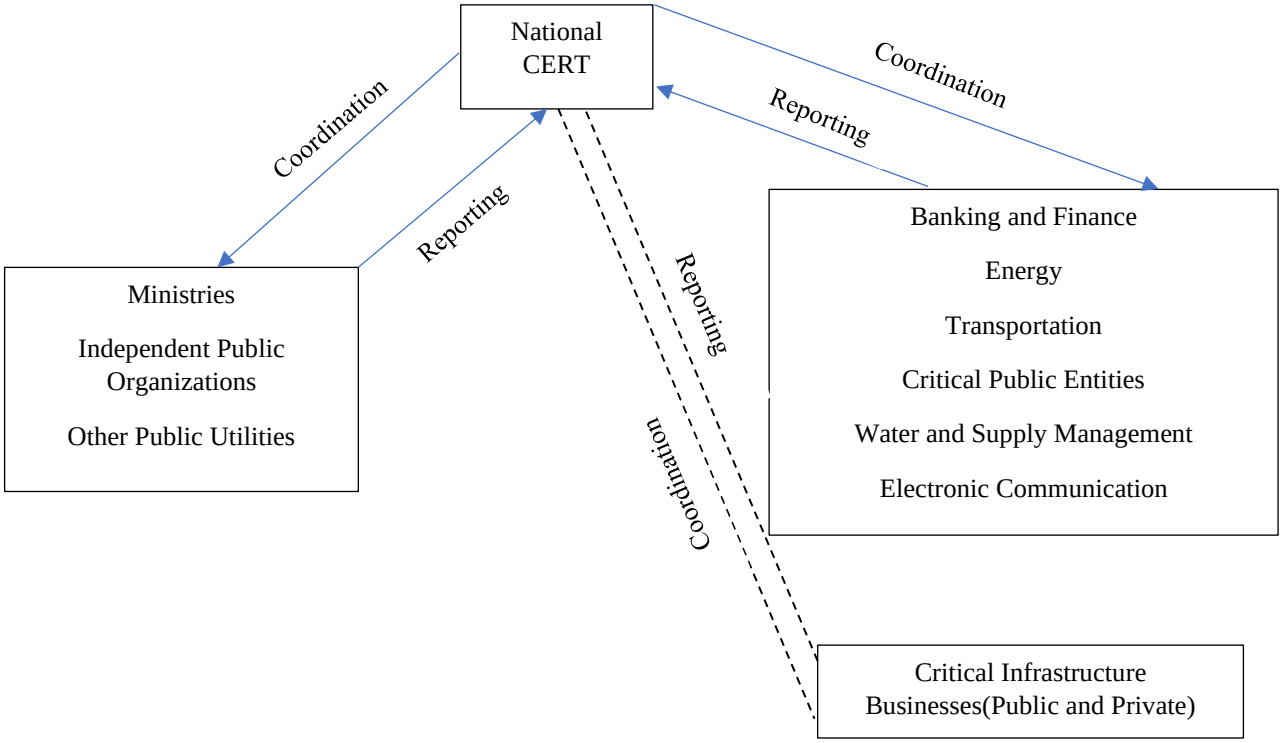


Figure 2.15. *Sectoral and Organizational Interaction of National CERT (Bilgi Teknolojileri ve İletişim Kurumu, 2017)*

In addition, National CERT was established under the constitution of the Information Technology and Communication Organization due to the frame of the fourth article of the 2013-2014 National Cyber Security Strategy and Action Plan which covers the settlement of the National Cyber Incidents Response Center and Sectoral and Corporate Cyber Incidents Combat Teams. In essence, the National CERT was formed to provide not only domestic but also international coordination by taking actions such as making alerts and cautions for responding to cyber incidents. Fundamentally, the missions of National CERT are stated as;

- Assuring coordination and communication for encountering the cyber crimes
- Working synchronously with Cyber Incidents Response Teams (CIRT)
- Providing support for the optimal security of critical infrastructures
- Sharing knowledge which is concerning to cyber incidents with governmental agencies and international authorized associations
- Making alerts, cautions, and notifications in terms of preventing and responding to cyber threats (Bilgi Teknolojileri ve İletişim Kurumu, 2017)

The implementation, administration, and coordination of national cyber security policies, plans, strategies, and activities were delegated to the accountability of the Transportation, Marine, and Communication Ministry in terms of providing feasible governance according to the Cabinet decision in October 2012. Also, the National Cyber Security Board, which was founded under the directorate of Transportation, Marine, and Communication Ministry, was consisted of the undersecretaries of Foreign, Internal, National Defense, Transportation, Marine, and Communication Ministries, Public Order and Safety, and National Intelligence Organization with presidents of General Staff Presidency Correspondence Electronic and Information Systems, Information Technology and Communication Organization, Scientific and Technological Research Council of Turkey, Financial Crimes Investigation Board, Telecommunication Connection and the senior level managers of public entities and governing bodies were selected by Transportation, Marine and Communication Ministry. The assignments of ministry were represented as;

- To set the policies, strategies, and action plans to provide national cyber security;
- To formulate principles and procedures for assuring the CIA triad of data, information, and knowledge assets of public organizations;
- To audit and control the installation activities of technical infrastructure at public enterprises through ensuring the validity of applications by testing their effectiveness;
- To define critical infrastructures and implement systems for observing, preventing, and taking actions in terms of mitigating the impacts of cyber threats and attacks by making studies for processing, auditing, and continuous improvement of such systems;

- To encourage the production, development, and usage of national solutions and tools for assurance of national cyber security;
- To plan, coordinate, and procure training and education activities for required capacity building of the development of personal staff at organizations that are critical for national cyber security;
- To cooperate with other countries and international associations for controlling national cyber security efficiently;
- To authorize natural and legal persons with certifications that have liability for educating personal, testing, and producing solutions that pertain to cyber security; (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2012)

The reviews and recoveries have been performed in National Cyber Security Strategy for the years between 2020 and 2023, through investigating the operations, plans, and conditions that were sustained in the period of 2013 and 2014, 2016 and 2019 years. Eight main motives have been stored according to this framework following as;

- The protection and enforcement of critical infrastructure
- The improvement of capacity
- Organic cyber security network
- The security of new generation technologies
- The combat with cyber crimes
- The development and support of local and national technologies
- The integration of cyber security to national security
- The enhancement of international cooperation (T.C. Ulaştırma ve Altyapı Bakanlığı, 2020, p. 10)

As a result, explicitly, Turkey's cyber security policy framework has been being developed and updated with principles, standards, and regulations since the establishment of the National Cyber Security Board with the governance of state organizations.

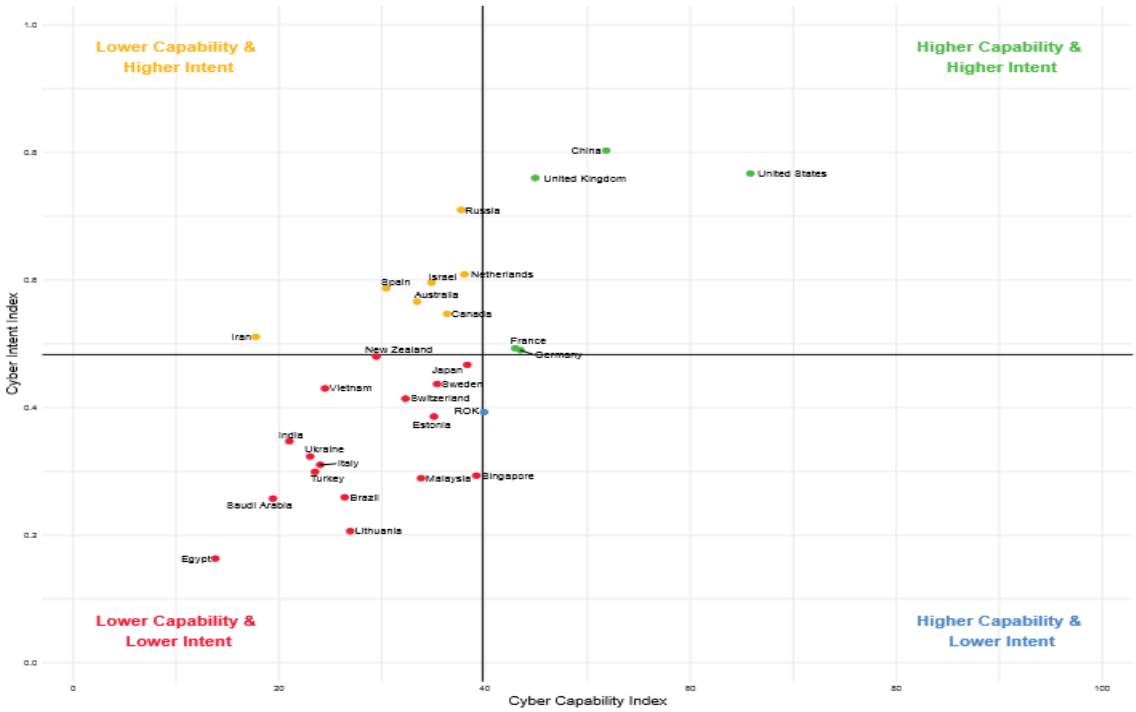


Figure 2.16. *Cyber Power Level of the Sampled Countries (Voo, et al., 2020)*

In addition, within the context of assessing the governance effectiveness and capability of the states' national policies and strategies due to the cyber security related issues, an applied model has been proposed by Belfer Center which can the capacity to measure the cyber skills of the thirty sampled countries relative to seven national goals with compiling thirty-two intent and twenty-seven capability indicators via the data and arguments that have been collected from the public sector which is transformed into output as National Cyber Power Index(NCPI). The seven national goals of states are defined as;

- Monitoring local groups
- Reinforcing and improving national cyber defense
- Controlling and utilizing the information landscape
- International intelligence gathering for national security
- Mercantile earning or strengthening national industry growth
- Terminating or deactivating the infrastructure and capabilities of adversaries
- Interpreting the international cyber ethics and technical standards (Voo, et al., 2020, p. 1)

$$\text{NCPI} = \frac{1}{7}\sum_{x=1}^{7} Capability_x * Intent_x$$

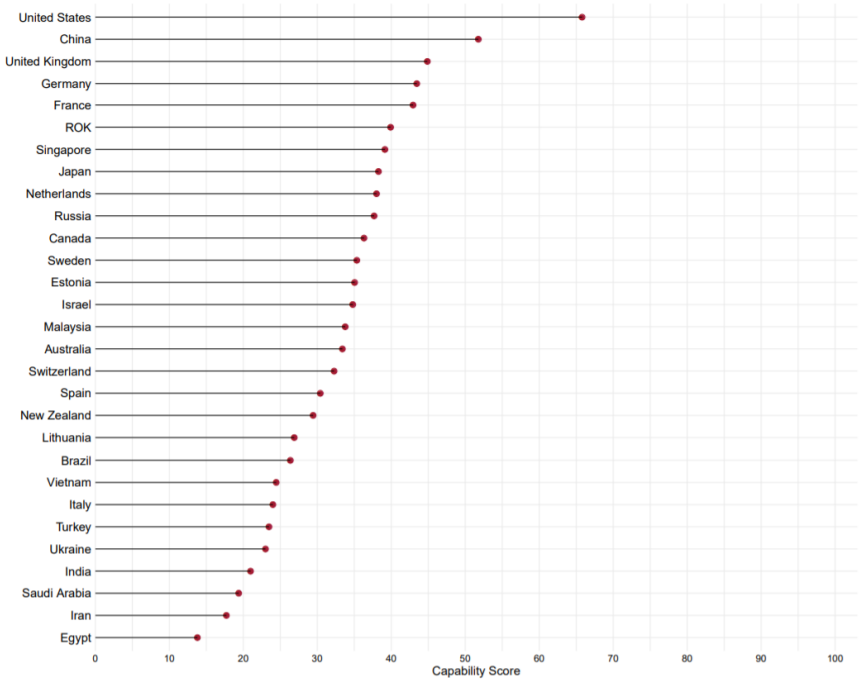


Figure 2.17. *CCI of the Nations relative to All Objectives (Voo, et al., 2020, p. 43)*

NCPI is compiled and calculated by the combination of the Cyber Capability Index (CCI) and Cyber Intent Index (CII) which are considered as independent, discrete, and standalone variables and measurements. Min-max normalization methodology is used to remodel the CCI indicators which can provide a simplex presentation to researchers, practitioners, and analyzers for reflecting the conceptual framework and data attributes. Therefore, NCPI can provide a plausible edge for the people who are involved in a specific native objective to better perceive their country's interest in cyber security-related subjects (Voo, et al., 2020, p. 3).

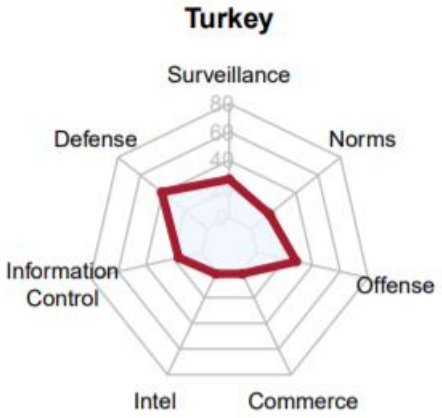


Figure 2.18. *Radar Chart of Turkey which Shows Whole Capability Conditions (Voo, et al., 2020, p. 71)*

- Commercial: Growing National Cyber and Technology Competence
- Defense: Strengthening and Enhancing National Cyber Defenses
- Intelligence: Foreign Intelligence Collection for National Security
- Information Control: Controlling and Manipulating the Information Environment
- Norms: Defining International Cyber Norms and Standards
- Offense: Destroying or Disabling Adversary Infrastructure
- Surveillance: Surveilling and Monitoring Domestic Groups (Voo, et al., 2020, p. 71)

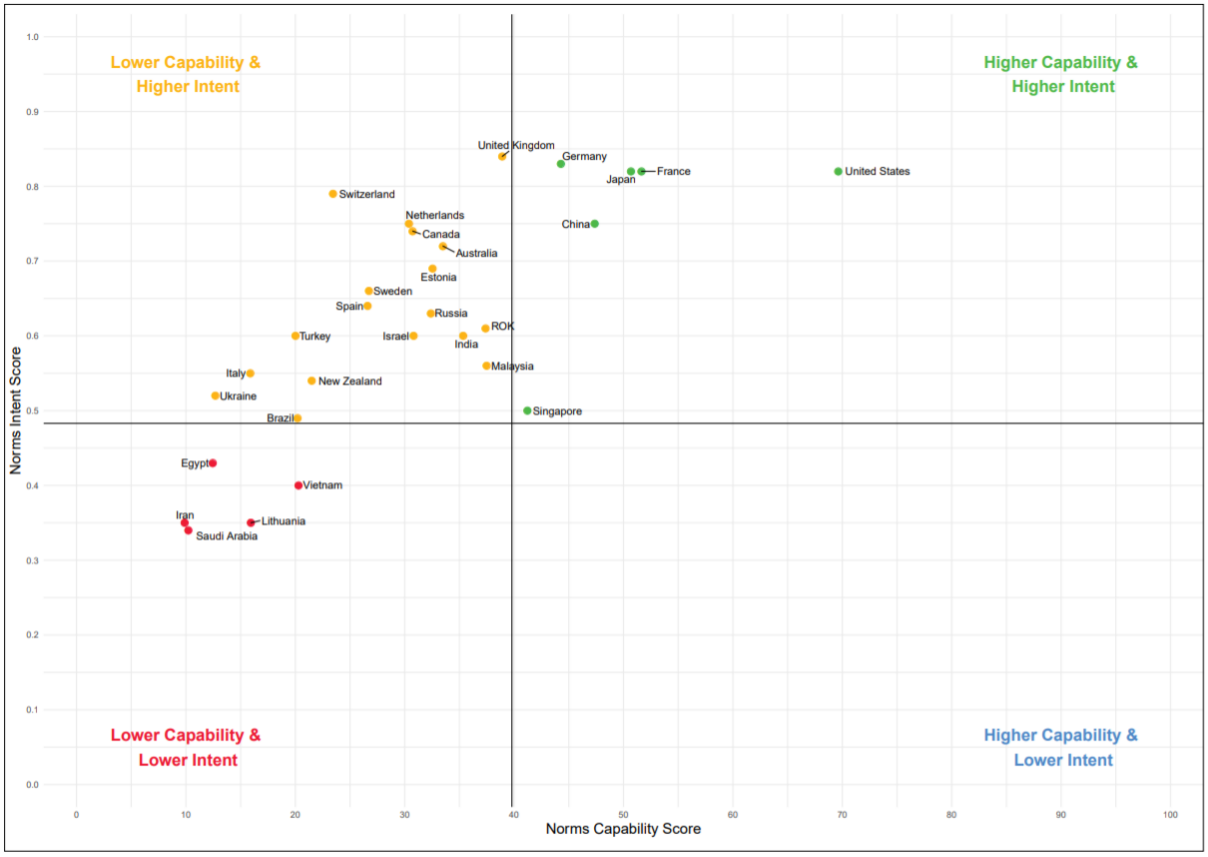


Figure 2.19. *NCPI Plot Chart by the Norms (Voo, et al., 2020, p. 54)*

The norms, which cover a country's understanding and approach, are demonstrated in the NCPI plot chart, can be used as an indicator for how the definition of international legitimacy and policy frameworks are perceived by the governing bodies with investigating the adjustments of them to national changes in economical, political, social, cultural, and technological environments. The advancements and expansion of cyberspace cause modifications and improvements in regulations, standards, rules, and practices for shaping how states, businesses, and individuals act in compliance with the cyber security governance framework. Turkey is in the lower capability and high intent field of the NCPI plot chart which is constructed by the norms. Therefore, the capability points are needed to be improved by structuring an optimal governance approach with the benchmarking of techniques that are being practiced by the United States, France, Japan, Germany, China, or Singapore which are the countries that have better and acceptable capability ratings relatively to Turkey.

2.2.1. Banking regulation and supervision agency (BRSA)

The implementation and administration of regulations are being performed by BRSA in terms of ensuring the reliability and consistency of financial markets through the establishment of effective credit mechanisms and strategies for the protection of both individual and corporate rights and interests of the savers and investors in similar to the SEC of U.S. Fundamentally, the mission of the agency is declared as providing the functioning of credit system efficiently through assurance of the institutions' operations are being performed properly to the Banking Law and Regulations for contributing to the development of financial markets' stability with the safeguarding of warranties and regards of savers. The organization's vision is stated as to transform into an ideal leading institution that prosecutes regulations and risk management guidelines for financial markets in compliance with national requirements. From the viewpoint of technology, an information security management system (ISMS) has been formed inside of the Data and System Management Department of BRSA which is being controlled and authorized properly relative to the standards of ISO/IEC 27001:2013 by the organizations that are certified for an independent audit. Therefore, the CIA triad of informational assets is being protected against cyber threats and attacks according to the rule-based system which is embedded in ISO 27001 standards. Likewise, the data transmitting and communication systems of the organization are being provided due to the ISO 27001 standards and employees are being educated regularly to ensure that the data breaches and suspicious cases are being reported to responsible personnel. Furthermore, the contributors are defined in the 5411 numbered Banking Law as personnel staff, the Data and System Management Department of BRSA, and third parties which were mentioned in this stage as independent auditors. Also, the requirements of those parties which refer to data security have been described within the policies, procedures, legislation, and documentation that can be shared with respective authorities if needed (Banking Regulation and Supervision Agency (BRSA), 2017).

The internal control and audit regulations of BRSA, which were stated in the seventh part of 31069 numbered official gazette on 15 March 2020, have guidance functions for the Turkish Banks. The articles which were shown in this stage of the documentation are as below;

Information Systems (IS) Internal Control Activities

Article 30-(1): An Information System internal control function should be established and executed by the responsible person who is assigned for detecting the activities of outside service providers and internal controls' compliance to policies, procedures, and standards within the bank.

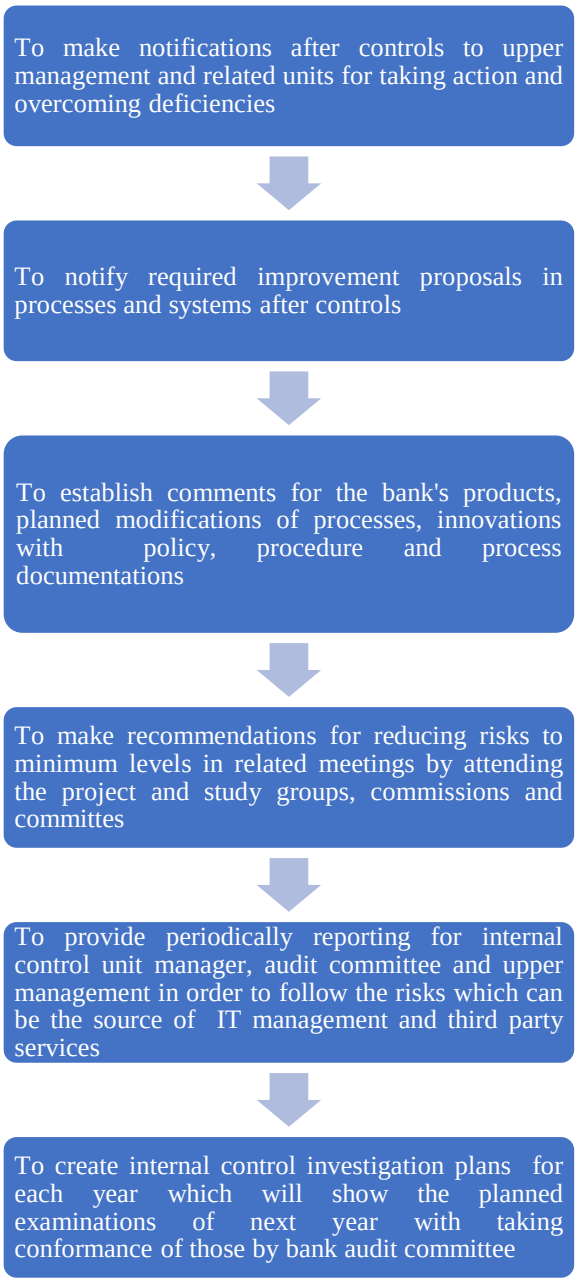


Figure 2.20. *Information Systems(IS) Internal Control Activities*

(2)IS internal control responsible has to have at least five years of professional experience in one or various of the fields were defined as IS internal control, IS internal audit, IS governance, or Information Security. Also, the personnel who are going to take a role in

IS internal control function must have proven knowledge and competence with the desired level in consideration of their education status or acquired certifications.

(3)The periodical controls, which are executed as a set of IS internal control activities, should be recorded and the activity documents have been kept for three years by the bank.

IS Internal Audit Activities

Article 31-(1): Respectively, an IS internal audit function should be developed, an internal audit responsible should be assigned to this unit, and IS internal audit activities are executed under the accountability of this person in order to assure to board management for the effectiveness and sufficiency of the risk management activities and internal controls which are related to IS by investigating both the outside service providers' and bank's IS management processes through searching their compliance to the legislative framework, policy, procedure and standards which are being used within the bank.

(2)IS internal audit responsible has to have at least five years of professional experience in one or various of the fields which were defined as IS internal control, IT audit, IS governance and controls, or information security. Also, the person who will take a role in IS internal audit must have proven knowledge and competence with their education levels and acquired certifications.

(3)The scope of IS internal audits should be prepared with a detail-oriented approach for ensuring the functioning of IS services, processes, and critical assets. Likewise, an IS audit plan, which covers the controllable fields of IS, should be formed annually with taking the confirmation of the audit committee of the bank.

(4)The IS internal audit cycles and frequencies of a bank must be provided in proportion to the criticality and risk of IS services, processes, and assets. Furthermore, the audit cycle, which is based on IS internal audits, should be determined for the utmost two years period to ensure that all of the judgments which were replaced in this regulation are fulfilled by the bank.

(5)Audit guidebooks and control lists should be prepared as written documentation and must be updated relative to up to minute technology through regular reviews for IS audits which will be performed by IS internal audit function. In addition, performance reports which pertain to those audits have been hidden by the bank for at least three years.

Examination of Findings and Provision of Assurance

Article 32-(1): The reviews of findings and critical subjects, which are obtained from IS internal control, IS internal audit and other IS audit activities, and guidance of board

management through taking necessary precautions should be executed and performed by the audit committee. The bank audit committee members should be composed of persons who have professional experience and knowledge capability to adequately assess the IS internal control and IS internal audit reports and findings.

(2)The findings which are diagnosed as a result of IS internal control, IS internal audit and other IS audit activities must be pursued by the bank through the action plans. The findings, which are not assigned, postponed, or exceeded the time constraints that are defined in action plans must be regularly reported to the audit committee and should be evaluated as critical subjects.

(3)IS internal control and internal audit functions have a role in making suggestions that are based on findings through setting precautions and actions. The final decision of findings, which can be recovered by the applications of recommendations and action plans, is taken after the reviews of IS internal control or IS internal audit function which are the responsible and holders of the findings.

(4)As a result of the activities which are performed by IS internal control and internal audit functions, an assessment should be made to objectively display the weaknesses of controls that are being operated by the independent organizations and examinations of the bank's IS controls and in this scope;

- The control weaknesses which can be an obstacle to the efficiency, adequacy, and compliance metrics which are defined in the methods and principles with the "Internal Control System" titled the second stage of Internal Systems and Internal Capital Adequacy Assessment Process regulation,
- The investigations of corruption or misuse cases in which the managers and personnel intervene who have critical roles in internal control systems and that affect the confidentiality, integrity, and availability of sensitive data for the bank like financial information and sustainability of the business activities which cause misrepresentation of financial statements,
- If there are such kind of findings under the scope of mentioned points, the assurance of reporting to the bank audit committee and board management,

should be provided as the main element.

The Personel Education and Resource Allocation

Article 33-(1) The basis is defined as allocating sufficient sources and hiring required personal capacity with adequate qualifications to effectively fulfill the IS internal control and audit activities. The employees, who will take a role in internal control and audit activities, should participate in pieces of education, conferences, and seminars that refer to IS internal control, IS internal audit, IS governance, and the establishment of controls or information security for at least twenty one hours in every year and one hundred twenty hours in every three years.

(2) The planning of internal control and audit activities for ensuring the timely reviews of systems, processes, and fields which have previously major significance in providing the allocation of required sources must be executed harmonically based on mutual collaboration and information transfer (BRSA, 2020).

2.2.2. Capital markets board of Turkey (CMB)

CMB is the authorized organization that provides governmental control in the security, asset, and equity markets of Turkey. In-depth legislations have been formed in order to regulate and organize the equity market environment by developing instruments and associations through Capital Markets Law (CML) which was established in 1981. Especially, CMB has an extensive scale of responsibilities for the protection of investors' rights and fairly organized functioning of the markets as its main objectives. Therefore, the major goal of the entity is to support the legitimate asset allocation mechanism in the nation by regulating the relations of lenders, debtors, and investors with respecting their rights. From the mission perspective, the organization aims to establish inventive and constructive regulations for performing the management of Turkish capital markets in terms of enhancing their international capabilities by the assurance of ethical codes, effectiveness, and clarity. In summary, the major strategic functions of an organization can be classified as;

- To improve the protection of investors
- To provide the adaptation and integration of international capital markets' norms into the national legislative framework
- To advance transparency and fairness of capital markets
- To support the infrastructure and structural development of capital markets

In connection with the thesis subject, a feasible digitalized surveillance mechanism is required to audit and control the equity markets. Correspondingly, the restructuring of

the Data Processing and Statistics department is provided and this unit is transformed into a separate form that has a role in establishing a real-time database by setting and launching systems to take computerized data processing in place (Capital Markets Board of Turkey, 2021).

2.3. The Relationship between Governance, Risk, and Compliance (GRC) Factors in Cyber Security

First, cyber security refers to intellectual capital, processes, technology environment, and tools which are being performed in a system development cycle as mentioned before. Correspondingly, this system cycle is being governed and supported according to the guidelines, standards, and policies which are structured internally by organizations' managements in compliance with an internationally accepted code of conduct. Governance models affect organizational behavior that constructs frameworks for intellectual capital to perform their business activities ethically via a set of procedures, principles, and strategies to achieve the targets (Schreider, Building an Effective Cybersecurity Program, 2nd Edition, 2019, p. 71).

From the point of ERM, an organized risk review mechanism must be planned by the board of directors in terms of examining the vulnerabilities and their effects according to the prioritization of risks by utilizing the organizational sources to mitigate them by adequate controls. In fact, ensuring the nominal security of an enterprise with a tolerable cost in contrarily to benefits by letting appropriate flexibility to personnel for performing their business activities efficiently, can be challenging to offset. Correspondingly, the limitations of data access in an organization for the protection of the assets and resources should be defined from a broad business perspective not just with a technical view. Therefore, technical solutions are needed with the coordination of business reviews while making decisions for what the requirements to be met for keeping the control systems effective, efficient, and agile. As a result, the proposals, which focus on organizational learning, awareness, and culture, are required through coordination and support of the tone at the top of management (Parker & Graham, 2008, p. 18). Relatedly, organizations need to transform their risk management frameworks through value chain models instead of integrating just the risk definitions, scores, and linear COSO mindset. In this sense, the Business Model for Information Security (BMIS) of ISACA can be a complementary

framework for circling the items which can be customized to the risk management transformation program.

Therefore, the cultural values and frameworks which are developed by management strategies that are formulated by considering the vision and mission principles which show the tone at the top relative to sustaining the core business functions, take in place for decision-making approaches while organizations are coping with risks in accordance with industrial standards. Respectively, in order to achieve risk management objectives in cyber security, the governance frameworks and compliance checks should be performed harmoniously for assessing how the organizational culture supports the IT functions and its role. The information assets which should be protected through risk management strategies are adapted to cyber security activities under the full responsibility of board management on the part of assuring the CIA triad of knowledge that is retained and circulated across the enterprise. Hence, from the standpoint of governance, the authority of board management in an organization can be deployed to the system owner or IT department to mobilize the decision-making approaches in cyber security processes. Furthermore, cyber security mechanisms and corporate governance frameworks should be synthesized with each other to provide adequate protection through risk assessments and controls for operational, financial, intellectual, and information assets in organizations (Calder, IT Governance Guidelines for Directors, 2005, pp. 30, 31, 32).

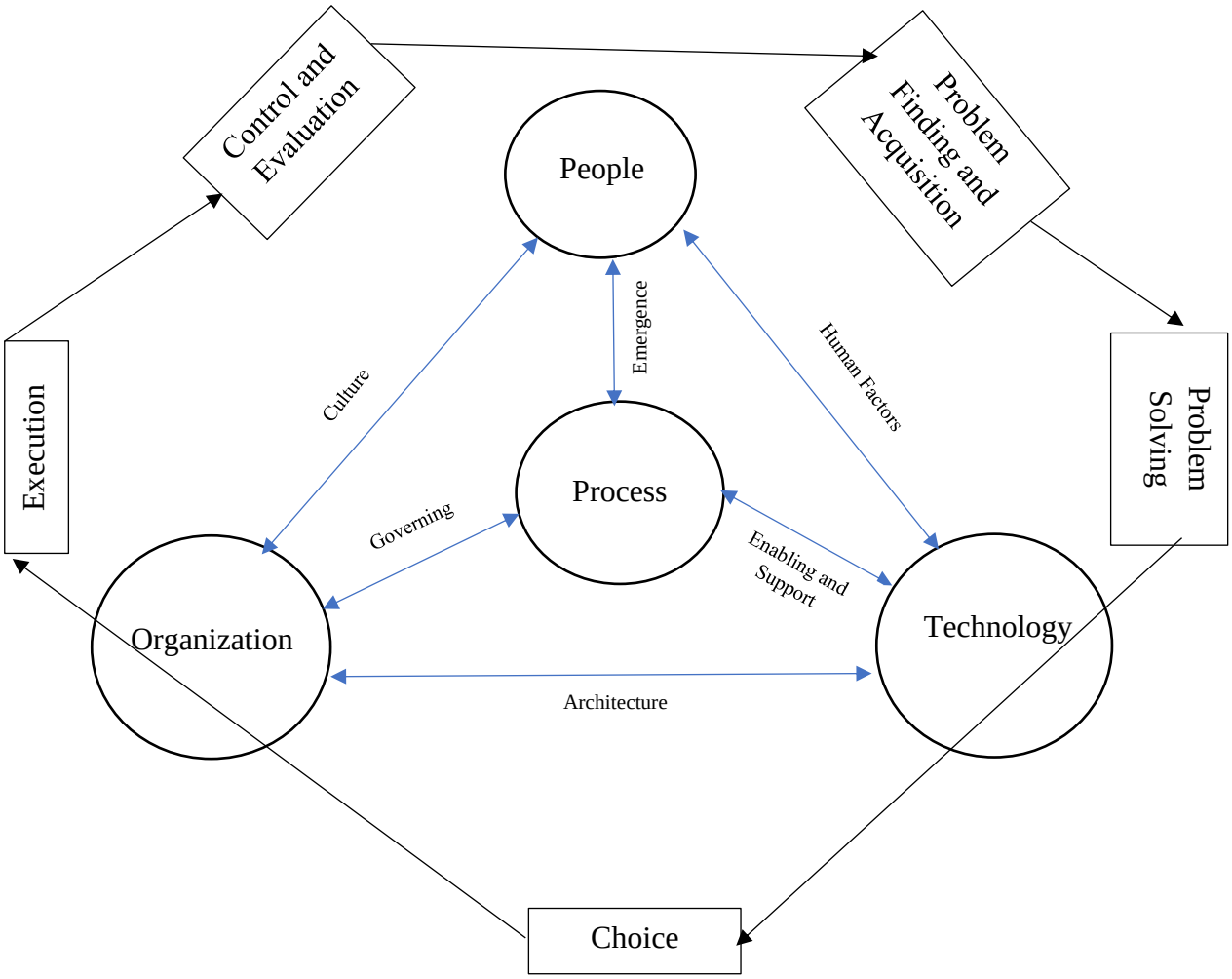


Figure 2.21. *Conceptual Framework of BMIS with Risk Transformation (Vohradsky, 2019)*

From the point of risk transformation, the major catalysts can be taken into account as constructing the appropriate technical tools, data structures, warehouses, applications, and procedures. Although merely focusing on the technical perspective of the organizational elements without discussing the entire set of capabilities which involve governance, risk, compliance, and business intelligence is not sufficient for ensuring a whole understanding of cyber security. Additionally, organizations need to develop a risk culture that covers the expected mindset of behaviors, code of ethics, and actions by the development of organizational learning and the settlement of intellectual capital with well-established tasks, key risk indicators (KRIs), and key performance indicators (KPIs). Particularly, the usage of risk measurement tools such as business intelligence, automation, data analytics, and scenario management via consolidated GRC can aid the

decision-making process in terms of reducing the cognitive biases which are resulted from the lack of organizational awareness (Vohradsky, 2019).

As mentioned before, depending on the interaction between the factors of governance, risk, and compliance, enterprises are investigating to develop inherent policies which comply with both governmental legislation and internationally accepted standards for managing cyber risks. In this case, organizations need to arrange their data assets' protection mechanisms dynamically to assure that their IT security structures are complying with national policies and industrial guidelines through internal controls and audit activities which are harmonized with risk management strategies that are established by the board and information systems management. However, the relational metrics between governance, risk, and compliance change according to the dynamic determinants which are affected from the regulatory aspect, organizational strategies, principles, technical standards, and cyber risks that are shifting continually. Therefore, systems, methods, and tools to audit the structure of governance, risk, and compliance in cyber security functions of organizations can be developed through rule-based algorithms which can be updated dynamically according to the changes in the legislative environment and internal control strategies for performing timely recoveries in IT operations. In assumption, a risk control framework can be designed and established internally according to the region, sector, and organizational culture of the enterprise. Correspondingly, internal audit functions can be integrated into this framework to support and review internal control which has a role in risk management processes of cyber security with an adequately designed organization scheme that demonstrates the layout of task units and business hierarchy to understand how the enterprise management takes in place the cyber risks and their impacts to critical assets. Also, clarifying the linkage between governance, risk and compliance can be perceived by searching for the problem that how the organization is sustaining and improving its cyber security activities relative to external developments concerning policy framework and cyber threats (Choudhary, Antony, Cooper, & Srinivasan, 2010, p. 8).

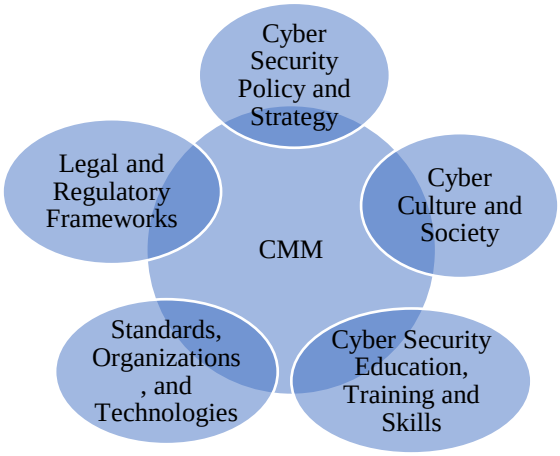


Figure 2.22. *The Five Standpoints of Cyber Security Capacity Maturity Model (CMM) (Global Cyber Security Capacity Centre, 2016, p. 5)*

CMM is launched by the Global Cyber Security Capacity Centre to improve the effectiveness of building processes for the enhancement of cyber security capacity by proposing five dimensions of the field. These are defined as cyber security policy and strategy, cyberculture and society, cyber security education, training and skills, legal and regulatory frameworks and standards, organizations, and technologies. At first, a country's capacity for designing and presenting a feasible cyber security framework is assessed according to the point of cyber security policy and strategy through efficient incident reaction, crisis management, and protection capabilities of critical infrastructure (Global Cyber Security Capacity Centre, 2016, p. 5).

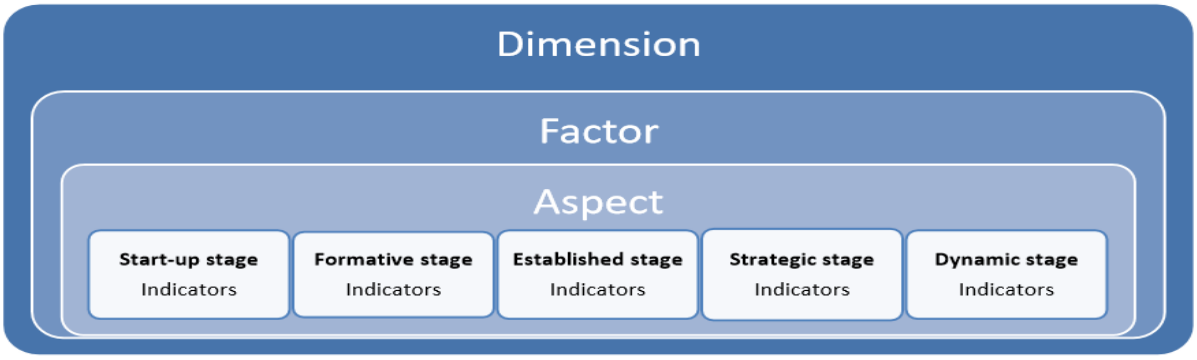


Figure 2.23. *Template of Layers in CMM (Global Cyber Security Capacity Centre, 2016, p. 6)*

According to this cluster, each of the dimensions states different investigation parameters for the factors, aspects, maturity stages, and capacity metrics of cyber security to enhance overall capability in terms of reaching expected protection levels. As well, every single dimension in this concentration demonstrates which capacity is being

analyzed and reviewed to identify the cyber security maturity level of a nation for deciding security objectives and plans. In this sense, factors can be considered as the items which represent the contribution to the improvement of the maturity level in a cyber security capacity. Correspondingly, every one of the factors is then demonstrated as scores of aspects to characterize a method through splitting indicators into smaller groups with five settings of maturity which can provide simplification for analyses and comprehensions (Global Cyber Security Capacity Centre, 2016, p. 5).

D X.X: Factor Title					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Aspect A	Indicator 1 Indicator 2 Indicator 3	Indicator 4 Indicator 5	Indicator 6 Indicator 7 Indicator 8	Indicator 9 Indicator 10 Indicator 11	Indicator 12 Indicator 13
Aspect B	Indicator 1 Indicator 2	Indicator 3 Indicator 4 Indicator 5	Indicator 6 Indicator 7	Indicator 8 Indicator 9 Indicator 10	Indicator 11 Indicator 12

Figure 2.24. *The Visual Diagram of How the Factors, Aspects, and Indicators are Clustered in Each Dimension of the CMM (Global Cyber Security Capacity Centre, 2016, p. 6)*

The representative template can be utilized for the determination of which maturity stage is belonging to specific indicators and can be outlined as;

- The start-up phase shows that an organization or a nation has either elementary level cyber security maturity or any. Therefore, there might be an embryonic exploration around the capacity building of cyber security, but there is no definite steps have been taken at this stage. In short, there is a lack of recognizable testimony which depends on cyber security capacity building and maturity.
- The formative stage indicates that a quantity of the aspects has started to develop and frame, but these are amateurish, unorganized, limited, and poorly formulated. Nevertheless, evidence of capacity building can be obviously verified.
- Established degree states that the parts of the aspect are functional, described, in line, acting, and performing, but there is no carefully planned discussion for the resource allocation as little decision-making processes of investments in the distinctive pieces of the aspect.
- Strategic category demonstrates that the decisions have been taken for which the specific elements of the aspect are significant and which of them are less crucial for a particular nation, sector, or a defined organization. This stage also observes

the cases due to the preferences that have been made for the conditions during the course of a nation's or an organization's particular state.

- The dynamic episode represents that either a nation or an organization has a recognizable structure for adjusting and reforming the strategy in relation to the common conditions in the threat landscape, cyber crimes, or secrecy. As a result, this stage covers constant cautiousness for changing circumstances and agile decision-making with optimal asset reallocation to improve cyber security capacity.

D 2.1: Cybersecurity Mind-set					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Government	Government has no or minimal recognition of the need to prioritise a cybersecurity mind-set. Leading agencies within government may have begun to consider cybersecurity.	Leading agencies have begun to place priority on cybersecurity, by identifying risks and threats.	Most government officials at all levels are aware of cybersecurity good practices.	Agencies across all levels of government have routinized a cybersecurity mind-set, employing good (proactive) practices as a matter of habit. Cybersecurity mind-set informs strategic planning.	The cybersecurity mind-set serves as a foundation for government official's operational practices and is evidenced as global good practice. Cybersecurity mind-set of government officials is related to a reduction of the overall threat landscape of the government.
Private Sector	The private sector has no or minimal recognition of the need to prioritise a cybersecurity mind-set.	Leading firms have begun to place priority on a cybersecurity mind-set by identifying high-risk practices. Programmes and materials have been made available to train and improve cybersecurity practices.	Most private sector actors at all levels are aware of cybersecurity good practices.	Most private sector actors, including SMEs, have routinized a cybersecurity mind-set, employing good (proactive) practices as a matter of habit. Cybersecurity mind-set, informs strategic planning.	The cybersecurity mind-set serves as a foundation for private sector operational practices, informs all IT related initiatives and is evidenced as global good practice. Cybersecurity mind-set of the private sector is related to a reduction of the overall threat landscape of the sector.
Users	Users have no or minimal recognition of the need to prioritise a cybersecurity mind-set and take no proactive steps to improve their cybersecurity.	A limited proportion of Internet users have begun to place priority on cybersecurity, by identifying risks and threats.	A growing number of users feel it is a priority for them to employ good cybersecurity practices and make conscious efforts to securely use online systems.	Most users have routinized a cybersecurity mind-set, employing secure practices as a matter of habit.	Cybersecurity mind-set of users is related to a reduction of the overall threat landscape of the country.

Figure 2.25. *Sample CMM Report for Cyber Culture and Society Dimension (Global Cyber Security Capacity Centre, 2016, p. 27)*

According to the representative visual display of the CMM report which is relative to the cyber security mindset factor of cyberculture and society, the evaluation has been made for understanding the level of cyber security efforts that involve values belonging to behavioral attitudes, code of ethics, and habits of both organizational experts and individual actors in a nation's or an industry's cyber security ecosystem with the aim of enhancing the resilience of defense mechanisms.

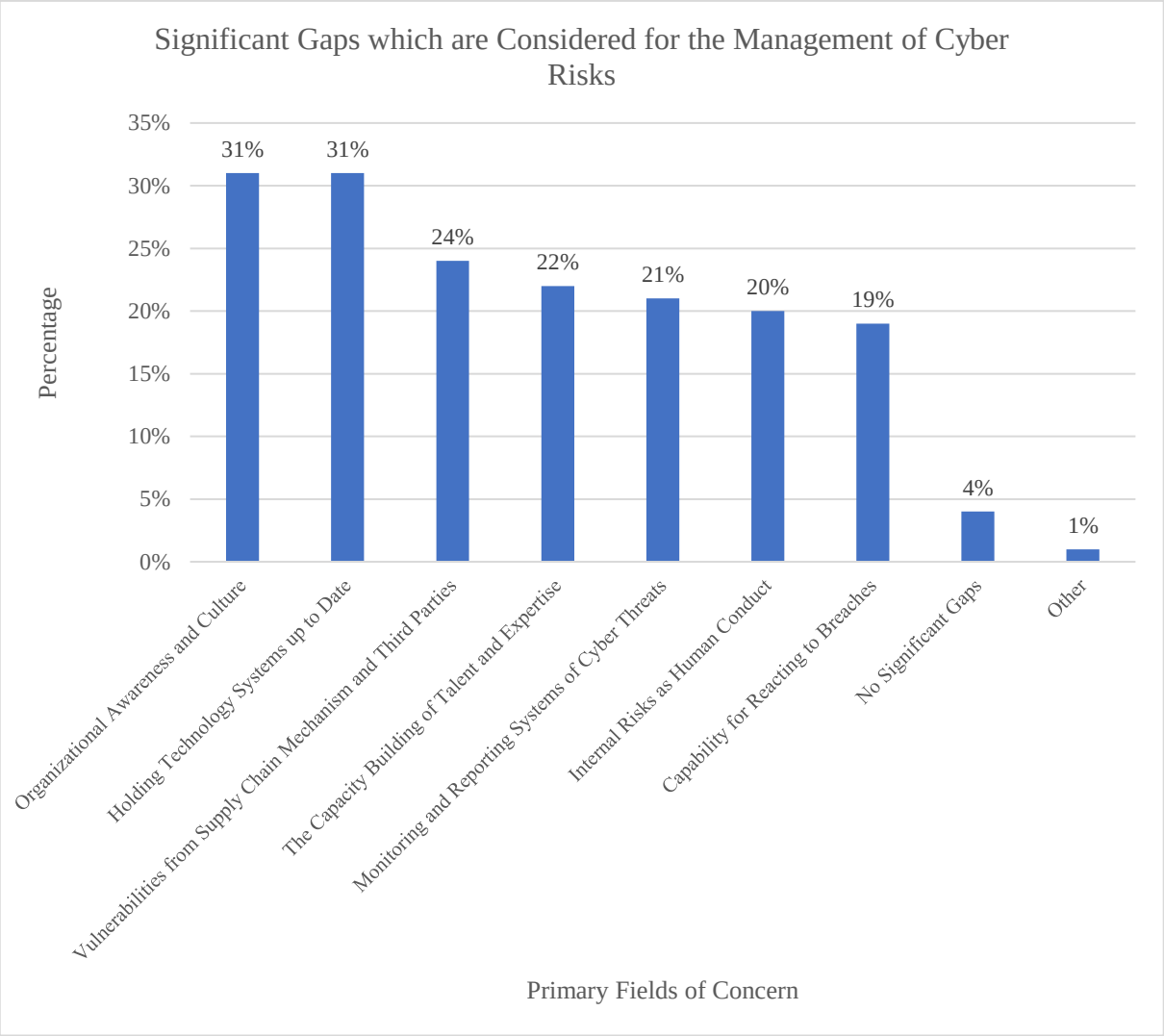


Figure 2.26. *The Critical Areas for Controlling Cyber Risks (KPMG's Audit Committee Institute, 2017, p. 4)*

Risk management is discussed as a major concern for the majority of internal audit teams according to the 2017 Global Audit Committee Pulse Survey which was designed to understand the main challenges in audit sufficiency, trust mechanism in financial processes, legislative liabilities, compliance-related requirements, cyber security risks and the management of control environment. The cyber risk perspective continues to be mercurial and enigmatic, although the deepening focus of enterprises on the security aspect of the issue has been escalating while the expectations are increasing for value-added engagement of control. Therefore, cyber risks should be considered comprehensively as an organizational risk not just as an IT risk. As a result, maximization of the value of internal audit activities for the corporations can be enhanced by concentrating on the major points of cyber security and the capability of risk management

approaches through proactive planning which is flexible and adjustable to dynamic business conditions not merely taking into account the financial reporting risks and their adequacy level (KPMG's Audit Committee Institute, 2017, pp. 4, 6, 7).

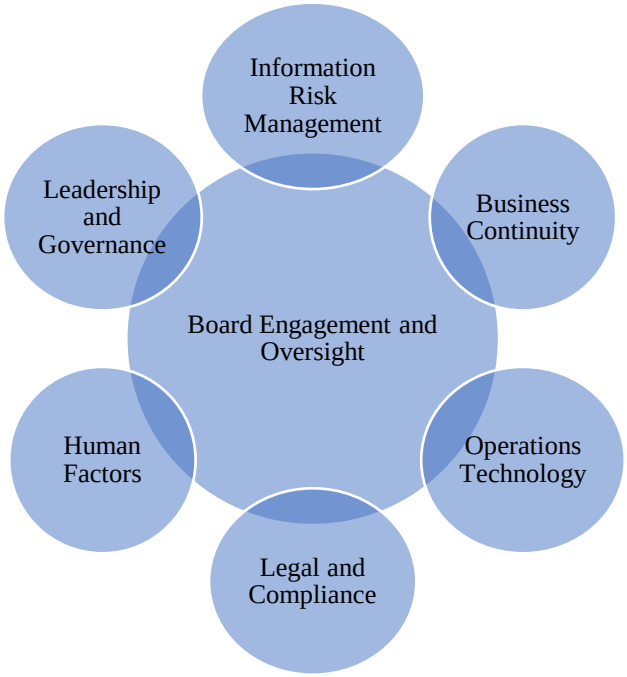


Figure 2.27. *Cyber Security Maturity Parts (KPMG, 2018, p. 31)*

The maturity of the cyber security framework of an organization is fundamentally dependent on six factors with the governance of board management according to the cyber security and insider threats report of Klynveld Peat Marwick Goerdeler (KPMG). Risk management methodologies, policies, the definition of risk tolerance, risk assessments, and measurements are performed under the title of information risk management. Board participation, third-party contractor relationship, classification of critical data, ownership, entitlement, and governance corresponding to data protection and project management are carried through the cover of leadership and governance. Plannings and testings of cyber security practices with cost and benefit analyses in budget management for identifying resources and training requirements are operated by business continuity and crisis management functions. Organizational awareness and culture, ethical behavior, talent development with technical education and training, personnel security roles, responsibilities, and metrics are evaluated as human factors. Insurance policies for providing appropriate cyber security events, compliance principles, and functions of audit commissions are involved by legal and compliance factors. Threat detection with vulnerability controls, security scanning, incident and hazard course of actions through

the support of IT service management are achieved within the context of operations and technology (KPMG, 2018, p. 31).

In theory, cyber security management covers organizational culture, behavior, and awareness to harmonize supervisory, technical and operational controls to ensure the adequate protection of information assets according to the CIA triad. Similarly, the controls are signified through the utilization of policies, procedures, and guidelines. In essence, the risk is related to how an organization is handling uncertainties and unexpected events through which approaches, methodologies, and tools are being carried out for internal controls to safeguard critical assets. Within the context of cyber security management, internal controls should be performed properly with business objectives through the support of the internal audit. Accordingly, the internal audit role in information security can be defined as assuring the validity of risk assessments through reviewing the control frameworks which are formed by standards and policies to assist the organizational management in how the risk management activities are being performed in compliance with organizational culture and governing bodies. Therefore, the interaction between governance, risk, and compliance terms in cyber security management can be provided through the supportive roles of internal audit and control. In this state, information security experts and their units have been authorized to assist the board management in establishing policy frameworks suitably with data protection standards and regulations. In addition, the policies should be formed adequately with organizational culture to achieve and improve the awareness of intellectual capital. Furthermore, collaborative efforts are needed for developing cyber security frameworks which include the proposals and projects of both board management and IT departments. Therefore, the governance models which take in place board managements and IT departments separately from each other may not be sufficient and feasible for the system development life cycle in cyber security frameworks for integrating security policy decisions into organizations. Particularly, the approaches which provide active participation of executive members to oversight the IT security objectives and policies can be applicable for getting expected impacts to governance issues in risk management of cyber security activities (Hernandez, 2007, pp. 8, 9, 10).

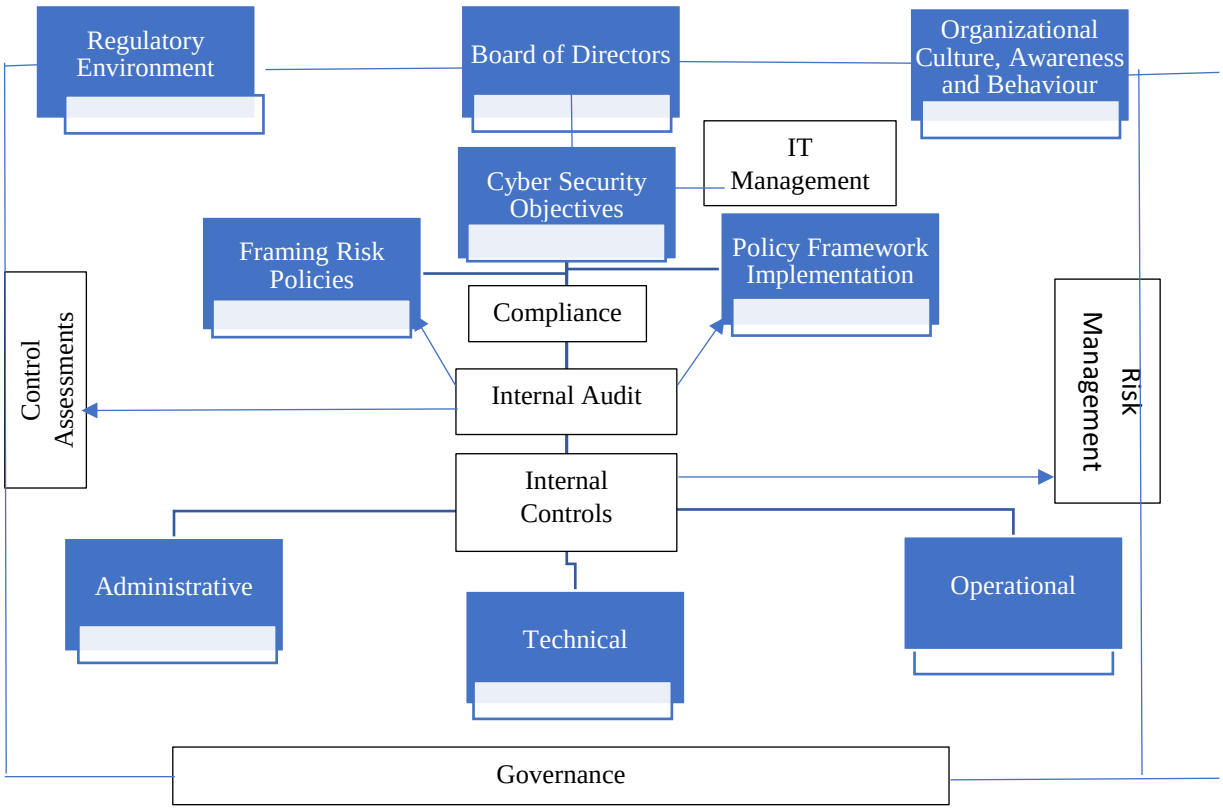


Figure 2.28. *Relational Model of Governance, Risk, and Compliance*

As mentioned before, framing policies just indoor of the IT departments or within the board management to conduct risk management activities of cyber security operations may cause organizations to miss the effective interaction between the factors of governance, risk, and compliance. On the other hand, policies are defined for providing internal controls which have a major role in risk management in compliance with business objectives, must make sense for employees to understand why their organization is implementing the cyber security policy frameworks.

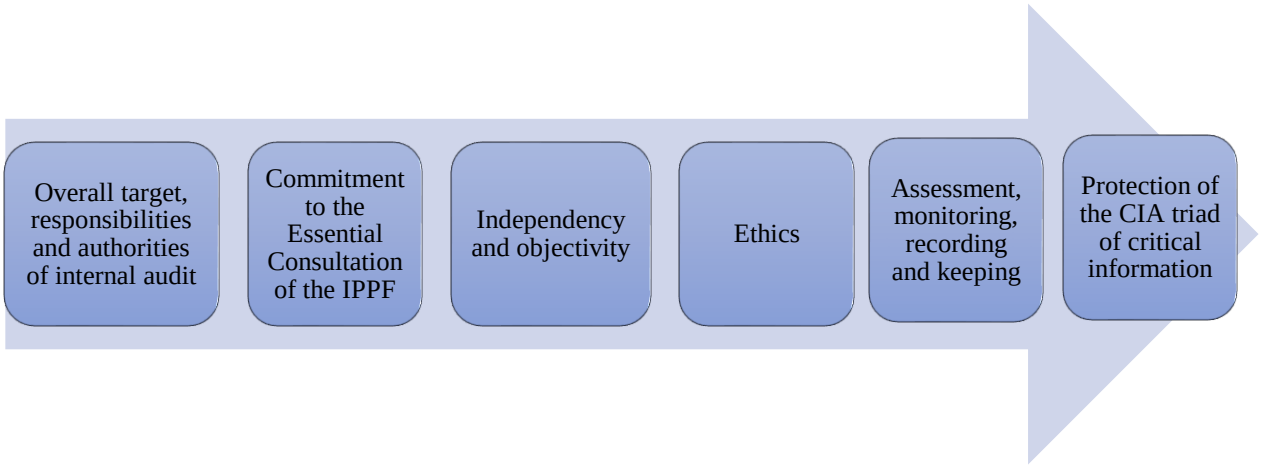


Figure 2.29. *Critical Factors in Internal Audit Policy Design*

From the point of internal audit, policies and guidelines should be established by the CAE for ensuring that the governance framework covers the organizational objectives, plans, and strategies with certain definitions of the entire goals of internal audit activities.

2.3.1. Governance models in cyber security

Technology and the innovations which have been being emerged through scientific developments in interdisciplinary fields that are related to cyber security, affect the traditional governance models in the corporate management of companies. Therefore, in order to improve the governance frameworks, approaches, and practices, the regulatory environment must be continuously examined. Accordingly, International Risk Governance Council (IRGC) was established as an association that has a major role to develop risk-based governance models for observing and controlling the systemic uncertainties which can be emerged in the fields of information technology, robotics, artificial intelligence, synthetic biology, nanotechnology, and personalized medicine. Correspondingly, adequate governance models are required for the enterprises which have business objectives to support their cyber security processes related to risk and compliance matters which dynamically change with digitalization and emerging technologies. In order to perceive how the organizations are overcoming the limitations of their governance levels, the workshop report of IRGC is examined which was published in 2015. According to this documentation, the common problem of enterprises is observed as cyber risks are frequently being assessed with qualitative terms such as low, medium, or high that can not be compared certainly with other business risks which can be evaluated in financial values. Therefore, this complication causes limitations for auditing the cyber security processes in compliance with conventional governance models (International Risk Governance Council (IRGC), 2015, p. 28).

An effective governance model should be equipped with the essentials which demonstrate and decipher a roadmap for how to frame the cyber security processes of an organization to ensure the business continuity and protection of sensitive information assets through administering the system developers and users. In that situation, appropriate control of governance practices must be provided through independent and objective analyses and reportings which support the factual acknowledgment for the

effective decision-making of the board management in their IT budgeting and cyber security investment goals and strategies. Therefore, in summary, the cyber security programs of enterprises should be built on adequate governance frameworks or models for reinforcing the organizational structure and culture to assess and guide the internal controls in the risk management practices. As a result, the governance framework which is selected has as many effects on cyber security activities, like the operational techniques and tools that are being used on enterprise's protection systems for countering the cyberattacks (Schreider, Building an Effective Cybersecurity Program, 2nd Edition, 2019, pp. 75, 78).

As mentioned previously, the internal audit processes support the organizations for the achievements of their objectives through the practices of well-organized and disciplined programs and systems to assess and improve the effectiveness of risk management, control, and governance-related activities. Therefore, the efficiency of internal audit functions is measured by analyzing the level of value-added activities in governance, risk management, and control processes (Zain, 2019, p. 7).

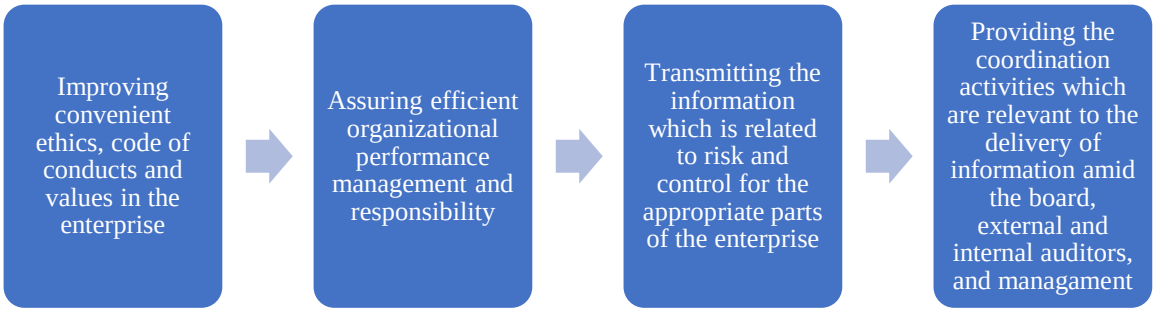


Figure 2.30. *2110 Coded Governance Functions of IIA Performance Standards (Moeller, IT Audit, Control, and Security, 2010, p. 70)*

Within the context of 2100 titled performance standards of IIA which is stated as nature of work, internal audit activities must cover involvements and evaluations for the progression of risk management and governance processes by practicing systematic and disciplined methodologies. Correspondingly, the 2110 coded standard is marked as governance which is discussed under the 2100 titled performance standards to demonstrate how the internal audit functions should assess and create proper offerings

for enhancing the governance systems (Moeller, IT Audit, Control, and Security, 2010, p. 70).

The codes of ethics can be evaluated as key essentials of not only IIA but also ISACA standards. The main goal of the code of ethics in IIA is to enhance an ethical culture for the internal audit profession. According to this objective, a code of ethics is needed for a trust mechanism of independent assurance in governance and risk management. Two necessary fundamentals are covered in IIA's code of ethics as follows;

- Principles that are related to the internal audit profession and practices
- The descriptions of behavior norms, which are expected from internal auditors, are defined in rules of conduct for supporting the interpretation of the principles into practices and guiding the ethical norms of internal auditors.

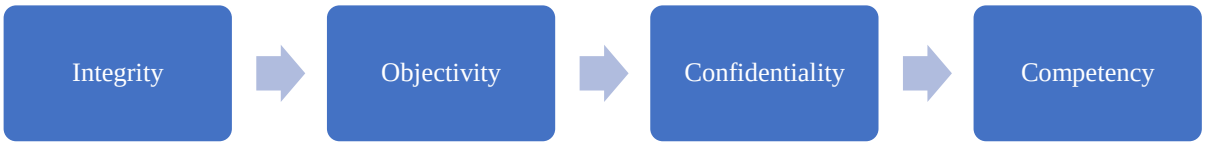


Figure 2.31. *Code of Ethics Principles (IIA, 2019)*

The descriptions of basic expectations and principles for the manners of individuals and organizations to govern internal auditing are stated via the code of ethics. The minimum essentials for conducting the behavioral expectancies in internal auditing activities are framed by the code of ethics to determine what the right or wrongdoings are. Thus, the IIA's code of ethics is designed to improve the level of ethical culture in the internal audit profession with the interest of its role in the objective assurance of governance and risk management. First, the establishment of trust assures the integrity of internal auditors which is fundamental for confidence in their assessments. Second, the top-level professional independence and objectiveness should be provided by the internal auditors while they are conducting their responsibilities as accumulating, evaluating, reporting, and transmitting the information that is related to the processes are being examined with unbiased assessments which are not intolerably originated from their judgments, beliefs, and interests of the whole of relevant conditions. Third, internal auditors should respect the value, privacy, and proprietorship of information that they gathered to not reveal without proper authority, legislative or professional commitment.

Fourth, internal auditors must put their knowledge, expertise, skills, responsibilities, and experiences into effect which are required for the achievement of internal audit services (IIA, 2019).

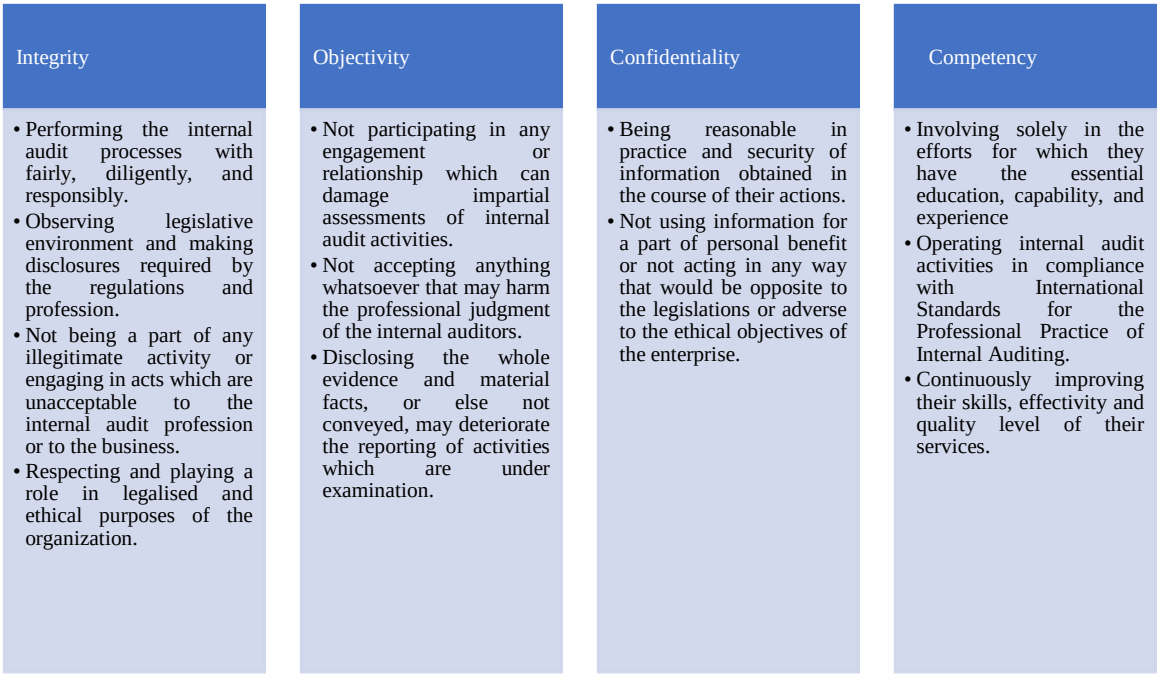
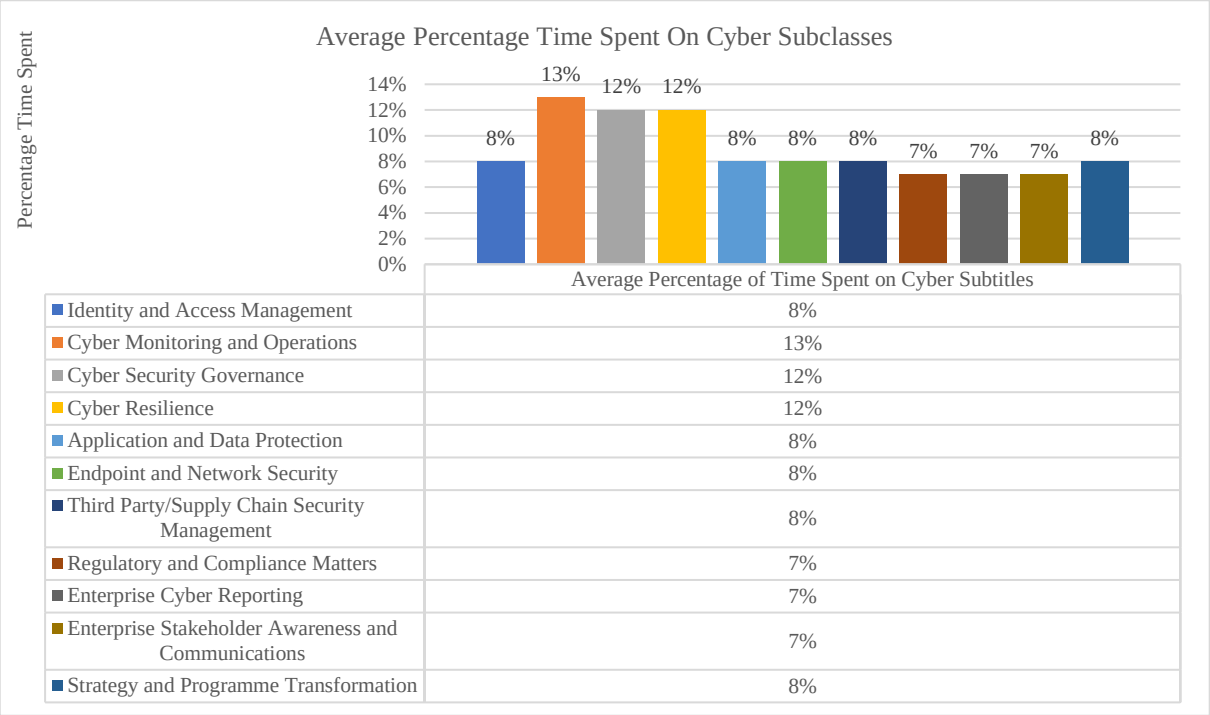


Figure 2.32. *Rules of Conduct that Internal Auditors must Follow (IIA, 2019)*

According to the ethics concept of the computer field, cyber security can be categorized through two elements as social science and technology management. Cyber security-related cases are defined by social scholars due to the national security problems which include disruption of IT systems by cyber terrorism or warfare that can have impacts on countries' national sources and sensitive assets of critical sectors. In essence, the vulnerabilities, which cause risks in cyberspace, are explored by these professionals, especially from the point of political science, economics, and organizational behavior. The creation of social turmoil in the cyber environment and adversary threats to critical infrastructures or industries are described by Nissenbaum (2005) as concerning points of the social scientists. On the contrary, the applications and technical procedures are examined by the technology management experts for securing the data and systems, no matter who the person or which conditions these mechanisms are belonging to. Therefore, security protocols that are relevant to techniques such as encryption or cryptography can be utilized by technology and cyber security experts, coupled with scanning of the viruses, malware, or malicious software by providing that the practices of cyber hygiene are being well organized and controlled to assure that the employees are not vulnerable

to cyber attacks as social engineering (Manjikian, 2017, pp. 13, 14, 15). Mainly, the norms, which can be evaluated as code of ethics, rules, or organizational principles as well, are set for making comparisons between expected standardized behavioral patterns and the act of human beings. Hence, a set of ethical guidelines support the organizations as a rule of thumb in the establishment of discipline, informative instructions, and coaching tools to reach their corporate objectives (Kizza, 2014, pp. 21, 22, 23).



	Average Percentage of Time Spent on Cyber Subtitles
Identity and Access Management	8%
Cyber Monitoring and Operations	13%
Cyber Security Governance	12%
Cyber Resilience	12%
Application and Data Protection	8%
Endpoint and Network Security	8%
Third Party/Supply Chain Security Management	8%
Regulatory and Compliance Matters	7%
Enterprise Cyber Reporting	7%
Enterprise Stakeholder Awareness and Communications	7%
Strategy and Programme Transformation	8%

Figure 2.33. *The Survey Data Which Demonstrates Time Spending Percentage of Executives in Cyber Fields (Deloitte, 2019, p. 4)*

Deloitte's survey study, that was applied online between 9th and 25th January 2019 to 100 Chief Information Security Officers (CISOs), 100 Chief Strategy Officers (CSOs), 100 Chief Technology Officers (CTOs), 100 Chief Information Officers (CIOs), and 100 Chief Risk Officers (CROs) as totally 500 executives who control cyber security operations in their enterprises which have at least $500 million annual income, illustrates that they are spending entirely 37% of their time to the fields in cyber monitoring and operations, cyber security governance, and cyber resilience which have respectively percentage rates as 13%, 12% and 12% that are above of 9% average. Also, this information proves that the organizations are conclusively focusing on these three subcategories to improve efficiencies in their cyber security plans and programs. In

addition, there is another assertion in this study as the NIST's two of the five major functions which are defined as detecting, responding and recovery are systematically being tried to integrate into enterprises' governance models of cyber security management strategies (Deloitte, 2019, pp. 1, 4).

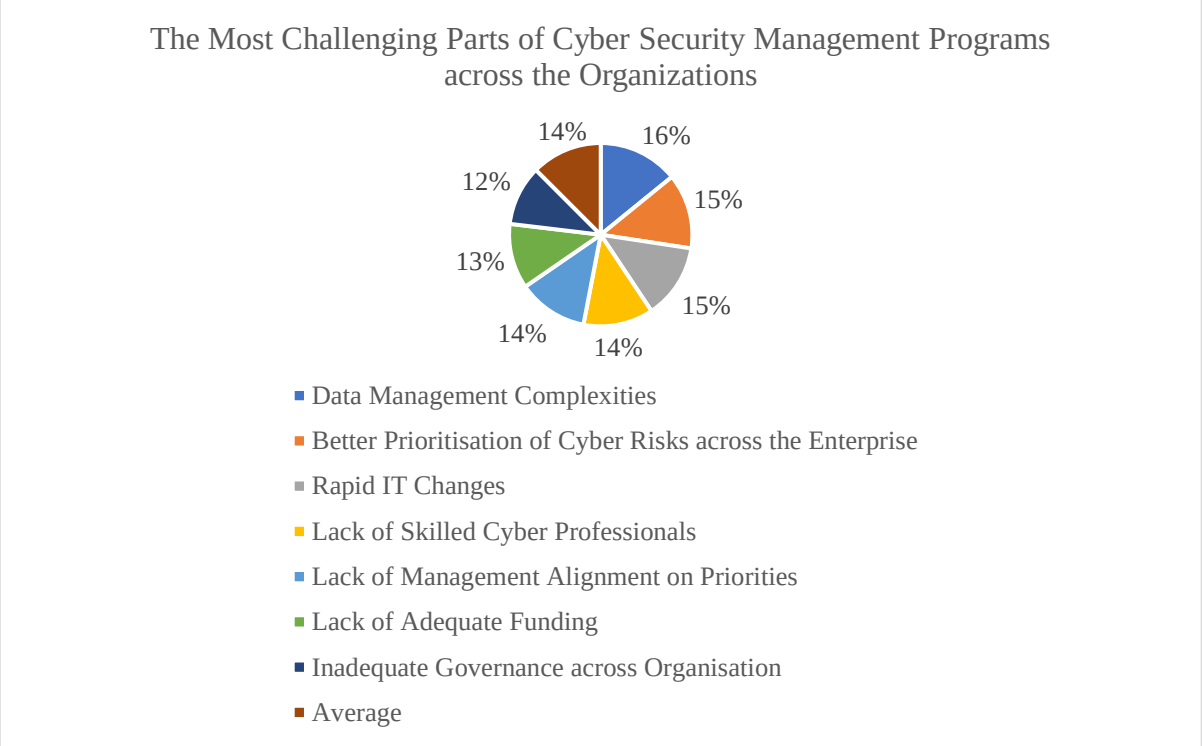


Figure 2.34. *Common Complications in Cyber Security Management of Enterprises (Deloitte, 2019, p. 6)*

Furthermore, this survey claims that there is a weakness in prioritization of the cyber risks according to their impacts and targets to information assets in organizations because teams related to cyber security processes haven't got a predefined governance model or framework. Also, there is another problem that comes up as how the executives must concentrate on efforts which refer to mitigation of the cyber risks with varying criteria and impact levels because there are multiple governance frameworks that can support the organizations to describe their cyber security posture. At the same time, there are further complexities that can be observed as the different governance models or frameworks can be carried out by internal audit and internal control units in enterprises for performing risk assessment activities. In other words, as an example, while internal audit experts are drawing attention to the COSO framework in their reviews, CISO, and internal control staff can use Information Governance Reference Model (IGRM). So, a collective approach may be needed to overcome this conflict through a common feasible

framework that can be used for both internal audit and control. In addition, there is another challenging governance issue as cyber security is grounded solely to the IT department instead of disseminated into the entire organizational culture and behavior according to the survey report. As a result of this fact, sticking cyber security systems in just to IT mechanisms under the responsibility of the CIO causes the reduction in the strategic management capability of organizations. Therefore, to figure out this problem, cyber security culture must be dispersed all through the organization with a balanced distribution of authorities and liabilities in both operational and decision making roles for achieving adequate awareness in functional level employees to acknowledge them for which investments are being made through what reasons to improve the cyber security posture of organizations. In summary, adopting a feasible governance framework to provide an effective cyber security structure is a comprehensive responsibility in enterprises which can be performed through the continuous communication between internal audit, control, and business departments which cover IT, finance, operational and, juridical functions with organizational arrangements and reporting mechanisms, because strategies which refer to cyber security are affected from both internal factors that are related with how the organizational activities are being activated and external cases that are correlated with governmental utilities, suppliers, business partners, and customers. Hence, the organizations need to develop and embed adequate cyber culture into their corporate governance practices for linking the strategies and operations between internal audit and control applications. Also, the relegation of governance frameworks in cyber security can cause a reduction of awareness and understanding of cyber risks in enterprises (Deloitte, 2019, pp. 6, 10). Unfortunately, both macro environment which includes a legislative structure with international standards and micro perspective which covers codes of ethics with corporate management principles are being left behind by momentum and complexity of the technological advancements which make the governance frameworks difficult to sustain because of their unpredictable social impacts for how to take action and behave in cyber security practices. Especially, cyber security applications, which turn around the governance aspect, are predominantly related to code of ethics and corporate management principles which hold a critical role to provide the safety of IT assets' CIA triad. So, the functions of cyber security professionals have been being altered in a multifaceted fashion with novel technical developments as guiding the lawyers by acknowledging them what the risks can come out with these advancements to

support their role while the regulations and standards are being arranged to track the adequate governance frameworks (Vallor & Rewak, 2018, pp. 3, 4). For example, tangible inputs are being switched by virtual entries through technological improvements as cloud-based environments which are developed on software as a service (SaaS) fabric that is able to enhance the speed of business processes in enterprises. On the flip side, the system applications which are being developed for such kinds of cloud-based platforms require constant internet connections with the authentication of user names, passwords, and transmission of sensitive data. So, these kinds of virtual ecosystems, which give soar to need for steady network accessibility, can be affected heavily by cyber risks because of the software layers which are sensitive to vulnerabilities in Transmission Control Protocol/Internet Protocol (TCP/IP) (Gupta, Agrawal, & Wang, 2018, pp. 34, 35, 36). Hence, the governance models should be resilient and adaptable in terms of underpinning the cyber security stance of an organization according to the technical breakthroughs that have effects on the transformation of business activities.

Consequently, to be able to sustain governance activities in an enterprise, the definition of organizational roles and responsibilities should be ensured in terms of laying out the cyber security plans and frameworks for overseeing the performance of protection systems through the allocation of resources and authorities to accountable personnel staffs who have access to the governing board. Therefore, participation of employees is required on time for sharing solid and sensible information which are related to cyber threats and vulnerabilities with internal and external shareholders that include private and public authorities to improve defense posture, limit losses, enhance organizational awareness, and learning. Informing about technical cases, such as threats and breach evidence to receive how insecurities were exploited, enables enterprises to keep up their defenses timely and control contemporary and nascent methods which are being used by adversaries (European Central Bank (ECB), 2016, pp. 1, 3).

2.3.2. Risk controls and assessments in cyber security

Due to the definition of ISO 31000, risk can be discussed as the effects of vagueness while the organizations are trying to reach their objectives. In case, what the impact of uncertainty can be as such an organization will be corrupted by malware. Extraordinarily, while the dependency of organizations on information and digital systems is raising, the controls of potential risk factors in the business environment are varying and

complicating. Therefore, understanding the definition and assessment of cyber security risks allows the organizations to measure their effects on the part of ERM. As a matter of fact, the organizations need to adopt a strategy as making investments to risk management techniques, tools, and mindset for minimization of cyber risks by taking decisions which are adequate with their business continuity plans, corporate culture, management, and governance structure (Humphreys, 2016, pp. 4, 5).

Correspondingly, the capability of a cyber security framework in an organization can be measured and evaluated as a cornerstone by searching for the capacity of controlling and managing the risks which result from threats that can exploit vulnerabilities in cyber assets with having impacts as damages and losses to the organization. Therefore, cyber risks can be shown as a function of the existence likelihood of threats and their effects on the organizations. For instance, a distributed denial of service (DDoS) attack is a kind of threat that can affect organizations by exploiting a vulnerability if there is no existing system for balancing to load of data sources from the Internet. In such this case, the risk can be determined as the combination of the occurrence possibility of a DDoS attack and its impact on organizations. Correspondingly, organizations need to control their risk landscapes in the context of topographic maps for demonstrating surface features with valuations of their cyber assets and perception of their vulnerabilities. In essence, risk management is all related to how the organizations mitigate their financial losses, avoid regulatory punishments, and temper damages to their firm images and reputations. However, the quantitative valuation of intangible assets which are placed in cyberspace is a challenging task. Therefore, the results of cyber attacks to organizations can be displayed as the cost of plunged brand images and reputations in non-current assets item of financial statements which is a guide to demonstrate intangible assets such as goodwill, license, registered trademarks, or intellectual property in balance sheets (Schreider, Building Effective Cybersecurity Programs: A Security Manager's Handbook, 2017, pp. 41, 42).

Table 2.6. *General Risk Types Which Should be Overviewed Regularly by Enterprises' Managements* **(Schreider, Building Effective Cybersecurity Programs: A Security Manager's Handbook, 2017, p. 43)**

Risk Category	Audit and Control
Compliance	Contractual Agreements
	Global Data Protection Requirements
	Violation of Laws or Regulations
	-Cyber Security
	-Data Breach
	-Data Privacy
Financial	Macroeconomic Risks
	Fraud or Corruption
	Financial Misappropriations
Operational	Cyber Attack
	Data Theft
	Disruption of Production Lines and Supply Chain
	Disruption to Utilities
	Inefficient Use of Resources, Increasing Business Costs
	Loss of Key Personnel
	Physical Property Damage or Disruption
	Product Counterfeiting
Strategic	Competition for Skilled Talent
	Loss of Intellectual Property and Confidential Information
	Loss of Trust and Organization Commitment
	Negative Impacts on Reputation
	Poor Business Decisions or Weak Governance

Particularly, organizations need to be aware of the operational side of risk classes in terms of constructing their cyber security infrastructures and programs. Also, the management parts of enterprises must control and consider the other risk fields on an ongoing basis to provide company-scale risk controls and assessments. Although, having an in-depth understanding of cyber risks is required to significantly focus on the operational risks from the CISO perspective. Therefore, operational risk scores which are mainly computed through the evaluation of variables that were shown in the table also designate the capability of an organization in cyber risk management. In practice, cyber risk assessments support the solution offerings of governance and compliance-related complexities which are performed through inspecting the adequacy of controls in cyber

security processes and management versus generally accepted standards and frameworks to define the risk scores (Schreider, Building Effective Cybersecurity Programs: A Security Manager's Handbook, 2017, p. 44).

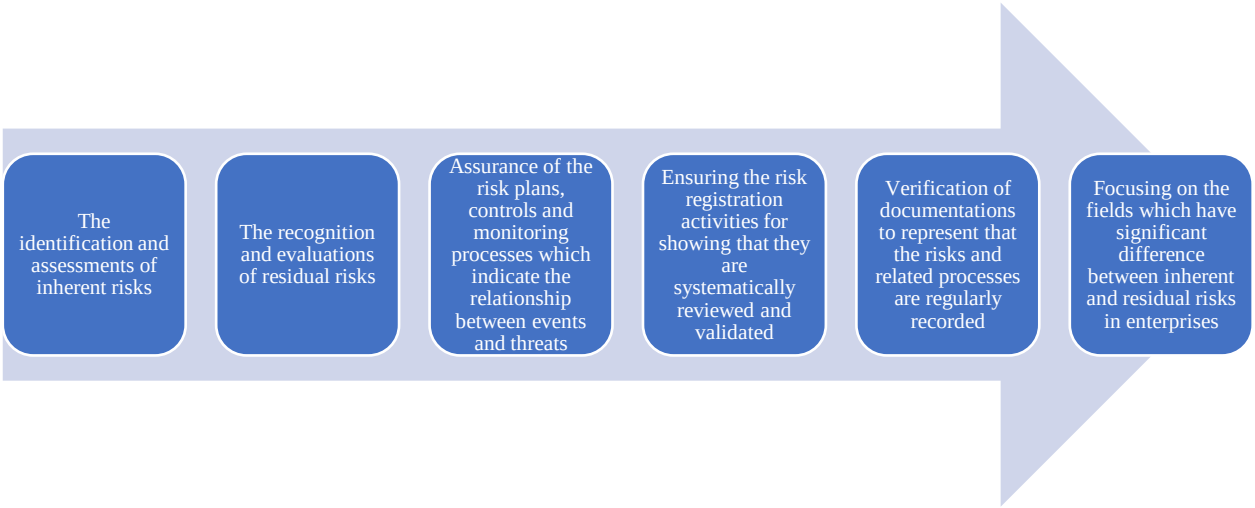


Figure 2.35. *The Major Determinants for Internal Auditors to Develop a Risk-Based Internal Audit Plan*

The examinations and performance measurements of the organizations' risk management systems in cyber security infrastructures can be provided by the applications of risk and control self-assessments (RCSA). Fundamentally, the utilization of RCSA initiates with the presumption which can be proposed as the range of control is significantly extensive as well as the momentum of the change is so boundless, so the sufficient capability of expertise level knowledge is needed for all of the employees who fulfill the specified works in order to assure the overall and appropriate assessments of control systems. Correspondingly, the sufficiency, professional capability, and expertise status of auditors may not be adequate lonely for the entire assessments of all the control systems which also cover the cyber security management structures, therefore the control systems have to need efforts, knowledge, and comprehension of each and every staff of the enterprise to make practices of RCSA (Zain, 2019, p. 16).

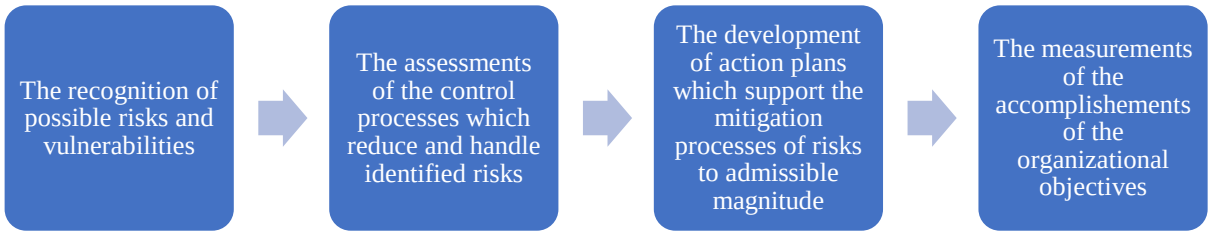


Figure 2.36. *RCSA Application Stages*

The practices of the RCSA program provide;

- Enhancement of organizational understanding in risk control processes
- Development of codes of ethics through the escalation of organizational awareness
- Implementation of a systematic approach for the proactive risk control mechanism
- Promotion of the collaboration and interaction between employees with continuous improvement approaches
- Empowerment of the employees by enhancing their authority and responsibilities (Zain, 2019, p. 16)

Particularly, robotic process automation (RPA) is being used in enterprises to systematize risk control activities through software applications that can perform customary cyber security functions such as classifying transactions, utilizing data, launching actions, and providing communication in the system. However, RPA is not capable of self-tutoring and reproducing the human sense or judgment as reasoning, comprehending, or thinking which are needed to make analyses and develop strategies. Machine learning, artificial intelligence, and natural language processing are being started to inject into RPA platforms for enhancement of their cognitive abilities by the organizations which aware of their weaknesses. Hence, there are enhanced RPA programs with a novel way of technologies which can be utilized by the enterprises to classify, record, transmit and protect the data-related assets via scanning and alerting the failures, threats, and cyber risks. From the point of audit, improvement of process performance and reduction of error rate and cost factors can be achieved efficiently by taking RPA in place for the routine functions of risk control. The annual global robotics survey of Deloitte UK which was issued in the 2017 report proves that RPA meets the expectations of organizations according to the multiple criteria which are defined as compliance enhancement, increased quality, improvement in productivity, and cost minimization respectively by ninety-two percent, ninety percent, eighty-six percent and fifty-nine percent. As a result, RPA platforms can assist the internal audit teams in the standardization of the processes with the reduction of defect rate and improvement of the quality. Especially, RPA can support the second line of defense role of internal audit which covers compliance-related operations through reducing the human engagement as routine or additional monitoring processes, so internal audit staff can perform strategic

tasks by saving their time with the support of RPA's integrated manner to risk management (Deloitte, 2019, pp. 5, 6, 18).

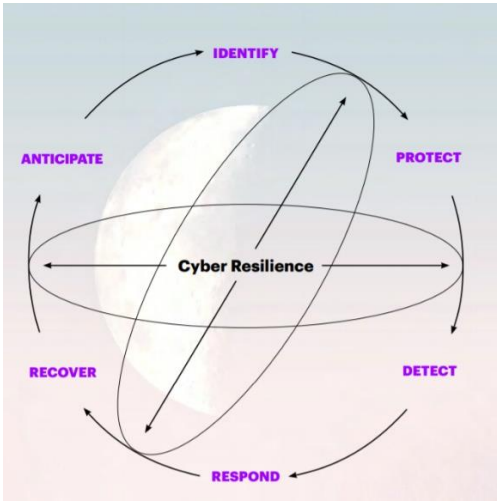


Figure 2.37. *Cyber Resilience Framework (Accenture, 2018, p. 5)*

From the point of the banking sector, the opportunities for innovation have been increasing by the growing potential of the internet and emerging technologies such as mobile and online banking services with the establishment of new applications and digital platforms which can mainly cause security risks in the cyber ecosystem. In short, the information dependency and IT intensity of business processes in the banking sector have been raising the occurrence probability of the intersection of vulnerabilities and threats simultaneously. Therefore, the cyber security framework should be combined with a risk management structure through organizational awareness, learning, and effective governance to detect and test the protection of the bank's assets (Greuning & Brajovic-Bratanovic, 2009, pp. 328, 329).

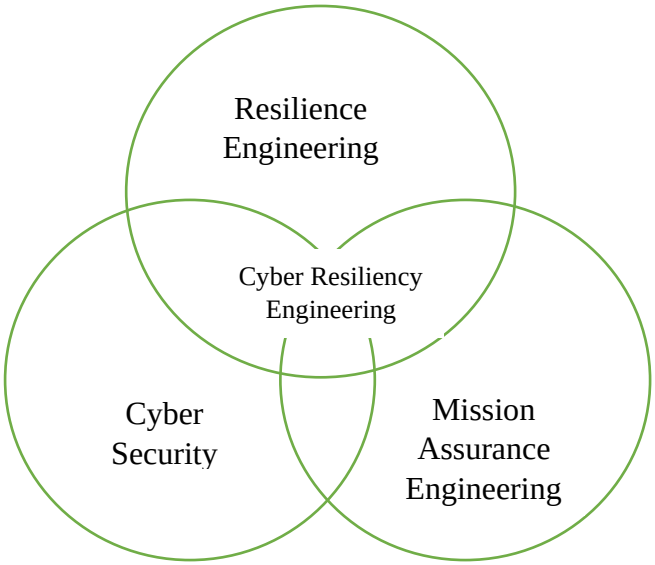


Figure 2.38. *Key Elements for the Cyber Resiliency Engineering Framework (Bodeau & Graubart, 2011, p. 13)*

In essence, the security of IT assets in a bank must be provided by the anticipation of cyber threats through a proactive manner not reacting when unexpected events occur. Accordingly, the cyber resiliency engineering model, which is the synthesis of resilience engineering, cyber security, and mission assurance engineering, can be applied to support the risk management framework of a bank for breaking the limitations of singular risk assessments. In this sense, the settlement of four steps of resilience engineering as anticipate, withstand, recover and adapt can be integrated with cyber security which has functions in pointing threats and mission assurance engineering which provides mission as enterprise systems engineering for handling the advanced persistent threats instantly with the adaptation of process tiers in the NIST risk control structure (Bodeau & Graubart, 2011, pp. 13, 14). Organizations should correlate cyber security risks with their business objectives, activities, missions internally, and essentials that arise from external conditions through legislation, policies, principles, and standards. As a result, the risk management approach of an enterprise in regard to cyber security risks must be compatible with financial, supply chain, marketing, production, or reputational risks which shouldn't increase defects or costs in alternative business functions. Because of this, system security engineers and risk management officers are charged with stating the potential risk effects of alternative solution proposals to evaluate those effects are in compliance with the organization's risk tolerance and risk management strategy by regularly informing the chief risk executives (Ross, Pillitteri, Graubart, Bodeau, & Mcquaid, 2019, p. 19).

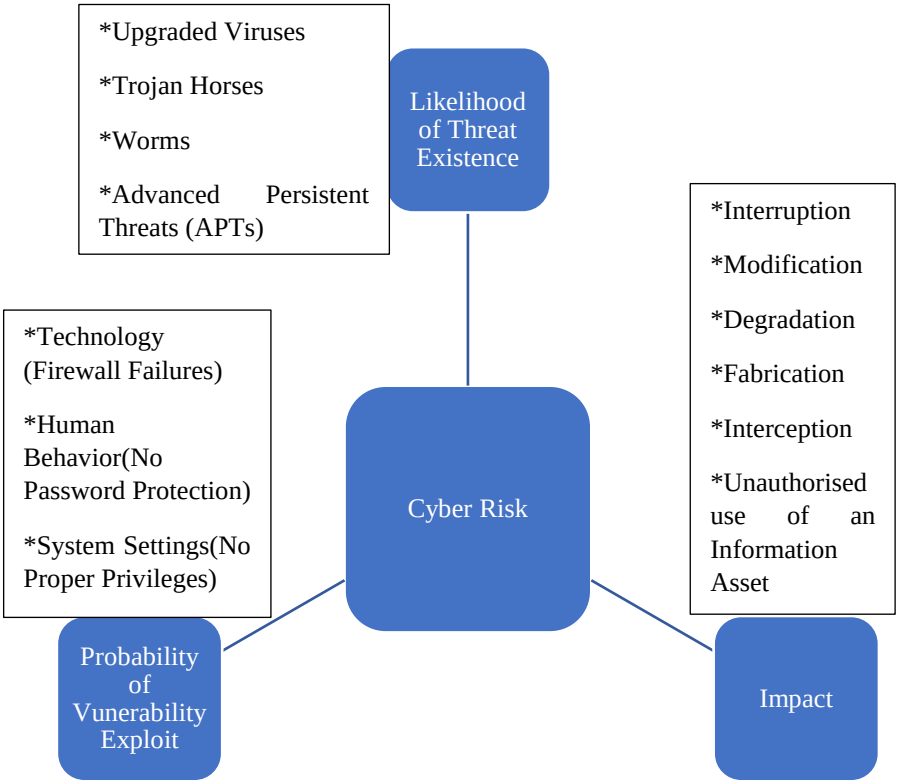


Figure 2.39. *Cyber Risk Emergence Cycle*

In summary, risk assessment which is performed to ensure adequate protection of information and cyber assets is considered as a core competency of cyber security management. Therefore, as an example, according to the ISO/IEC 27002:2005 (ISO 27002), the requirements of cyber security management frameworks or models must be described through the methodological assessments of cyber risks. Also, the expenditures of internal controls are needed to be balanced versus the business damages which result from security threats, vulnerabilities, and failures to understand annualized loss expectancy through risk assessments. In practice, ISO 27001 is consistent and applicable with other governance frameworks and models for measuring the validity of risk management approaches and activities in terms of compliance with internal controls and audits. Furthermore, ISO 27001 is framed and developed in line with the Payment Card Industry Data Security Standards (PCI DSS). Also, enterprises, that build and establish Information Security Management Systems (ISMS) in conformance with ISO 27001, are reviewed by an independent certification body and after this audit, if the organizations will be found in line with ISO guidelines, an authorized conformity certificate can be

issued to each of the enterprises (Calder & Watkins, Information Security Risk Management for ISO 27001/ISO 27002, 2019, pp. 11, 12).

Cyber risk assessments can be operated either through qualitative or quantitative techniques and tools. However, in general, three major factors of cyber risks are frequently described qualitatively through categorical variables with ordinal level, because, qualitative methods provide rapid and cost-effective routes to measure and evaluate risks in ISMS. In practice, qualitative risk considerations which are based on judgmental approaches can be performed by three main methodologies as Delphi technique, scenarios analyses, and decision trees. Delphi technique can be used for soft problems which are related to strategic decision taking and forecasting. The main objective is to reach a data-oriented consensus about a subject by getting the opinions of the set of experts through intensified series of questionnaires which are applied at a minimum in two rounds. In practice, the Delphi methodology covers four key conditions as anonymity, iteration, controlled feedback, and the collection of group responses such as general agreement. From the point of risk assessment in cyber security, the Delphi method can be feasible to understand the general perception of threats, their targets, and their effects on enterprises. On the other hand, the scenario analyses can be proper for possible forthcoming events to define positive and negative outcomes of cyber risks through simulating alternative circumstances. Correspondingly, the main objective of this tool is to provide alternate scenarios for emerging and expected cyber attacks. In addition, qualitative information which supports decision-making in risk assessment can be gathered through the prediction of occurrence likelihoods and their impacts with the classification of accumulated data in ranges as low, medium, or high to diagnose cyber threats and security breaches. Semi-quantitative approaches which are composed of both qualitative and quantitative methodologies can be implemented like multi-criteria decision analysis (MCDA) and risk matrices. MCDA technique can be feasible for complexities that involve contradictory weighted factors. This method is put to work in the context of cyber risk assessments through the harmonization of technical information and judgmental knowledge. Risk matrixes can be used for graphical illustration of assessments which are fulfilled by taking into account the probabilities of the emergence of threats and their impacts on cyber assets. This tool can be useful for monitoring the cyber risks through visual indicators which can have the capability to model and represent the assets' urgency levels and vulnerabilities with threats and their impacts. Also, the risk

matrix technique can be classified respectively as quantitative, qualitative, or semi-quantitative, if the valuations of assessments are shown as numeric expressions through ratios and intervals, categorical terms, or both of them. In general, the application of quantitative methods in cyber risk assessments is performed through probabilistic models with graph-based tools with the aid of mathematical models and simulation (Sokri, 2019, pp. 468, 469).

The cyber security risk control and evaluation approaches of the enterprises can vary according to their sectors, business size, assets, data sources and types, risk profile, and organizational culture as well as their interrelations, correspondences, and third parties which have relative importance for the assessments of their respective structures to counter the cyber risks. Accordingly, identification and implementation of risk control elements, which are covered by security systems, corporate management principles, and training, are coordinated by governing parts of the organizations to provide optimal protection against cyber threats and vulnerabilities. In practice, the inherent cyber risks, which are arisen from the employees, business operations, information technology systems, and technical tools, should be assessed through the main function of an acting enterprise risk management (ERM). Also, the effectiveness and efficiency of risk controls must be identified and evaluated by the ERM mechanism which provides to converge inherent cyber risks to residual cyber risks for the feasible security of an organization. Risk mitigation can be ensured by controlling, sharing, or transferring the risks within the tolerance frontiers which are defined according to the organizational culture and corporate management principles (European Central Bank (ECB), 2016, pp. 1, 2).

2.3.3. Compliance matters in cyber security

In connection with the former explained reasons, the cyber security policies can not be charged to a specific part of an organization. Therefore, both active and passive participation of employees is required across the multiple departments in terms of developing a feasible policy framework that contains not only micro elements of the organization but also the macro-environment conditions such as regulations, industry standards, economic, political, technological, social and cultural risks. Correspondingly, an applicable cyber security infrastructure should improve organizational culture which has the capability to overcome compliance-related issues that can be existed because of the changing situations in international standards and governmental legislations.

However, disputes between organizational policies and macro environment conditions can cause ineffective interaction amid governance and risk management activities. Therefore, in the beginning, organizational requirements can be defined through the adaptation of risk culture in favor of ensuring the compliance between cyber security framework which is being used in an organization and the regulatory environment that is being affected by national policies and international institutes (Venkatraman, 2011, p. 10).

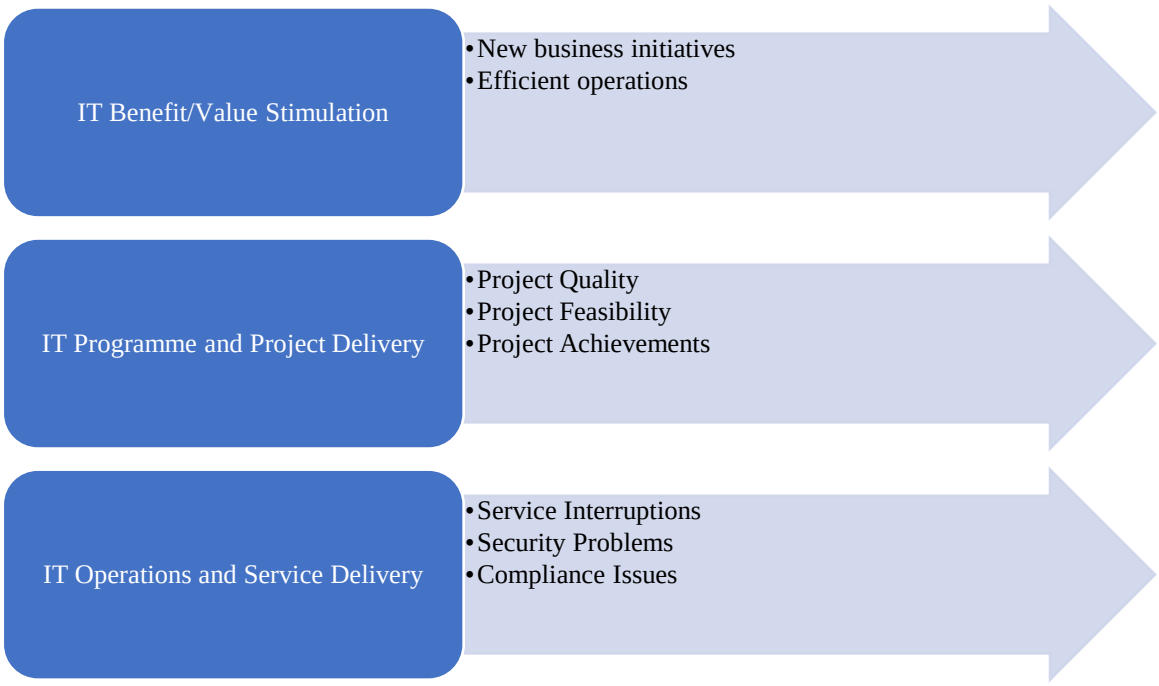


Figure 2.40. *IT Risk Categories (ISACA, 2009, p. 7)*

The assurance of adequate protection of the CIA triad of corporate data is a central liability of the enterprises in terms of providing trustworthiness to the business partners, suppliers, investors, stakeholders, internal and external customers (Smedinghoff, 2008, p. 29). On the other hand, governmental attempts for the protection of critical infrastructure alter against each of the countries on the globe. In practice, national policies relative to providing security of critical infrastructure should be arranged through dialogue and information sharing ways with taking the assistance of the mutual efforts of both public and private sectors. For an instance, NIST is a kind of nonpartisan civil agency inside the U.S. Commerce Department which has a major mission to establish a framework for promoting information systems security by searching and guiding the enterprises for the identification of the vulnerabilities along with developing measurement metrics and standards. As a matter of fact, the examinations of the technical

design and functioning of cyber security plans, policies, and procedures are required for measuring how the business processes are being operated and executed in compliance with these parameters. Therefore, the validation of a cyber security framework in an enterprise can be scaled on a regular basis through the assessments of compliance-related metrics which depend on organizational adapted standards and governing legislation. As a result, organizations need to prove that the information, which they are receiving, keeping, processing, and sharing, is secure by taking approvals from internationally recognized associations and their governments for assuring that their cyber security frameworks are legitimate. So, to manage this cycle, enterprises have to implement systems, technologies, and supportive services which will have a core function to evaluate and control the compliance associated instabilities. In connection with this situation, internal and external audits can be used to offset the compliance between cyber security frameworks which are performed in an enterprise and regulatory environment. Feasibly, no matter which audit type is being engaged, the processes, which are being utilized for showing at which level an organization's cyber security efforts are being achieved in compliance with standards and regulations, begin with internally made assessments (Westby, 2004, p. 237).

Figure 2.41. *Internal Audit Role in Cyber Security Framework*

Fundamentally, internal audits have major roles in cyber security frameworks for providing an independent review of risk management activities through the analyses of

the capability of internal controls with making the inspections of the state of compliance to laws and standards. In the context of the cyber security audit, the competence and effectiveness of control mechanisms should be evaluated proactively with taking the support of both the information technology department and the board of directors. In essence, auditors' main goal in cyber security examinations is to understand that the capacity level of practices which takes place in providing the optimal assurance of critical assets is adequate with internationally accepted guidelines and policies. Correspondingly, the suggestions of the National Association of Shareholder&Consumer Attorneys (NASCAT) show that the verification of cyber security frameworks which are worked in process in organizations is needed for conformance of the validity of internal controls, assurance of the implementation of priorities that are required for enterprise asset protection and ascertaining that the qualified personnel is in line to surmount with varying degree of cyber threats, risks, and incidents. Especially, as the nature of active changing conditions in the cyber environment and related regulations, continual, periodic staff education and coaching are necessary to provide maximum efficiency of internal audit functions. Moreover, regular audits can be expanded and adapted to explore the capabilities of intrusion detections and patch management activities in terms of reviewing and promoting the effectiveness of cyber security infrastructure for virtual private networks which are performed to catalyze the data-relevant processes in public and private enterprises. Although the preliminary structure of network systems may be observed as thoroughly safe, regular internal audits are still essential for exploring the security flaws and breaches will naturally occur as a result of system improvements, architecture transformations, or fresh protection requirements. Therefore, the security of IT systems can not be ensured entirely without the conduct of periodic audits. Likewise, the frequency period of internal audits can be specified relative to the inherent risks and dependency on IT systems. Similarly, in assumption, if an enterprise has business functions that are being operated and coordinated heavily depending on IT systems through digitally connected data servers and network structures, can counter cyber risks steadily, so that the internal audit frequency can rise. In common sense, an average entity should make the evaluations of risks at least annually and subsequently build an audit plan based on that reviews according to the advice of the National Association of State Auditors, Comptrollers, and Treasurers (NASACT). In the current state, automated audit mechanisms and compliance systems can be used with a critical security baseline that

provides instant alerts of any variation or anomaly from standard or accepted business processes and practices. So, assessment tools that are enhanced with automation can support the organizational culture by contributing to extended awareness in the understanding of cyber risks through the verification of security controls' effectiveness. Although, putting automated assessment tools into action is not solely enough, furthermore the involvement of capable cyber security professionals is required to achieve the entire protection of IT systems (Westby, 2004, p. 241).

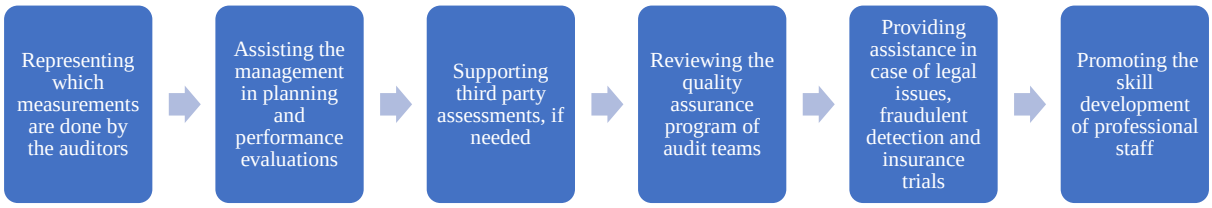


Figure 2.42. *The Documentation Functions of Cyber Security Audit (ISACA, 2021, pp. 5, 6, 7, 8, 9)*

The records of audit activities that are performed and the evidence that endorses the findings and suggestions of the auditor are provided by the documents of the cyber security audit. The potential utilization of such a documentation system is summarized in the figure above.

Especially, the financial sector, which is composed of banks, insurance enterprises, advisory firms, and intermediaries with their interconnection in the international business environment, has a strategic role to keep and protect the data of clients to sustain their operations and interaction. Each kind of cyber attack can affect the financial industry and legislative part of the sector. Therefore, the enterprises, which are standing their business activities in the financial industry, should work in coordination and collaboration with governing and regulatory bodies through devising their corporate management principles, strategies, and cyber security frameworks placed on business volume, risk perception, and organizational culture (Walker, Gramlich, Bitar, & Fardnia, 2020, pp. 409, 410). According to the 2020 Data Breach Investigations Report of Verizon, 63% of the attack

vectors in the finance industry are being launched by external actors which are being financially encouraged for acquiring the data to convert them into money. On the other hand, 18% of the attacks are being conducted by internal actors who are monetarily motivated as well as 9% percent of the attacks are being covered by unclassified personal errors. The finance sector is a major target for adversaries because of the data assets which are collected from the customers. The research which was made by Verizon presents that this sector keeps its position to be the leading open space for organized criminal factors. Especially, web application assaults, which are the principal reason for most breaches, are in contention with the rate of miscellaneous errors. In detail, the top three causes of the vulnerabilities in the finance industry that reflect 81% of breaches are formed by web applications, miscellaneous errors, and everything else (Verizon, 2020, p. 52). Everything else is used by Verizon as a term to describe the attack type which does not belong to the nine attack classes that have been being used by Verizon since 2014 as crimeware, cyber espionage, denial of service, insider and privilege misuse, miscellaneous errors, payment card skimmers, point of sale intrusions, physical theft and loss and web applications attacks (Morrow, 2020). As a result, it is a part of trouble when an organization recognizes that the mistakes of its employees charge approximately the same amount of breaches as external actors who are targeting the data assets of a bank or an insurance company. Thus, one crux of the matter is showing particularly that the weakest part of organizations in the finance sector is their workforce. Accordingly, the key control precautions, which are being utilized in terms of managing the cyber risks, are the implementation of a security awareness and training program (CSC 17), boundary defense (CSC 12), and secure configurations (CSC 5, CSC 11) (Verizon, 2020, pp. 52, 53).

3. RESEARCH DESIGN

First, internal audit has conventionally functioned on the operational, technical, tactical, and strategical levels of business processes. However, the classical approaches which consider internal audit as simply an assurance activity of internal controls are not sufficient in cyber security management, because of the unpredictable and chaotic nature of cyberspace. The legislative frameworks, standards, and national policies have been dynamically shifting through emerging technologies and cyber risks and therefore internal auditors' objectives should be modified to these latest conditions to be capable of understanding how the cyber security governance frameworks must adapt to variations

in information systems. Correspondingly, there is a lack of common perception on which internal audit functions have effects on cyber security governance, so the Delphi method which is a type of group interview by using the combined opinion of experts can assist in reaching the main objective of the thesis subject as to where the knowledge is imperfect. Mainly, the Delphi technique is used for formulating expert-based data collections which are provided via questionnaires to develop a cardinal consensus refers to the main problematics of the thesis. Also, panel members and questions are selected according to the relevant subcategories of the thesis study which are defined as internal audit, cyber security, governance, and the banking sector of Turkey.

In general, Delphi is a research methodology that can be utilized for establishing forecasts about cases if quantitative predictive tools are not alone capable as available information provides limited evidence and confirmation in terms of defining the probabilities. In other words, it can be useful for cases where there is a lack of consensus or an incomplete form of knowledge is available. Also, Delphi presents a format of remote communication in which the common opinion of panel experts are collected by both open-ended questions and questionnaires that are distributed via mail, fax or e-mail. Particularly, an iterative research methodology is applied for getting summarized opinions and feedbacks with the responses of relevant experts through the recursive series of written questionnaires that can be called rounds until the agreement in an opinion has been reached.

Two research scientists, whose names are Olaf Helmer and Norman Dalkey, who had been working for the Rand Corporation had developed the Delphi survey technique in the 1950s. Their goal was to form a tool for estimating the upcoming events by operating a sequence of concentrated questionnaires rotated with feedback of controlled responses. Typically, open-ended questions are implemented in the first series of the Delphi technique, because these are needed for the researcher to perceive and present the intense, profound, and particularized points and content of the research question which is being worked on (Custer, Scarcella, & Stewart, 1999).

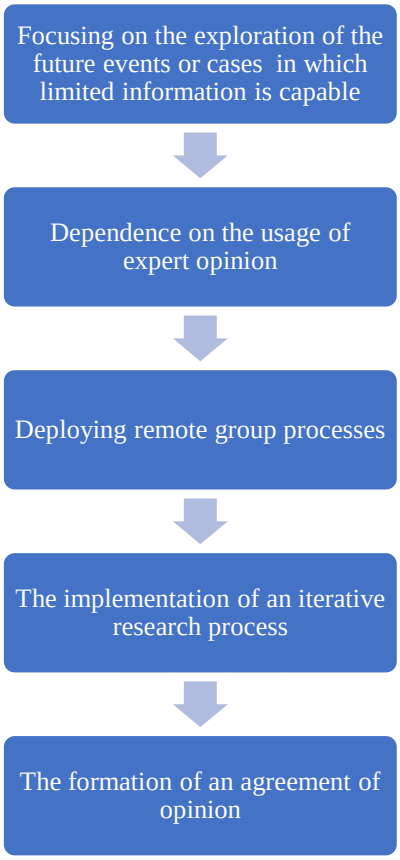


Figure 3.1. *The Research Conditions of the Delphi Technique (Amos & Pearse, 2011, pp. 103, 104, 106, 107, 108)*

The research subject of the thesis study concentrates on future essentialities rather than current effects as well as a relatively small amount of scientific knowledge is known about these future requirements. Also, while the Delphi methodology is able to point to these future recommendations, most of the other research techniques don't focus on them, as they have a tendency to address past, historical or present facts. The research question of the thesis which is determined to investigate the internal audit role in cyber security governance by using the banking sector of Turkey as the population is a qualitative matter that can be analyzed via exploration and description of multiple opinions which can be shown as the major intention of the researcher to eliminate preconceived information about the subject. Of course, this does not mean that every generated idea for the open-ended subquestions will be accepted, so the main goal is for using this approach is to understand the common consensus of experts which is needed to be achieved for the next plays of the researcher through the iterations of data collection stage.

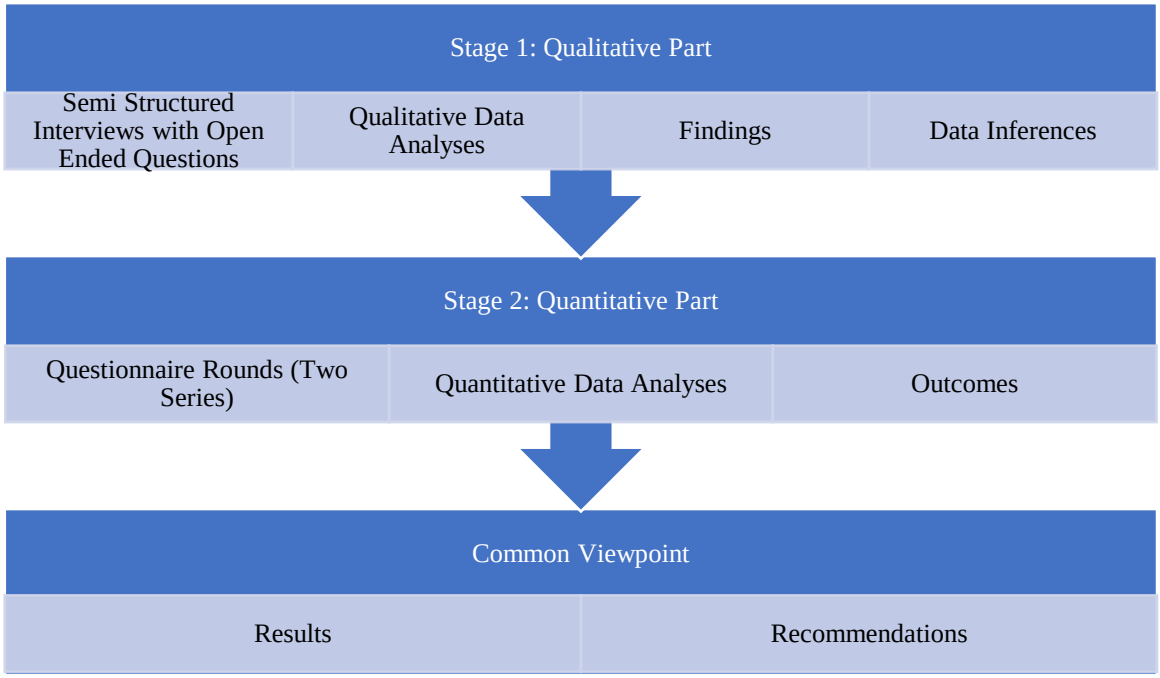


Figure 3.2. *The Research Plan of Thesis Study*

The Delphi technique is applied as mixed methods research from the perspectives of both qualitative and quantitative approaches to perceive the general agreements of the panel participants. In this regard, for the first phase, the outputs of the qualitative data collection process are transformed into meaningful data, and then for the second phase, questionnaires are designed according to the outcomes of the qualitative part which are used as inputs for the second stage that is carried out quantitatively with the design of questionnaires by sending and taking feedback from the panel experts in two rounds.

3.1. Expression of Thesis Proposal and Subject

From the beginning, in 2019 the rate of global economic growth is approximately 5.82 times greater than in the 1960s when mainframe computers were rolled out according to the gross domestic product (GDP) time-series data of the World Bank (The World Bank, 2020). Certainly, the effects of technological developments on this indicator can not be neglected according to the contribution of industrialized countries, which have high tech investment strategies and policies, to world economic growth is relatively forty-two percent. This proportion demonstrates that the improvement of efficiency and reduction of costs to increase productivity and effectiveness through compliance with quality specifications and expectations of customers depend on digital transformation

besides economic, cultural, political, and social norms of nations. Correspondingly, the technological transformations accompany chaotic conditions, threats, and risks such as criminal and fraudulent acts along with their positive impacts and advantages to national and organizational productivity. Therefore, the illegitimate activities and behaviors which depend on information technology systems should be deeply investigated to overcome the problematics in trust mechanisms between countries and enterprises for sustainable development of the international business interactions. Especially, misusing of computerized systems and technological devices such as committing fraud, theft of sensitive data and hacking acts differs from conventional criminal acts relative to where and how the crime attempts are realized because such these activities are emerged by attackers in an intangible location is called cyberspace by using of software codes, viruses, and networks. Therefore, the issues related to cybercrime acts and security structures should be explored and analyzed by synthesizing engineering and management disciplines by taking the guidance of the legislative framework. Briefly, this thesis study is proposed for researching and understanding the internal audit operations in cyber security governance both conceptually and applicatively with deep investigations of literature reviews and observations of cases in the Turkish banking sector by the Delphi technique. Particularly, the subject of this study is based on both technical and legislative points which cover and discuss how the internal audit is being functioned in cyber security governance mechanisms of enterprises to perceive not only national but also global norms for existing and emerging cyber threats by considering the requirements of industry standards and organizational culture for assisting the banking sector of Turkey in establishing effective interaction between audit, control and governance processes of cyber security.

3.2. The Goals and Problem Structuring of Thesis Research

Technical breakthroughs in information flowing systems through mobile data utilities and voice over internet protocol (VOIP) provide the individuals and enterprises to interact with each other in cyberspace. Fundamentally, the interactive relations between people, enterprises, sectors, and nations frame the international business environment which arises in digital platforms by taking the support of hardware, software, data, and web servers to realize the investment, supply chain, purchasing, marketing, and risk management activities. However, attacks against information technology and

communication systems have possible harmful effects on international business relations and activities. Therefore, the functions of cyber security in the continuous improvement of information systems should be enhanced and supported by international regulatory associations and governing bodies that have the authority to build up principles, sectoral standards, laws, and frameworks for auditing and controlling the business relations between nations and organizations. In essence, the protection of critical and sensitive tangible and intangible assets is mandatory for enterprises to sustain their business activities. In this regard, the harmonization of internal audit, cyber security, and control processes should be provided by board managements with appropriate governance structures and practices which vary according to the industry and region of organizations. Thus, the main goal of this thesis study is determined as to discover the objectives of an internal audit on cyber security governance by focusing on the banking sector of Turkey with the support of conceptual fabric and research studies that were applied through factual data. Correspondingly, the legislative, strategical, organizational, and technical issues of information management systems in enterprises are challenging factors for establishing cyber security governance. In this context, the motivation of the researcher is to analyze the internal audit functions by taking into account those conflicts between the functioning of information systems and cyber security governance. Particularly, this research study covers not only technical parameters which concentrate on key measurements for the development of risk management practices and protection mechanisms in cyberspace by constructing and proposing blueprints and standards to verify the tools and methodologies which are used in security systems but also the regulatory associations and organizational structures that demonstrate how an enterprise is compatible to international legislations in investigation and prosecution of cybercrime through which ways are being applied in enterprises to prevent, audit, control and counteract the cyber attacks for the safeguarding of critical information assets (Gercke, 2012).

In general, scientific methods which are feasible and recommended for complicated cases in the real world perform effectively in the lower levels of complications, although have challenges to overcome the upper level of complexities. In this regard, the designation of the subproblems relative to the main subject of the thesis through system science can support to clarify the results and recommendations of the research study which involves comprehensive data collection and analyses with the Delphi technique.

From the standpoint of typology, the problematic cases can be classified as hard and soft problems. In explanation, hard problems can be defined clearly and figured out with positivistic techniques such as operations research and decision science like maximization of the profits or minimization of the operating costs. However, defining the internal audit processes on cyber security governance is a soft problem and is not amenable to offer solutions by pure positivistic methods, because each description of sub-problems related to the subject is relatively varied depending on the observers' perception which is formed by personal and judgmental opinions. Therefore, the main problem of the thesis subject can not be solved uniquely with precise and stable outputs as one size fits all equation but explained through qualitative observations and analyses like the issues as how to define the vision of an enterprise or culture of an organization (Degtiar, 2009, pp. 138, 142, 143, 144, 145, 146). As a result, the Delphi technique, which is heavily used in qualitative research methods, is agreed on to figure out this fuzziness through the accumulation of significant data from both academics of universities and business experts of the Turkish Banking Sector who are going to contribute to the open-ended questions session with semi-structured interviews and questionnaire rounds as panelists.

3.3. The Intention of Researcher and Importance of Study

As mentioned in the theoretical part of the thesis, no matter how an organization has talented intellectual capital or advanced technological tools to scan and mitigate cyber risks, there are always possibilities that can cause vulnerabilities and skeptical attitudes, especially because of human conduct and lack of ethical perception. Therefore, internal audit functions which ensure strategically objective reviews are certainly required that perform as an extra set of eyes, ears, legs, and hands for the enterprises which aim to build effective cyber security governance frameworks with continuous improvement philosophy. Correspondingly, the researcher intends to understand how the cyber security governance approaches and models of the sampled banks are being formed and evaluated. Also, the researcher desires to determine in which way they are performing their cyber security risk assessments with their workforce or by outsourcing this service from independent audit firms which work as third parties and are being used by BRSA as well. In essence, the regulations will be taken into consideration as bases which were published in the official journal by BRSA on 15 March 2020, including internal audit functions to show the banks how they should systematize and execute their internal audit operations.

Likewise, ISO is used as an origin fundamental for the sampled banks in terms of investigating their current cyber security governance framework to demonstrate how their structure is being performed in compliance with the standards. Thus, in summary, the researcher intends to propose a cyber security governance model which covers the internal audit framework for the Turkish banks to provide them a road map and performable strategy for their information technology and communication systems. Within the context of the researcher's goal, the Turkish banking sector will be clustered and progressively, the ethical norms, which are framed by IIA, are going to be employed as the control variables in order to understand how the internal audit functions are being performed and sustained in cyber security management of these bunched organizations. The open-ended questions, which are going to be transmitted to the panelists of the research study, are outlined in the following order;

- Which processes do internal auditors take responsibility for in your organization within the cyber security services?
- How do you explain the competency of internal audit functions which are being conducted as part of cyber security?
- How is the interaction mechanism between internal audit and management board formed for the issues which are related to cyber security?
- How do the confidentiality, integrity, and availability concepts remind you within the context of your organization?
- What does the code of ethics recall you of when the internal audit and cyber security principles are discussed simultaneously?
- How are the ethical rules defined inside your organization, in terms of the methodologies which are tracked by the internal auditors for performing the role of internal audit in cyber security processes?
- How does the internal audit take part in cyber security management relative to the monitoring activities of the legislative framework and international standards?

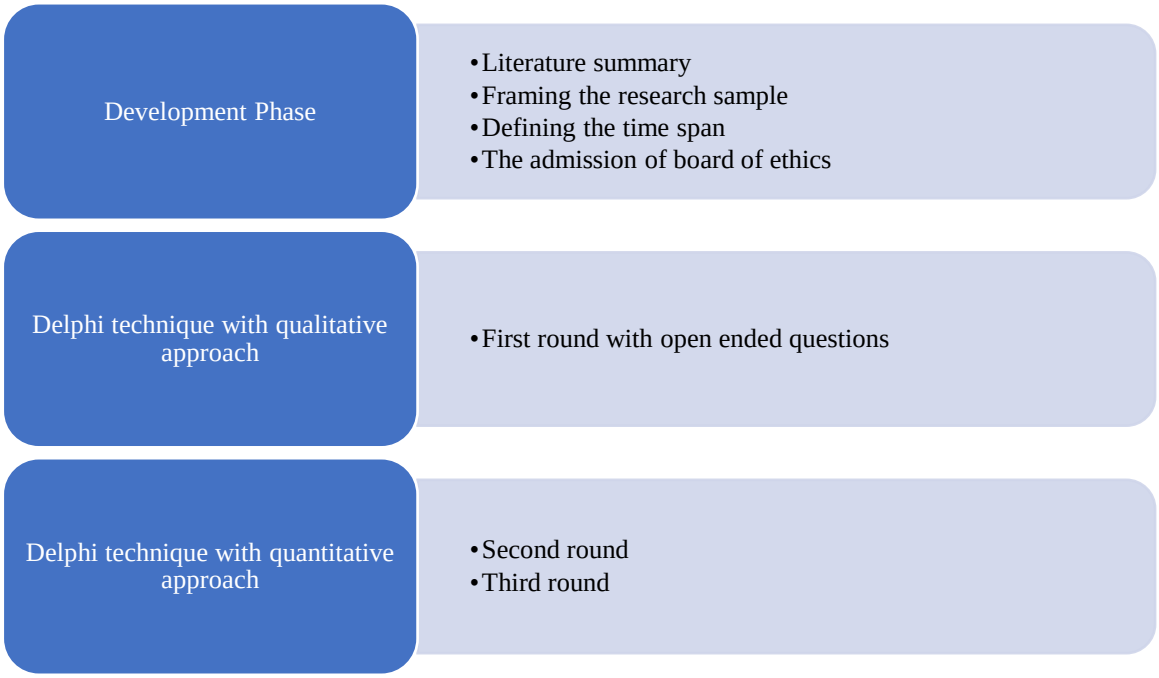


Figure 3.3. *The Stages of Future Proof Research Formation*

As well, this research study diverges from its peers, because of its subject, application methodology, sample, conceptual model, and variables, as a result, the researcher aims to bring novelties, original, and valuable perspectives to the literature by well documented deeply investigations of cyber security field which mostly contains technical subjects and internal audit which covers social and human aspects thoroughly. The study is being prepared through the usage of both epistemic knowledge and applicative researches to find out optimal solution recommendations for the main problem. As a result, this thesis study uniquely holds importance that makes contributions to both internal audit and information technology literature by presenting functional methods which can enhance the viewpoints of not only the academicians but also the practitioners for their assessments of multifactorial parameters in cyber security, internal audit, control, banking, governance, risk, and compliance.

3.4. Background Studies of Research Subject

The research studies related to the thesis topic, which covers the subjects as internal audit, cyber security governance, code of ethics, risk management, internal control, banking, and Delphi technique, are examined for trying to understand both from the perspective of the research title and method. Therefore, in this part of the thesis study, the researcher designs the literature check in two parts as research topic and application

technique. At first, in parallel with this strategy, the previous researches are examined according to the conceptual framework and fundamentals of the thesis title which are relative to the major elements that are defined as internal audit, cyber security governance, internal control, cyber risks, code of ethics, organizational culture and behavior, corporate management principles, legislative environment, cyber risk management, and cyber security standards.

The research studies, which are analyzed and connected with the theme of the thesis, are shown in order as follows;

Von Solms (2005) investigated the differences between the operational and compliance management of information security by proposing the philosophy of information technology governance and information security governance should be discussed as two discrete parts of information security management (Solms, 2005).

Von Solms (2005) made a study to present the existing interdependent practices of COBIT and ISO 17799 by showing the harmony of the two frameworks with mapping (Solms B. v., 2005).

Brown and Nasuti (2005) tried to observe the effects of SOX of 2002 on the information technology governance in terms of understanding the internal control evaluations of the IT security governance operations and systems (Brown & Nasuti, 2005).

Weidenmier and Ramamoorti (2006) presented the research options for the information technology relevant to internal audit functions through three governance-related processes which are driven by the risk assessment role of internal audit, detecting assurance, and adequacy of assessments in cyber security (Weidenmier & Ramamoorti, 2006).

Ula, Ismail, and Sidek (2011) proposed a general framework in terms of demonstrating the governance processes of the information security structures in banking operations (Ula, Ismail, & Sidek, 2011).

Steinbart, Raschke, Gal, and Dilla (2012) introduced exploratory research to discover the interaction between internal audit and information security by framing the key factors which have effects on both concepts.

Lanz (2014) researched the role of audit committees and certified public accountants (CPA) in cyber security governance for projecting how the tools that they are carrying out, are transforming through technology-based applications. Therefore, the cyber security field should be discussed with the entire business units of an organization,

because if an organization takes cybersecurity-related issues into consideration with just an IT perspective, cyber security governance can not be performed holistically and feasibly.

Karabacak, Yıldırım, and Baykal (2016) discussed the regulatory practices for arranging the cyber security of critical infrastructures in Turkey by executing the study with three steps for the recognition of suitable approaches in regulations.

Carataş, Cerasela, and Gheorghiu (2017) offered a research study for finding out the major function of the internal audit in evaluations of cyber security processes by presenting that governing with management can support the role of internal audit to assure the establishment of adaptive capacity and business continuity. Also, they claimed in their study that cyber resiliency plans are needed to develop with the guidance of internal audit for the implementation of cyber security culture (Carataş & Gabriela, 2017).

Ojeka, Be-Caleb, and Ekpe (2017) investigated the relationship between cyber security and the performance of audit trustees in the Nigerian Banking sector by functioning the independent variables as autonomy, technological and financial expertise of audit teams. As a result, they observed that there is no significant relationship between variables. Therefore the audit committees' general features which are defined as having an objective and independent manner with technological and financial knowledge, are not mostly related to cyber security according to the data that was gathered from the framed sample of the Nigerian Banking sector.

Sabillon, Serra-Ruiz, Cavaller, and Cano (2017) made a study by introducing an audit model for cyber security operations to evaluate and validate the audit processes for assuring preventive controls.

Islam, Farah, and Stafford (2018) explored the factors which are affiliated with cyber security from the viewpoint of the internal audit by concentrating on the functions of the chief audit executive, chief risk officer, and audit committee. As result, they found that internal audit is heavily connected with governance, risk, and control functions in cyber security controls (Islam, Farah, & Stafford, 2018).

Steinbart, Raschke, Gal, and Dilla (2018) examined the internal audit role from the perspective of validation of information security operations with proposing the outcome as the performance of internal audit has effects on the reduction of the internal control weaknesses in information security-related activities (Steinbart, Raschke, Gal, & Dilla, 2018).

Kahyaoğlu and Çalıyurt (2018) investigated how the cyber security systems and internal audit processes can interface with each other by analyzing cyber security assurance models for defining key issues and weak points in the internal audit and risk management operations.

Jamison, Morris, and Wilkinson (2018) made a research study about how the internal audit staff can adapt their skillsets to cyber security (Kahyaoğlu & Çalıyurt, 2018).

Stafford, Deitz, and Yaojie (2018) designed a study to examine the serving of information security policies and audit processes according to the definitions of the malicious acts by applying a qualitative approach with the examination of the auditors' opinions for explaining how the behaviors of technology users should be standardized and in which approaches auditors can effectively support management to handle the cybersecurity-related problems.

Islam and Lee (2018) introduced research that covers the internal auditors' competencies and cyber security audit operations by proposing a research model to determine the internal audit role in information technology, governance, risk, and compliance.

Shamsuddin, Adam, Adnan, Madzlan, and Yasin (2018) developed a research study in terms of demonstrating the effectiveness of the internal audit role in cyber security management operations in banking corporations of Malaysia. As a result, the three factors, which were identified as internal auditors' awareness, organizational policy, and risk management corresponding to cybersecurity-related activities, have significant effects on the effectiveness of internal audit processes.

Öztürk (2018) designed a research study to represent the entire mechanism of cyber security audit steps by taking the inner and outer causes into consideration. As a result, a structural diagram was developed to illustrate the consolidated processes of the cyber security audit.

Seliomoğlu and Saldı (2019) developed an explanatory study for showing that the general methods are being used in cyber risk measurement efforts by integrating the internal audit functions in information technology controls. Due to this, the internal audit methods, tools, and operations have been affected by technological tendencies and so, the internal controllers have to gain further technical knowledge and competencies to execute IT-related audits and also they must particularly take responsibility for the cyber risk assessment processes.

Table 3.1. *The Research Studies are Related with Thematic Part of Thesis*

Author and Year	Article Name	Subject and Scope	Findings
S.H.(Basie) Von Solms (2005)	Information Security Governance-Compliance Management vs Operational Management	Computers and Security, Discussing the differences between information security operational management and compliance management	The two aspects of information security management which are considered as good information security governance and information technology governance should be installed separately from each other.
William Brown and Frank Nasuti (2005)	Sarbanes-Oxley and Enterprise Security: IT Governance-What It Takes to Get the Job Done	Information Systems Security, Many sections of the Sarbanes Oxley Act(SOX) of 2002 have direct effects on-information technology governance.	SOX can be used for investigating the internal control assessments of the IT security governance structures and processes.
Basie Von Solms (2005)	Information Security Governance: COBIT or ISO 17799 or both?	Computers and Security, Investigating the existence and complementary applications of COBIT and ISO 17799.	The Synchronization of the two frameworks was provided by mapping.
Marcia L. Weidenmier and Sridhar Ramamoorti (2006)	Research Opportunities in Information Technology and Internal Auditing	Information Systems, Presenting research alternatives in the field of information technology in connection with internal audit role.	The research questions, which are related to IT and internal audit, were developed for three governance regarding activities which are executed by risk evaluation function of internal audit, controlling assurance, and compliance of assessments in security and privacy.
Munirul Ula, Zuraini bt Ismail and Zailani Mohamed Sidek (2011)	A Framework for the Governance of Information Security in Banking System	Information Assurance and Cybersecurity, Recommending a framework for the governance of the information security structures in banking mechanism.	The framework which was proposed in the research represents a general model for information security governance to banks.
Paul John Steinbart, Roby L. Raschke, Graham Gal and William N. Dilla (2012)	The Relationship between Internal Audit and Information Security: An Exploratory Investigation	Accounting Information Systems, Presenting an examination for the relationship between internal audit role and information security.	An exploratory model was recommended in order to frame factors that have effects on the interaction between internal audit and information security processes.
Joel Lanz (2014)	Cybersecurity Governance: The Role of Audit	Technology, Exploring the functions of CPAs and audit teams on the navigation of	Cyber security is an important business concern which affects the overall organization's value-

	Committee and the CPA	cyber risks which are faced by all sizes of enterprises.	added activities, financial performance, external and internal governance approaches.
Bilge Karabacak, Sevgi Özkan Yıldırım and Nazife Baykal (2016)	Regulatory Approaches for Cyber Security of Critical Infrastructures: The Case of Turkey	Computer Law and Security Review, Presenting-a three-step research methodology for the identification of the appropriate approaches to protect the critical infrastructures of Turkey.	In general, the critical infrastructure of Turkey is executed in compliance with the regulatory environment.
Maria Alina Carataş, Spatariu Elena Cerasela and Gabriela Gheorghiu (2017)	Internal Audit Role in Cybersecurity	Economic Sciences, Internal audit has a major role in the assessments of cyber security processes through working with management for providing the development of adaptive capacity and business continuity.	Organizations need to establish cyber resilience plans by taking the support of internal audit functions for implementing a cyber security culture to enhance their employees' perception and awareness.
Stephen A. Ojeka, Egbide Be-Caleb and Edara-Obong Inyang Ekpe (2017)	Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness	Management and Marketing, Evaluating the relationship between cyber security and effectiveness of audit committee by applying independence, technological and financial expertise of audit committee as independent variables.	A significant relationship was not found between dependent and independent variables, so audit committees are not enabled to ensure controls in cyber security functions of the Nigerian banking sector.
Md. Shariful Islam, Nusrat Farah and Thomas F. Stafford (2018)	Factors Associated with Security/Cybersecurity Audit by Internal Audit Function: An International Study	Managerial Auditing, Exploring the factors which are associated with-cybersecurity from the internal audit perspective by focusing on the roles of chief audit executive, chief risk officer, and audit committee.	The expansion of cybersecurity audits through the internal audit function is positively associated with the capability of the audit role that refers to governance, risk, and control.
Paul John Steinbart, Roby L. Raschke, Graham Gal and William N. Dilla(2018)	The Influence of a Good Relationship between the Internal Audit and Information Security Functions on Information Security Outcomes	Accounting, Organizations, and Society, Examining the internal audit role on assurance of information security activities and how to enhance these processes.	The quality of this interaction has a positive impact on the quantity of reported internal control weaknesses and noncompliance cases, as well as the amount of security breaches which were detected and cause financial loss.
Sezer Bozkuş Kahyaoğlu and Kıymet	Cyber Security Assurance Process	Managerial Auditing, Analyzing cyber security assurance models for the identification of key	A conceptual model is proposed to demonstrate how the cyber security and internal audit

Çalıyurt (2018)	from Internal Audit Perspective	problematics and weaknesses in the internal audit and risk management functions.	processes can collaborate with each other.
John Jamison, Lucas Morris, and Christopher Wilkinson (2018)	The Future of Cybersecurity in Internal Audit	Cybersecurity, Examining the solution proposals for the question of how the internal audit committees can adapt their competencies to cyber security.	Audit professionals need to establish their perceptions through the development of creative approaches for the attraction of talents in the fields of data security principles and cyber security frameworks.
Thomas Stafford, George Deitz, and Yaojie Li (2018)	The Role of Internal Audit and User Training in Information Security Policy Compliance	Managerial Auditing, Investigating the functions of information security policies and audit through the definitions of the malicious behaviors in organizations.	A qualitative case approach was applied by examining the opinions of the auditors to explain how the behaviors of technology users should be and in which ways auditors can optimally support management to overcome the cyber security issues.
MD. Shariful Islam and Jaeung Lee (2018)	Internal Audit Function Competencies and Cybersecurity Audit	Accounting Information Systems, Examining the role of internal audit in cybersecurity risk management.	A research model was proposed in terms of explaining the internal audit functions in information technology, governance, risk, compliance, and communication capabilities.
Amanuddin Shamsuddin, Muhammad Afi Adam, Saiful Ariff Adnan, Siti Nur Izzati Madzlan and Yasreen Mohd Yasin (2018)	The Effectiveness of Internal Audit Functions in Managing Cybersecurity in Malaysia's Banking Institutions	Industrial Management, Exploring the internal audit effectiveness in cybersecurity management operations of banking organizations in Malaysia.	The three factors which are identified as awareness of internal auditors, organizational policy, and risk management relative to cybersecurity have significant effects on internal audit effectiveness in cyber security management processes of the Malaysian banking sector.
Mahmut Sami Öztürk (2018)	Cyber Attacks, Cyber Security Audits, and an Integrated Audit Model Proposal	Accounting and Tax Applications, Demonstrating the entire system of cyber security control in a framework with an integrated approach.	A flow chart was introduced by explaining the complete process from the planning phase to the assurance and reporting stages.
Seval Kardeş Selimoğlu and Mustafa Hakan Saldı (2019)	The Role of Internal Audit: Analysis, Mapping, and Assessment of Cyber Risks in Enterprises	Accounting and Auditing Review, Presenting the theoretical techniques which are utilized for analyzing, charting, and evaluating cyber risks.	The role of internal audit has been modified through emerging technological trends and this situation brings new competency fields for internal controllers to execute their tasks in cyber risk management and

			information technology audit operations.

The research studies, which are scanned in reference to the practice of research methodology, are explained axiomatically as below;

Dalkey (1967) had made the research study, which was named “Delphi” by constructing the structure of the Delphi methodology in terms of describing the processing mechanism of the Delphi technique. As a result, the Delphi methodology had been recommended for the long-term predictions by refining the personal judgments of panel members with the statistical computations of the classified data that are extracted from a questionnaire.

Helmer-Hirchberg (1967) had introduced a research study with the title of “Analysis of the Future, The Delphi Method” to explain the basic patterns of Delphi. Consequently, the agreement had been reached as the Delphi technique can be used for converting personal ideas to long-term forecasting.

Kurubacak (2007) presented a research study which is cited as “Identify Research Priorities and Needs for Mobile Learning Technologies in Open and Distance Education: Delphi Study”. In this research, the Delphi technique was operated for showing the categorization of research options in mobile learning technologies.

Kurubacak (2011) performed a research study that is named “E-learning for Pluralism: The Culture of E-Learning in Building a Knowledge Society” for defining and classifying the forthcoming edges in e-learning with the application of the Delphi technique. In this study, the Delphi method was utilized in three rounds to collect data from the professionals.

Omari, Barnes, and Pitman (2012) established a research study which is titled “An Exploratory Study into Audit Challenges in IT Governance: A Delphi Approach” to observe the IT governance of the Australian public industry by using the Delphi survey.

Vasarheyli, Lombardi, and Bloch (2014) developed a research study that is named “The Future of Audit: A Modified Delphi Approach” for considering the audit profession’s future with the modified Delphi technique via gathering the raw data from the experts.

Davidson and Hasledalen (2014) formed a research study which is marked “Cyber Threats to Online Education: A Delphi Study” for examining the cyber risks which can harm the online learning systems through the practice of the classical Delphi method.

Smits and Hillegersberg (2015) designed a research study that is displayed as “IT Governance Maturity: Developing a Maturity Model Using the Delphi Method” to develop an IT governance system that includes formational processes and soft parts of the organizations.

Karabacak, Yıldırım, and Baykal (2016) prepared a research study, which is built as “Regulatory Approaches for Cyber Security of Critical Infrastructures: The Case of Turkey”, by applying grounded theory for qualitative analyses and Delphi study for group discussion.

Haqaf and Koyuncu (2018) revealed a research study, that is named “Understanding Key Skills for Information Security Managers” to explore the key skills needed for the information security managers with the usage of the Delphi technique. Project and risk management were defined as two main fields according to the sixteen skills that were identified as a result of the application of the Delphi method.

Altınpulluk, Kesim, and Kurubacak (2020) generated a research study which is named “Usability of Augmented Reality in Open and Distance Learning Systems: A Qualitative Delphi Study” for discovering the effectiveness of augmented reality in remote education through the Delphi study. Delphi technique was used in three rounds by using a qualitative questionnaire at first which includes twenty-one open-ended questions as the primary data collection tool and after that, in the second round, the processed data was used to engage a six-point Likert scale questionnaire and finally, in the third round, the transformed data from second round was reached from the findings were analyzed and another six-point Likert scale questionnaire was performed.

Table 3.2. *The Research Studies are Related with Methodology of Thesis*

Author and Year	Article Name	Subject and Scope	Findings
Norman Crolee Dalkey(1967)	Delphi	An outline of the Delphi methodology had been explained.	Delphi method had been introduced for the long-term forecasting through filtering the opinions of a category of advisers or experts with the statistical calculations of the group responses.
Olaf Helmer-Hirchberg(1967)	Analysis of the Future, The Delphi Method	Delphi methodology had been described with basic principles.	Delphi technique could be used to attempt the processing of informed intuitional judgments for long-term predictions.

Gülsün Kurubacak (2007)	Identify Research Priorities and Needs for Mobile Learning Technologies in Open and Distance Education: A Delphi Study	The Delphi technique was applied to demonstrate the identification, categorization, and classification of the research opportunities for mobile learning technologies in open and distance education.	Briefly, public responsibility, management of online society, and specialists who are engaging in digital transformation are determined as the major research fields in the paper subject.
Gülsün Kurubacak (2011)	E-learning for Pluralism: The Culture of E-learning in Building a Knowledge Society	The main objective of this research was to determine and classify the upcoming forces and needs for e-learning.	Delphi method was used with three rounds for gathering data from twenty-eight e-learning experts who evaluated major problematics and criticisms in this subject.
Loai Al Omari, Paul Barnes, Grant Pitman(2012)	An Exploratory Study into Audit Challenges in IT Governance: A Delphi Approach	Examining the IT governance in the Australian public sector with an empirical approach by using the Delphi survey.	Ten major IT governance audit concerns were presented according to the Delphi study.
Miklos A. Vasarheyli, Danielle Lombardi, Rebecca Bloch(2014)	The Future of Audit: A Modified Delphi Approach	Discussing the future of the audit profession through modified Delphi technique with gathering the consensus of expert opinions which provide foresight in audit methods, standards, and mindsets.	Forecastings were proposed by the author for future functions of audit as database management, sampling, extensible markup language processing, and clustering.
Philip Davidson, Kenneth Hasledalen(2014)	Cyber Threats to Online Education: A Delphi Study	Investigation of the cyber threats and vulnerabilities, which could damage online learning systems by applying an e-Delphi survey with the classical design of Delphi methodology.	The leadership was noticed in terms of understanding the cyber security risks and their costs as a general solution.
Daniel Smits, Jos Van Hillegersberg(2015)	IT Governance Maturity: Developing a Maturity Model Using the Delphi Method	A description of developing an IT governance maturity model was proposed with both the hard parts which cover structural processes and soft elements that include organizational culture and behavior.	One maturity model was developed for the hard side of information technology governance, but the soft part requires more specific competencies for each focus field.
Bilge Karabacak, Sevgi Özkan	Regulatory Approaches	First, the critical infrastructures data of Turkey were analyzed	Particularly, the critical infrastructure employees of

Yıldırım, Nazife Baykal(2016)	for Cyber Security of Critical Infrastructures: The Case of Turkey	qualitatively with the grounded theory method, second, the Delphi survey was applied with six experts to derive regulations, and finally, a focus group interview was carried out.	Turkey which includes privately held contractors are mainly in favor of compliance.
Husam Haqaf, Murat Koyuncu(2018)	Understanding Key Skills for Information Security Managers	Investigation of the major capabilities required for the information security management role with the adoption of the Delphi technique.	Project and risk management were determined as two major categories from the sixteen skills that were accepted as the key classes for information security management by the implementation of the Delphi methodology.
Hakan Altınpulluk, Mehmet Kesim and Gülsün Kurubacak(2020)	The Usability of Augmented Reality in Open and Distance Learning Systems: A Qualitative Delphi Study	The primary goal of this research is to define the functionality of augmented reality in open and distance learning ecosystems in compliance with international design laws for predicting the outlook through taking the opinions of experts with Delphi methodology.	Delphi technique was carried out to fourteen experts with three rounds by using a qualitative questionnaire that covers open-ended questions as a primary data collection tool and a six-point Likert scale questionnaire as a secondary data gathering method.

No master or doctoral thesis has been found from the literature reviews of thesis research studies in Turkey which specifically cover both internal audit and cyber security subjects. Therefore, the literature analyses of the theses are made by focusing on each of the subjects separately and the research methodology of the thesis.

In general, the researchers, who particularly studied social sciences, highlighted the cybersecurity-related subjects through focusing on the regional parameters, national strategies, policy frameworks, critical infrastructure, and awareness.

Table 3.3. *The Thesis Studies that are Related to the Subject*

Author and Year	Thesis Type and Name	Subject and Scope	Findings
Bilge Karabacak (2015)	Doctoral Thesis, Developing and Verifying a set of Principles for the Cyber Security of the Critical	Public Administration, Proposing a model to evaluate the critical infrastructure capacity from the perspective of cyber security.	The intensity of privatization in critical infrastructures can significantly affect the national policies in the cyber security field and a well-framed and comprehensive set of legislations can be effective for Turkey.

	Infrastructures of Turkey		
Ahmet Bozgeyik (2018)	Doctoral Thesis, Analysis of Cyber Security Management Approaches in Medium and Large-Size Enterprises Operating at Gaziantep	Business Administration, Surveying to measure cyber security awareness of middle and large companies in Gaziantep.	The researcher showed that cyber security awareness of the enterprises in Gaziantep varies according to their size and demographic factors.
Volkan Göçoğlu (2018)	Doctoral Thesis, The Assessment of Turkey's Cyber Security Policies in the context of Public Policy Analysis	Public Administration, the connection between public policy and cyber security was analyzed to demonstrate the direction of national perception and critical infrastructure plans of Turkey.	The researcher stated that Turkey's public policies are in the initial phase and these are needed to be improved for the redesign of critical infrastructure through the support of educating the personnel for information systems.
Gülcihan Aydaner (2019)	Master Thesis, Measurement of the Impact of Social Engineering and Cyber Security Awareness of Young Consumers on Online Shopping Intentions	Business Administration, Surveying to measure the online shopping behavior of customers relative to social engineering and cyber security parameters.	The researcher proposed a model which depicts the relationship between social engineering activities and cyber security awareness in online shopping intentions of customers.
Ahmet Korkusuz (2020)	Master Thesis, Cyber Security and Cyber Risks in Institutions	Business Administration, Investigating strategies and major cyber attacks by comparing Turkey and the global landscape with the assessments of statistical data which are corresponded to cyber security.	The researcher claimed that countries have to improve their cyber security infrastructures through the usage of innovative risk control methods.

In common, the Delphi technique was used by researchers for the collection of data from field experts to cluster main factors in terms of framing root causes that are related to their thesis problems.

Table 3.4. *The Thesis Studies that are Related with Method*

Author and Year	Thesis Type and Name	Subject and Scope	Findings
Gül Yeşilçelebi (2019)	Doctoral Thesis, Creating Combined Assurance for the Integrated Reports: A Delphi Technique Investigation on the Awareness in Turkey	The goal of this study is to identify the assurance mechanism of the integrated reports by taking the judgments of the framed sample which was defined as auditors, academicians, and the institutions which are publishing integrated reports. In this study, a two-phase Delphi technique was applied.	The integrated assurance process criteria in consolidated reports were recommended due to the consensus of opinions that were taken from the research sample through the Delphi technique.
Hamza Yakar (2019)	Doctoral Thesis, Determination of the Climate Literacy Competencies at Secondary School Level by Delphi Technique	The main purpose of the study is to specify the abilities to improve secondary-level education curriculum relative to climate subjects.	The climate literature sufficiencies cover six major classes that were defined through the Delphi method as climate-associated terms, primary climate comprehension, regional and domestic climate awareness, the link between climate and life, capacities, and code of behaviors.
Burçin Turan Bektaş (2020)	Doctoral Thesis, A Scale Development Study to Determine Public Science Literacy: Delphi Technique	Reconceptualizing the design of science literature to build a novel framework for integrating intellectual values to improve the cultural perspective of Turkish society.	Delphi technique was applied for the determination of the features of science literated persons.

3.5. Structuring the Research Variables and Sample

According to the theoretical and applicative research studies and papers, the complexity of harmonizing governance, risk, and compliance mechanisms is being perceived as one of the main challenges in cyber security for chief executive officers (CEOs), chief risk officers (CROs), chief information officers (CIOs), chief information security officers (CISO) and auditors. Therefore, the relationship between these three elements is deeply investigated from the theoretical framework with factual research findings from the past studies in the conceptual part of the thesis. In essence, the pieces of evidence show that the interaction between GRC in cyber security is mainly performed under the full responsibility of board management with the guidance and support of the internal auditors and controllers. Also, within the context of cyber security governance, the findings of former surveys demonstrate that the governance frameworks and models which are designed by internationally accredited associations have a key role in providing the synchronization between internal audit and control. Therefore, proper governance frameworks or models can be preferred to improve the accordance between internal audit and control for the ongoing development of cyber security processes in enterprises. The internal audit's main goal is discussed in the theoretical part of the study as to oversight of the internal controls for validating the competency of risk management activities to ensure the full protection of information and cyber assets. As well, hypothetically, the internal audit may have a supportive function for guiding the board management in terms of the selection of an adequate governance framework that will be implemented in cyber security systems to catalyze the risk management activities that are performed by internal controls.

The purposeful sampling can be used no matter the way is going to be applied to qualitative research by allowing the researcher to intendedly pick informationally qualified and professionally experienced participants for specifically designed in-depth research studies. Patton claims that the validity of a qualitative study is predominantly related to the comprehensiveness of the participants' profile with examinations and analyses of the researcher rather than the research study's sample size (Conway, 2020, p. 7).

Additionally, the conceptual part of the thesis study adequately supports that the objectives of internal audit in cyber security governance are based on the code of ethics, the principles of corporate management, and the legal framework as the main variables

which can present an optimal route for designing the research model. Therefore, the sample of panelists' responses to the Delphi survey is going to be clustered according to these three factors for the breakdown of how the cyber security governance systems are being framed in the banks.

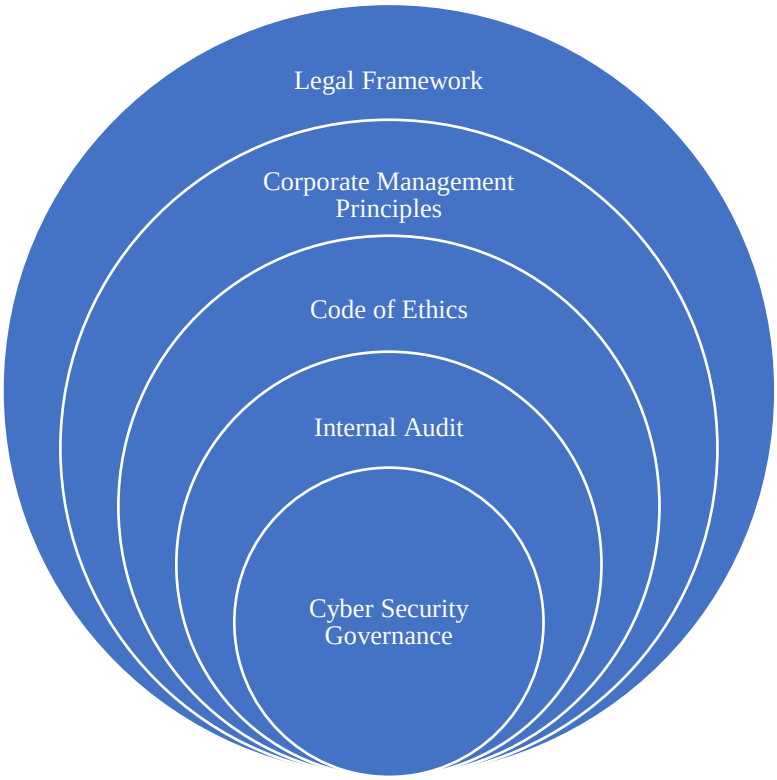


Figure 3.4. *The Multifactorial Variables in Research Model*

The functions of internal audit in cyber security governance are investigated relative to the factors which are framed as;

- The code of ethics
- Corporate management principles
- Legal framework

Especially, the diagnostics of the compound items of the research study are shown in the figure above for organizing the framework of relations between research parameters. Therefore, mainly, the internal audit functions in cyber security governance can be examined based on the codes of ethics which are assumed as a subset of corporate management principles and legal framework. According to this presumption, the simplification of the thesis goal is accomplished through structuring the code of ethics as

mediating variable to funnel the internal audit functions in cyber security governance for reducing the complexities.

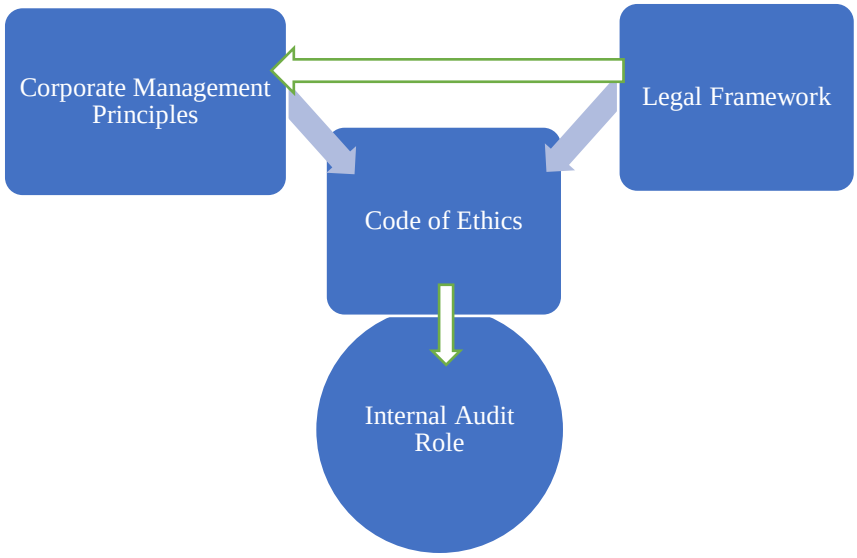


Figure 3.5. *Relational Demonstration of Research Variables*

Therefore, the set of ethical principles, which is based on 2110 coded governance functions of 2100 titled IIA performance standards, is selected as a control variable to constrain and narrow the research scope for more effectively and deeply investigating the internal audit operations in cyber security governance.

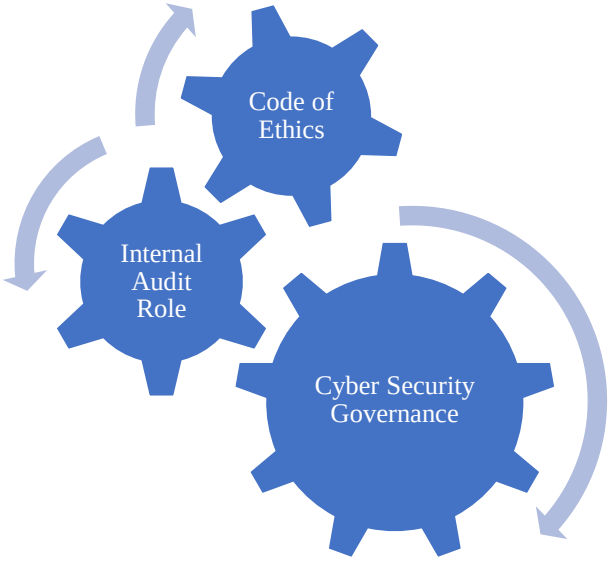


Figure 3.6. *Hypothetical Notation of Processing Mechanism for Organized Research Variables*

The research sample is framed as demonstrated in figure 3.7, according to the population of the thesis subject which is planned as the Turkish Banking industry. The

main objective of the sample of the thesis study which is defined is to better perceive the cybersecurity-related concerns and risks from the perspective of internal audit, because, presumably, deposit banks have extraordinarily many online and digital transactions because of their customer profile, in comparison with alternate ones.

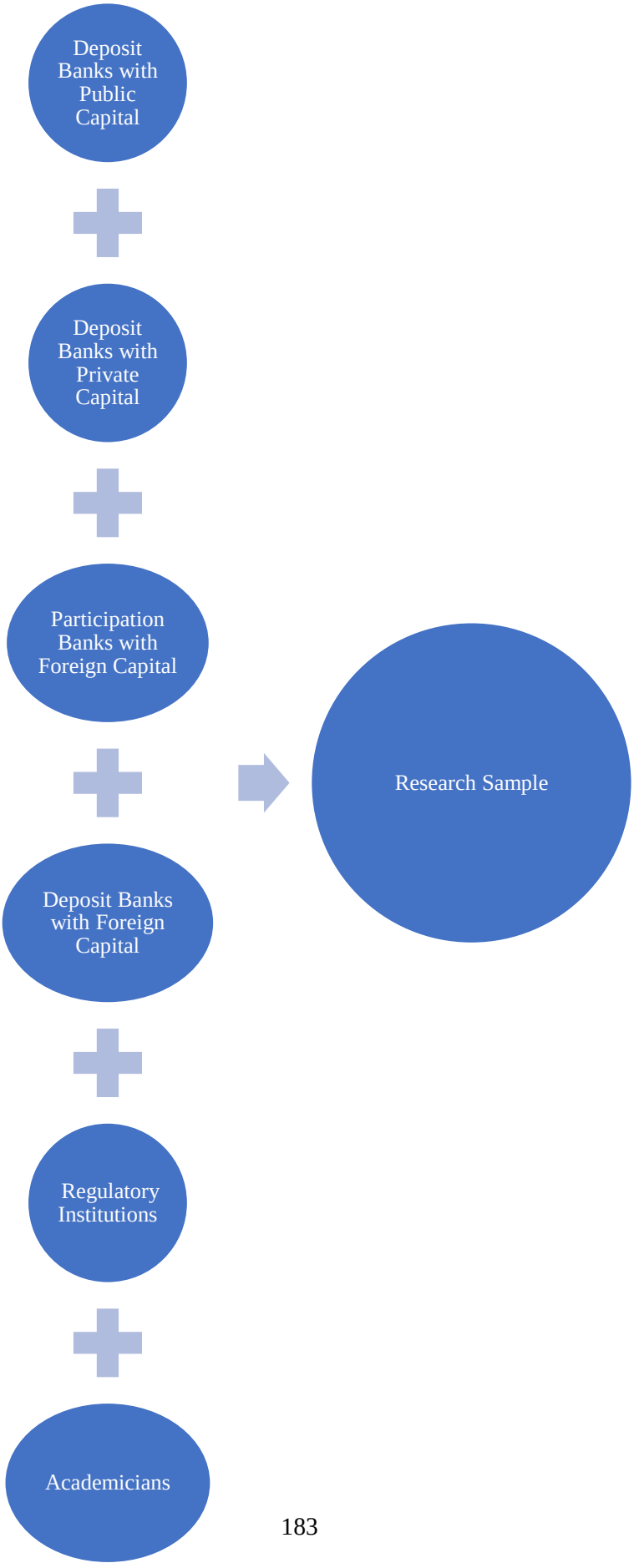

Deposit Banks with Public Capital
Deposit Banks with Private Capital
Participation Banks with Foreign Capital
Deposit Banks with Foreign Capital
Regulatory Institutions
Academicians
Research Sample

Figure 3.7. *Framed Research Sample*

3.6. Assumptions and Limitations

The researcher assumes that;

- The participants who attend the Delphi study are accepted as authorized and accredited professionals who have expert-level knowledge and experience about the research subject.
- The attendees, who participate in the Delphi survey, responded to the questions objectively and without any bias.
- The data, which are gathered by Delphi methodology, cover the control variables that are processed for understanding the common sense of the research sample.

The research study is limited with;

- The personal opinions and judgments of experts who take part in the Delphi study.
- Qualitative and quantitative data analyses through the Delphi technique.
- Independent research variables are framed as codes of ethics, corporate management principles, and legal framework in the governance system.
- The panelists, who accepted to participate in this study from the bank sample, are mostly performing their profession in cyber security, information technology, risk management, and internal audit-related fields.
- The panelists, who accepted to join this study as academics, have professional lecturing experience in universities with cyber security, internal audit, and ethics background.
- The panelists, who accepted to take part in this research from regulatory agencies, have the responsibility in establishing and controlling the legislations related to information systems, cyber security, and the banking sector.
- The data are collected in the period between 1 March 2021 and 31 December 2021.

3.7. Data Collection and Analyses

Predominantly, the mindsets of researchers in social and behavioral disciplines can be classified into three categories as;

- Quantitatively adapted standpoints, that are mainly based on positivist or postpositivist norms, provide computational data and analyses.

- Qualitatively focused on philosophies that are primarily derived from constructivism with its' paradigms that use narrational data and analyses.
- Both quantitatively and qualitatively built on ways of thinking within the bounds of realist patterns as mixed methods researches perspective (Tashakkori, Johnson, & Teddlie, 2020, p. 2).

In harmony with the problem of the thesis, exploratory sequential mixed methods research design is decided to carry on the data collection and analysis sections to fit with the Delphi technique. This research approach is being performed by firstly starting with the qualitative stage to explore the data of interviews by making analyses of the data as transforming the audiovisual and textual raw data into meaningful information for constructing the second stage which is going to be the quantitative part of the research. Principally, the qualitative stage can be used for modeling the tools and itemizing variables which guide the researcher in terms of following the quantitative step (Creswell, 2014, p. 16).

Especially, mixed methods research is applicable when the research design involves both the qualitative and quantitative approaches in the data collection and analyses part of the study. Similar to the research problem of the thesis study, mixed methods research is selected for collecting data and performing data analyses with the integration of both thematic and numerical data interpretation.

Therefore, in this research study, the Delphi technique is used as mixed-method research via designing the route map as at first, the set of open-ended questions is engaged as a qualitative data collection tool through the utilization of semi-structured interviews to perceive the personal opinions of the target panelists with the discussion documents and records, and after this operation, secondly, the acquired data from the conversations are analyzed with qualitative explorations and then transformed into questionnaires, which are considered as the application tools of quantitative research methodologies, are delivered by online to the framed sample in two rounds, and finally, the received data are interpreted through quantitative techniques for findings and recommendations part of the thesis study.

The semi-structured interviews are selected for the qualitative data collection part of the study because this method provides a range of alternatives by presenting an organized approach for the specified points which depends on the facts of the research by leaving blanks for the panel members to suggest new tenors to the study. Semi-structured interviews can be used as either the unique methodology in a research model or one of the various methods by providing multidimensionality with the design of questions to generate meaningful data. Fundamentally, semi-structured interviews can support the researchers by allowing them in developing open-ended questions before achieving interviewing operation by catching their attention to certain arguments to ensure that the execution of the interview is well focused and effectively performed within the time and budget constraints. Also, this technique can assist the researcher in the data analysis part by providing the evaluations of gathered replies much feasible to examine and compare. In practice, the researcher must be an active listener with avoid talking reflexively for conducting the semi-structured interview fairly. The researcher can get an objective opinion set of the participants by reaching perceptions for the particular subject or theory through the semi-structured interviews. Therefore, the researcher can mine deeply the main themes of the research problem by allowing the participants to widen their mindset with semi-structured interviews (Andrew, Pedersen, & McEvoy, 2011, pp. 100, 101, 102).

3.7.1. Delphi round one

In this stage, the semi-structured interviews are organized with panel members through video conferences, phone calls, and electronic mails by applying open-ended questions for collecting textual data. The data, which are gathered from panelists, are represented in appendices.

3.7.2. The analyses of the first round

The critical marks can be identified through the Pareto principle which provides a small number of essential causes that contribute to the complexity (Joiner Associates Incorporated, 1995, pp. 4, 16). Correspondingly, the Pareto charts are used as analytical and visual tools to specify the subplots of the thesis problem which are measured through the qualitative data that are collected with semi-structured interviews via open-ended questions in Delphi round one. Nvivo software is used for the classifications and analyses of the qualitative data in terms of defining the most emphasized fields which are going to be presented in Pareto charts. Briefly, the categories are tried to be shown with underlying reasons which are described with the usage of the Nvivo program by transforming them

into Pareto charts for analyzing how the responses of panelists are mostly concentrated, scattered, and plotted.

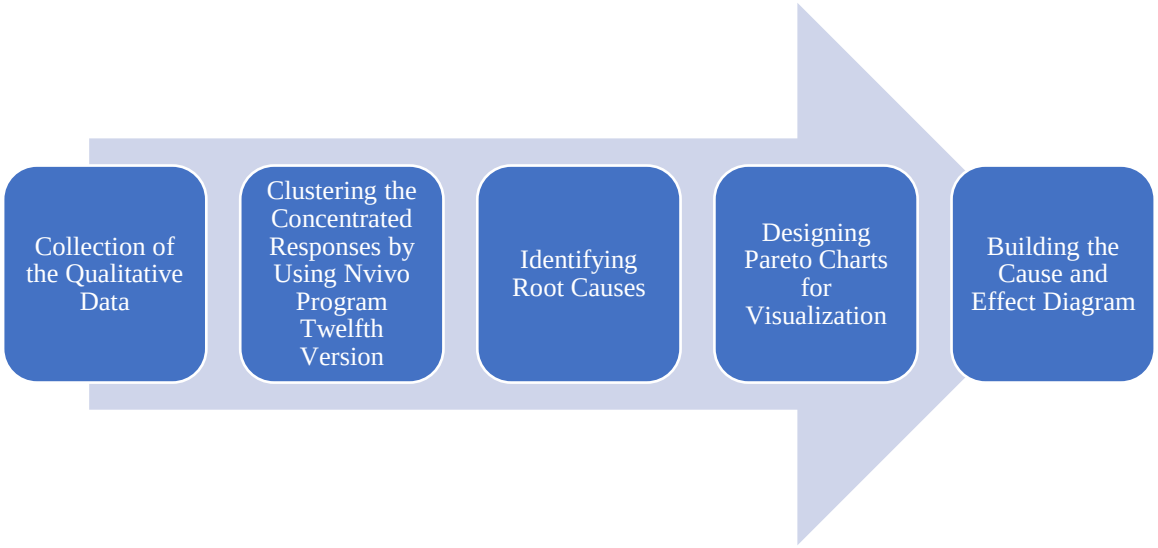


Figure 3.8. *Qualitative Data Analysis Plan for Delphi Round One*

The frequency distribution shows that control and compliance-related functions and reporting tasks are mostly focused on by the panelists as the main responsibilities of internal auditors. Especially, according to the responses of panelists, the internal audit teams have a role in auditing the validity of risk management activities by reporting the findings to upper management by assuring their compliance through monitoring and partially process development.

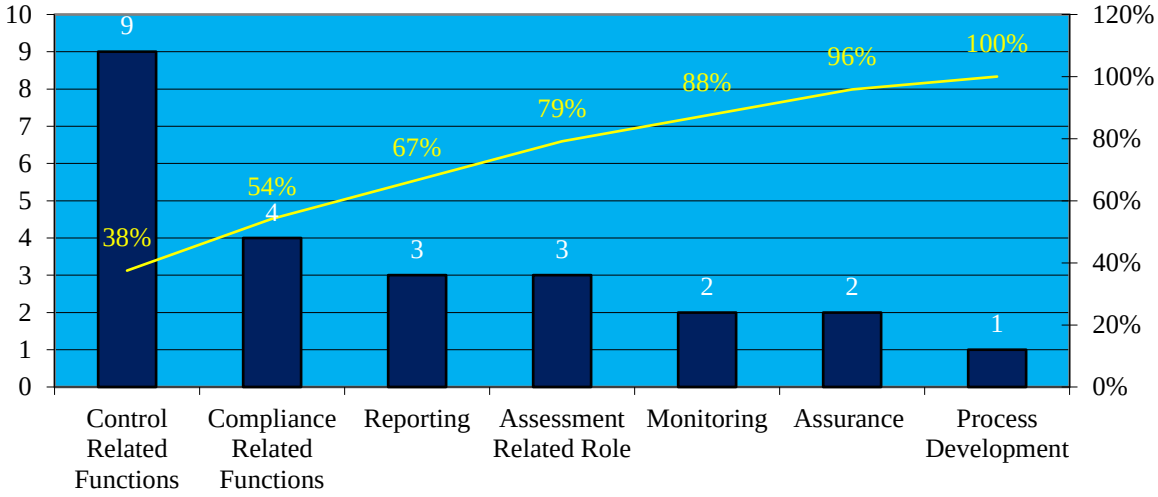


Figure 3.9. *Pareto Chart for the Responses to First Question of First Round*

The panelists emphasized that the internal auditors are mostly concentrating on controlling compliance which is related to local regulations and international policy

frameworks in accordance with their competencies. Also, they mentioned that the internal auditors partly have functions in technical controls, SWIFT audits, and detection of vulnerabilities. Correspondingly, a minority of the panelists expressed that their internal audit services are not as much as sufficient in terms of performing technical controls and discovering the vulnerabilities because of the scarcity in labor markets and higher turnover rates. Likewise, they remarked that the internal audit teams should be supported with technical training events and specialized certification programs to improve information security awareness.

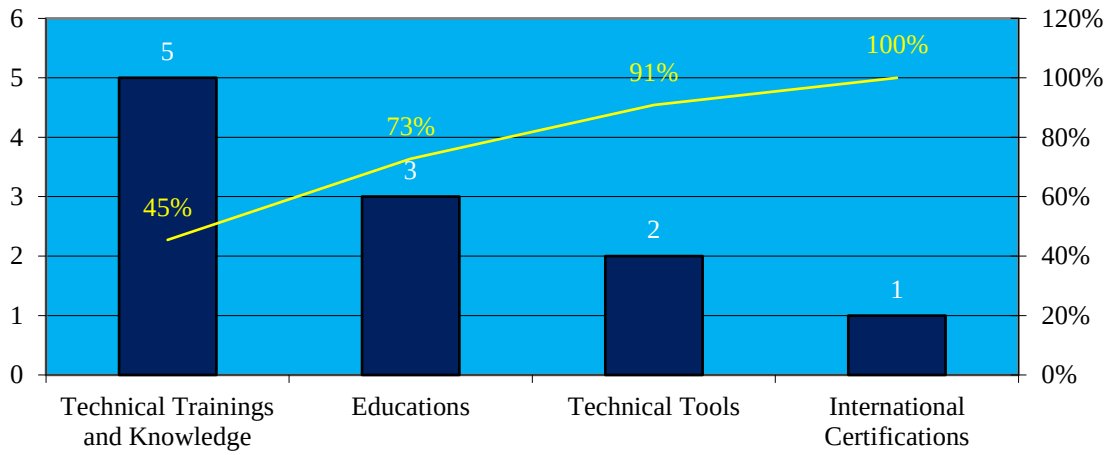


Figure 3.10. *Pareto Chart for the Responses to Second Question of First Round*

The panelists broadly specified that their audit parts are performing their processes as a review committee which is directly attached to the general manager by reporting their findings to the management board with regular meetings after the BRSA regulation which was established on 15th March 2020. Correspondingly, they noted that the governance approach, which was introduced after this regulation, provides much effectiveness for integrating the cyber security culture into business functions and corporate management principles. As well, they stated that the internal audit teams have supportive functions such as guiding the upper management, planning audits, and reviewing the reports and findings through monitoring the risk management activities.

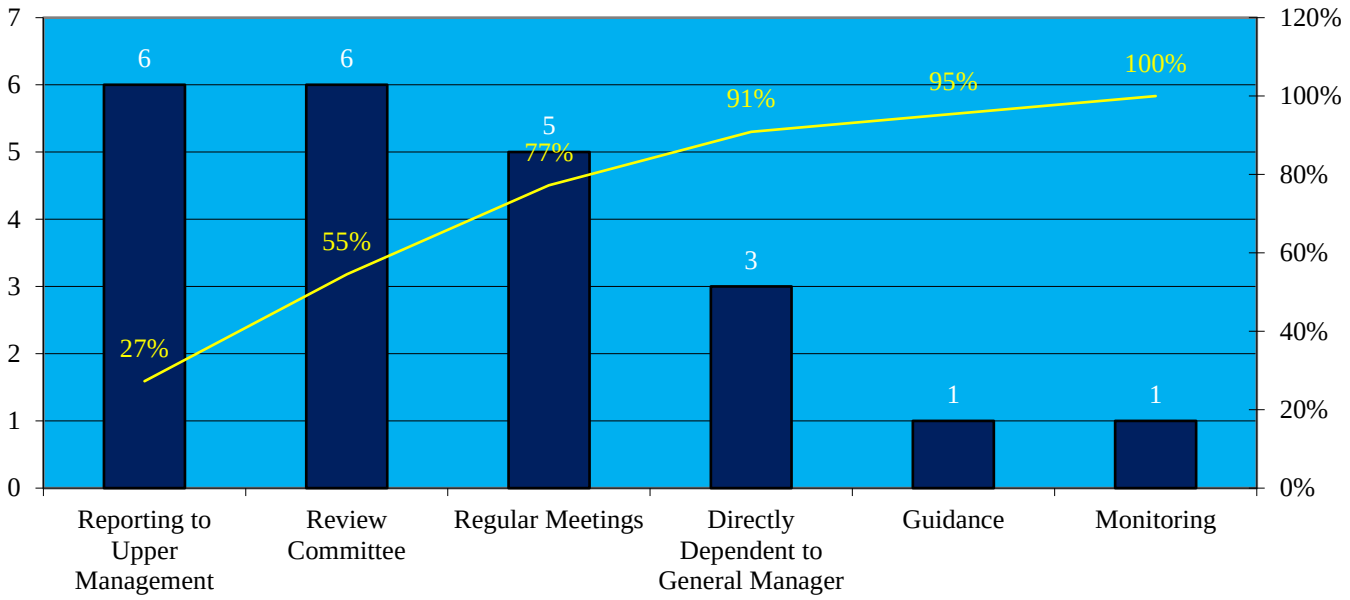


Figure 3.11. *Pareto Chart for the Responses to Third Question of First Round*

Most of the panelists widely underlined that the new BRSA regulation, which was developed relative to frame the standards for the information systems of the banks, has positive effects on the cyber security awareness and safeguard of the CIA triad. Also, they stated that the internal audit services have functions in controlling the adequacy level of cyber security processes through monitoring activities due to the international policy frameworks which are particularly pointed out as COBIT and ISO 27001. Equivalently, they emphasized that the CIA triad subject is often considered in the authorization mechanism while providing data access and flow in the banks.

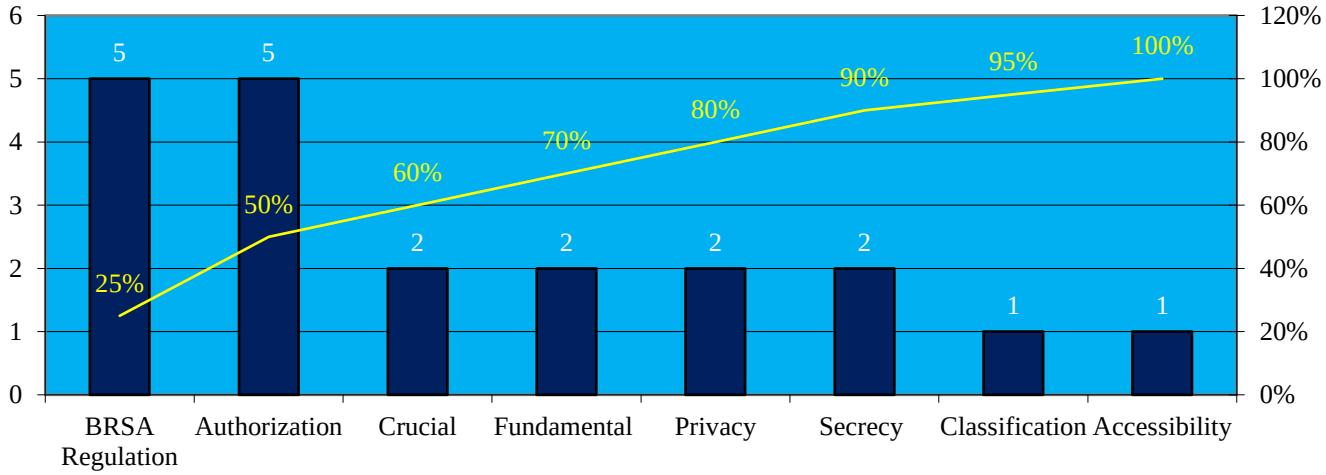


Figure 3.12. *Pareto Chart for the Responses to Fourth Question of First Round*

The panelists especially deepened that the set of code of ethics is considered as fundamentals in conjunction with compliance-related cases for the assurance of cyber security governance through policy frameworks and IIA standards. Their responses showed that the organizational culture can be improved with educations, case studies, and simulations for the practices of ethical principles. Also, they proposed that continuous audit methods can be applied for ensuring authorizations because authorization is scored as the most significant subject in cyber security from the point of an audit.

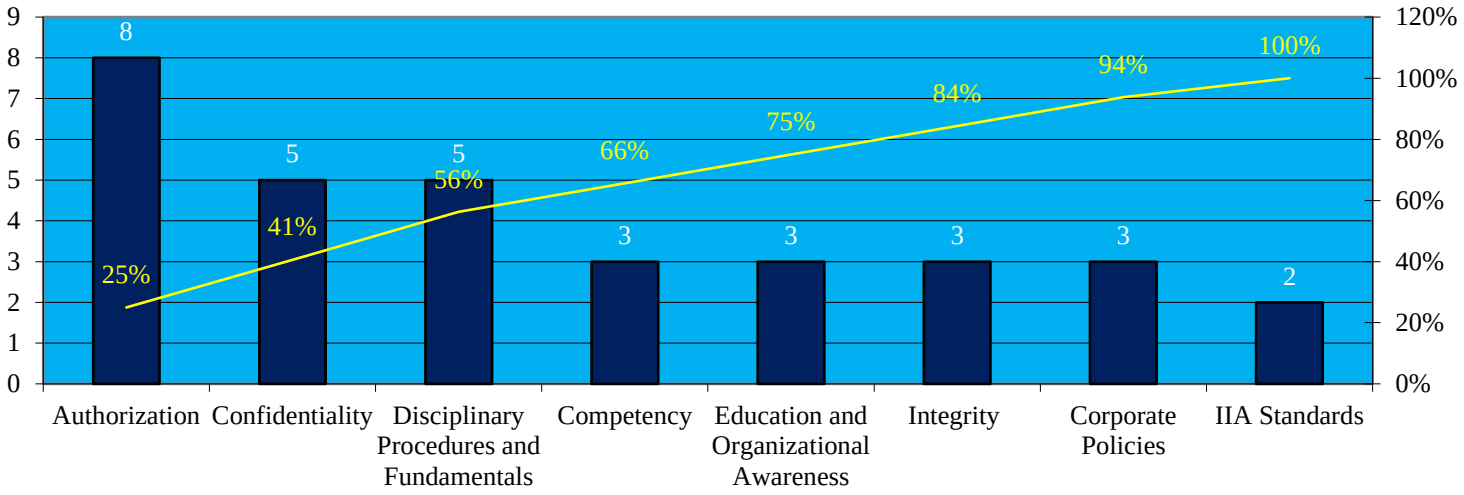


Figure 3.13. *Pareto Chart for the Responses to Fifth Question of First Round*

The responses of panelists described that in general internal audit has responsibility for reporting the cases and findings which are related to the violation of the ethical rules. They also have functions in risk assessment and review processes in terms of controlling the authorization mechanism in the banks.

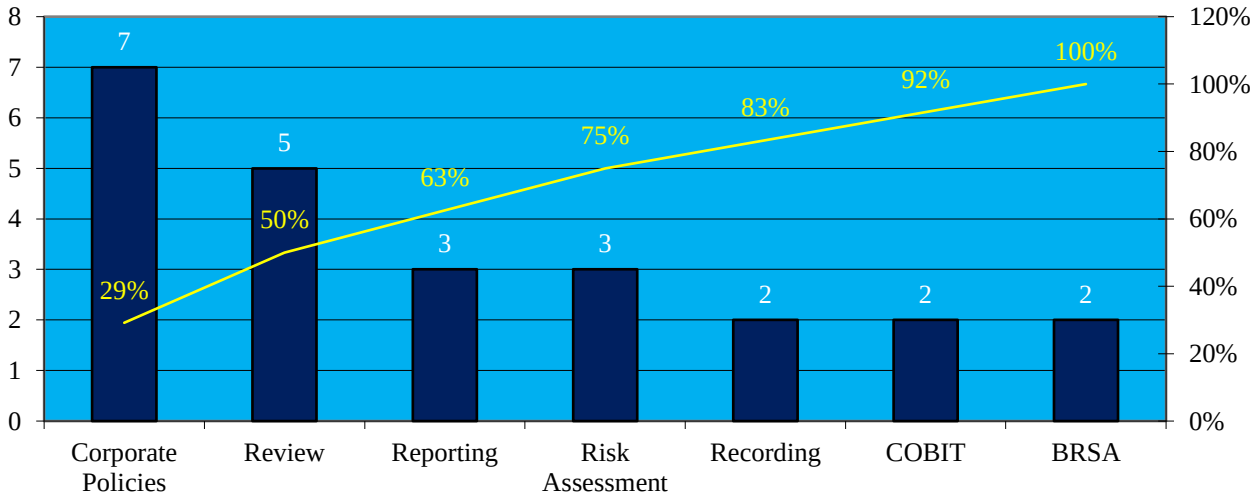


Figure 3.14. *Pareto Chart for the Responses to Sixth Question of First Round*

The panel members mentioned that the internal audit committees have a responsibility in controlling the compliance of banks to BRSA regulation, COBIT, and ISO 27001. Also, their answers indicated that monitoring and reporting activities are mainly performed by auditors to assure that the compliance controls are being executed in line with the legislative and international policy frameworks.

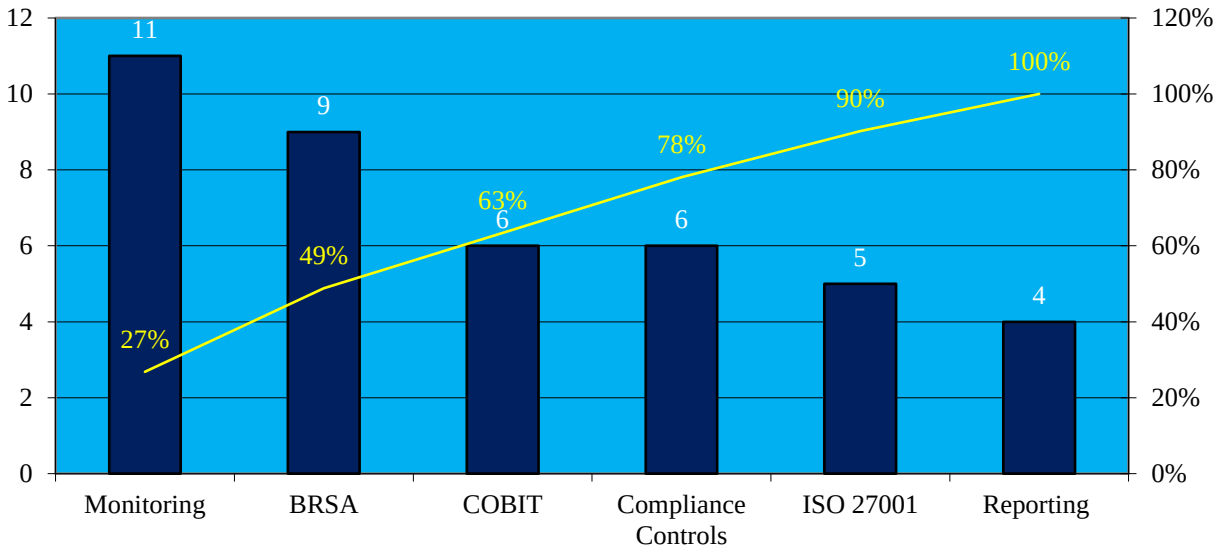


Figure 3.15. *Pareto Chart for the Responses to Seventh Question of First Round*

The conceptual model of internal audit functions in the cyber security governance structure is established through the mind mapping tool of Nvivo software. The goal of this relational framework is to specify the main actors of the legislative environment, external performers, organizational roles, and responsibilities of internal auditors which are partially related to corporate management principles and code of ethics in the processes of cyber security governance. As a result, ISO 27001, COBIT 4.1, and particularly BRSA regulation with the performers of external audit activities which are described as independent accredited firms for technical controls and independent audit firms for process controls have major authority in the scanning of cyber security management activities for Turkish Banking Sector. Therefore, these parts of the conceptual model have direct effects on the banks' corporate cultures, ethical understandings, and internal audit functions which are related to cyber security.

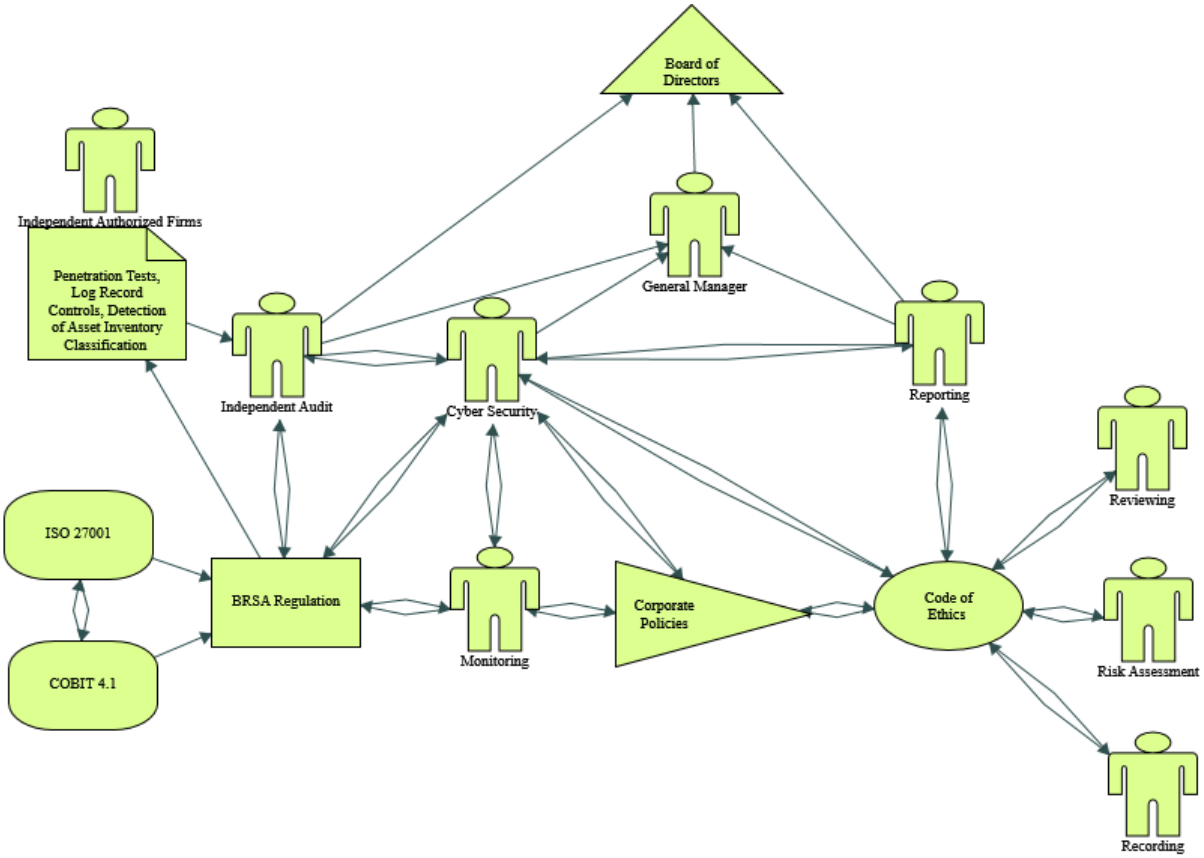


Figure 3.16. *Mind Map for Internal Audit*

The cause and effect diagram, which is also known as Ishikawa or fishbone diagram, is used as an analytical tool to identify and visualize the probable causes of the thesis problem to present an organized formation. In essence, the main goal of using this diagram is to focus on the problem which is under examination by outlining the major reasons through identifying the interrelations between them (Joiner Associates, 1995, p. 15). Therefore, the data, which are analyzed through Pareto charts, are categorized with a cause and effect diagram, which supports the researcher in terms of managing time constraints for providing a common perception to logically evaluate the following phases as to which elements can be used to gather the meaningful data.

Because of the above-mentioned reasons, the objectives of internal audit functions in cyber security governance are outlined through a cause and effect diagram, according to the qualitative data which are acquired from semi-structured interviews with personal opinions of panelists that are analyzed in Pareto charts. Therefore, the main areas are defined for the determination of root causes in order to cluster the common judgments of panelists with respect to demonstrating the diagnostics for reaching the main goal of the research study. As a result, relative to this following outline, the survey questions are going to be designed through focusing on major determinants and their subitems for collecting quantitative data in connection with the second and third rounds of the Delphi technique. Within the context of responses of participants to seven open-ended questions,

the responsibility, competency, governance, CIA triad, code of ethics, legislative and international policy frameworks are identified as core elements to deeply explore the internal audit functions in cyber security governance.

As well, the subclasses are defined due to the frequency of collected data from the Pareto analyses in the qualitative part of mixed methods research to design the primary concerns which facilitate for framing the survey questions that will be used to test the validity of common opinions of participants in the quantitative section. So, the main objective of the following representative model is to demonstrate the statements of panelists by sorting them into specified fields with qualitative analyses.

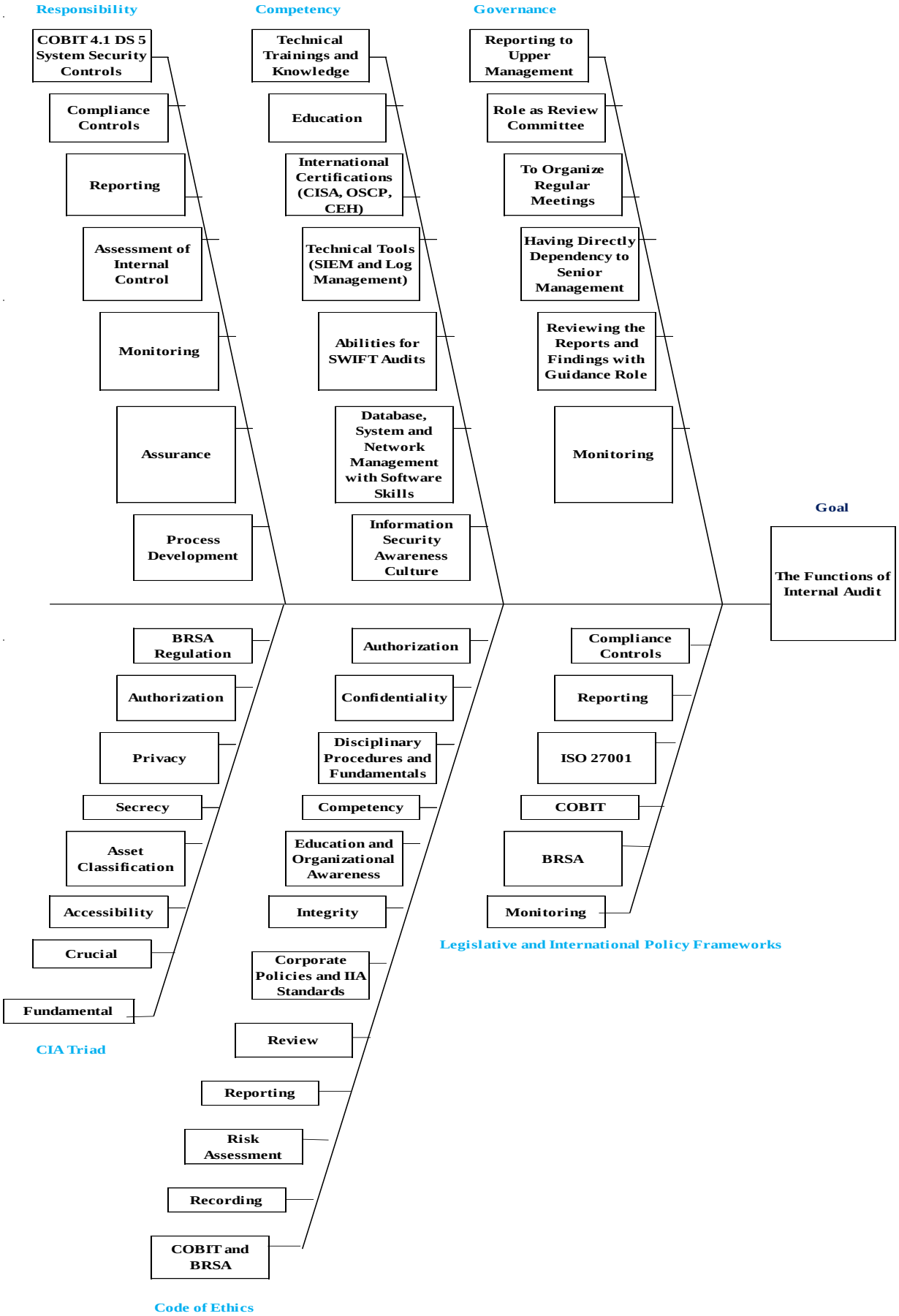

Responsibility
Competency
Governance
COBIT 4.1 DS 5 System Security Controls
Compliance Controls
Reporting
Assessment of Internal Control
Monitoring
Assurance
Process Development
Technical Trainings and Knowledge
Education
International Certifications (CISA, OSCP, CEH)
Technical Tools (SIEM and Log Management)
Abilities for SWIFT Audits
Database, System and Network Management with Software Skills
Information Security Awareness Culture
Reporting to Upper Management
Role as Review Committee
To Organize Regular Meetings
Having Directly Dependency to Senior Management
Reviewing the Reports and Findings with Guidance Role
Monitoring
Goal
The Functions of Internal Audit
BRSA Regulation
Authorization
Privacy
Secrecy
Asset Classification
Accessibility
Crucial
Fundamental
CIA Triad
Authorization
Confidentiality
Disciplinary Procedures and Fundamentals
Competency
Education and Organizational Awareness
Integrity
Corporate Policies and IIA Standards
Review
Reporting
Risk Assessment
Recording
COBIT and BRSA
Code of Ethics
Compliance Controls
Reporting
ISO 27001
COBIT
BRSA
Monitoring
Legislative and International Policy Frameworks

Figure 3.17. *Cause and Effect Diagram for Defining Major Parts*

3.7.3. Delphi round two

A questionnaire is designed according to the inferences of the data which are collected and analyzed in the first round of Delphi. Correspondingly, the quantitative part of this research study covers the collection and analyses of the data which are mainly based on the questionnaire plan which is prepared due to the seven open-ended questions and their root causes. Therefore, five sets of questions are adapted for each section of the open-ended questions relative to the qualitative data analyses which are performed in Nvivo software and programming tools through nodes, treemaps, and word clouds. As a result, thirty-five questions are arranged for the questionnaire which is designed due to the five-point Likert scale as strongly disagree (1), disagree (2), neutral (3), agree (4), and strongly agree (5).

3.7.4. The analyses of the second round

First of all, the statistical inferences are shown quantitatively through measures of dispersion after the collection of ordinal data, which are the class of categorical variables, are collected with closed-ended questions that are ranked with a five-point Likert rating scale questionnaire design as mentioned in the previous section. The threshold value is decided as the interquartile range (IQR) must be less or equal to one and at least seventy-five percent consensus rate must be reached for each of the statements which represent the closed-ended questions.

The facts, which are provided through the set of statements, which is shared with panelists due to the responsibility element, prove that the participants have an agreement with each other. These results test the validity of panelist opinions which are obtained in the first round in terms of showing the commonality relative to framed responsibilities of internal auditors in cyber security processes. Therefore, the internal auditors have main functions in control processes, compliance mechanisms, reporting, assessment, and monitoring activities.

Table 3.5. *The Statistical Inferences for Responsibility*

Statements for Responsibility	Mean	Standard Deviation	Median	Interquartile Range	Frequency			Consensus
					(4-5)	(3)	(1-2)	
1	4,466667	0,498887652	4	1	15 (100%)	0 (0%)	0 (0%)	Achieved
2	4,333333	0,699205899	4	1	13 (87%)	2 (13%)	0 (0%)	Achieved
3	4,466667	0,718021974	5	1	13 (87%)	2 (13%)	0 (0%)	Achieved
4	4,2	0,653197265	4	1	13 (87%)	2 (13%)	0 (0%)	Achieved

5	4,533333	0,618241233	5	1	14 (93%)	1 (7%)	0 (0%)	Achieved

The competency related statements, which are sent to panelists in order to measure the necessary skills for internal auditors in cyber security activities, present that the participants have no common opinions in the seventh, eighth, ninth, and tenth statements which are shown respectively as;

- Internal auditors must have a basic level of software knowledge in order to maintain the audit activities which are carried out by BRSA in accordance with the information systems regulation.
- Internal audit must have system and network management knowledge to be effective in the process of controlling and conforming to the penetration test findings which are carried out by independent audit firms after they are ensured.
- Internal audit must have technical level knowledge and sufficient experience on information security architecture and infrastructure to be effective in the auditing process of control lists that are prepared for information security within the scope of the regulations that are designed by BRSA.
- Internal audit should be a master of using SIEM tools to take an active role in monitoring and surveillance activities within the scope of cyber security.

Table 3.6. *The Statistical Inferences for Competency*

Statements for Competency	Mean	Standard Deviation	Median	Interquartile Range	Frequency			Consensus
					(4-5)	(3)	(1-2)	
6	4,6	0,489897949	5	1	15 (100%)	0 (0%)	0 (0%)	Achieved
7	4,066667	0,77172246	4	2	11 (73%)	4 (27%)	0 (0%)	Not Achieved
8	4	0,894427191	4	2	11 (73%)	3 (20%)	1 (7%)	Not Achieved
9	3,933333	0,679869268	4	1	11 (73%)	4 (27%)	0 (0%)	Not Achieved
10	3,8	0,909212113	4	1	11 (73.3%)	2 (13.3%)	2 (13.3%)	Not Achieved

The governance-related statements, which are revealed to panel members, in terms of understanding the functions of internal auditors in cyber security management, show that they are not in agreement for the eleventh, thirteenth, and fifteenth statements which are respectively determined as;

- Internal audit has a consultancy role in the governance between the board of directors, general manager, and information technology department.
- Internal audit must have direct authority for cyber security controls.

- Internal audit has the responsibility for informing the senior management necessarily with regular interval periods in cases related to cyber security.

Table 3.7. *The Statistical Inferences for Governance*

Statements for Governance	Mean	Standard Deviation	Median	Interquartile Range	Frequency			Consensus
					(4-5)	(3)	(1-2)	
11	3,666667	0,788810638	4	1	9 (60%)	5 (33.3%)	1 (6.7%)	Not Achieved
12	4,666667	0,471404521	5	1	15 (100%)	0 (0%)	0 (0%)	Achieved
13	3,733333	0,928559218	4	1	10 (66.6%)	3 (20%)	2 (13.3%)	Not Achieved
14	3,8	0,8326664	4	0	12 (80%)	1 (6.7%)	2 (13.3%)	Achieved
15	3,8	0,909212113	4	1	11 (73%)	2 (13.3%)	2 (13.3%)	Not Achieved

The panel members have common answers for the statements according to the CIA triad, therefore, they agree with each other on the subjects such as authorization, accessibility, privacy, integrity, and availability. Also, these results prove that the internal auditors have to be aware of cyber risks which can damage the sensitive assets of the banks due to the fundamental elements of security.

Table 3.8. *The Statistical Inferences for CIA Triad*

Statements for Confidentiality, Integrity and Availability	Mean	Standard Deviation	Median	Interquartile Range	Frequency			Consensus
					(4-5)	(3)	(1-2)	
16	4,4	0,711805217	5	1	13 (87%)	2 (13%)	0 (0%)	Achieved
17	4,333333	0,699205899	4	1	13 (87%)	2 (13%)	0 (0%)	Achieved
18	4,066667	0,573488351	4	0	13 (87%)	2 (13%)	0 (0%)	Achieved
19	4,2	0,54160256	4	1	14 (93%)	1 (7%)	0 (0%)	Achieved
20	4,2	0,653197265	4	1	13 (87%)	2 (13%)	0 (0%)	Achieved

The answers of panelists relative to the statements of corporate management principles represent that they have a consensus with each other through the investigation

of how the internal auditors must perform their functions respectfully to the governance mechanism of both the bank, sector, and regulators.

Table 3.9. *The Statistical Inferences for Corporate Management Principles*

Statements for Corporate Management Principles	Mean	Standard Deviation	Median	Interquartile Range	Frequency			Consensus
					(4-5)	(3)	(1-2)	
21	4,2	0,54160256	4	1	14 (93%)	1 (7%)	0 (0%)	Achieved
22	4,6	0,611010093	5	1	14 (93%)	1 (7%)	0 (0%)	Achieved
23	4,533333	0,618241233	5	1	14 (93%)	1 (7%)	0 (0%)	Achieved
24	4,333333	0,596284794	4	1	14 (93%)	1 (7%)	0 (0%)	Achieved
25	4,4	0,611010093	4	1	14 (93%)	1 (7%)	0 (0%)	Achieved

The panel members agree with themselves in the twenty-sixth, twenty-seventh, twenty-eighth, and twenty-ninth statements but they have split in the thirtieth statement which is defined as;

- Internal audit teams should evaluate why the laws have been being reframed while they are controlling the compliance of institutions with the legislative framework.

Table 3.10. *The Statistical Inferences for Code of Ethics*

Statements for Code of Ethics	Mean	Standard Deviation	Median	Interquartile Range	Frequency			Consensus
					(4-5)	(3)	(1-2)	
26	4,333333	0,596284794	4	1	14 (93%)	1 (7%)	0 (0%)	Achieved
27	4,2	0,653197265	4	1	13 (87%)	2 (13%)	0 (0%)	Achieved
28	4,133333	0,618241233	4	1	13 (87%)	2 (13%)	0 (0%)	Achieved
29	4,066667	0,442216639	4	0	14 (93%)	1 (7%)	0 (0%)	Achieved
30	3,733333	1,06249183	4	2	10 (66.6%)	2 (13.3%)	3 (20%)	Not Achieved

The panel members have a commonality in their answers to the statements which are based on legislative and international policy frameworks. Especially, these results

support the first round of Delphi as banking law no. 5411 of BRSA, ISO 27001, and COBIT 4.1 DS5 frameworks are accepted as main references in terms of structuring the cyber security governance.

Table 3.11. *The Statistical Inferences for Legislative and International Policy Frameworks*

Statements for Legislative and International Policy Frameworks	Mean	Standard Deviation	Median	Interquartile Range	Frequency			Consensus
					(4-5)	(3)	(1-2)	
31	4,333333	0,471404521	4	1	15 (100%)	0 (0%)	0 (0%)	Achieved
32	4,266667	0,77172246	4	1	14 (93%)	0 (0%)	1 (7%)	Achieved
33	4,4	0,611010093	4	1	14 (93%)	1 (7%)	0 (0%)	Achieved
34	4,066667	0,679869268	4	1	12 (80%)	3 (20%)	0 (0%)	Achieved
35	4,133333	1,024152766	4	1	13 (87%)	1 (7%)	1 (7%)	Achieved

3.7.5. Delphi round three

The answers of panel members to the questionnaire in the second round of Delphi showed that seventh, eighth, ninth, tenth, eleventh, thirteenth, fifteenth, and thirtieth statements are defined for the reassessment process because the participants' responses to these statements are inconsistent with each other. Therefore, these statements are resent to the panelists whose responses are deviated from the median of data sets.

3.7.6. The analyses of the third round

The answers of the panel members for the competency-related items, which are not reached consensus in the second round, are succeeded in agreement in the third round of the Delphi study. Therefore, their views prove that if the internal auditors have a basic level of technical knowledge about software, system and network management, information security architecture, and SIEM tools, they can better understand the findings of information technology controls which are relative to cyber security governance.

Table 3.12. *The Transformations of Statistical Inferences for Competency Factors*

Statements for Competency	Mean	Standard Deviation	Median	Interquartile Range	Frequency			Consensus
					(4-5)	(3)	(1-2)	
7	4,2	0,653197265	4	1	13 (87%)	2 (13%)	0 (0%)	Achieved

8	4,066667	0,853749898	4	1	12 (80%)	2 (13.3%)	1 (6.7%)	Achieved
9	4,066667	0,573488351	4	0	13 (87%)	2 (13%)	0 (0%)	Achieved
10	4	0,730296743	4	0	13 (86.6%)	1 (6.7%)	1 (6.7%)	Achieved

The responses of the panelists to the eleventh and fifteenth statements of the governance-related factors, which are not reached consensus in the second round, are succeeded in agreement in the third round. However, they couldn't reach a consensus again in the third round of the Delphi study for the thirteenth statement which is presented as;

- Internal audit must have direct authority for cyber security controls.

to panel members.

Table 3.13. *The Transformations of Statistical Inferences for Governance Factors*

Statements for Governance	Mean	Standard Deviation	Median	Interquartile Range	Frequency			Consensus
					(4-5)	(3)	(1-2)	
11	3,866667	0,718021974	4	0	12 (80%)	2 (13.3%)	1 (6.7%)	Achieved
13	3,733333	0,928559218	4	1	10 (66.6%)	3 (20%)	2 (13.3%)	Not Achieved
15	4,066667	0,679869268	4	0	14 (93%)	0 (0%)	1 (7%)	Achieved

The panelists' answers to the thirtieth statement of the codes of ethics-related factors, which are not reached consensus in the second round, are succeeded in agreement in the third round. They agree with each other in eighty percent that if internal auditors investigate, why the regulations are being renovated, can have better controls for compliance of banks to the legislative framework.

Table 3.14. *The Transformations of Statistical Inferences for Code of Ethics*

Statements for Code of Ethics	Mean	Standard Deviation	Median	Interquartile Range	Frequency			Consensus
					(4-5)	(3)	(1-2)	
30	3,933333	0,928559218	4	1	12 (80%)	1 (7%)	2 (13%)	Achieved

3.8. Findings and Recommendations

The business conditions of the current era have been modifying highly with the technology trends which commonly affect the international trade activities through innovation, automation, and speed in financial transactions which provide the asset allocation activities in the global economy. Especially, the banking sector, which is accepted as the fundamental part of the financial industry, can also be defined as a significant subset of critical infrastructure for the sustainability and development of global economic activities. Because of these reasons, the internal audit functions in cyber security governance-related processes are investigated within the context of the banking sector of Turkey. Delphi technique is chosen for both collecting the qualitative data from panelists and examining the depth of panelists' opinions relative to the subject and goal of the thesis study. Therefore, initially, the sampling is defined by framing two deposit banks with public capital, two deposit banks with private capital, one participation bank with foreign capital, one deposit bank with foreign capital, one regulatory institution, and academic environment. According to this plan, semi-structured interviews are realized in the first round of the Delphi study with four-panel members from public capital banks, two-panel members from private capital banks, three-panel members from a participation bank with foreign capital, a panel member from a deposit bank which is launched in Turkey with foreign capital, a panel member from a regulatory institution and four-panel members who are from the academic environment with having a background in internal audit and cyber security subjects to better measure and understand the banking sector's viewpoints and awareness for the processes of internal auditors in cyber security governance. In the first round of the Delphi study, the qualitative data are collected by asking the seven open-ended questions to panel members, and then the answers of panelists are analyzed qualitatively through the Nvivo program for a better understanding of the distribution of panelists' opinions relative to their responses. In this context, the Pareto charts, mind mapping tool of the Nvivo program, and Ishikawa diagram are used to visualize the responses of panel members for the first round of the Delphi study. After this process, the questionnaire design is performed by taking the support of analytical tools which are used in the first round. In the second round of the Delphi study, the questionnaire is prepared by clustering a set of five statements for each of the defined titles in the first round. Therefore, thirty-five statements are presented to the panelists with five points Likert scale which is framed as strongly disagree (1), disagree (2), neutral (3), agree (4), and strongly agree (5) to collect ordinal data as a class of categorical variables. According to the results of the second round, the panel members' responses to the seventh, eighth, ninth, tenth, eleventh, thirteenth, fifteenth, and thirtieth statements show that the consensus is not achieved in these assumptions. These statements are shown respectively as below;

- Internal auditors must have a basic level of software knowledge in order to maintain the audit activities which are carried out by BRSA in accordance with the information systems regulation.
- Internal audit must have system and network management knowledge to be effective in the process of controlling and conforming to the penetration test findings which are carried out by independent audit firms after they are ensured.

- Internal audit must have technical level knowledge and sufficient experience on information security architecture and infrastructure to be effective in the auditing process of control lists that are prepared for information security within the scope of the regulations that are designed by BRSA.
- Internal audit should be a master of using SIEM tools to take an active role in monitoring and surveillance activities within the scope of cyber security.
- Internal audit has a consultancy role in the governance between the board of directors, general manager, and information technology department.
- Internal audit must have direct authority for cyber security controls.
- Internal audit has the responsibility for informing the senior management necessarily with regular interval periods in cases related to cyber security.
- Internal audit teams should evaluate why the laws have been being reframed while they are controlling the compliance of institutions with the legislative framework.

So, these statements are resent to the panel members whose answers are deviated from the median value of the data in the third round. Finally, they reached an agreement for all of the statements except the thirteenth one which is stated as "Internal audit must have direct authority for cyber security controls."

As a result, the findings of the thesis research study show that the opinions of panel members are mostly supporting each other according to the statistical tests of their awareness for the functions of internal auditors in cyber security governance processes except the thirteenth statement. So, the fundamental reason for this disagreement in the thirteenth statement can be explained with the authorization that is assessed as the first critical priority to be sensitive in particular for cybersecurity-related processes. Therefore, the answers of panelists are observed mostly deviated from the median value of the data set for the thirteenth statement.

According to the statistical inferences for responsibility related statements, the observations show that internal auditors have functions in;

- Performing controls after the findings of information technology audits are ensured within the context of cyber security.
- Annual controls related to cyber security in compliance with the regulation of BRSA which was established on 15 March 2020.
- Validation of penetration test results after these results are secured.
- Identification of security vulnerabilities from the point of cyber security.
- Reporting of findings directly to the general manager or management board.

Therefore, significantly, internal auditors have supportive functions in cyber security management as their main objectives can be defined such to control and validating the information technology audit results which are prepared by information security departments of the banks, and penetration testing findings which are performed by independent audit associations. Furthermore, their role is covering partially the recognition of security breaches and most importantly the reporting of information technology audits' results and penetration testing findings to the general manager and management board. So, their main responsibility is circling around the process controls

which can be explained with the third line of defense of 3LoD and reporting to upper management that can be described through 5LoA.

According to the competency related statements, the statistical inferences demonstrate that internal auditors had better;

- Carry out the audit process of control lists by taking the support of IT auditors.
- Have a basic level of software knowledge.
- Have the system and network management knowledge.
- Have technical level knowledge and sufficient experience.
- To be familiar with using SIEM tools to take an active role in monitoring activities.

So, the internal auditors, who aim to be effective in cyber security controls, should continuously improve their technical abilities in computer science and advanced security intelligence tools usage. As well, the opinions of panelists showed that the skills of auditors can be enhanced through the organizations of technical educations.

In respect of the statistical inferences for governance statements, reviews show that internal auditors have;

- A consultancy role in the governance between the board of directors, general manager, and IT department.
- To get required training to improve governance in cyber security processes.
- Supportive function in cyber security controls with its advisory role.
- Responsibility to inform the senior management on regular periods.

Therefore, this can be said that the internal auditors are performing as consultants to provide healthy governance between management parts and the IT department. As well, their main function can be defined as informing the senior management in defined periods.

According to the statistical inferences for the CIA triad, the examinations show that the internal auditors must;

- Record, keep, and report the pieces of evidence of audit activities in accordance with the principles of the CIA triad.
- Sustain their activities by tracing the path of authority principle.
- Ensure that the access of the results of controls should be operated in a well-organized manner.
- Assure the findings of controls haven’t been modified.
- Ensure that the findings of cyber security controls are not being permitted to be accessed by unauthorized persons.

So, the internal auditors, who are effective in cyber security governance, must be aware much for compliance with the principles of the CIA triad, authorization, and privacy concepts.

In respect of the statistical inferences for corporate management principles, the indicators demonstrate that the internal auditors must;

- Follow the legal environment and provide necessary reportings to related authorized persons.
- Execute their roles in accordance with professional ethics as not being involved in any of the illegal acts.
- Carry out their operations in a manner that respects the ethical principles and management standards of the corporation.
- Participate in tasks in accordance with their skills, knowledge, and experiences.
- Continuously improve their abilities, effectiveness, and quality level of their services consistently with developing technologies.

Therefore, the internal auditors must continuously control the latest developments in both national regulations and international policy frameworks relative to cyber security and they must perform their operations in harmony with the principles of corporations. Also, they must enhance their skills continuously in how to use emerging technologies, and especially within the context of cyber security which covers advanced technical subjects, they must take over the responsibilities that are in line with their knowledge and experiences as a part of ethical principles.

According to the statistical inferences for the code of ethics, the survey shows that the banks should;

- Have written documents in which the ethical principles are clearly defined.
- Have reporting systems which can be effectively operated for the controls of functioning of ethical rules.
- Instantly provide information to upper management in case of violation of the ethical principles.
- Provide synergy to improve coordination between internal audit and cyber security teams to prevent the violation of ethical rules.

So, the banks have to be aware of the risks, which can be emerged from the weaknesses in the setting of ethical rules and the difficulty of carrying out rigid ethical principles, which can cause security vulnerabilities. Also, the internal auditors had better control the compliance of banks to legislations, if they undermine the reasons in the trends of modifications in regulations.

Depending on the statistical analyses of the legislative and international policy framework, the general view shows that the internal auditors must;

- Regularly keep their eyes on the national regulations and international standards to ensure the validity of compliance of control lists that are formed relative to cyber security governance.
- Report the defects in control mechanisms which are related to compliance for legislations to upper management.

Therefore, internal auditors have responsibilities in both controlling insides of the organizations and outside conditions which can be considered here as a legislative and international policy framework in terms of providing the compliance of the banks to the regulations and international standards. Correspondingly, BRSA regulation, which was issued on March 15, 2020, is related to the information systems and electronic banking services of the banks, ISO 27001 and COBIT 4.1 DS5 processes are taken up as references to control the compliance of banks to the regulatory environment for cyber security governance. Particularly, all of the banks, which are sustaining their businesses in Turkey, must systematize their information technology structure in line with the banking law no. 5411. Also, BRSA is accepted as the full authorized institution by the Turkish Government for carrying out this law.

Additionally, the regulation, which was established by BRSA to define the independent audit principles of information systems and business processes of the organizations that are under the supervision of BRSA were issued in the official gazette on 31st December 2021, states evaluations about internal control and internal audit systems in 26th article to consider the activities which are performed by the audited within the framework of internal control and internal audit relative to their priority criteria. The statements are shown as follows;

a. While examining the activities that are carried out regarding the internal control system as a minimum;

- Issues that are related to the control environment,
- The approach and implementation that are adopted by the management regarding the establishment, operation, and supervision of an effective and adequate internal control system,
- Implementation of ethical principles that are determined by the professional associations established in accordance with the legislation to which the audit is subject and the level of awareness of the employees in this regard,

are considered.

b. Evaluating the activities and performance of the internal audit unit regarding the supervision of the effectiveness, competence, and compliance of the internal control system.

c. Within the scope of the evaluation of the internal audit unit, the information systems audit activities of the audited are taken into account. As a minimum when evaluating the audited information systems control function;

- The position and independence of the team within the organization,
- The competence of the personnel who make up the team in terms of quality and quantity,
- Audit studies that are planned and carried out,
- Follow-up of audit results,

are examined.

ç. The auditor evaluates the activities and performance which are carried out during the risk assessment process regarding the internal control system of the audited (BRSA, 2021).

Thus, according to this policy framework, the independent auditors' missions are defined precisely within the context of the assessment of internal control and internal audit systems' performance. As a result, BRSA's regulation, which was issued on 15th March 2020 related to the information systems and electronic banking services, is being supported by this framework to improve consistency in the governance of regulatory agencies and audit parts.

In particular, blockchain technology can be recommended for the banks' information security improvement approaches to make lean the complex processes in the authorization and reporting mechanisms for better governance in cyber security. In this context, BRSA's last published legislation should be enhanced with the international standards which have been continuously upgraded through the developments in emerging technologies such as blockchain. Especially, penetration testings, the controls of log records, and asset classifications can be executed by using the decentralized infrastructure of blockchain technology with real-time audits and continuous monitoring approaches rather than conventional and cumbersome risk management models. As a result, overprocessing in governance parts of audit can be eliminated by the implementation and support of blockchain technology applications to the Turkish banking sector's information systems and security designs to get a competitive advantage in the international finance industry, for an instance, SWIFT operations can be feasibly coordinated through the utilization of decentralized finance forms such as ripple.

Additionally, this research study can be improved with the extension of the sample by adding panelists from every bank in the Turkish banking sector and all of the regulatory institutions to the sample or by expanding the sample through selecting panel members from the global bank industry. Also, this study can be enhanced as a subject to better guide the persons who aim to investigate the role of emerging technologies in information technology audits relative to cyber security controls. Especially, this research study can be supported with the deep examinations of advanced technical developments and tools which can be specified as artificial intelligence, robotic process automation, machine learning, and blockchain in terms of understanding their usages in audit practices.

REFERENCES

Abawajy, J., Choo, K.-K. R., Islam, R., Xu, Z., & Atiquzzaman, M. (2018). *International Conference on Applications and Techniques in Cyber Security and Intelligence ATCI 2018: Applications and Techniques in Cyber Security and Intelligence.* Warsaw: Springer.

Abdullah, H., & Valentine, B. (2009). Fundamental and Ethics Theories of Corporate Governance. *Middle Eastern Finance and Economics*, 89-96.

Accenture. (2018). The Nature of Effective Defense: Shifting from Cybersecurity to Cyber Resilience. Virginia, U.S. Retrieved from https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/en/Accenture-Shifting-from-Cybersecurity-to-Cyber-Resilience-POV.pdf

Accenture Security. (2019). The Cost of Cybercrime. Michigan, North Traverse City, United States of America. Retrieved from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Al Omari, L., Barnes, P., & Pitman, G. (2012). An Exploratory Study into Audit Challenges in IT Governance: A Delphi Approach. *IT Governance, Management and Audit*, 1-12. Retrieved from https://eprints.qut.edu.au/53110/22/An_Exploratory_Study_into_Audit_Challenges_in_IT_Governance_A_Delphi_Approach.pdf

Alina, M. C., Cerasela, S. E., & Gabriela, G. (2017). Internal Audit Role in Cybersecurity. *Ovidius University, Economic Science Series, 17*(2), 510-513.

Altınpulluk, H., Kesim, M., & Kurubacak , G. (2020, April 2). The Usability of Augmented Reality in Open and Distance Learning Systems: A Qualitative Delphi Study. *International Council for Open and Distance Education, 12*(2), 283-307. Retrieved from https://files.eric.ed.gov/fulltext/EJ1267133.pdf

Amos, T., & Pearse, N. (2011). Pragmatic Research Design: An Illustration of the Use of the Delphi Technique. In A. Bryant, *Leading Issues in Business Research Methods* (pp. 101-116). London: Academic Publishing International Limited.

Andrew, D. P., Pedersen, P. M., & McEvoy, C. D. (2011). *Research Methods and Design in Sport Management.* Human Kinetics.

Antonucci, D. (2017). *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities.* New Jersey: John Wiley&Sons.

ASQ. (2021). *What is Auditing?* Retrieved from Learn About Quality: https://asq.org/quality-resources/auditing

Aydaner, G. (2019). Measurement of the Impact of Social Engineering and Cyber Security Awareness of Young Consumers on Online Shopping Intentions. Yükseköğretim Kurulu Başkanlığı Tez Merkezi.

Banking Regulation and Supervision Agency (BRSA). (2017). *Mission and Vision, ISO 27001 Information Security Management System*. Retrieved from ISO 27001 Information Security Management System: https://www.bddk.org.tr/AboutUs/Mission-and-Vision/17

Bektaş, B. T. (2020). A Scale Development Study to Determine Public Science Literacy: Delphi Technique. Yükseköğretim Kurulu Başkanlığı Tez Merkezi.

Bilgi Teknolojileri ve İletişim Kurumu. (2012). *Siber Güvenlik Kurulu*. Retrieved from Siber Güvenlik Stratejisi ve Eylem Planı: https://www.btk.gov.tr/siber-guvenlik-kurulu

Bilgi Teknolojileri ve İletişim Kurumu. (2017). *Ulusal Siber Olaylara Müdahele Merkezi (USOM) ve Kurumsal Siber Olaylara Müdahele Ekibi (SOME).* Retrieved from USOM, Sektörel SOME ve Kurumsal SOME İlişkisi: https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi

Bodeau, D. J., & Graubart, R. (2011). *Cyber Resiliency Engineering Framework.* Bedford: MITRE. Retrieved from https://www.mitre.org/sites/default/files/pdf/11_4436.pdf

Bozgeyik, A. (2018). Analysis of Cyber Security Management Approaches in Medium and Large-Size Enterprises Operating at Gaziantep. Yükseköğretim Kurulu Başkanlığı Tez Merkezi.

Brown, W., & Nasuti, F. (2005). Sarbanes-Oxley and Enterprise Security: IT Governance-What It Takes to Get the Job Done. *Security Management Practices, 14*(5), 15-28.

BRSA. (2020, Mart 15). *Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik.* Retrieved from Yönetmelik: https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm

BRSA. (2021). *Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Hakkında Yönetmelik (The Regulation related the Independent Audit of Information Systems and Business Processes).* BRSA. Retrieved from https://www.resmigazete.gov.tr/eskiler/2021/12/20211231M6-3.htm

Calder, A. (2005). *IT Governance Guidelines for Directors.* Ely, Cambridgeshire: IT Governance Publishing.

Calder, A. (2018). *NIST Cybersecurity Framework: A Pocket Guide*. Cambridgeshire: IT Governance Publishing.

Calder, A., & Watkins, S. (2019). *Information Security Risk Management for ISO 27001/ISO 27002* (Vol. 3). Ely, Cambridgeshire: IT Governance.

Capital Markets Board of Turkey. (2021). *Capital Markets Board of Turkey*. Retrieved from Capital Markets Board of Turkey: https://www.cmb.gov.tr/Sayfa/Index/0/0

Carataş, M. A., & Gabriela, G. (2017). Internal Audit Role in Cyber Security. *Economic Sciences Series, 7*(2), 510-513.

Carretta, A., Fiordelisi, F., & Schwizer, P. (2017). *Risk Culture in Banking.* Cham: Springer Palgrave Macmillan.

Cascarino, R. E. (2017). *Data Analytics for Internal Auditors.* Florida: CRC Press.

Chartered Institute of Internal Auditors. (2014, October 8). *Risk Based Internal Auditing*. Retrieved from Risk Based Internal Auditing: https://global.theiia.org/standards-guidance/topics/Documents/201501GuidetoRBIA.pdf

Choudhary, U., Antony, J. M., Cooper, M. H., & Srinivasan, P. (2010). System and Method for Auditing Governance, Risk, and Compliance Using a Pluggable Correlation Architecture. *United States Patent Publication*, 1-10. Retrieved from https://patentimages.storage.googleapis.com/20/79/20/30c05df47e5cca/US2010 0198636A1.pdf

Conway, C. M. (2020). *Approaches to Qualitative Research: An Oxford Handbook of Qualitative Research in American Music Education* (Vol. 1). New York: Oxford University Press.

Cooperative Cyber Defence Centre of Excellence (CCDCOE). (n.d.). *CCDCOE*. Retrieved from CCDCOE: https://ccdcoe.org/

COSO. (2013). *Internal Control-Integrated Framework.* Durham: American Institute of Certified Public Accountants and COSO.

COSO. (n.d.). *COSO Internal Cotrol-Integrated Framework Principles*. Retrieved from COSO.ORG: https://www.coso.org/Documents/COSO-ICIF-11x17-Cube-Graphic.pdf

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4 ed.). Lincoln, Nebraska: Sage.

Cuong, N. H. (2007). The Need for Legislation Like Sarbanes-Oxley for IT Governance: An Australia Perspective. *Academia*, 1-5.

Custer, R. L., Scarcella, J. A., & Stewart, B. R. (1999). The Modified Delphi Technique-A Rotational Modification. (K. Swortzel, Ed.) *Journal of Vocational and Technical Education, 15*(2), 50-58. Retrieved from https://files.eric.ed.gov/fulltext/EJ590767.pdf

Dalkey, N. C. (1967). *Delphi.* The Rand Corporation. Santa Monica, California: Clearinghouse for Federal Scientific & Technical Information. Retrieved from https://apps.dtic.mil/sti/pdfs/AD0660554.pdf

Davidson, P., & Hasledalen, K. (2014). Cyber Threats to Online Education: A Delphi Study. In P. Dover, S. Hariharan, & M. Cummings (Ed.), *Proceedings of the 2nd*

International Conference on Management, Leadership and Governance, ICMLG 2014 (pp. 68-77). Massachusetts: Academic Conferences and Publishing International (ACPI).

Defond, M. L. (2005). Audit Research after Sarbanes-Oxley:. *American Accounting Association Auditing* , 5-30.

Degtiar, V. U. (2009). Cybernetics and Communication. In F. Parra-Luna, *Systems Science and Cybernetics* (Vol. 2, pp. 129-146). Encyclopedia of Life Support Systems (EOLSS).

Deloitte. (2019). Moving Internal Audit Deeper into the Digital Age: Part 1, A Structured Methodology for Leveraging Automation to Modernize the Internal Audit Function. Florida, Lake Mary, United States of America (USA). Retrieved from https://www2.deloitte.com/content/dam/Deloitte/xe/Documents/risk/me_moving-IA-deeper-into-digital-age_part1.pdf

Deloitte. (2019). The Future of Cyber Survey 2019: Cyber Everywhere. Succed Anywhere. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/us-the-future-of-cyber-sphere.pdf

Eulerich, M., & Lenz, R. (2020). *Defining, Measuring, and Communicating the Value of Internal Audit: Best Practices for the Profession.* Dallas: IIA. Retrieved from https://na.theiia.org/iiarf/Public%20Documents/Measuring-Value-Report.pdf

European Central Bank (ECB). (2016, October). G7 Fundamental Elements of Cybersecurity for the Financial Sector. Retrieved from https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

European Union Agency for Cybersecurity. (2018). *ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends.* Heraklion: European Union Agency for Network and Information Security .

Ford, G., & Gibbs, N. E. (1996). *A Mature Profession of Software Engineering.* Pittsburgh: Software Engineering Institute.

Fourkas, V. (2002). Cyber Space: Theoretical Approaches and Considerations. *1st International Conference on Typography and Visual Communication* (p. 424). Thessaloniki: History Theory Education. Retrieved from https://www.researchgate.net/profile/Vassilys_Fourkas/publication/274385763_Cyber-Space_Theoretical_Approaches_and_Considerations/links/5bebdf3292851c6b27bd45a4/Cyber-Space-Theoretical-Approaches-and-Considerations.pdf

Gallotti, C., Cottafavi, M., & Ramacciotti, S. (2019). *Information Security: Risk Assessment Management Systems the ISO/IEC 27001 Standard.* Lulu Press.

Gantz, S. (2014). *The Basics of IT Audit, Purposes, Practices, and Practical Information.* Massachussets: Elsevier.

Geers, K. (2011). *Strategic Cyber Security.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) Talinn.

Gercke, M. (2012). *Understanding Cybercrime: Phenomena, Challenges and Legal Response.* ITU. Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Giacomello, G. (2014). *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals.* Newyork: Bloomsbury Academic.

Global Cyber Security Capacity Centre. (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM).* University of Oxford. Retrieved from https://gcscc.ox.ac.uk/files/cmmrevisededition090220171pdf

Göçoğlu, V. (2018). The Assessment of Turkey's Cyber Security Policies in the context of Public Policy Analysis. Yükseköğretim Kurulu Başkanlığı Tez Merkezi.

Greene, F. (2015). *ISACA Journal.* Retrieved from Selected COBIT 5 Processes for Essential Enterprise Security: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-2/selected-cobit-5-processes-for-essential-enterprise-security

Grembergen, W. V., & Haes, S. D. (2007). *Implementing Information Technology Governance: Models, Practices and Cases.* Antwerpen: IGI Global.

Greuning, H., & Brajovic-Bratanovic, S. (2009). *Analyzing Banking Risk: A Framework for Assessing Corporate Governance and Risk Management* (Vol. 3). Washington, D.C.: The World Bank.

Griffiths, D. (2006). Risk Based Iternal Auditing: An Introduction. *Academia*, 17-26.

Gupta, B. B., Agrawal, D. P., & Wang, H. (2018). *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives.* Florida: CRC Press.

Haqaf, H., & Koyuncu, M. (2018). Understanding Key Skills for Information Security Managers. *International Journal of Information Management, 43,* 165-172.

Helmer, O. (1967). *Analysis of the Future: The Delphi Method.* The Rand Corporation. Santa Monica, California: Defense Technical Information Center. Retrieved from https://apps.dtic.mil/sti/pdfs/AD0649640.pdf

Hernandez, S. (2007). *Official (ISC)2 Guide to the CISSP CBK.* (S. Hernandez, & CISSP, Eds.) Florida: CRC Press.

Humphreys, E. (2016). *Implementing the ISO/IEC 27001 ISMS Standard* (Vol. 2). Norwood: Artech House.

Hutchins, E., Cloppert, M., & Amin, R. (2012). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill

Chains. In J. Ryan, *Leading Issues in Information Warfare and Security Research* (p. 80). London: Academic Publishing International Limited.

IIA. (2019). *Introduction to the Code of Ethics*. Retrieved from Code of Ethics: https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Code-of-Ethics.aspx

IIA. (2019). *The IIA Releases New Implementation Guidance for Code of Ethics*. Retrieved from The IIA Releases New Implementation Guidance for Code of Ethics: https://global.theiia.org/news/Pages/The-IIA-Releases-New-Implementation-Guidance-for-Code-of-Ethics.aspx

International Risk Governance Council (IRGC). (2015). *Cyber Security Risk Governance.* Zurich: IRGC. Retrieved from https://irgc.org/wp-content/uploads/2018/09/Cyber-Security-Risk-Governance-29-30-October-2015-Workshop-Report.pdf

ISACA. (2009). *The Risk IT Framework.* Illinois: ISACA.

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.* Illinois: ISACA.

ISACA. (2013). *Transforming Cybersecurity Using COBIT 5.* Illinois: ISACA.

ISACA. (2020). *COBIT 2019 Responsible Accountable Consulted Informed (RACI) by Role April 2020.* ISACA. Retrieved from https://www.scribd.com/document/465071934/COBIT-2019-RACI-by-Role-April-2020

ISACA. (2021). *Information Systems Auditing: Tools and Techniques, Creating Audit Programs.* Audit and Assurance Programs. ISACA.

Islam, S., & Lee, J. (2018). Internal Audit Function (IAF) Competencies and Cybersecurity Audit. *Accounting Information Systems*.

Islam, S., Farah, N., & Stafford, T. F. (2018). Factors Associated with Security/Cybersecurity Audit by Internal Audit Function: An International Study. *Managerial Auditing Journal, 33*(4), 377-409.

ISO. (2018). *ISO 27000 Compliance for Information Security*. Retrieved from ISO 27000 Compliance for Information Security: https://www.infratech.com.sa/iso-27000-compliance-information-technology/

ISO. (2018). *What was the Reason behind the Revision of ISMS Standard ISO/IEC 27000*. Retrieved from Information Security Management Systems ISO/IEC 27000 Family: https://www.isocertificateonline.in/revision-of-isms-standard-iso-iec-27000/

IT Governance Institute. (2007). *COBIT Security Baseline: An Information Security Survival Kit.* Illinois: IT Governance Institute (ITGI).

ITU. (2018). Global Cybersecurity Index (GCI) 2018. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Jain, A. (2005). *Cyber Crime: Issues Threats and Management.* Delhi: ISHA Books.

Jamison, J., Morris, L., & Wilkinson, C. (2018). The Future of Cybersecurity in Internal Audit. *Internal Audit Foundation*, 4-27.

Japan Times. (2020, 01 26). Software Employee Arrested Leak Proprietary Information Russia Spies. Retrieved from https://www.japantimes.co.jp/news/2020/01/26/national/softbank-employee-arrested-leak-proprietary-information-russia-spies/#.Xi7AF0BuI7M

Joiner Associates. (1995). *Cause and Effect Diagrams: Plain and Simple.* Madison: Joiner Associates Incorporated.

Joiner Associates Incorporated. (1995). *Pareto Charts Plain & Simple Learning and Application Guide.* Madison: Joiner Associates Incorporated.

Kahyaoğlu, S. B., & Çalıyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal, 33*(4), 360-376.

Kahyaoğlu, S. B., & Çalıyurt, K. (2018). Cyber Security Assurance Process from the Internal Audit Perspective. *Managerial Auditing Journal, 33*(4), 360-376.

Karabacak, B. (2015). Developing and Verifying a Set of Principles for the Cyber Security of the Critical Infrastructures of Turkey. Yüksek Öğretim Kurulu Başkanlığı Tez Merkezi.

Karabacak, B., Yıldırım, S. Ö., & Baykal, N. (2016). Regulatory Approaches for Cyber Security of Critical Infrastructures: The Case of Turkey. *Computer Law & Security Review, 32*(3), 526-539.

Karabacak, B., Yıldırım, S. Ö., & Baykal, N. (2016). Regulatory Approaches for Cyber Security of Critical Infrastructures: The Case of Turkey. *Computer Law & Security Review, 32*(3), 526-539.

Katayama, A., Shinji, U., Tamura, H., Naemura , T., Kaneko, M., & Harashima, H. (1998). A Cyber Space Creation by Mixing Ray Space Data with Geometric Models. *Systems and Computers in Japan, 29*(9), 21-31.

Kesetovic, Z., & Putnik, N. (2013). Cyber Security. In K. B. Penuel, M. Statler, & R. Hagen, *Encyclopedia of Crisis Management* (Vol. 1, pp. 217-219). London: Sage.

Kizza, J. M. (2014). *Computer Network Security and Cyber Ethics.* North Carolina: McFarland.

Koehn, J. L., & DelVecchio, S. C. (2006). Revisiting the Ripple Effects of the Sarbanes-Oxley Act. *The CPA Journal*, 14-19.

Kohnke, A., Shoemaker, D., & Sigler, K. E. (2016). *The Complete Guide to Cybersecurity Risks and Controls.* Florida: CRC Press.

Kooiman, J. (1993). *Modern Governance: New Government-Society Interactions.* London: Sage.

Korkusuz, A. (2020). Cyber Security and Cyber Risks in Institutions. Yükseköğretim Kurulu Başkanlığı Tez Merkezi.

KPMG. (2018). *Cyber Security & Insider Threats.* IIA. Retrieved from https://chapters.theiia.org/milwaukee/News/ChapterDocuments/Cyber%20Security%20and%20Insider%20Risk%201.17.18.pdf

KPMG. (2018). *Cyber Security & Insider Threats.* KPMG. Retrieved from https://chapters.theiia.org/milwaukee/News/ChapterDocuments/Cyber%20Security%20and%20Insider%20Risk%201.17.18.pdf

KPMG's Audit Committee Institute. (2017). *Is Everything Under Control? Audit Committee Challenges and Priorities 2017 Global Audit Committee Survey.* KPMG. Retrieved from https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/01/2017-global-audit-committee-pulse-survey-global-non-interactive.pdf

Kumar, R., & Sharma, V. (2013). *Auditing: Principles and Practice.* New Delhi: PHI Learning Private Limited.

Kurubacak , G. (2011). E-Learning for Pluralism: The Culture of E-Learning in Building a Knowledge Society. *International Journal on E-Learning, 10*(2), 145-167.

Kurubacak, G. (2007, July 1). Identify Research Priorities and Needs for Mobile Learning Technologies in Open and Distance Education: A Delphi Study. *Mobile Learning Technologies, 19*(2), 1-31. Retrieved from https://files.eric.ed.gov/fulltext/ED495997.pdf

Lanz, J. (2014). Cybersecurity Governance: The Role of the Audit Committee and the CPA. *The CPA Journal, 84*(11), 6-10.

Leech, T. J., & Hanlon, L. C. (2016). Three Lines of Defense versus Five Lines of Assruance: Elevating the Role of the Board and CEO in Risk Governance. *Wiley*, 335-355.

Leech, T., & Hanlon, L. (2016). Three Lines of Defense vs. Five Lines of Assurance: Elevating the Role of the Board and CEO in Risk Governance. Retrieved from https://riskoversightsolutions.com/wp-content/uploads/2020/06/3LoD-vs-5LoA-Elevating-the-Role-of-the-Board-and-CEO-May-31-2016-Risk-Oversight-Solutions-Inc.pdf

Lockheed Martin Corporation. (2015). *Gaining the Advantage Applying Cyber Kill Chain Methodology to Network Defense.* Retrieved from Lockheed Martin Documents: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Lopez, J., Setola, R., & Wolthusen, S. (2011). *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense.* Chennai: Springer.

Manjikian, M. (2017). *Cybersecurity Ethics: An Introduction.* New York: Routledge Taylor & Francis Group.

Mehan, J. E. (2008). *Cyber War, Cyber Terror, Cyber Crime: A Guide to the Role of Standards in an Environment of Change and Danger.* Cambridgeshire: IT Governance Publishing.

Moeller, R. R. (2010). *IT Audit, Control, and Security.* New Jersey: John Wiley&Sons.

Moeller, R. R. (2014). *Executive's Guide to COSO Internal Controls: Understanding and Implementing the New Framework.* New Jersey: John Wiley&Sons.

Moeller, R. R. (2016). *Brink's Modern Internal Auditing: A Common Body of Knowledge* (Vol. 8). Danvers: Wiley.

Morrow, S. (2020). Verizon Data Breach Investigations Report (DBIR) 2019 Analysis. Retrieved 2020, from https://resources.infosecinstitute.com/topic/verizon-dbir-analysis/#gref

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity. (1.1). Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST. (2018). *NIST Cybersecurity Framework The Five Functions*. Retrieved from NIST Cybersecurity Framework: https://www.nist.gov/cyberframework/online-learning/five-functions

NIST. (2020). NIST Cybersecurity Framework. *An Introduction to the Components of the Framework*. Retrieved from https://www.nist.gov/cyberframework/online-learning/components-framework

NIST. (2020). *NIST Cybersecurity Framework (CSF)*. Retrieved from NIST Cybersecurity Framework (CSF): https://www.itgovernance.co.uk/nist-cybersecurity-framework

North Atlantic Treaty Organization (NATO). (2020). *Number of Military Personnel in NATO Countries in 2020*. Retrieved from Number of Military Personnel in NATO Countries in 2020: https://www.statista.com/statistics/584286/number-of-military-personnel-in-nato-countries/

Olson, D. L., & Wu, D. D. (2015). *Enterprise Risk Management* (Vol. 3). Danvers: World Scientific.

Öztürk, M. S. (2018). Cyber Attacks, Cyber Security Audits and an Integrated Audit Model Proposal. *Muhasebe ve Vergi Uygulamaları Dergisi*, 208-232.

Parker, X. L., & Graham, L. (2008). *Information Technology Audits.* Chicago: CCH Wolters Kluwer.

Pathak, J. (2005). *Information Technology Auditing an Evolving Agenda.* Windsor: Springer.

Penuel, K. B., & Statler, M. (2013). *Encyclopedia of Crisis Management.* New Delhi: Sage.

Pickett, K. H. (2011). *The Essential Guide to Internal Auditing.* Chichester: British Library.

Progrebna, G., & Skilton, M. (2019). *Navigating New Cyber Risks: How Businesses Can Plan, Build and Manage Safe Spaces in the Digital Age.* London: Palgrave Macmillan.

PWC Turkey. (2019). Information Technologies Risk and Governance Services: Meet Your Changing Needs with Developing Technology Solutions. Turkey. Retrieved from https://www.pwc.com.tr/tr/Hizmetlerimiz/dijital-hizmetler/bilgi-teknolojileri-risk-hizmetleri/bilgi-teknolojileri-risk-ve-yonetisim-hizmetleri-en.pdf

Radvanovsky, R., & Brodsky, J. (2016). *Handbook of SCADA/Control Systems Security.* Florida: Taylor&Francis Group.

Raggad, B. G. (2010). *Information Security Management Concepts and Practice.* Florida: CRC Press.

Republic of Turkey Ministry of Transport Maritime Affairs and Communications. (2016). *National Cyber Security Strategy 2016-2019.* Retrieved from https://www.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf

Republic of Turkey Ministry of Transport Maritime Affairs and Communications. (2016). *Ulusal Siber Güvenlik*. Retrieved from National Cyber Security Strategy: https://www.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf

Reuvid, J. (2016). *Managing Cybersecurity Risk: How Directors and Corporate Officers Can Protect Their Businesses.* London: Legend Business.

Rose, J. (2015). *Mapping Your Career: Competencies Necessary for Internal Audit Excellence.* Institute of Internal Auditors.

Rose, J. (2016). *The Top 7 Skills CAEs Want: Building the Right Mix of Talent for Your Organization.* U.S.: IIA.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & Mcquaid, R. (2019). *Developing Cyber Resilient Systems: A Systems Security Engineering Approach.* U.S. Department of Commerce. NIST Special Publication. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

Ryder, R. D., & Madhavan, A. (2019). *Cyber Crisis Management Overcoming the Challenges in Cyberspace.* New Delhi: Bloomsbury.

Santos, O. (2018). *Developing Cybersecurity Programs and Policies.* Pearson IT Certification.

Savaş, O., & Deng, J. (2017). *Big Data Analytics in Cybersecurity.* Florida: CRC Press.

Schreider, T. (2017). *Building Effective Cybersecurity Programs: A Security Manager's Handbook.* Brookfield, Connecticut: Rothstein Publishing.

Schreider, T. (2019). *Building an Effective Cybersecurity Program, 2nd Edition* (Vol. 2). Atlanta, Georgia: Rothstein Publishing.

Selig, G. J. (2008). *Implementing IT Governance A Pocket Guide.* Amersfoort: Van Haren Publishing.

Selimoğlu, S. K., & Saldı, M. H. (2019). The Role of Internal Audit: Analysis, Mapping and Assessment of Cyber Risks in Enterprises. *Accounting & Auditing Review, 19*(57), 1-18.

Shailer, G. (2018). Corporate Governance. In A. C. Deborah C Poff, *Encyclopedia of Business and Professional Ethics* (pp. 1-6). Springer International Publishing.

Shamsuddin, A., Adam, M. A., Adnan, S. A., Madzlan, S. I., & Yasin, Y. M. (2018). The Effectiveness of Internal Audit Functions in Managing Cybersecurity in Malaysia's Banking Institutions. *International Journal of Industrial Management (IJIM), 4*, 61-69.

Smedinghoff, T. J. (2008). *Information Security Law: The Emerging Standard for Corporate Compliance.* Ely, Cambridgeshire: IT Governance Publishing.

Smits, D., & Hillegersberg, J. V. (2015). IT Governance Maturity: Developing a Maturity Model Using the Delphi Method. *48th Hawaii International Conference on System Sciences* (pp. 4534-4543). Kauai: Institute of Electrical and Electronics Engineers (IEEE).

Sokri, A. (2019). Cyber Security Risk Modelling and Assessment: A Quantitative Approach. In T. Cruz, & P. Simoes (Ed.), *Eighteenth European Conference on Cyber Warfare and Security (ECCWS)* (pp. 466-474). Academic Conferences and Publishing International Limited.

Solms, B. v. (2005). Information Security Governance: COBIT or ISO 17799 or both?İ. *Computers&Security, 24*(2), 99-104.

Solms, S. V. (2005). Information Security Governance-Compliance Management vs Operational Management. *Computers&Security, 24*(6), 443-447.

Stafford, T., Deitz, G., & Li, Y. (2018). The Role of Internal Audit and User Training in Information Security Policy Compliance. *Managerial Auditing Journal, 33*(4), 410-424.

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice.* Pearson Education Limited.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The Relationship between Internal Audit and Information Security: An Exploratory Investigation. *International Journal of Accounting Information Systems, 13*(3), 228-243.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society, 71*, 15-29.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The Influence of a Good Relationship between the Internal Audit and Information Security Functions on Information Security Outcomes. *Accounting, Organizations and Society, 71*, 15-29.

Stephen, O., Ben-Caleb, E., & Ekpe, E.-O. I. (2017). Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. *International Review of Management and Marketing, 7*(2), 340-346.

Stevens, M. (2015). *Trends in European Governance and Internal Audit.* Lisbon: European Confederation of Institutes of Internal Auditing (ECIIA). Retrieved from https://www.ipai.pt/fotos/gca/iia_portugal_eciia_presentation_1448359723.pdf

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016). *Ulusal Siber Güvenlik Stratejisi.* T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. Retrieved from https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf

T.C. Ulaştırma ve Altyapı Bakanlığı. (2016). *Siber Güvenlik*. Retrieved from Siber Güvenlik: https://hgm.uab.gov.tr/siber-guvenlik

T.C. Ulaştırma ve Altyapı Bakanlığı. (2020). *Ulusal Siber Güvenlik Stratejisi 2020-2023.* T.C. Ulaştırma ve Altyapı Bakanlığı. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/NationalCybersecurityStrategyOfTURKEY.pdf

Tashakkori, A., Johnson, R. B., & Teddlie, C. (2020). *Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences.* California: Sage Publications.

The Institute of Internal Auditors (IIA), The American Insitute of Certified Public Accountants (AICPA), Association of Certified Fraud Examiners (ACFE). (2007). Managing the Business Risk of Fraud: A Practical Guide. California, United States of America. Retrieved from https://na.theiia.org/standards-guidance/Public%20Documents/fraud%20paper.pdf

The World Bank. (2020). *Gross Domestic Product (GDP)*. Retrieved from Gross Domestic Product (GDP): https://data.worldbank.org/indicator/NY.GDP.MKTP.KD?end=2019&start=1960&view=chart

Tipton, H. F., & Krause, M. (2007). *Information Security Management Handbook.* Florida: Taylor&Francis Group.

Trenerry, A. (1999). *Principles of Internal Control.* Sydney: University of New South Wales.

Trim, P., & Yang-Im, L. (2014). *Cyber Security Management: A Governance, Risk and Compliance Framework.* New York: Gower Publishing.

U.S. Department of Commerce. (2004). *Standards for Security Categorization of Federal Information and Information Systems.* Gaithersburg: Federal Information Processing Standards Publication (FIPS).

UcedaVelez, T., & Morana, M. M. (2015). *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis.* Massachusetts: Wiley.

Ula, M., Ismail, Z. b., & Sidek, Z. M. (2011). A Framework for the Governance of Information Security in Banking System. *Journal of Information Assurance&Cybersecurity*, 1-12.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. (2012). *Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar.* Retrieved from Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar: https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf

United States Government. (2021). *IT Disaster Recovery Plan*. Retrieved from Ready: https://www.ready.gov/it-disaster-recovery-plan

United States Government Accountability Office. (2019). *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas.* Government Accountability Office (GAO). Retrieved from https://www.gao.gov/assets/700/697245.pdf

Vallor, S., & Rewak, W. J. (2018). An Introduction to Cyber Ethics. 1-65. Santa Clara University. Retrieved from https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf

Vasarhelyi, M. A., Lombardi, D., & Bloch, R. (2014). The Future of Audit: A Modified Delphi Approach. *Canadian Academic Accounting Association (CAAA) Annual Conference 2011* (pp. 1-31). Social Science Research Network (SSRN).

Vay, D. L. (2006). The Effectiveness of the Sarbanes-Oxley Act of 2002 in Preventing and Detecting Fraud in Financial Statements. *A Dissertation Presented to the Faculty of the Argosy University-Orange Country in Partial Fulfillment of the Requirements for the Degree of Doctor of Business Administration*, 1. Florida.

Venkatraman, S. (2011). A Framework for ICT Security Policy Management. In E. E. Adomi, *Frameworks for ICT Policy: Government, Social and Legal Issues* (pp. 1-15). Hershey: Information Science Reference.

Verizon. (2020). *2020 Data Breach Investigations Report.* Verizon. Retrieved from https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Vohradsky, D. (2019). A Model and Best Practices for Risk Transformation. *ISACA Journal, 3*, 1-12. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2019/volume-3/a-model-and-best-practices-for-risk-transformation

Voo, J., Hemani, İ., Jones, S., DeSombre, W., Cassidy, D., & Schwarzenbach, A. (2020). *National Cyber Power Index 2020: Methodology and Analytical Considerations.* Cambridge: Harvard Kennedy School Belfer Center for Science and International Affairs. Retrieved from https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

Walker, T., Gramlich, D., Bitar, M., & Fardnia, P. (2020). *Ecological, Societal, and Technological Risks and the Financial Sector* (409-410 ed.). Cham: Springer Nature.

Weidenmier , M. L., & Ramamoorti, S. (2006). Research Opportunities in Information Technology and Internal Auditing. *Journal of Information Systems, 20*(1), 205-219.

Westby, J. R. (2004). *International Guide to Cyber Security.* Chicago: American Bar Association (ABA).

Wilson, C., Gaidosch, T., Adelmann, F., & Morozova, A. (2019). *Cybersecurity Risk Supervision.* (M. a. Department, Ed.) Washington, D.C.: International Monetary Fund (IMF).

Yakar, H. (2019). Determination of the Climate Literacy Competencies at Secondary School Level by Delphi Technique. Yükseköğretim Kurulu Başkanlığı Tez Merkezi.

Yeşilçelebi, G. (2019). Creating Combined Assurance for the Integrated Reports: A Delphi Technique Investigation on the Awareness in Turkey. Yükseköğretim Kurulu Başkanlığı Tez Merkezi.

Zain, M. (2019). *CIA Part 2: Practice of Internal Auditing Tips and Tricks on Internal Audit Practice for Excellence.* Zain Academy.

Appendices

Appendix-1. Admission of Ethics Committee

Appendix-2. Invitation Statement for Research Study in Turkish

Appendix-3. Invitation Statement for Research Study in English

Appendix-4. Research Sample

Appendix-5. Semi-Structured Interview Questions for First Round of Delphi

Appendix-6. Panelist Responses to First Round

Appendix-7. Gauges of the Panelist Responses for the First Round of Delphi in Nvivo

Appendix-8. Text Search Query Results

Appendix-9. Tree Maps

Appendix-10. Word Clouds

Appendix-11. Questionnaire for Second Round of Delphi

Appendix-12. Panelist Responses to Second Round of Delphi

Appendix-13. Questionnaire for Third Round of Delphi

Appendix-14. Panelist Responses to Third Round of Delphi

Appendix-1. Admission of Ethics Committee

Appendix-2.Invitation Statement for Research Study in Turkish

İç Denetimin Siber Güvenlik Yönetişimindeki Rolüne Yönelik bir Farkındalık Araştırması,

Sayın Katılımcı,

Doktora tezi kapsamında iç denetimin siber güvenlik yönetişimdeki fonksiyonlarını incelemeye yönelik bir araştırma geliştirilmektedir. Araştırmanın konusu kapsamında tasarlanan veri toplama yöntemleri vasıtasıyla, bilgilerinizden ve deneyimlerinizden faydalanmanın, araştırmanın sonuçlarına ve önerilerine rehberlik edeceği düşünülerek, çalışmaya katılımınız talep edilmektedir. Araştırmaya katılımınız ile ilgili geri bildirimlerinizi aşağıda belirtilen biçimde elektronik posta yolu ile iletmeniz rica edilmektedir. Kıymetli vaktinizi ayırdığınız için teşekkürlerimizi sunarız.

- Araştırmaya Katılacağım(Uygun Tarih)
- Araştırmaya Katılamayacağım

Bildiri: Araştırma için organize edilecek yarı yapılandırılmış görüşmeler (semi structured interview) tez izleme komitesine ve Anadolu Üniversitesi'ne kanıt olarak sunulmak üzere çevrimiçi olarak Zoom programı üzerinden dijital platform vasıtasıyla kaydedilecektir ve korunacaktır. Kayıtlar katılımcıların fikri mülkiyet haklarını muhafaza etmek açısından korunacak ve belli bir süre içerisinde ortadan kaldırılacaktır.

Saygılarımızla,

Doktora Öğrencisi Danışman

Mustafa Hakan SALDI Prof. Dr. Seval Selimoğlu

Appendix-3.Invitation Statement for Research Study in English

A Case Study for Internal Audit Role in Cyber Security Governance,

Respected Participant,

A research study is being designed in order to examine the internal audit functions in cyber security governance as a part of a doctorate thesis. The invitation is requested for your participation in the study as a panel member through thinking that benefiting from your industry knowledge and experience can guide the results and recommendations of the research by the defined data collection methods within the context of the research subject. The feedbacks according to your participation status to research are requested through the transmission of replies with electronic mail as shown below. We are expressing our thanks for your valuable time.

- I will participate in the research as an interviewee (Available Date)
- I will not participate in the research

Notice: The semi-structured interviews, which are going to be organized, will be executed through the digital platform in an online system by recording and keeping in Zoom video conferencing software to present as proof for the thesis review committee and Anadolu University. The records will be protected and then eliminated in a defined period in terms of conserving the intellectual property rights of participants.

Kind Regards,

Doctorate Student — Thesis Advisor

Mustafa Hakan SALDI — Prof. Dr. Seval SELİMOĞLU

Appendix-4.Research Sample

Denetçiler					
#	Katılımcı Kodu	Görevi	Görüşme Türü	Çalıştığı Firma	Görüşme Süresi
1	K4	Teftiş Kurulu Üyesi	Çevrimiçi Görüşme	Kamu Bankası	59 dk 17 sn
2	K3	Bilgi Teknolojileri Denetçisi	Çevrimiçi Görüşme	Kamu Bankası	35 dk 54 sn
3	K7	Bilgi Teknolojileri Denetçisi	Çevrimiçi Görüşme	Kamu Bankası	1 saat 5 dk 48 sn
4	K8	İç Kontrol Bölümü Müdür Yardımcısı	Çevrimiçi Görüşme	Özel Banka	19 dk 22 sn
Bilgi Güvenliği Uzmanları					
#	Katılımcı Kodu	Görevi	Görüşme Türü	Çalıştığı Firma	Görüşme Süresi
5	K1	Bilgi Güvenliği Yöneticisi	Çevrimiçi Görüşme	Kamu Bankası	13 dk 32 sn
6	K2	Bilgi Güvenliği Uzmanı	Çevrimiçi Görüşme	Özel Katılım Bankası	23 dk 56 sn
7	K5	Bilgi Güvenliği Servisi Takım Lideri	Çevrimiçi Görüşme	Özel Katılım Bankası	39 dk 13 sn
8	K6	Bilgi Güvenliği Servis Yöneticisi	Çevrimiçi Görüşme	Özel Katılım Bankası	50 dk 35 sn
9	K9	Bilgi Güvenliği ve Bilgi Teknolojileri Risk Yönetimi Bölüm Müdürü	Çevrimiçi Görüşme	Türkiye'de Kurulmuş Yabancı Sermayeli Banka	22 dk 34 sn
10	K11	Kıdemli Bilgi Güvenliği Uzmanı	Elektronik Posta	Özel Banka	-
Akademisyenler					
#	Katılımcı Kodu	Görevi	Görüşme Türü	Çalıştığı Firma	Görüşme Süresi
11	K10	Akademisyen	Çevrimiçi Görüşme	Devlet Üniversitesi	28 dk 2 sn
12	K12	Akademisyen	Telefon	Devlet Üniversitesi	13 dk 20 sn
13	K13	Akademisyen	Çevrimiçi Görüşme	Devlet Üniversitesi	43 dk 14 sn

14	K15	Akademisyen	Çevrimiçi Görüşme	Devlet Üniversitesi	1 sa 41 sn
Yasal Düzenleyiciler					
#	Katılımcı Kodu	Görevi	Görüşme Türü	Çalıştığı Firma	Görüşme Süresi
15	K14	Uzman(Veri ve Sistem Yönetimi Daire Başkanı)	Elektronik Posta	Kamu Kurumu	-

Auditors					
#	Participant Code	Organizational Role	Interview Type	Enterprise	Interview Length
1	K4	Audit Committee Member	Online	Public Bank	59 minutes 17 seconds
2	K3	IT Auditor	Online	Public Bank	35 minutes 54 seconds
3	K7	IT Auditor	Online	Public Bank	1 hour 5 minutes 48 seconds
4	K8	Assistant Manager of Internal Control Department	Online	Private Bank	19 minutes 22 seconds
Information Security Experts					
#	Participant Code	Organizational Role	Interview Type	Enterprise	Interview Length
5	K1	Information Security Manager	Online	Public Bank	13 minutes 32 seconds
6	K2	Information Security Expert	Online	Private Participation Bank	23 minutes 56 seconds
7	K5	Information Security Services Team Leader	Online	Private Participation Bank	39 minutes 13 seconds
8	K6	Information Security Services Manager	Online	Private Participation Bank	50 minutes 35 seconds
9	K9	Head of Information Security and IT Risk Management Department	Online	Private Banks which are Established in Turkey with Foreign Capital	22 minutes 34 seconds
10	K11	Senior Information Security Expert	Electronic Mail	Private Bank	-
Academicians					

#	Participant Code	Organizational Role	Interview Type	Enterprise	Interview Length
11	K10	Faculty Member (Associate Professor)	Online	State University	28 minutes 2 seconds
12	K12	Faculty Member (Associate Professor)	Phone Call	State University	13 minutes 20 seconds
13	K13	Faculty Member (Professor)	Online	State University	43 minutes 14 seconds
14	K15	Academic (Assistant Professor)	Online	Independent Consultancy Firm and State University	1 hour 41 seconds
Legal Regulators					
#	Participant Code	Organizational Role	Interview Type	Enterprise	Interview Length
15	K14	Specialist (Head of Data and System Management Department)	Electronic Mail	Governmental Authority	-

Appendix-5.Semi-Structured Interview Questions for First Round of Delphi

Açık Uçlu Sorular

- İşletmenizde, siber güvenlik hizmetleri dahilinde, iç denetçiler hangi süreçlerde sorumluluk üstlenmektedir?
- Kurumunuzda, iç denetimin, siber güvenlik kapsamında yürütülen fonksiyonlarının yeterlilik düzeyini nasıl ifade edersiniz?
- Siber güvenlik ile ilgili sorunlarda, iç denetim ve yönetim kurulu arasındaki etkileşim mekanizması nasıl oluşturulmaktadır?
- Organizasyonunuz değerlendirmeye alındığında, gizlilik, bütünsellik ve kullanılabilirlik kavramları sizde nasıl bir çağrışım yapmaktadır?
- Etik kurallar, iç denetim ve siber güvenlik kavramları ile birlikte değerlendirildiğinde, sizde neleri çağrıştırmaktadır?
- Size göre, organizasyonunuzda, etik kurallar, iç denetimin siber güvenlik süreçlerinde üstlendiği rolü gerçekleştirirken takip ettiği yöntemler açısından nasıl tanımlanmaktadır?
- Kurumunuzda, siber güvenlik yönetiminde yer alan yasal çerçevenin ve uluslararası standartların gözetilmesi süreçlerinde iç denetim nasıl bir rol üstlenmektedir?

Open-Ended Questions

- Which processes do internal auditors take responsibility for in your organization within the cyber security services?
- How do you explain the competency of internal audit functions which are being conducted as part of cyber security?

- How is the interaction mechanism between internal audit and management board formed for the issues which are related to cyber security?
- How do the confidentiality, integrity, and availability concepts remind you within the context of your organization?
- What does the code of ethics recall you of when the internal audit and cyber security principles are discussed simultaneously?
- How are the ethical rules defined inside your organization, in terms of the methodologies which are tracked by the internal auditors for performing the role of internal audit in cyber security processes?
- How does the internal audit take part in cyber security management relative to the monitoring activities of the legislative framework and international standards?

Appendix-6.Panelist Responses to First Round

Primarily, the data, which are gathered from semi-structured interviews, are signified as follows;

Question 1- Which processes do internal auditors take responsibility for in your organization within the cyber security services?

Panelist 1- There is a department of the review committee in the bank. This department is not specifically making audits by using technical controls namely penetration or bound security testings for the cybersecurity-related processes. In this context, penetration testing, which has to be performed by an independent association, is necessary to provide compliance with the regulations of BRSA. The findings, which are identified by the assessments of the independent auditors, are reported to the information security department of the bank which has responsibility for stepping into the breaches. Accordingly, before the reportings are made to the BRSA by the information security part of the bank, the review committee has a function for the validation of that breaches, which are identified by the independent auditors, are repaired by the information security department of the bank. The processes, which are executed in the penetration testing operations, relative to cyber security management, are as explained above, besides these, other than cyber security, there are regulations, which are established by BRSA for the information systems and electronic banking services, address the elements of information security and relative to these regulations the audit operations are being performed annually by the review committee through the control lists with reporting the findings to the information security department of the bank. This year the audit operations were executed in this way, in past years, COBIT 4.1 framework, which was established by ISACA, was being adopted by the usage of DS5 system security controls, these elements

are adapted according to the information systems and electronic banking services regulations which are developed by BRSA. Therefore, the internal audit has two main roles in cyber security services, one of them is to validate the findings which are identified by the independent audit organization after the breaches are patched by the information security department of the bank, and the other one is to provide information security through examining the control lists within the context of regulations which are formed by BRSA.

Panelist 2- First, the information security department has predominantly functions in monitoring to provide security stably. On the other hand, in general, the internal audit department is mainly related to reporting and process development operations. Also, the weaknesses of information security are being identified by the internal audit part with the efforts of improvement to fix the security breaches. Additionally, after the internal audit team determined the defects in information security, they are reporting the findings to their management units and information security department.

Panelist 3- There is a COBIT standard that was established by ISACA and was named DS5, in this frame, cyber security processes are being executed within the context of information systems by using this element in the bank. Also, there is a separate organization that serves in technology-related operations of the bank, cyber security is being evaluated separately in this part of the bank, but there is no audit department in this section, the function of this technology segment of the bank is just related with performing of the penetration testing.

Panelist 4- First of all, there is a regulation side of the subject, we are executing many audit operations within the context of the cyber security field in processes of information technology units, with the associations which are providing supportive services and

independent partnerships according to the laws of BRSA which were updated. COBIT 4.1 framework had been being used with DS5 standards until the new laws are developed by BRSA. Also, we who are working as the auditors have been performing our functions as part of management statement due to the organizational objectives in cyber security management according to COBIT standards and risk control matrices are being designed by us as audit department. In addition, the educations are being organized before these audit activities are performed, primarily the system part is being overviewed from the point of cyber security, there are some control points in the organization, the user educations are important for the organization.

Panelist 5- As you know, we as a bank are being audited within the context of the regulations of BRSA, COBIT, and ISO 27001. Also, security information and event management (SIEM) and log management are being used as software tools for security tests and infrastructure which are being audited in the cyber security field that is considered as a part of information security. In these audits, due to the legislative obligations of BRSA, we who are working as an information security department have to perform and sustain SIEM processes with executing and keeping the security and trace records. Also, the information security department is being controlled by both internal and external audits, as a bank, we have two departments which are categorized as internal control and audit board. The information security part of the organization is performing the cyber security efforts in collaboration with internal controls, and the audit board has responsibility for evaluations of these processes within the context of defined scope annually for one time.

Panelist 6- I have been working as an information security manager since 2015 up to the present in B6 bank. In 2015, I was the manager of the risk compliance service until the

end of 2019, in 2019 risk compliance service and information security parts of the organization were merged and then these functions have been being executed under the responsibility of the information security department. We are currently involved in the establishment of an information security management system with designing processes that are related to COBIT 4.1 adequacy and compliance to BRSA regulations to ensure audit and coordination, internal control, and review. As well, we have the authority to execute the follow-up activities for coordination which covers that presenting documents are related to BRSA controls and independent audits by monitoring all necessary infrastructure of B6 Banking Group (B6BG) with detecting the findings and the efforts which are being carried out to fulfill them. Also, we are executing IT risk management projects of the bank, additionally, we are extracting the information assets with all the business units and IT teams with practicing the risk sessions as definitions of threat, probability, and effect for the calculation of risks to determine actions that are being taken. Furthermore, we have processes to ensure compliance for Payment Card Industry (PCI)-Data Security Standard (DSS) because of being a bank and having the card data of customers, so we are also responsible to make efforts for gap and compliance studies. As well, we have compliance studies related to SWIFT systems and Customer Security Controls Framework (CSCF). In terms of performing new projects or major project changes, we are also responsible for security tests, dynamic and static tests, web application tests, mobile application tests, code quality, and code security-related tests, network infrastructure tests. Correspondingly, not only we are assigning personnel within the organization to execute these tests with the applications as NESUS but also taking assistance of enterprises that are able to make penetration testings. Moreover, we are a bank and we have an obligation relative to BRSA regulation so we have to get

comprehensive security tests which are done by an independent penetration testing company at least once a year. These tests include Automated Teller Machines (ATMs), bank branches, branch networks, the awareness of employees, and social engineering simulations. We have a team in security operation center (SOC) inside information security where we have many scenarios such as monitoring the movements of both network infrastructure, servers, and systems, such as SIEM, Guardian, Data Loss Prevention (DLP), Algusec where we make logging and keep loggings with a time-stamped. Also, we have scenarios for fraud or malicious activities or situations which may cause threats. Our rules and alarms work here, and if there is an extraordinary situation or a distressing case, we are also involved in the retention of records with resolution and monitoring of the problem. Likewise, we have products in the areas for managing privileged user accounts and managing application accounts in systems and servers so we are making follow-up audits of them. In addition, we have applications which are called Shell Control Box (SCB) that we call connection recording in privileged admins, thus we are recording and tracking their movements. As well, we are also organizing awareness training to improve the information security awareness of employees within the corporation. These training events are being organized as both in-person education and distance learning as we are now carrying out because of the pandemic period, we organize training events for both business units, IT employees, and other relevant stakeholders. We also do phishing studies related to awareness, we have efforts such as sending phishing through electronic mails or phone for trying to get critical information, if the employees are acting in violation of our information security policies and if there is a lack of awareness, we practice additional studies and we follow up to address the deficiencies. We have applications where we can make risk records and where

we can track our own risk management, as well, we have a special application inside the organization and we have rule sets, we have also actions to ensure that the files which we call common restore or the data on the computers of users to comply with bank policies, so we have corporate principles that we follow here. Furthermore, we have also full responsibility and authority for the operations, which are controlling the access of affiliates, monitoring risks and ensuring compliance, improving processes to manage gaps in audits. Correspondingly, we have committees, we are performing as a team that is affiliated to the General Manager like information security, IT risk management, and IT process management committee. BRSA issued a new regulation on March 15, 2020, and declared to all banks that the information security function in banks is going to be directly affiliated to the general manager or the board of directors and according to these reasons, we are pursuing our reporting and following up our efforts directly connected to the general manager. On top of that, we are responsible for the intelligence part too and as well, we have efforts for topology review, security architecture evaluations, and risk assessments with external companies. We have both internal control and audit departments and there are IT auditors, in these parts of the organization. We are performing as a bank in Turkey as participation of a foreign holding company, therefore, the auditors, who are working as employees of this company, are participating in assessment activities in the bank regularly. Furthermore, as I mentioned before, we are sustaining as a bank so we have to perform cyber security activities in compliance with the regulations of BRSA and according to this reason the bank is being audited annually by one of the four big audit firms which are known as Ernst&Young (EY), Klynveld Peat Marwick Goerdeler (KPMG), Deloitte and PricewaterhouseCoopers (PwC). Also, the audit operations can be performed by assigned employees of BRSA in the bank

corresponding to ISO 27001, if BRSA would like to execute audit operations by its own employees in the bank. Therefore, we can mention four audits that cover internal and external audits to ensure the validity of cyber security management. In practice, the policies and procedures are being observed by the auditors and then they are controlling the records and studies of the information security department in order to understand the precautions, applications, tools, and approaches which are used for performing the cyber security activities. The sampling method is mostly being used by them during cyber security audits, within the context of their audit method, generally, they are demanding record-keeping materials, for example, if there is a fraud or something like that, they are searching for the intelligence records and efforts of information technology.

Panelist 7- There are DS5 processes in the COBIT framework that we are denominating on the subject of cyber security. I mean, I have observed that the audits have been being performed due to the COBIT DS5 process as well as firewall and active directory controls. For sure, I have taken part in DS5, I haven't participated in firewall and active directory. There are numerous control points which we have been evaluating not only cyber security but also system security that covers data classification, user administration, and network security management. Correspondingly, the auditors generally focus on DS5 processes with controlling the structures of intrusion prevention systems (IPS) and intrusion detection systems (IDS). The devices are defined to search the attacks to the network systems which are named IPS and IDS. The alerts are being generated for anyone who tries to make detection with the network. The auditors make controls for the configurations are being executed accurately or not. Also, they make audits in terms of investigating the servers and applications which are used by defined users for understanding whether they honestly need these tools or not. In addition to these, we are

controlling for the updates of security and antivirus software in all fields which are being audited through accurate controls for the investigation of all the security applications and programs that are being scattered to all business machines and devices. As a result, the cyber security cautions can be explained in this form.

Panelist 8- As a part of the cyber security audit, we are now working at the bank and the bank is B5 bank, we are mostly making audits for controlling the compliance of business activities to the regulations of BRSA regarding information systems as the other banks in Turkey. When we look at it from the point of view of cyber security, there is a methodology which is called COBIT and the control fields, that are under the DS5 process, are being checked, so in terms of cyber security we are making audits for what these fields are covering, is there a cyber security program or cyber security policy and are the controls and necessary applications being used, is anti-virus software being installed, are there patch programs in systems and servers. Then, there are controls on the management of user accounts, there are controls on authorizations, and then there are controls on database security and network device security, and the controls are being executed for these fields in the bank on both the internal control side of information systems and inspection board side.

Panelist 9- Internal audits are being carried out by the inspection board within the bank. And then there's a three-level security control mechanism. We have the team that performs information security operations the most which we call phase one. Straightaway, the second line is information technology control and we are in this line as an information security risk team and at the last point, we have an audit team in the third line. As a result, our audit team is responsible for reassuring the board of directors about work done. Technically, they are competent and they are making the audits of us with

assuring for the validity of operations, which are being performed by the information security risk team, to the board of directors.

Panelist 11- They are doing their controls within the framework of BRSA law, information systems management rules, personal data protection law (PDPL) and similar legislation. I am not extending the subject with details because this field is not exactly covering my expertise. However, they have functions in incident control, authorization control, and review of availability. Also, they are making revisions in the processes of third parties.

Panelist 14- In the Turkish Banking Sector (TBS), banks are obliged to establish and carry out their internal audit systems within the scope of the Regulation on Banks' Internal Systems and Internal Capital Adequacy Assessment Process. The purpose of the internal audit system is to assure the senior management about the effectiveness and adequacy of internal control and risk management systems, in which bank activities are being carried out under Law and other relevant legislation and intra-bank strategies, policies, principles, and objectives. In addition, within the context of this regulation, the internal audit unit of the banks;

In Article 21, under the 3rd paragraph;

Information systems are reviewed within the framework of the procedures and principles are set out in the fifth part of the regulations which was published in the 27461 numbered 13th January 2010 dated Official Gazette, as the Control of Bank Information Systems and Banking Processes to be carried out by Independent Audit Organizations, including electronic information system and electronic banking services. Therefore, there is a legal obligation. In addition, cyber security is expressed as information security, which can be considered as a higher concept and it is stated that the responsibility in banks is ultimately

on the Board of Directors (B of D). There is also a separate internal audit approach within the scope of information security.

Regulation on Banks' Information Systems and Electronic Banking Services (Information Systems Regulation), Article 8:

The final responsibility for ensuring information security within the Bank belongs to the B of D. The B of D is obligated to demonstrate the necessary commitment to the appropriate level of security measures related to information systems and to allocate sufficient resources for the activities to be carried out for this purpose.

The article, which was mentioned above, can be considered as the responsibility of B of D is not only confined with the allocation of the necessary resources but also covers to ensure its functioning.

In addition, banks have obligations to carry out internal audit activities of information systems separately in compliance with the information systems regulations.

Article 31: Internal audit function in information systems is established and the assignment of the internal audit responsible is executed to assure the B of D regarding the activities related to information systems management through the bank and the bank's external service providers, by also ensuring the processes supporting these activities and the compliance of the established information systems controls with legislation and internal policies, procedures, and standards, the effectiveness, and adequacy of internal control and risk management activities related to information systems under the responsibility of this person.

Question 2- How do you explain the competency of internal audit functions which are being conducted as part of cyber security?

Panelist 1- First, there are two classes of auditors as part of their efforts which can be defined as focusing on banking processes and pursuing IT processes. In the IT department, there is a team, which is formed by twelve employees, whose profession is computer engineering who are working as IT auditors. From the point of audit, they are not authorized for penetration testing, or they haven't got licenses of certified ethical hacker (CEH) or offensive security certified professional (OSCP) to perform cyber security activities. However, each of the twelve members of this audit team has authorization with certified information systems auditor (CISA), therefore, they can be considered as competent professionals for performing cyber security management processes, because they have both computer engineering degrees and international certifications, on the other hand, they have some weaknesses in finding out vulnerabilities, but we do not need to do this operation, because an independent association is periodically performing these controls, so the internal auditors which have a role in review committee can be marked as sufficient for executing their activities in cyber security management.

Panelist 2- In my opinion, the audit operations which were performed, can be assessed as sufficient according to the recent controls that they executed.

Panelist 3- Primarily, we, who are performing each of us as an IT auditor, are responsible for many subjects which are related to cyber security management with the categorization of organizational roles. First of all, we are starting our job from policy frameworks with controlling the information security policies and we have controls to provide compliance for policy frameworks. Also, we are executing audits for messaging systems, access controls, network controls, and then we are mostly taking care of authorizing, this operation is particularly significant, so the function of defining the authorization levels

matters for us. In addition, we are responsible for virtual private network (VPN), antivirus and firewall controls, so, in this framework, we are performing the controls for how the system can be operated and handled. Therefore, briefly, in general, we are executing the control operations for determining the degree to how the information system is being protected.

Panelist 4- From the point of cyber security, the banking sector can be considered as much developed in comparison with other enterprises in different industries. In our corporation, the cyber security activities started with an information security directorate and then a specific department was established in order to perform operations in the cyber security field. I can rate the sufficiency of internal audit operations relative to cyber security controls as four out of five, but there are some extra requirements for establishing security teams, user educations, or technical training to improve cyber security culture, for example, we initiated to open banking and as a result of these kinds of innovations we have to adapt the bank to the new policies, also we have efforts for personal data protection law. As well, in some cases, regulations can be challenging, for example, there may be some corruptions in banks as data leak in swift related systems, we who are working as internal auditors intervene in the cases in these kinds of special situations. Despite everything, briefly, I can rate the competency of internal audit activities as four out of five as I mentioned before.

Panelist 5- In practice, our bank is being audited by both the internal control department and review committee auditors to comply with regulations of BRSA because the activities, which are related to cyber security, have to be recorded and reported regularly. In addition to these audit operations, independent firms which are assigned by BRSA, are performing audit processes for cyber security and information security activities of the

bank. Also, the auditors of BRSA are executing control processes for the cyber security management of the bank. The performance and adequacy of their audit efforts relative to cyber security are tolerable and reasonable, because all the auditors, who are responsible for controlling the cyber security mechanism of the bank, are observing the proofs of concepts to understand the processing of these operations.

Panelist 6- The competency of internal audit efforts is not capable because of the bottleneck in the number of internal auditors. Also, employee turnover rate is higher in IT audit teams, internal control departments, and review committee parts, actually, this means that they need long term goals to understand the cyber security ecosystem of a bank because every bank has a different structure, there are lots of software applications, security tools, and architectures, so at least six months or one year is needed for them to perceive these elements. Actually, the main problem of internal audit teams who are responsible for controlling cyber security processes, is they haven't got enough experience and knowledge to understand the technical part of cyber security governance so they need to have experience in IT departments and adequate educational background such as system administration, database management, network control or monitoring part of cyber security because these fields require technical competencies. According to these reasons, we are organizing technical educations and inviting the audit teams to improve their professional skills in controls of cyber security processes by explaining how the applications and tools are being utilized in an effort to motivate them to collaborate with information security staff. Some of them are acquiring expert-level knowledge, but some of them are leaving their job without finding any opportunity to attend these technical training events. I think the auditors have to be much qualified than the persons who are reviewed, so in general, there are some weaknesses in providing the workforce for cyber

security in the banks, because this field is fresh and developing rapidly. As well, the bank managements have to take several precautions to retain human capital because there are not enough qualified human resources to operate cyber security field and to enact its audits.

Panelist 7- Before everything, IT auditing is not being performed in the proper sense, for example, there are many qualifications which are needed to be a competent person in the cyber security field. That is to say, first of all, a person should understand software operations, in addition to this, he or she must have network and system management knowledge by combining them to use devices. Also, in this context, this person should use programs and tools, but, actually, we are performing our audits tangentially because of this I can say that the competency level of audits is not sufficient in general. For example, we are not able to make audits as much as capable to control for the detailed actions of Cyber Incident Response Team (CIRT) units, because we don't have comprehensive knowledge of the subject. Accordingly, the audit activities are falling slightly behind the operated actions in the B1 Bank instance. I am comparing with other banks up to the present, for example, B2 Bank or B3 Bank, these banks are directly coaching their auditors in particular subjects, especially IT auditors. Although, an IT auditor is making both division controls and process controls, the rest of the time he or she is making IT controls. As I explained, the IT auditor is making controls to COBIT processes, so the value addition and effectiveness of this person are staying low levels as one-third of normal in cybersecurity-related activities because this person has been trying to do all of the three tasks. The effectiveness of these audits relative to cyber security is standing one-third of the ideal levels. First, the internal auditors have to develop their skills in multiple fields for making audits due to the cyber security discipline sufficiently,

to verify the validity of steps that are taken and to report the flaws. One of them is software, an IT auditor must have sufficient knowledge with intermediate level, second more importantly than this, network and system management knowledge like Windows and Linux administration with knowing how the devices are being connected and how the communication system is being performed. After that, performing the investigations and taking cyber security actions can be much feasible for an IT auditor who has these competencies and then the next step is auditing that the tools are being used validly or not, the tools here I mean are SIEM tools or the regular reviews which are performed to find waste materials by different units. As a result, after having sufficient ability in these three elements which I defined as software, network knowledge, and system management, the person who is going to execute the cyber security audits, can acquire the core competencies. These competencies have to be, if we evaluate the IT auditors of B1 Bank, these particles are not being tutored. The reason for this can be explained as IT auditors are taking part in division and process controls that are related to banking processes besides the cyber security audits.

Panelist 8- In Turkey, BRSA had created the information systems infrastructure of the banking sector for the first time in 2006 with a regulation. In the banking sector before 2006, of course, the actions, which are related to information security or cyber security, had been left to initiatives of the institutions themselves. The banks had been left to their own initiatives, but cyber security and information security in banks had been regulated in 2006 anyway due to the legislative obligations because of the importance of customer privacy and bank secrets. The bank is in a continuous improvement state in this process, of course, when we look at the situation between 2006 and 2008 before 2010, this is actually true in the whole bank sector in Turkey. When we compare it with other banks,

we hear the same things when we talk, information security awareness was low, but as time went on, the awareness increased here because of BRSA regulations and the bank began to provide regular educations to bank staff on information security. Of course, efforts are being made to raise awareness for information security subjects, not only to bank employees but also to customers, so this has come from 2006 to the present day. In terms of cyber security controls and in terms of technical controls which are implemented by the bank, certainly, banks have to be at the forefront of technology relative to cyber security, if you are one step behind, maybe a malicious attacker will harm you, so you should always be one step ahead, so banks are permanently investing and taking action to be one step ahead of malicious people, these investments and actions are being functioned in our bank too. We are taking these actions too, we haven't had a case so far, as a result, I can sum it up in that way.

Panelist 9- We are now subject to BRSA, like all banks. There are the information systems regulations and we're accountable for that, and so currently we have an information security management mechanism in the audits that the inspection board is doing. If they have any findings as a result of their inspections, they are stating. We are taking necessary actions to fulfill those findings by presenting documents to show that the audit findings have been closed and then the reporting is made to the management board.

Panelist 11- In comparison with other sectors, the tasks and responsibilities are precisely defined from the angle of compliance and regulations according to me as who is performing as an employee of a bank. As a result, I can state this level as good.

Panelist 14- The level of competence of the functions, which are carried out within the limits of cyber security in the banks, can be defined mainly as being compliant with the relevant legislation. This level of competence can be categorized mainly as processes

within the bank, independent audit process and supervision of public authority. The level of proficiency can be evaluated as compliance with the minimum requirements of legislation and also it can be considered with administrative sanctions in case of any noncompliance. In this context, all elements of the legislation are controlled by independent audit companies. Another thing that can be noted in this regard is that information security in banks is not only a necessity when technological developments are taken into account, but also it provides a competitive advantage.

Question 3- How is the interaction mechanism between internal audit and management board formed for the issues which are related to cyber security?

Panelist 1- As I mentioned in my response to your first question, we are presenting our findings through reporting to board management regularly with three months periods, in this context, according to the new regulations which were established by BRSA, we, who are sustaining our organizational functions as information security department, are directly depended to general manager. We are organizing information security commission meetings at least two times a year with the participation of the president of the review committee who is also a member of this commission. Within the context of this mechanism, we are reporting our information security actions to board management regularly every year and our bank's review committee is presenting the results of penetration testings to the confirmation of the board of directors four times in a year to control that the security breaches, which are stated in the reports, are patched. Additionally, there is a report which is named as a management statement and this report is being prepared by the review committee and being presented to the conformance of the management board annually.

Panelist 2- The information security committee meets in council with the collaboration of the internal control team and as a result, the decisions which are taken in these meetings are being transmitted to the management board, therefore, there is a continuous interaction between the information security, internal control, and management board parts of the organization.

Panelist 3- Risk control matrices are designed and every risk has its own level, so according to these risk levels, the actions are taken with the discussions. In general, our bank predominantly cares about cyber security risks, because of the sector's sensitivity. Therefore, the interaction between information security and the board of directors is being coordinated sustainably, but it is not possible to produce solutions instantly for every type of cyber risk. As I explained before, we have risk matrixes for cyber security decisions in order to provide decision proposals. In this context, budget management is also important through the values and solutions which are being offered with their effectivity for the decisions of management part of the bank that are related to cyber security.

Panelist 4- We as a bank established our corporate management principles due to the standards of IIA, therefore, we have objectives for periodically informing the review committee and management board. In practice, we, who are working as internal auditors, are linked to the audit committee and we are all presenting our reports to the audit board after that we are transferring our findings to the board of directors. Also, there is not any limitation for access of the review board manager with the audit committee and management board, so, the president of the review board can collaborate with the audit committee and management board without any time constraints. Therefore, if any kind of cyber security risk occurs in the bank, we are informing directly to the audit committee, and as well auditors are providing support and guidance to business units if any

vulnerability in cyber security systems is observed in the organization. In essence, if the risky cases are monitored in information systems of the bank, we are examining the special causes by acting our consultant role, so, we are not directly making controls, but we are supporting them with our guidance function to assure that cyber security management is well organized. We are presenting our reports in three monthly periods and as well audit committee is organizing meeting events twenty times on average in quarter periods to evaluate risk management activities' validity.

Panelist 5- First, you are asking me within the context of cyber security but in our bank, we are discussing cybersecurity-related cases in the information security field, therefore in this context, we, who are executing our functions as information security department, are directly linked to general manager in accordance with the regulations of BRSA. As well, the information security committee is being gotten together three or four times a year, so both from the perspective of auditors and the point of information security governance, informing mechanism is being coordinated through these meetings with presentations of finding reports due to information security risks and vulnerabilities four times in a fiscal year. Additionally, the internal audit part of the bank has its own processes relative to information security within the context of sustaining relations with the internal control department and review committee, so, they are reporting their findings to upper management. Meanwhile, we are informing the other business units with committee sessions too. But mainly, from the point of the audit function, there are internal auditors who are assigned by the organization and independent auditors who are assigned by BRSA to provide intelligence for the decisions of senior management in the information security field.

Panelist 6- Our audit committee and management board organize regular meetings quarterly. As I mentioned before, our bank is a foreign-capital enterprise, so our shareholders request meetings for every quarter of a fiscal year. In these meetings, the findings, which are identified through the audits that are executed by the internal control and review committee of the bank, are shared with top management, therefore, we have an effective monitoring system for cyber security management.

Panelist 7- Normally, according to this, related with cyber security subjects, due to the current regulation, there are a couple of mechanisms as a matter of information systems regulation which directly links with the management board, are transmitting the cyber security subjects to the management board. However, this is not related to internal audit certainly, internal audit is responsible for regularly making reports to the board of directors and they haven't got a specific function to cyber security, there is no link.

Panelist 8- Now, as internal audit units, internal control and audit committees have been already operating directly under the board of directors in the bank, so we, as an independent eye from information systems management, are carrying out routine, planned audits and controls at work, as a result of these controls, the reports, which are being prepared by us, are directly revealed to the board of directors. A small audit committee, that is consisting of members of the management board, has also been established within the audit board and we are sending reports directly to them. They are reviewing our reports and findings, and then that report goes to the administrators in charge of information systems at the head office, and they take are taking actions to clear up the findings. In other words, if a glitch in the cyber security infrastructure is detected, even if this negativity is small or large, then our interlocutor of internal audit and internal control units is directly the board of directors, so the management board is assigning us for these

tasks, because of their appointment to us, we are referring our report to them first, then they are sending these breaches and findings to other units through requesting needed actions.

Panelist 9- Let me put it this way, the information security function can depend on either the general manager or the board of directors in the banks. As a bank, we are carrying out our operations under the administration of the chairman of the audit committee which is dependent on the board of directors. Here, as the review board, internal control and risk management, and information security in the bank, we report our current risks to the inspection board every three months, including cyber security. If there are cases that the review board considers as risky in their audits, they are reporting them to the management board every month. Thus, if there are risks in this way regarding cyber security, or for example due to changing and evolving cyber risks, we are making assessments and after that, we are taking necessary actions if we have to do through reports that present which actions are being taken. Accordingly, we are following these reports by enabling them to be turned into information technology projects. As well, all the projects are being reported to the board of directors as part of the plan.

Panelist 11- This mechanism is being executed through the committees and internally determined teams with planned or case-based meetings.

Panelist 14- Aforementioned mechanism is determined consistent with the relevant legislation, the board of directors has the final responsibility, but the audit mechanism of the banks in this regard is established within the framework of the activities which are carried out by the bank in compliance with the relevant legislation and in a way that requires it to develop and implement appropriate methods. In this sense, intra-bank parts

of the process can be defined as the B of D, the audit committee, the internal audit system, and the IT audit system.

Question 4- How do the confidentiality, integrity, and availability concepts remind you within the context of your organization?

Panelist 1- The recent regulations, which are established by BRSA corresponding to information security, accompanied advantage not only for our bank but also every bank, because, mainly there is a point in the legislation which states that the information security functions of a bank have to be directly linked to the board of directors or general manager. Therefore, because of this reason, the organizational structure was changed approximately one year ago and the information security administration is directly linked to the general manager. Thus, as you mentioned in your question, before this regulation, CIA triad of assets had been being ensured just within the context of information technology, but after the establishment of recent regulations, information security and cyber security functions have been being dispersed into the corporate culture of the bank with the modification of the organizational hierarchy. As a result, we are taking the advantage of this structural change not only in the cyber security field but also in every part of the bank which redesigned the command chain that was adapted to the organization.

Panelist 2- Our team is executing the studies relative to the audit activities of information security through the ISO 27001 and COBIT frameworks, therefore, especially, the information security department is sufficient for providing the CIA triad of data assets. Information security is an extensive field that also covers cyber security, therefore within the context of these subjects, there is an integrity principle for the processes which are being performed in information security both for the controls and improvements. I can

explain the availability term like, for instance, while we are handling a process, we have authorization levels to use applications or tools and we are responsible to ensure information security with optimal usage of sources in the bank.

Panelist 3- Especially, the confidentiality part is very important for the banks. As you know from the regulations of BRSA, the first priority of a bank can be considered as to ensure the confidentiality of data. Also, the availability is being evaluated as a critical item, because the availability of information has to be ensured to serve customers promptly for their satisfaction. On the other hand, the bank is taking care of assuring the integrity part of the CIA triad through monitoring the information systems. Therefore, the sustainability of a bank can not be provided without ensuring the CIA triad of assets, but I can particularly underline the importance of the confidentiality item of the CIA triad in the banking sector.

Panelist 4- Confidentiality, integrity, and availability elements are too crucial for our bank and audit operations. The integrity of data has to be ensured in terms of executing our audit processes through a clean-cut manner and ethical principles. We are adopting the standards of IIA which are defined in the code of ethics part, these rule sets have been being integrated into our corporate management principles. We are paying attention to these principles as all the audit arguments must be formed according to the CIA triad and as well, data governance unit is established for ensuring the validity of our efforts relative to these three items. The audit activities of this unit provide controls for the CIA triad which are performed within the context of COBIT goals. As a result, if these three elements are not ensured, we are not presenting audit arguments, because the process is not being completed and stated as incomplete.

Panelist 5- Information security is based on confidentiality, integrity, and availability elements as you mentioned in your question. These three factors have to be certainly applied to the bank as a part of the efforts of the information security department by fitting in with this set of matters.

For example, the confidentiality term is primarily reminded that every person or business unit, that has authorization in an organization, has to access systems and platforms according to the frame of approval principles. The information systems infrastructure has to be accessed if needed constantly to provide the business continuity without defect and latency from the perspective of availability. The integrity part of the CIA triad is related with an information security expert has to provide that the data are not changed and the integrity of the data is not deteriorated, therefore, we have to prove that the data in the information systems are not modified by using monitoring tools and applications. For example, there are data assets in files, file directories, and file servers, so we have to follow up all the documentaries with also searching for the created dates to identify the operations of altering or deleting the files. If we observe these kinds of acts, we have to use logging and take records of these cases. Therefore, the activities, which are being carried out for ensuring integrity, can be explained as above.

Panelist 6- There are three fundamental titles of ISO 27001 and these are shown as confidentiality, integrity, and availability. Therefore, while we are examining the inventory of data assets with making their classifications, these three elements are being used for assessment processes. Accordingly, we have ISO 27001 certification as a bank and because of this reason we are familiar with this subject, so the asset classification is being made relative to the CIA triad and as well, we are sharing this classification with auditors who are executing their operations based on ISO 27001, regulations and COBIT

framework. In addition, the information security policy procedures are being established according to the CIA triad besides the asset classifications. In banking operations, a large size of data is needed such as customers' home addresses, phone numbers, account balances, card information, or payments from their credit cards. Therefore, if the criticality level of data is high as the data includes customer information, this data can not be permitted to transfer to another device by any way like transmitting the data with universal service bus or electronic mail, because the authorization is not being validated in these type of events. BRSA is making assessments to protect the data assets of the banks by observing the CIA triad conditions, and as well BRSA specifically defines a categorization for the data assets within the context of their sensitivity and secrecy degrees. Furthermore, personal data protection law is being followed besides ensuring the CIA requirements. As I explained before, the qualification of the data assets is being defined within the context of personal data protection law and CIA triad. Basically, in our bank, the assets are being classified in four categories as very confidential, only for the bank, only for service and the public due to the BRSA regulations, personal data protection law, and CIA triad.

Panelist 7- These are the fundamental concepts of security, confidentiality, integrity, and availability. Actually, I explain integrity as honesty or trustworthiness, not the totality, because integrity doesn't span all the meaning. One of them is confidentiality, one is integrity, completeness, wholism or rather is trustworthiness, the other one is availability. What is integrity, this word is unfamiliar to us, actually when I just say integrity, it doesn't include any meaning, let me say so. But, if you say the integrity of something, to be sure that a data is being changed by the right person, I mean, I am getting the data but am I certain that this data is modified by the correct person, so assuring for this principle means

integrity. As a matter of fact, this data is complete, thus this data is defined by the right person and when it is being changed, the authorized person makes the action. In other words, the data, that arrive at you, in total, this concept can be stated like that. In English, this principle is being explained by integrity term. Integrity means honesty, indeed. Beyond everything, the audits are regularly being made every year for confidentiality principle in our main banking application that is named as the finart. This process covers one of the control points which can be evaluated not rather technical for a person at first glance to engage with, because of this reason this one is being functioned smoothly. Literally, we are able to see that the data is being transmitted to authorized person and similarly while this data is being modified for example an interest rate change will be made, the audits are being functioned firmly in order to determine which persons are going to modify this data due to the integrity principle. Moreover, this type of audits is being performed at different times of the year more than one time. Generally, the stoppage times are definite for B1 Bank systems, every system is usually attainable, as well the definition of availability is made as to access the data when needed, the processes are being executed free of problems in both internet banking and bank division services dependent on availability principle. Sometimes, it may become cut-offs over a certain capacity, for instance, in the past years it became a one-hour stoppage because of a time-stamping server. Because of this case, a big problem emerged which is related to availability. I think that the availability concept is being provided adequately in B1 Bank as one of the subjects. The confidentiality, integrity, and availability controls are the fundamentals of information security, therefore these three particles have to be adapted holistically to the audits by the person who is responsible for controls in cyber security. Your audit can be different, as I told you, I am responsible for the banking process which

is related to credit cards and chargeback subjects, I have a control list for these processes and so I am performing my audits concerned with these controls, but on the other hand, I have to pay attention to assure the conditions of confidentiality, integrity, and availability concepts in the controls which I have been making or that is to say, these concepts can not be audited tangibly by making evaluations or doing controls for each of the principles separately through one by one approach. As I explained before, these are the basics of information security, as an IT expert, you need to investigate these elements for every kind of your audit. Wherever you are making audits if you observe any vulnerability relative to confidentiality, integrity, and availability requirements you have to report. As a result, we can consider these three parts as essentials for your audits in terms of reviewing the breaches in organizational processes.

Panelist 8- There are very crucial practices relative to confidentiality, integrity, and availability in the bank, as I said in the first place, the banking sector is inherently sensitive which needs for taking serious actions in protection of customer secrets, so banks are trust institutions and customer privacy is very important. These are available in BRSA regulations, the issue of customer secret is vitally important, when there is a data leak without the customer's permission, it has a way of going to jail, so actions are being taken to prevent these kinds of cases like encrypting the customer information in databases with cryptographing all the infrastructure for internally and externally data transferring, as well, even the internet and mobile banking applications are being operated through encrypted protocols, therefore there are very serious actions regarding cryptography. In terms of integrity, the manipulation of data by malicious individuals is closely related to encryption, and the more you protect a flowing data, the more you protect its integrity, where, naturally, these hash algorithms such as Secure Hash

Algorithm (SHA), such as NB5, are used to ensure control of integrity. In terms of availability, I think you mean availability as accessibility because there is the word availability in Turkish, which means usability, but you mean is accessibility. There are very serious precautions within the context of corporate policies or service continuity policies and there are important actions to counteract a variety of risks as keeping the data center in reserve and keeping backup copies of the data center in two different locations.

Panelist 9- Now there is something like this, normally confidentiality, integrity, and availability are being assessed to understand the adequacy of cyber security management, now privacy is involved after the Personal Data Protection Law (PDPL). This term is considered as secrecy and now we are making evaluations both for the privacy concept and CIA triad. For example, if you are a customer of our bank, your one hundred Turkish Liras in your deposit account, which you look at from mobile banking and see, is related to the integrity of this data, because it is not shown as seventy Turkish Liras when you actually have a hundred Turkish Liras. While the confidentiality of data is being ensured through user name, passwords, and one-time passwords (OTP), we are also using service set identifier (SSID) to block the unauthorized persons to see the data in terms of providing you to access your data holistically which only you can see. This is about availability that you can access your data every twenty-four hours of seven days.

Panelist 11- The application processes of these concepts were transformed into written statements by the corporate data office and information risk management teams.

Panelist 14- If we consider this issue hereof the banking sector, we can mention that BRSA is one of the first institutions for structuring the information security to realize these concepts as legislation and in terms of implementing practices which provide a competitive advantage both on the basis of the sector and the bank, rather than just one

security element. General literature descriptions, which are introduced for the terms of confidentiality, integrity, and availability, are already known to everyone. Personally, it is possible to handle them with very detailed explanations and different aspects. In short, these concepts can be evaluated with the parts of the bank, public, customer, bank sides, etc.

Question 5- What do the codes of ethics recall you when the internal audit and cyber security principles are discussed simultaneously?

Panelist 1- There are ethical principles that are established by our bank. These rules are evaluated as fundamentals not only from the point of security functions but also on the part of all the business efforts in the organization. Therefore, if we consider the codes of ethics from the perspective of integrality, we have to obey the ethical rules in our bank within the context of all the business processes, in every field of the corporation, not just in security-related operations. As a result, there are not any kind of abnormal cases which are observed due to the violation of ethical principles in our organization.

Panelist 2- Information security and internal audit functions have to be performed sustainably with coordinated approaches in the management of both internal audit and cyber security processes. Because, as you considered, the cyber security landscape is expanding, developing, and renovating as a sector, so we could not expect that the internal audit staffs have to be competent as cyber security experts. Therefore, cyber security services can support the internal audit part of the organization by guiding them for which processes they must trace. The findings, which are acquired by internal auditors after the controls within the context of cyber security, are being reported to the information security department, and then, information security team focuses on the defects and breaches which are defined in the finding reports of the internal auditors to holistically

improve the functioning of all the processes. As a result, ethical rules have to be in the move to manage these processes.

Panelist 3- As I mentioned before, compliance with ethical rules is very important in our organization, therefore, the authorization is considered as critical, so we are paying much attention to authorization and the organization has limitations for the authorization of the employees while they are accessing the data assets. So, it is not permitted to access the critical data assets for every person in the organization and within the context of obeying these principles, the ethical rules are being taken care of by the internal audit part of the organization too. The audit segment of the organization is especially taking the code of ethics into consideration and the audit teams are paying extra attention to following these rules in authorizations and assurance of confidentiality. As well, the controls are being performed according to the standards which are being framed by IIA and so we are operating our audits according to this mindset. We have some sections which are being restricted, there are regulations that are being developed by BRSA and also we have rules which are being based on the framework of these legislations and other than these, we are making controls according to the ISACA. Until the last year, COBIT 4.1 was taken into account which was accepted by BRSA as a reference, in contrast, BRSA established a fresh regulation for information systems, and a legislative framework was developed due to the evaluations of COBIT fields with this new regulation that is displayed by BRSA. The regulators have a key role in the constitutions of ethical principles. Particularly, the ethical principles are being followed certainly and doubtlessly in the banking sector.

Panelist 4- As I mentioned before, we are dependent on the code of ethics which are framed by IIA and we adapted ourselves to this mentality, for example, there is a competency term in this mindset, so we have to be competent when a cyber case emerges

to know how to approach and we have to be well educated and we have to improve ourselves. If we are not as much as capable of executing these audits, we have to quit the tasks and we have to outsource the competent persons externally. Therefore, if an auditor has not got enough adequacy and expertise level knowledge to perform the controls and if we have not got enough sources as a lack of personnel, we are not doing this task, we are retreating and the outsourcing is taken into place. Outsourcing activities are defined in our corporate management principles, but before outsourcing the audit experts, we are educating our auditors and we have also audit plans, everything is planned and well organized, so we intend them to gain experience in the cyber security field. We are performing cybersecurity-related audits with making rotations in our control functions, so we are not making outsourcing directly, first of all, we have educational training events generally to fill the gap between the competency of auditors and requirements of the audits. Therefore, we are providing the competency concept of ethical behavior principles in such kind of manner, as I explained. If we consider the integrity concept as the other part of ethical principles, we are recording our audit proofs electronically for presenting them to the business units in the organization. As a result, we are sharing our audit findings adequately with the integrity principle of the code of ethics, we are making final meetings and ethical principles are being followed like that.

Panelist 5- As we mentioned a short while ago, the fundamental principles of information security are defined as confidentiality, integrity, and availability of assets. Actually, the confidentiality part of this triple has further importance and there are some platforms in the organization which can be quoted databases, systems, applications, and application servers as examples of such these environments. Therefore, there are teams that have authorization to perform their tasks on these platforms, this side of the situation can be

considered as an ethical concept, because, just the authorized personnel can reach the data assets in these platforms to execute their business processes and there are authorization limitations for other staffs who are not recognized to reach these cyberspaces. Similarly, we can mention these concepts in order to exemplify the information security part in managing applications, servers, or infrastructure, so every team has its own authorization level which is defined through the matrices of segregation of duties and the ethics as a concept can be explained as every team can sustain their business activities in a limited context, therefore there is any kind of issue in this sense. For instance, in internal controls and independent audits, a database server should not be logged in by the experts who are not registered as responsible persons for the database, so the admin who is working exclusively from the database team mustn't be permitted to access the database. As a result, the authorized personnel has only freedom to access any kind of cyber environment, applications, or tools and I can assure you that this attitude is being used in every infrastructure of the bank.

Panelist 6- The ethical principles have to be worked in process, quite simply, codes of ethics can be explained as, an employee who is working for an enterprise must be motivated in terms of compliance to corporate policies and guidelines through codes of ethics. The ethical principles of an organization are also important in both cyber security and internal audit functions. From the point of cyber security, there are many new attack types, new pishing types, and cases which can cause troublesome conditions. If the employees within the organization deliberately or inadvertently violate the ethical rules of the corporation as becoming a weak link, I mean, if they share the information of the bank with someone else, firstly, we have to know, measure or follow up such this kind of events and secondly, after this data leak or violation case occurred, we need to know the

causes of this event to find out how this act happened, why happened and who made it. We as an information security part of the bank have to organize awareness educations or system arrangements to prevent such this type of events reappear. As well, the audit teams have to proactively identify the vulnerabilities through regular controls by following up the reporting processes and improvements. Moreover, if an employee disregards the ethical principles within the context of ensuring cyber security and if a data leak event happens, the internal audit teams have to pursue and investigate this situation by applying disciplinary punishments to the persons who involve abusing if needed. Actually, we are carrying on such these types of cases by sending phishing emails, initially, we are making educations and then sending phishing emails, we are alerting the person not to share his or her password, but he or she participates the password, after that, we are reeducating the person to be aware of this event, and then the phishing email is resent, if the person is going to reshare the password, we are discussing this person as the weakest link of the cyber security process. Accordingly, the disciplinary process of human resources is being activated, after organizing educations, training events, and awareness events with three scenarios, if still, a person shares the password, this person is defined as the weakest factor of this process. Basically, you can be considered as much as weak as your weakest personnel as a bank, for example, if this person is an employee of a subsidiary, he or she may transfer funds from an account to another account by falling for social engineering acts. Codes of ethics, disciplinary policies, procedures, and preventive controls exist in our company within the context of ethical principles, but we couldn’t control written policies and procedures systematically. Therefore, the audits of internal control and the scenarios of the information security department as one of them is phishing are being stepped in. Exemplary, it is written to not share the passwords in our written policies.

There are documentary statements as do not share bank information or do not share system information of the bank in labor contracts. As well, we are both signing a confidentiality agreement and organizing educations every year, for all that, if a person violates the ethical principles, we apply different ways for the protection of system security. These kinds of cases weren't evaluated critically in previous years as much as the period after the pandemic, but we are executing our organizational functions from home, as you know call centers have been already operating from home. Formerly, we are doing our jobs in buildings, there are cameras, passing systems with cards, internet outputs, and computers which are protected in the bank property. But nowadays, the employees of the bank are sustaining their duties from other locations with remote working, so the criticality level of information and the screens which the employees connect are becoming much more important comparatively before pandemic period, so we expect that the employees have to pay much attention to phishing activities and this type of events.

Panelist 7- A cyber security auditor or the person who is working in this field has all sorts of authority. There is not any kind of data that we can not reach from the point of audit, in this context, we can query every confidential data of the customers or persons. Because of this reason, at this point, it is needed to have an ethical principle or the authority, that is given to you, which can accommodate some privilege as you can get personal interest like transferring money from an account to another one. Therefore, at that point, ethical principles must be defined certainly and this set of rules should be presented as a corporate policy to everyone because if these are not being presented as corporate policy, fraud activities can emerge. I think that the framework of ethical principles must be displayed clearly and it is required to commit this framework to disciplinary regulations because

there are extensive authorization fields for the auditors in information systems, also auditors are able to think that it is not as much as important to make queries, because of this reason the codes of ethics must be framed. I just saw that there are clear rules for the accounts of a president, according to this situation, the warnings are being made to persons to not attempt for accessing the account of deputies or ministers. The auditors and the persons who take in place for cyber security processes have much authority for databases, therefore they can use this wide range of authority for their personal interest. As a result, firstly, from the viewpoint of ethics concept, a person must have own values relative to ethics term and then secondly a corporate policy must be framed, so ethical values are needed to be defined by corporate policies and these values should be accepted by every employee.

Panelist 8- Cyber security is actually the implementations that can be defined as the actions, controls, and ethics are being executed by a corporation that are part of the standards of internal auditing, which are in your interest from an auditor's point of view for your controls that are related with cyber security. For example, if the administrator in charge of cyber security or a staff member, who implements cyber security related controls, is a close friend of yours, it is unethical for you to execute this audit, so this is the standard of internal audit, this is ethics, or in assumption, there is a breach in cyber security infrastructure where the persons of organization can suffer from that vulnerability, but on the other hand, some persons, who exploit that vulnerability, are the beneficiaries, as well as if you are the beneficiary of that vulnerability, this case is considered as unethical for you to audit there and to comment on that vulnerability. This is general audit ethics. In this regard, we provide very strict training of ethics to all auditors in our bank, that is, to everyone who is just starting out on the job. We are

continuously taking educations to absolutely not compromise in violation of ethics and we are paying extra attention to ethics subjects while we are giving educations due to ethical principles. Cyber security ethics is related to ethical understanding in audit subjects.

Panelist 9- When we say ethical rules, our bank has a confidentiality commitment which we have signed to the bank employees. Confidentiality commitment ensures that not to disclose the data of bank and customer information in any way. Correspondingly, we are setting limitations as information technology to not permit access to the data if not needed and not included in the task description. Other than that, there is an ethics line in our bank, if an administrator wants to make a transaction against his/her affiliated staff that is contrary to the banking law and contrary to the ethical principles which are published by our bank, this personnel can make notifications directly through calling this line to indicate his/her department. Apart from that, we already have a lot of ethical controls within the bank, if we have staffs who are doing what we call internal fraud that must not be made or who are trying to do it, we are following them and sending them to the disciplinary committee.

Panelist 10- Now this question actually shows that in your study, yes, the studies in the field of cyber security, my doctoral thesis was in the field of cyber security too, the studies in the field of cyber security are somewhat difficult because there is a lot of lack of sources, especially in Turkey. You can anyway access some information and documents in developed countries, but there is a shortage of access in Turkey because these documents have not been formed yet, and the shortage of resources comes to the forefront when coming into cyber security. Now, we are in the process of new policy-making namely policy-making from scratch, defining and assimilating the concepts of cyber

security in my opinion. You know, the ethics issue has just become debatable in many areas, not in newer areas, but even in more established old areas. In other words, if we think about it in a business field, new literature is actually developing as what we call professional ethics and business ethics, so the saturation point has not yet been reached. While concepts are just beginning to be absorbed in a very new field such as cyber security, even when there are new concepts to be put forward and added to the literature, the ethical rules part is at the very beginning of the road, so we can say like a newly sprouted seed for these ethical rules. The ethical rules in the internal audit itself have been established, yes, an auditing mechanism has been established in Turkey which has a long-established state tradition that has passed from an imperial period to a republic, and no one can say anything about it, but when cyber security is involved, we have not yet fully established the rules of cyber security and ethics, we are at the beginning of this process, let me put it this way. Therefore, the ethical rules can be established by stages which are supported with the efforts of the academics and researchers like you and us, so I mean first we're going to put cyber security in place, then we're going to put policies in place, and then we're going to have information security, we are going to have a lot of policies that institutions, universities are going to have, there is going to be documented, then we're going to have policies that public institutions implement, after that, we are going to have cyber security policies which are being framed in the private sector. Similarly, we're going to argue that there's an ethical deficiency here, that there's an ethical problem in this practice, and then we're going to start gradually establishing the code of ethics, but I don't think we have an application, a set of documents, a resource to talk about ethical rules right now.

Panelist 11- All of the ethical principles are entirely being performed, so we have to write what we do and we have to do what we write.

Panelist 12- While evaluating this subject, if we consider this subject in a somewhat corporate sense, companies, which are especially large and corporate enterprises, now usually follow their transactions in enterprise resource planning (ERP) platforms. Therefore, I think that ERP platforms or computer usage should be evaluated together in business activities. Hence, first of all, as a nature of the business environment, ethical rules are much important for an enterprise, so ethical rules should be established for frauds or irregularities at first, and then these ethical rules should be reported to employees with written statements. Also, I think that the codes of ethics should be converted into programs under the name of ethical principles and introduced to the ERP environment or to the software applications which are utilized for business continuity with the programming languages within the scope of internal audit. If these rule sets are very well established, detected, then encoded and transferred to a programming environment with notifications to company employees, I think that employees can be prevented from cheating or making mistakes or abnormalities in the technology environment. Of course, this approach can also be applied within the scope of cyber security, because as a result of the technological environment, computer environment, or ERP environment, as I said, since the business transactions are being followed in these spaces, as you know the inconsistencies can emerge as a violation of the framework of the ethical codes, as you know, these issues are caused because of cyber attacks or cyber risks, so the encoding conversion of ethical principles to programming environment can provide feasible applications against cyber attacks or cyber risks. Therefore, if you transform the ethical codes into a programming environment, the threat factors, which are being existed

because of human conduct, automatically can be minimized. For example, companies now use electronic signatures and electronic authorizations, as you know, for example, not every employee has access to every program, so such applications can be expanded even further and the authority of employees can be limited, as I said, the frauds can be avoided. As well, one of the things that can be done here is that it is important to follow the logs, log records. As you know, log records are used for monitoring and following up the transactions of every employee in a computer environment, if you do so, precautions can be taken against cyber attacks. After that, the ethical principles must be encoded and controlled within the scope of internal audit systematically. In addition to internal auditing, it is necessary to consider internal control and to use the methodology of continuous auditing. You know, continuous auditing provides real-time controls and reviews of all transactions which are being executed in digital platforms electronically. Therefore, I think internal audits should be used with automation such as continuous auditing. In particular, the banking sector is among the most frequently used industries of continuous auditing methods.

Panelist 13- In general, while the issue of cyber security has only been considered with the professional expertise of certain individuals, currently it can be expressed as an area that must be included among the mandatory field for the persons. Perhaps, we can explain this field as one of the subjects which should be at the forefront of the competency set. We need to master our skillsets in the cyber security field for providing factual and valid recommendations that we have made after our audit operations to ensure the necessary protection against cyber risks, otherwise, how can we perform our information technology audit activities. What we call ethics can be expressed as follows, we have no tolerance there anyway, an auditor must necessarily fully comply with the ethical rules

and perhaps an auditor need to have role model characteristics, we can not make any concession there anyway. So, if we assume that as a structure, this can cause too much riskier cases no matter how a person is very competent but if he/she is unethical and not behaving professionally. Even if an unethical person is very competent, you can't expect him/her to be the auditor. The lack of information can be overcome, but on the other hand, if they are very competent but ethically and morally weak, that person is not acceptable to me, and it is a very basic recommendation of international standards. It is expected that internal auditors should necessarily make their statements and training related to ethics by expressing their character as a role model every year, which is important in this respect. Professional ethics, besides universal ethical values, are not available for every profession, but professional ethics term is certainly described for the audit profession and it is expected to entirely comply with this. For example, a person does not know enough about cyber issues according to international standards, the standards explain that if you are not competent in that field, you can supervise this task by taking assistance from outside, there is no problem with this. However, external support on ethical issues can not be complementary if the employees of an organization have no moral values. So, the persons have to be ethical and have to take over an ethical role in their own character. Therefore, a person can get guidance support on every subject other than ethics. Acting in accordance with ethical rules is much more important and fundamental than the technical skills of the auditor, if the person who will conduct the audit does not have ethical or moral values, others do not matter. The training events need to be organized by necessity, this situation can not be discussed as I know that I don't need to look again, it is necessary to keep awareness at a high level and alert regularly, it should not fall off the agenda in any way. If the issue is to be evaluated within the framework of the bank sector,

the audits in the banks are carried out entirely through technology-based infrastructures and all transactions are carried out in real-time. In addition, due to the structure of the data, the financial markets are based on high-frequency time series, so it is already difficult to perform without continuous audit techniques. While auditing processes related to cyber issues, you can test processes that are vulnerable to cyber risks and people, which are also considered as critical assets, in terms of authority, for evaluating their predisposition to the ethical dilemma or ethical violation. In this context, the audits of ethics should be carried out along with cyber security audits. Ethical standards of behavior should be integrated into corporate culture and must be spread throughout the organization. Where ethics are most violated as conflicts of interest, where we call it the conflict between personal interests and corporate interest if a person accesses a data, this data will be used for personal interest or corporate interest. A number of remedies are sought for prevention, such as transparency or accountability. Especially in the banking sector, it is a very sensitive issue, I have experience and background in the bank inspection board, what we are looking for is the bilateral control mechanism and what we call the trilateral agreement, which is important for the borrowers to be aware of these and to prevent possible thefts, losses and when third parties are involved in the virtual environment. If moral awareness of individuals is increased within the corporate culture, the risks in terms of cyber security can be reduced. Of course, there are indicators of ethical leadership, dissemination, and strengthening of the corporate culture. The ethical issue is such that, as I said in its absence, others don't matter, it can be thought of as the first number in front of a million, even if you have so many zeroes which can be assimilated as your competencies, you will have just zeros if you don't have one which can be shown as ethics in front of these zeros, so, the competency level doesn't mean

anything if ethical values are missing. There are findings in the literature that the corporations, which provide this foundation in terms of institutional structure and support it as strengthening effect with social responsibility projects and activities, reach success.

Panelist 14- It is an important and necessary fact that ethical rules are important and necessary in each line of business and type of organization. However, control stages are needed to be designed as independently, transparently, and accountably as possible in business processes, from the bottom operational unit to the top managerial unit, especially in critical, complex, and large organizational structures. Banks are regulated more strictly in these matters than normal commercial enterprises and subject to many additional legal obligations. One of the most important reasons for this is that the banks are not only commercial entities, but also they are performing critical public service. Therefore, in addition to the ethical rules and organizational activities of banks, which are respected as trustworthy organizations, they are audited by many different associations in terms of both internal audit, independent audit, and public audit. The fact that cyber security transactions in the banking sector have a separate set of legislation and detailed rules can also be considered as an indication of how sensitively the issue is being handled in our country.

Panelist 15- Ethics means that doing the right, good, and fair as a practical definition. When we say ethical rules, there are three systems that can be classified as values at the top, principles under the set of values, and rules under principles. When we consider ethical rules, what can happen if you basically determine your values like honesty, also values can be categorized in various ways, there are corporate governance values, there are basic values, there are some principles under these values, for example, honesty is value, but not to lie can be evaluated as a principle under the value concept.

Correspondingly, the codes of conduct arise, in this logic, there is already a framework, basically, there is a value at the top, for instance, an institution may have seven or eight values, there are principles below this framework as well, also under this category there are the codes of conduct in order to define expected behaviors, so from this point of view values are formed in this way. On the other hand, internal auditing is defined primarily as the principles, procedures, institutional structure, and above all, the control mechanism of that institution to add value for an institution, because the control mechanism is controlled by internal control, two parts of the organization should be evaluated differently. Internal audit has the main objective of systematically examining the control mechanism to detect that this mechanism is working to add value for the institution. One of the important concepts here is to add value and the other is a systematic review. There is security within internal audit, cyber security is one of the very important areas, I can define cyber security as a system that will allow an organization to control its information processing, information security systems, and protection structure against threats with a very rough definition. In this context, penetration tests can be given as an example. The protection of critical information can be basically called cyber security. Information technology security is actually one of the areas that internal auditing should control. On the information technology side, there is also the control part, it is a newly developing field, so it is difficult to control because it is not a well-known field. However, not many details are needed to be known, it may be enough to know what to control in information technologies. From my point of view, I have a checklist, for example, where passwords are being stored securely or are they being backed up, so these are all parts related to information technology security. After all, the auditor doesn't need to know how to make the backup, but the auditor needs to know if the password security is intact or if the backup

has been made, or if the firewall is being used. In short, the person who will oversee information security doesn't have to be the most expert on these issues, this person just needs to ask the right questions about these issues. So, the important thing is to ask the right questions. Of course, these responses may be misleading and so the auditors need to have some technical knowledge to control them. In fact, in summary, the competence related to information systems can be accomplished by the auditor or the person who has capability in information systems can be assigned to audit role. Both methods can be used, in my opinion, there should be internal auditors who are familiar with the subject of IT and experts in the field of IT who know the subject of internal auditing. Information technology control is a specialty, but as I said, as an auditor, you do not necessarily have to be an expert in IT, because it is a technique, you can comprehend what, how to control with logic through asking the right questions, also the expertise support can be taken if it is required. From the point of ethics, for example, ensuring the confidentiality of the information which are obtained during the audit or the methods which are used to get findings can cause problems that are related to ethics. In fact, the subject can be divided into two parts in the form of the ethics of internal control and the control of ethics. It can then be examined as the ethics of cyber security and the interaction between internal audit and cyber security. Besides, there is the intersection of three elements which means there are both ethics, cyber security, and internal audit. The general technique is always the same, first, you must define the risk field, while the functions of internal audit in cyber security are being performed and then you must map the risk by the determination of the probability with the impact. For example, if there will be phishing attacks on the system, how much damage they will make or some cases happen once, but the effect can be huge, they are also called black swan risks. In terms of cyber security, earthquakes are very rare

and when they emerge, you can suffer much, so it is necessary to back up and diversify the region. Therefore, a risk map is created for each category and then the tests are done.

Question 6- How are the ethical rules defined inside your organization, in terms of the methodologies which are tracked by internal auditors for performing the role of internal audit in cyber security processes?

Panelist 1- We have an internal control directorate except for review committee administration and this internal control part of the bank is consistently making daily weekly and monthly controls. The internal control directorate doesn't take executive actions, this department has a role in finding out the inconvenient cases and reporting them as findings to the management board.

Panelist 2- An internal audit team has to commit ethical principles while executing functions in cyber security and information security. In our bank, ethical principles are being used as fundamentals while the audits are being operated and reports are being formed. After these processes are completed, the cyber security team gives feedback related to those subjects like informing the internal audit team as we did these operations, we did these studies about these subjects, we identified weak points, Certainly, all this process has to be performed in commitment with ethical principles.

Panelist 3- Actually, the auditors have warranties to watch many factors, but there are some restrictions to eliminate unnecessary elements in the banking part, so our audit activities are being limited in the security-related processes as we are not authorized to audit some factors. This situation can be explained as, if we begin an audit process, we have permission to access just the related fields and we have time limitations while performing our operations. For instance, an audit operation is planned to be completed in two or three days, so we have defined time constraints to finish our audits. From the point

of cyber security, control points are being organized to charge extra responsibility for IT auditors. The regulations mostly fall behind the developments in technology. The regulations which were established for information systems have to be designed and executed a long time before, however, this legal framework was merely issued last year. We are performing our audit processes by firstly making researches of changing and developing system, namely what conditions change and what can be done, there are some bases but there may be some modifications on these bases, for example, new software can emerge, so in this case, we are making reviews and examinations, the audit process starts like that. After that, the controls are being initiated based on new concepts. This situation doesn't cover the legislative framework, the legislations can just frame defined principles, it is needed to understand the bases of regulations.

Panelist 4- Principally, first of all, we are trying to be proactive in this subject related to cyber security and information security activities, so we are handling risk assessment studies. As a part of these efforts, we are using the control category assessment method through this way the discussions are being made with all the senior managers as well there is a GRC module which is applied on Archer GRC platform and tools, so by using this application, we are presenting a questionnaire to the managers and all the shareholders are providing data through these questionnaires before the risk evaluations. After that, we are assessing these data and then we are planning our audit operations according to the criticality level of the risks, for example, cybersecurity-related events are often classified in risky fields, but the reason for this issue is not associated with an organizational structure or weak controls, the main reason of this situation is interconnected with cyber security is an expanding and developing field. As a result, we are primarily paying attention to the cyber security field and this field is being stated as high risky, we are

gathering data from both stakeholders and past audit proof of concepts by using the infrastructure of information systems, the planning activities are being realized like that.

Panelist 5- Definitely, this process has to be available and this process can vary due to the corporation or infrastructure, as I mentioned a short while ago, every department or business unit should perform the tasks according to the separation of duties, this principle is mandatory in our bank. Inevitably, there may be some weaknesses relative to improvements, but these types of issues are existing in every corporation, as a result, the problems must be determined and analyzed by taking the necessary actions within the context of ethical concepts to expand the usage of them in audits.

Panelist 6- Actually, it can be much helpful to ask this question to human resources (HR) and internal audit, but our ethical rules are framed through the policies and procedures which are established with documentaries by HR. The internal audit department has been already making studies and examinations relative to controlling the compliance-related cases. If there is any kind of violation, the internal audit part of the bank is initiating and executing the particular studies and investigations, so the disciplinary process is being performed in that way. If you consider these efforts as sufficient or not, if I search for information security these are adequate from my standpoint. Nevertheless, cybersecurity-related developments have been rising each day, and if I evaluate B6 bank, B6 bank is much a merciful and humanitarian bank, likewise, we have human assets directorate instead of an HR directorate. Perhaps, in later times, it may be much effective to take many solid sanctions into consideration there. The lay-offs can be stepped in as a result of findings of the internal auditors according to the code of ethics. This commentary is mine, but. It is much relentless to lay-off, but if a person doesn’t obey the ethical principles, there is nothing to do for this person. In other words, the question that, are the

ethical rules sufficient or not for internal control, has to be replied to by internal control, but we can rank it as sufficient. In practice, they have not been following up the cyber security processes totally, because they haven't got enough sources so their audits are not being executed comprehensively because of the lack of sources. There are weaknesses. If they have source and time, and if they concentrate, perhaps, they will audit much efficiently. They are auditing one of them and leaving the other one. My IT auditors are especially interested in compliance to the COBIT standards which are being ordered by BRSA and the new regulation that is established by BRSA rather than making controls through discussing the integrity or some other principles which you told. Probably, the log management activities and the recording processes of them can be given as an example, they are periodically making audits for these activities relative to cyber security controls. However, this doesn't mean that internal auditors are making near-perfect audits. They are trying to execute their profession as they can because there are some weaknesses in sourcing, so in order to solve this issue, the budget should be planned. In Turkey, the sources must be increased in both the information security field and internal audit part. Especially, there is a bottleneck in the amount of qualified professionals, so the educations must be organized. Also, experienced and well-educated personnel staff must be retained in the organization. You are asking whether the ethical codes are adequate or not, of course, these principles should be framed in a plan continuously through making discussions with shareholders. Therefore, you are telling that the data inside the corporation must be protected with the definition of roles and responsibilities of the employees and the awareness of them should be provided through ethics. I am extending this mentioning, when it comes to ethics, while you are working with a firm, you mustn't have any contact or you mustn't accept present, so these types of events are

recurring to the mind. However, you are trying to recall that the policies and procedures relative to data sharing and authorization, so the adequacy level of them. As a result, possibly, it contributes many benefits to the bank if the auditor colleagues should perform systemic controls rather than manual controls.

Panelist 7- The truth of the matter is that the ethical principles are not defined in a framework, one of the weaknesses is that these are defined by word of mouth in B1 Bank and as a result the persons especially the auditors are being perceived as a most reliable part of the organization and actually this perception is right, because of this reason they don't look to apply each of the ethical concepts one by one. In contrast, the persons are losing their jobs because of these reasons as doing a query which mustn't be executed or like that. In this context, there is not certainly defined ethical principles structure in B1 Bank.

Panelist 8- While taking actions that are related to cyber security, for example, for the period that the units, which are relative to cyber security, are taking actions, the auditors must put aside their personal interests. For example, there are organizational units which have authority to get decisions in cybersecurity-related activities, there are a department, team, and manager that are responsible for IT, also there are business units and there is a separate cyber security unit. Now, each unit actually has a different target, a cyber security unit demands that the information of the bank, the institution, or the company are not be stolen or are not be hacked because of data security to be safe, but the other business units want us to open up our business all the time for getting new customers, so they want to take some actions to make money for the company, maybe they are opening new doors to expand our business, at that point, there is emerging a conflict here between cyber security and organizational goals because they want to increase profitability and the cyber

security department aims to provide safety in fact. Therefore, while other business units are taking as many different risks as possible, on the other hand, the cyber security side is trying to reduce the risk as much as possible if these two functions depend on the same person, that is, if both the IT side, the business units, and the information security part that wants to eliminate the risks depend on the same person, then there may be a conflict of interest so that the manager who is related with all these units cause much worse cases because of the conflict between the ambition to earn much profit and cyber security risks. Therefore, cyber security units need to be independent and autonomous in corporation. In other words, it should be independent of the departments which have the responsibility in sales, marketing, or IT due to ethics. I can tell you that.

Panelist 9- Now we have something like this, we anyhow have a principle that needs to be known, we call this need to know, we have a role-based system that we use in applications which demonstrates defined authorizations besides the task description. There is no question of appointing any staff member to a role that is not authorized, approval must be obtained while giving authorization. Aside from that, there are ways for whichever operations are being executed and they are being reviewed regularly. As I mentioned earlier, if anyone is trying to access data or doing abnormal work without authorization, an investigation is being launched for this personnel because this act is deemed unethical. This principle involves cyber security too, if any of the bank staff involves in an activity which exceeds their authority, whether they are a division employee or a director in cyber security, if they engage in activities that do not comply with the bank's ethical policy, we are anyhow identifying them and reporting them to the inspection board. There are such routine controls that the review committee has done anyway. I mean, the inspection board is performing as an internal audit committee.

Panelist 11- I can not share certain knowledge because this part includes internally kept information.

Panelist 14- The answer to this question was explained in the response to the previous question.

Question 7- How does the internal audit take part in cyber security management relative to the monitoring activities of the legislative framework and international standards?

Panelist 1- In the framework of regulations and legislative standards, we are following up with the regulator associations in Turkey as an information security directorate. There is an information security and communication guide book which was established by the Presidency of Digital Transformation Office of Turkey and there are regulations which are issued by BRSA for information security and electronic banking services, when these regulations are preliminary presented, these regulations are denoted by legislation and compliance administration part of the bank to our department. Therefore, we are trying to reflect these control points to our business processes, from the perspective of audit functions, our review committee is executing the audit activities are based on the control lists that are being formed due to these local standards and international legislations. The findings which are acquired through these audits are reported to the board of directors and the monitoring function is being performed periodically for six months.

Panelist 2- There are a lot of associations and procedures which are related to the assessments of cyber security processes in the context of working both nationally and internationally such as if I consider the banking sector, as a result, the corporation is a bank that we are working for and this bank is a participation bank which is dependent on the BRSA processes. There is a regulation that is related to the banks and issued by

BRSA, in general, this regulation can be updated from year to year in various periods. Therefore, we have to comply with this regulation completely as a bank, otherwise, there are severe punishments and sanctions to corporations, particularly in consideration of this year if BRSA identifies any kind of finding corresponding to cyber security vulnerabilities of the banks, it can enforce severe penal sanctions. In other words, there are processes are being controlled by the internal audit and information security teams on the subject of international frameworks including COBIT, Payment Card Industry Data Security Standard (PCI-DSS), and ISO 27001 which cover the sets of rules. There are a lot of policies and procedures and all the banks and financial institutions have to fit in with these regulations, this situation can be explained in such a manner.

Panelist 3- If you don't meet the international standards, there are a lot of international banks and financial institutions which are collaborating with banks, because of this, all of them are expecting that competency, so you have to care to provide their conditions. COBIT has different thirty-four criteria which are established by ISACA, each of the criteria is being audited individually, the system may be needed to be audited according to the frameworks of ITIL and ISO 27001. Also, as I mentioned before, rather than these, we have separate audits which are being accomplished in terms of system base, active directory controls are being performed separately, messaging system audits are being performed separately, additionally, penetration testings are being applied and as well the audits are being functioned for the identification and detection of security breaches and vulnerabilities. We have single audits from the aspect of DS5 and the perspective of IT. Our audits have been being performed in a fiscal year relative to information security and other banking processes, more than these, we have activities to review, process, and findings are being controlled, the adjustments are being followed up and the controls are

being made to understand the level of adjustments. After these operations, the actions, which are utilized, are depended upon the criticality level of finding, are being controlled once more, the discussions are made with business units all over again, the responses are demanded further and then the reporting activity is made to senior management and board of directors. From the point of banking side, the reporting to the management board is not singly satisfying, besides, we have independent auditors, before all else, these independent auditors are executing their controls in both banking processes and information systems after they completed their audits, they are controlling the audits that we performed and also the reviews are being made by the controllers of BRSA, finally these audit findings are being presented as management statement to BRSA. As I mentioned before, risk ratings are being made in our risk matrices, secondly, the bank is not singly under our custody, the independent auditors are fulfilling controls separately, therefore we can't evaluate our system as perfect, because an independent audit is being carried out, so you have to put forth the best system for consideration. The banking sector is already risky and very risky, as I told you, this sector is very rigid because the monetary operations are being made in banking processes, therefore there is no remission and you have to provide your audits above a defined rank. B1 Bank is the biggest bank in Turkey and it is also the most deep-rooted, because of this reason the systems have been being developed gradually and step by step approaches with years of experience.

Panelist 4- I mentioned about Society for Worldwide Interbank Financial Telecommunications (SWIFT) audit to you, for instance, there is a framework related to customer security which was established by SWIFT corporation, so we are taking our actions instantly if needed, when we discovered something about this framework, because of this, the educations are being organized at first, after that the framework of SWIFT is

being integrated and then we are initiating the audits of this through forming control points. Similarly, we were performing our audits according to the COBIT standards, nowadays we are keeping aside the COBIT standards because there are new elements that came along with information systems regulation. Before this regulation was established, the audits were being functioned due to the thirty-four items of COBIT which were requested by BRSA, but currently, these thirty-four fields were reduced to thirty. Therefore, we did that, we matched the COBIT standards and the regulations of BRSA, in this way we formed an integrated framework, as a result, we are both operating with international standards and complying with the regulations of BRSA, so we did an adaptation in that manner, we also integrated this to our audit plan and then our auditors have CISA according to the regulation, there are ten IT auditors and almost each of them has the international certification. As well, we are arranging annual education plans for IT auditors and the condition of one hundred hours of education for every three years was stated in regulations, in spite of that, we are not affected by these kinds of cases because we have already installed our system according to the international standards and we are following on this direction.

Panelist 5- As I stated at the beginning of the conference, first of all, we are dependent on the regulations of BRSA as a bank, in addition, correspondingly we have certification in the context of ISO 27001 so we are involved in the ISO 27001 too. At the same time, we are liable to function of the DS5 article of COBIT which explains the execution processes of infrastructure activities. Hence, independent and internal audits are being performed based on cyber security and information security according to these accepted international frameworks. Independent firms make audits in accordance with the regulations which were established by BRSA due to the bank unions. In general, the banks which are

sustaining their businesses in Turkey, are dependent on the regulations of BRSA, in addition to that, they are coherent to control points in the DS5 article of COBIT within the context of ISO 27001 compliance. Together with, if I give you the technical details about this subject, technically, in every field we have to operate the security controls by using the globally accepted tools, for example, when a penetration test is being functioned, Open Web Application Security Project (OWASP) Top 10 control lists have to be applied. Meanwhile, we need to utilize SysAdmin, Audit, Network, and Security (SANS) or other globally conformed control lists in order to provide tests both globally and nationally accepted. Add to that, from the point of log management, we are executing our efforts in Security Incident and Event Management (SIEM) part upon regulations, especially, some of the actions or some of the rule correlations can be technically adapted to some of the standards framework or regulations for taking advantage. For example, there is a mitre attack framework as a part of SIEM for the banks to improve their infrastructure. SIEM is actually not an exact log management, log management part is just for the management of the logs. However, the SIEM part is not simply accepted as log management, because this structure is used for the analyses are made by matching and parsing with the logs through combining them for building the correlational rules. For example, when any kind of software is accessed to a server, first of all, I have to determine that the type of this software by looking for the logs in all the bank's infrastructure. If I identify a malicious act, I have to find the sources of this malicious software by matching the name of this software with analyses and alerts in such cases as brute force attacks. As a result, SIEM is an extensive mechanism. Therefore, I am the opposite to evaluating SIEM like a log management system as an information security expert because log management is just the small particle of SIEM and SIEM is a big world

in comparison with log management. IBM Q Radar, Splunk, and Microfocus R Side are the most known SIEM products. There is a National Cyber Event Response Team (CERT), in this association there is an application platform that is named as Cyber Intelligence Platform, you can make necessary notifications on this platform. If I explain this situation much rationally, for instance, if someone makes to your bank a phishing act, you can request to block the email addresses which cause phishing acts in both Turkey and the globe by using this Cyber Intelligence Platform. In practice, when you come under a phishing attack, you can enter this platform with your user information and then CERT is taking over the case to get necessary actions. As a matter of fact, this process has refrained because of the pandemic, the meetings were being organized two or three times in a year before the pandemic, in my opinion, these meetings have to be arranged much frequently, the collaborative relations are needed to improve this process. Something like this happens, for example, a security vulnerability or hacking case emerges in whichever a bank, naturally, these cases aren't reported to CERT because of the loss of prestige and other reasons. Therefore, almost all the banks avoid some more in this type of notifications, they are trying to solve these types of situations internally because no one wishes that these kinds of events happen in their organizations. In my personal opinion, the relationship between CERT and the banks has to be much consistent and continuous. In this context, the interaction between the banks, BRSA, and Information Technology Communication Corporation has to be much strong.

Panelist 6- Internal audit part of the organization is performing audit activities that depend on the compliance of information security processes to COBIT 4.1 because BRSA requests that we have to be adequate with COBIT 4.1. As you probably know, COBIT 4.1 is an international standard and a framework. COBIT 5 was established, COBIT 2019

was launched, but still, BRSA has been asserting to us, I mean the banks that to comply with COBIT 4.1. This standards framework was designed to form and control IT processes, so our internal control teams are executing audits every year according to COBIT 4.1. COBIT 4.1 has thirty-four processes, essentially, internal controllers are making audits partially on at least seventeen or twenty processes. In practice, they are recording the findings and they are tracking the actions related to these findings. Aside from this, our bank has ISO 27001 certification, therefore the associates in internal control are making controls in the context of ISO 27001 too. Also, there are regulations of BRSA and the internal control department is doing works across the compliance to regulations of BRSA.

Panelist 7- As I mentioned before, there is a monitoring process which is being performed for controlling the existing steps that are related to cyber security through checking how these steps are being controlled with making audits for compliance of these actions to Turkey legislation, international standards, and corporate culture. Therefore, if we find any control deficiencies over a categorical level, we are reporting to the management board, so control and monitoring operations are based on these processes. Actually, internal auditors are performing their tasks that are related to all the cyber security infrastructure with accepted levels for every fiscal year and they have sufficient capacity to monitor all infrastructure. At this point, there are some inefficiencies because of the task description of the IT auditors which is not just covering the IT-related subjects. In general, we are trying to meet the requirements of BRSA and in this context, the monitoring function is being executed as reporting the deficiencies, which are identified in controls, to the management board. ISO 27001 and ISO 22301, in other words, business and system continuity, information security, and the controls of references as

COBIT, NIST are being directly monitored by IT auditors, therefore, we are the main responsible persons for controlling the compliance of decisions and actions which are taken in terms of performing cyber security management to the legislations of Turkey and international regulations. Based on this, the IT auditorship is the unique controlling authority within the context of monitoring processes, the reports, which we prepared for the management board and which we presented directly to the board of directors, are being too much effective. In practice, the reports which you prepare for any bank division are not directly reported to the management board, the entire reports which cover all of the audit activities are only being reported to the management board with three monthly periods, but if you observe something in firewall audit, this type of findings is being directly reported to the board of directors, therefore the monitoring operations, which are relative to cyber security, are being transmitted by us. We have internal control and an auditor, the auditor is playing a role as an internal auditor, internal control is being performed within the context of BRSA concepts, there is a different unit which has functions as an auditor. As I mentioned, there is a fundamental of this action, because especially the positioning of IT auditors which is called as process controls, so process controllers and IT auditors are being perceived as same in our bank, because of this reason the IT auditors have been being called as process controller since 2007 for fourteen years. I have been here since 2015, but this process is being performed as same before too like process controller is taking a function as IT auditor. First of all, this is wrong, however, process controls are being evaluated much significantly than division audits and the interaction between an associate of general manager, review committee chief and management board is being functioned accurately in B1 Bank. Actually, positioning is right, thus the mechanism is defined correctly, in my opinion, I think that private banks

are especially much strong in comparison with public banks. In general, the system, which is trying to be established by BRSA, is right and is exactly defined what it should be, I mean, the controls and IT audits, which are being done on the spot within the context of cyber security by auditors who are able to submit relevant reports to the management board directly and also other internal auditors know your presence if you are collaborating with the team in terms of making integrated audit. Let's say, the audits, which are related to corporate credits, are being made and in this process, you are doing queries relative to infrastructure as an IT auditor, as well other internal auditors are looking for control deficiencies that are related to the process. There is a defined basic here, however, the question is all the time this process is functioning or not in B1 Bank, at that point IT auditor must just focus on IT-related processes, process controller or administrative auditor should focus on process part and this can be a much accurate method if these two of the audits are performed separately and the reportings are made together. Therefore, the delphic thing is that in B1 Bank, thus, IT audits and process audits have to be performed uniquely in terms of work done although not as report, through this mindset, IT auditors can concentrate on much to the cyber security field and they can improve their abilities relative to information security. If IT auditors are making audits by only focusing on the cyber security field or one of the subjects of the cyber security field, they can function in one area by using their knowledge and skills. In this context, the reports, which are being presented by us, are directly reported to the related authority and are determined by the related mechanism, so B1 Bank is one of the best banks in this mechanism because it is a state bank with regard to behaving sensitively for the findings of audits are being transmitted to the right authority. For example, the finding that is relative to the subject is not perceived as personally or everybody assists each other to solve a problem, and

then when this is reported, the management board knows that this finding is surely presented to the management board, so we can consider that the mechanism is functioning accurately. Even so, as I mentioned before, in my opinion, the insufficient point of this mechanism is that there are adequate audits are being performed or not for cyber security and IT related subjects, I think, there is not a sufficient amount of audits are being executed in B1 Bank, there is only one missing here so. On the other side of the situation, the mechanism is being functioned in compliance with international legislations which are being tried to establish by BRSA. If we talk for other banks, this mechanism is being executed much sufficiently by some of the private banks, but surely, there will also the banks where this mechanism can not be adequately operated and there are fifty-five banks so there's definitely a bank that executes audit for just doing as a simple game in terms of just BRSA demands to do that. Accordingly, the reviews of BRSA which are related to your reportings can be much better, much frequent, and much detailed. But, I haven't received any criticism for the comprehensiveness of the report that I have written, at this point, maybe more beneficial results can be obtained, if BRSA much better supervises the system which is established. In this context, I think, what BRSA is doing, is a little more superficial. At B2 Bank, for example, each of the auditors is being evaluated as a very detailed penetration tester, although, in our bank, the auditors are just spending thirty percent of their time for writing their audit reports. From our point of view, there is a lot of difference between B2 Bank and a few other banks on the IT side because, as I said, they focus only on the IT side and we as IT inspectors do not just focus on IT, but we do more than one job, which naturally makes a cumulative difference over the years, so they are coaching persons for improving their abilities to make detailed penetration tests due to the auditor skills and audit adequacy, in contrast, we have more superficial but better

experts in audit operations for banking processes. I don’t know if it is right to separate this in the form of the private sector and state bank, I am only talking about a few big banks of the private sector in my own experience, these are B4, B2 and B3 banks that have much desire for training considerably qualified auditors for IT field when compared with B1 Bank because of their policies. I am saying particularly that the general policy of B2 Bank shows that they desire to coach penetration testers in the proper sense. On the contrary, the policy of B1 Bank is like the auditor does everything in every field, there is this kind of mind, I personally go for division controls, also investigations, process controls and as well I execute IT audits in the rest of my time, now there is a difference between such an institution and the other institutions which motivate their persons for just penetration tests. For five years, a person has been constantly trying to get certificates about system security, Certified Ethical Hacking, OSCP, et cetera, and so on, also they have been struggling with these related terms, but we have been dealing with concepts until the present which are related with banking and that is the main difference between them and us. But already, CISA is the fundamental of this process, which BRSA brought in time for the banks to get CISA certification as a license. The CISA certificate is the most easiest certificate to acquire in comparison with other ones, so let me put it in that way. There’s no difficulty, I can call it a money trap, so if you ask me my sincere opinion, if a person works a little bit in this subject, this person can take CISA absolutely, I mean, there’s not necessary to have four years or five years of experience in IT field as they specify, so everybody can get through getting a little familiar with the issues and solving a few of questions related with the subject. You don’t have to be an engineer to do that, and you don’t have to have work experience in IT auditing, of course, your professional experience certainly contributes to you, so it’s easier to get a CISA certificate because

you're constantly looking at those control points in that COBIT with trying to make some audits in that, but I don't think it's such a difficult test, but certificates like Certified Ethical Hacking, OSCP are more specialized certificates. For example, in B2 bank, people have efforts to get them, but as I have seen in B1 Bank and other state banks, there are no such kinds of attempts. Within the top banks, we can set apart state banks and private banks and we can make such a generalization, yes, specialization of persons in private banks means a lot due to the IT audit tasks, and in-state banks, the sense is that the auditor understands everything, especially for the level of supervision.

Panelist 8- We as internal audit units have been already performing our tasks based on both the legal framework and the controls related to cyber security, whether the bank is operating properly or not, whether they are carrying out cyber security controls in the organization or not, we are completely making our audits are based on these. Also, there are controls on information security that was drawn up by BRSA, all of which are based on internal audits and topics are covered by internal control functions.

Panelist 9- Like I just said, they are executing their audits and controls according to the regulations to which we are subject. As a bank, we are subject to the banking law numbered 5411 of BRSA and as information systems, we are subject to newly published banking processes and electronic banking regulations. The audits, which have been already performed for assessing the presence and effectiveness of the controls in the legislative framework from the point of internal audit side. If there is a control that is not competent or never existed major concerns are written, and if an existing control is not effective enough, the necessary referrals are made. Furthermore, we have a foreign partnership that is a shareholder of the bank in Emirates in Dubai and there is an

international standard for cyber security. We are also making the control lists within the bank by using this framework.

Panelist 11- The internal audit has a role in activities that are related to control and follow-up functions to control whether these processes are being performed adequately or not, through an independent eye.

Panelist 14- The security of the information systems of the banking sector in Turkey is strictly regulated with banking transactions and is created with the aim of ensuring the security of the citizens receiving the service and the goal of increasing the reliability of the banking sector both based on banks and sector. Nonetheless, cyber security efforts in the banking sector are comprehensively updated with international practices are taken into consideration and most importantly, with the legislation, methods, and practices that are being developed in accordance with our country's ecosystem.

Soru 1- İşletmenizde, siber güvenlik hizmetleri dahilinde, iç denetçiler hangi süreçlerde sorumluluk üstlenmektedir?

Panelist 1-

Bizim bünyemizde teftiş kurulu başkanlığımız var, bankamız bünyesinde, siber güvenlik anlamında yaptıkları denetimler şu şekilde oluyor, siber güvenlik özelinde bir denetim yapmıyorlar, yani bir pentest ya da sınır testi anlamında bir denetimde bulunmuyorlar ama, biz BDDK regülasyonları kapsamında sızma testi yaptırmamız zorunlu, bağımsız bir kuruluşa, bağımsız kuruluşun yaptığı denetimler sonucunda ortaya çıkan bulguları bize teslim ediyor bağımsız denetçiler biz de o bulguları kapatmaya çalışıyoruz. Yalnız, orada teftişin şöyle bir rolü var, biz bulguları kapattığımız zaman BDDK'ya bildirmeden önce doğrulama fonksiyonunda bulunuyorlar, herhangi bir bulgu gerçekten kapandı mı kapanmadı mı sızma testi kapsamında siber güvenliğe dokunan kısımlar bunlar. Bir de aslında siber güvenlik değil de, biz bankalar, bankaların bilgi sistemleri ve elektronik bankacılık hizmetleri hakkında yönetmelik, özellikle bu sene yayınlanan yönetmelik kapsamında bilgi güvenliğini adresleyen unsurlar var, o kapsamda da, denetim gerçekleştiriyorlar yıllık olarak, teftiş kurulu başkanlığımız, belli kontrol listeleri var, bu listeler kapsamında kontrolleri yapıyorlar ve bulgu olarak da raporluyorlar, bizim tarafta, bu yıl bu şekilde değişti, geçtiğimiz yıllarda da COBIT'in ISACA'nın yayınlamış olduğu COBIT framework var 4.1 framework'üne tabiydik, orada da DS5 sistem güvenliğinin sağlanmasına yönelik kontrolleri vardı, o kontroller şimdi işte bankaların bilgi sistemleri ve elektronik bankacılık hizmetleri yönetmeliği kapsamında evrildi. Yani şöyle diyebiliriz, bir sızma testi, bağımsız firmanın yaptığı sızma testi bulgularının kapatıldıktan sonra doğrulanması işi, iki de BDDK'nın çıkarmış olduğu regülasyonlar

kapsamında, bilgi güvenliğinin sağlanmasına yönelik yapmış olduğu kontrol listeleri sonucundaki kontroller, iç denetim bu şekilde çalışıyor.

Panelist 2-

Geçtiğimiz hafta bir denetim bir çalışması olmuştu, bankada, bizim ekibimizle alakalı, orada benim sorumluluğumda olan bir ürün vardı, onunla alakalı bir denetim yapmışlardı, açıkçası, daha çok monitoring tarafı ile ilgili, ürünlerin daha stabil bir şekilde çalışması ile alakalı, o kısımlardaki işlerden sorumluyuz, iç denetim tarafındaki kişiler genelde raporlama, süreç geliştirme ve eğer herhangi bir eksiklik tespit edilirse bizim süreçlerimiz ile alakalı, onunla ilgili iyileştirme çalışmalarında bulunuyorlar, genelde iç denetçilerin sorumluluğu bu şekilde oluyor ve onlar da bizdeki eksikleri tespit ettikten sonra, bunları kendi bölüm başkanlarına raporluyorlar sonrasında da bizim yapmamız gerekenler ile ilgili, bize bulguları yayınlıyorlar, biz de onlar ile alakalı gerekli aksiyonları alıyoruz. Süreç bu şekilde sağlanıyor.

Panelist 3-

Bankamızda ISACA'nın yayınlamış olduğu bir COBIT standardı var, bu çerçevede DS5 tarafında bilgi sistemleri güvenliği altında incelenmekte, siber güvenlik tarafı, onun haricinde şöyle söyleyebilirim, bizim bankamızda ayrı bir teknoloji firması bulunmakta, bu bölümde de siber güvenlik tarafı ayrıca değerlendiriliyor, ama o kısımda bir denetim fonksiyonu yok, onlar sadece sızma testi üzerine çalışıyorlar.

Panelist 4- Bankamızda öncelikle bir regülasyon tarafı var, biz BDDK'nın yönetmelikleri gereği bilgi sistemleri yönetmeliği çıktı yeni, bu yönetmelik gereği biz siber güvenlik alanında birçok denetim yapıyoruz, hem bankanın BT birimlerinin süreçleri hem de destek hizmeti alınan kişi kuruluşların denetimi, bağlı ortaklıkların denetimi, bunların

hepsinde biz denetimler gerçekleştiriyoruz, yeni yönetmeliğe kadar COBIT 4.1 standardı ile ilerliyorduk DS5 bilgi güvenliğinin sağlanması, müfettişler yönetim beyanı çalışmaları kapsamında organizasyonel hedeflere göre COBIT standartlarına göre denetliyorlar ayrıca Risk Kontrol Matrisleri oluşturuyoruz, bu denetimler öncesi eğitimler de oluyor, öncelikle bu müfettişleri eğitiyoruz ama siber güvenlik özelinde düşünülürse, öncelikle sistem tarafına bakılmakta, organizasyon içerisinde bazı kontrol noktalarımız var, kullanıcı eğitimleri organizasyon için önemli.

Panelist 5- Bildiğiniz üzere biz banka olarak hem BDDK regülasyonları hem de COBIT ve aynı zamanda ISO 27001 kapsamında denetimlere tabi tutulmaktayız, bilgi güvenliği olarak da siber güvenlik alanında da hem loglama olarak SIEM dediğimiz hem güvenlik testleri dediğimiz hem de change management dediğimiz tüm yapılar üzerinde denetimlere tabi tutulmaktayız, bu denetimlerde SIEM tarafı ile ilgili yani log management tarafı ile ilgili BDDK aynı zamanda yasal gereklilik olarak da biz BT altyapı operasyonlarındaki geçen sunucularla ilgili logları almak ve onlarla ilgili işleyişi sürdürmek zorundayız hem güvenlik anlamında hem de iz kayıtları anlamında bu süreci işletmek zorundayız. Hem iç denetimler hem de dış denetim firmalarında da biz bu denetim süreçlerine tabi olmaktayız, bizim banka olarak iç kontrol ve teftiş başkanlığı olarak iki ayrı başkanlık vardır, iç kontrolle beraber bu süreçleri tasarlayarak süreçleri bitirmeye çalışıyoruz daha sonra da teftiş başkanlığı da gelip gerçekten bu süreçlerin belirlenen kapsamda yapılıp yapılmadığını kontrol eden bir başkanlıktır, ek olarak da bağımsız denetimler kapsamında da bu süreçler yılda bir kez denetime tabi tutulmaktadır.

Panelist 6- Bankamızda 2015 senesinden şu ana kadarki dönemde bilgi güvenliği yöneticisi olarak çalışıyorum, 2015'te risk uyum servisinin yöneticisiydim 2019 sonuna kadar, 2019 senesinde risk uyum servisi ile bilgi güvenliği birleşti ve daha sonra bilgi

güvenliği olarak devam etti, şu anda bilgi güvenliği yönetim sisteminin kurulması, BDDK yönetmelik ve yasalara COBIT 4.1 uyumluluğu ile ilgili süreçlerin tasarlanması, denetim ve koordinasyonun sağlanması, iç kontrol ve teftiş, holding grubu, bağımsız denetim, BDDK denetimlerinde gerekli tüm altyapının, koordinasyonun, dökümanların takip edilmesi eğer bulgu tespit edilirse bunlarla ilgili çalışmaların yapılması gibi durumlarda biz dahiliz, yine bankada BT risk yönetimi projesini yapıyoruz, tüm iş birimleri ve tüm bt ekipleri ile birlikte bilgi varlıklarını çıkarıp üzerinde de risk seanslarını gerçekleştiriyoruz tehditti, olasılıktı, etkiydi, bunların hesaplanmasıydı, alınacak aksiyonların belirlenmesiydi süreçlerimiz var, yine banka olmamızdan ve müşterilerin kart verilerini bulundurmamızdan dolayı PCI DSS uygunluğumuz var, PCI DSS ile ilgili gap çalışmalarının yapılması, uygunluk çalışmalarının yapılması da bizim tarafta, swift sistemleri ile ilgili swift Customer Security Framework (CSF) ile ilgili uygunluk çalışmalarımız var, yeni projeler ile ya da büyük proje değişikliklerinde, güvenlik testleri dinamik ve statik testler olmak üzere web uygulama testleri, mobil uygulama testleri, kod kalitesi ve kod güvenliği ile ilgili testler, network altyapı testleri gibi test süreçlerimiz bizim bünyemizde burada hem içerideki görevlendirdiğimiz arkadaşlar testleri yapıyorlar NESUS gibi uygulamalar kullanarak hem de birlikte çalıştığımız pentest firmaları var onlardan destek alıyoruz yine burada banka olmamızdan dolayı BDDK zorunluluğumuz var yılda en az bir kez bağımsız bir pentest firmasına kapsamlı bir güvenlik testi yaptırıyoruz, bunların içerisinde ATM'ler, şubeler, şube networkleri, çalışanların farkındalığının, sosyal mühendislik testlerinin yapılması da dahil oluyor. Yine, bilgi güvenliği bünyesinde SOC dediğimiz bir ekibimiz var, burada SIEM, Guardian, DLP, Algusec gibi hem network altyapısı hem sunucu ve sistemler hem ayrıcalıklı adminlerin hareketlerin izlenmesi gibi pek çok senaryomuz var, burada loglama yapıyoruz zaman

damgalı bir şekilde logları tutuyoruz, bir de dolandırıcılık veya kötü niyetli kullanım veya herhangi bir tehdit olabilecek durumlara ait senaryolarımız var, burada kurallarımız ve alarmlarımız çalışıyor, ve olağanüstü bir durum var ise veya sıkıntılı bir durum var ise kayıtların tutulması ve sorunun çözülmesi ve takip edilmesi gibi kısımlarında da yer alıyoruz. Yine sistemlerde ve sunucularda ayrıcalıklı kullanıcı hesaplarının yönetilmesi ve uygulama hesaplarının yönetilmesi gibi kısımlarda ürünlerimiz var bunlarla ilgili takiplerimizi yapıyoruz, yine ayrıcalıklı adminlerde bağlantı recording dediğimiz SCB dediğimiz uygulamalarımız var, bunların hareketlerini kaydedip, takip ediyoruz, yine kendi bünyemizde, çalışanların bilgi güvenliği farkındalığını artırmak için farkındalık eğitimleri düzenliyoruz, bu eğitimler hem sınıf içi eğitimler oluyor, hem pandemi döneminde şu anda sizinle yaptığımız gibi uzaktan eğitimler oluyor, hem iş birimlerine hem bt çalışanlarına hem ilgili diğer paydaşlara eğitimler düzenliyoruz, yine farkındalık ile ilgili oltalama çalışmaları yapıyoruz, mailler ile oltalama mailleri göndermek ya da telefon ile arayıp kritik bilgilerini elde etmeye çalışmak gibi çalışmalarımız var bünyemizde, bütün bu çalışmaları ölçüp eğer çalışanlar bizim bilgi güvenliği politikalarımıza aykırı şekilde davranıyorlarsa, farkındalıkta eksiklik varsa, bu eksiği gidermeye yönelik ek çalışmalar yapıp takip ediyoruz. Kendi risk yönetimimizi takip edebileceğimiz risk kayıtlarını yapabileceğimiz uygulamalarımız var, içeride özel bir uygulamamız var ve kurallarımız var, ortak restore dediğimiz dosyaların veya kullanıcı bilgisayarında bulunan verilerin banka politikalarına uygun olması için yine çalışmalarımız var burda takip ettiğimiz kurallarımız var, bağlı iştiraklerin erişimlerini kontrol etmek riskleri takip ederek uyumluluklarını sağlamak denetimlerde çıkabilecek açıklıkları yönetmek için süreçlerin iyileştirme kısımları bizim tarafta, komitelerimiz var, Bilgi Güvenliği, BT Risk Yönetimi, BT Süreç Yönetimi komitemiz gibi Genel Müdüre

Bağlı bir ekibiz, BDDK 15 Mart 2020'de yeni bir yönetmelik yayınladı, ve bütün bankalara şunu söyledi dediki bankalarda bilgi güvenliği fonksiyonu doğrudan genel müdüre veya yönetim kuruluna bağlı olacak dedi, biz de doğrudan genel müdüre bağlı bir şekilde raporlama ve takip çalışmalarımızı sürdürüyoruz. İstihbarat kısmı da bizde, topoloji inceleme, güvenlik mimarisi değerlendirilmesini yapma, dış firmalarla yaptığımız risk değerlendirme çalışmalarımız var.

Bir iç kontrol başkanlığımız var, iç kontrol başkanlığı içerisinde bt denetçileri var onlar bizim süreçlerimizi denetliyorlar, teftiş başkanlığımız var, teftiş başkanlığı içerisinde de bt denetçi arkadaşlar var, yine onlar bizi denetliyor, biz bir yabancı şirketin alt bir şirketiyiz, Bahreyn'deki bir holdingin Türkiye deki bankasıyız, dolayısıyla yurtdışındaki bir holdingin alt şirketi olmamızdan dolayı holding bünyesindeki BT denetçi arkadaşlar da yine düzenli olarak bizim bt süreçlerimizi denetliyorlar, bunun dışında bir banka olmamızdan dolayı BDDK zorunluklarından dolayı BDDK nın yasa yönetmelik ya da yapmasını zorunlu tuttuğu kısımlarla da yine 4 büyük firma dediğimiz Ernst&Young, KPMG, Deloitte, Price gibi firmalardan hangisi ile anlaştıysak bu firmalardan biri gelip bizi düzenli olarak her sene denetliyor, dolayısıyla 4 tane denetimden bahsedebiliriz iç denetimler ve dış denetimler olmak üzere bir de BDDK isterse kendi denetçilerini gönderip bankanın BT kısmına denetim yaptırabiliyorlar, siber güvenlik anlamında da bilgi güvenliği tarafında kullanılan uygulamalar ve süreçlerimiz var bütün bt denetçileri geldikleri zaman bu arada ISO 27001 sertifikamız da var ISO 27001 kapsamında da her sene sertifika denetiminden geçiyoruz, orda da denetçi arkadaşlar bizi denetliyorlar, bütün denetçiler bizim önce süreçlerimizi dinliyorlar, politikalarımızı ve prosedürlerimizi anlamaya çalışıyorlar, sonra süreçlerin işleyip işlemediği ile ilgili kayıtları ve çalışmaları kontrol ediyorlar, siber güvenlik anlamında da işte saldırı oldu şu oldu bu oldu vesaire

kısımlarında bizim güvenlik ile ilgili almış olduğumuz önlemler, kullanmış olduğumuz uygulamalar, izlemiş olduğumuz, yapmış olduğumuz çalışmalara bakılıyor, örneğin banka içerisinde siber güvenliğin sağlanmasında kullanılan uygulamalar ile çıktı istiyorlar, örneklem seçerek gidiyorlar, denetçiler kayıtları talep ederek, eğer bir olay olduysa örneğin banka faaliyetlerinde herhangi bir fraud oldu, teftişçiler bunlarla ilgi özel bir inceleme yapıyorlar, istihbarat araçlarındaki kayıtlara, BT'nin çalışmalarına ve kayıtlarına bakıyorlar.

Panelist 7- Siber güvenlik dahilinde, bizim COBIT süreçleri dediğimiz DS5 süreçleri vardır, yani şu ana kadar siber güvenlik ile alakalı baştan sona süreç olarak COBIT DS5 süreci ve onun yanısıra firewall ve active directory denetimleri yapıldığını gördüm. Tabii ben DS5'e katıldım bir tek firewall ve active directory denetimlerine katılmadım. DS5'te de burada hani baştan sona sadece siber güvenlik değil de sistem güvenliği adı altında baştan sona, yani verilerin sınıflandırılmasından kullanıcı yönetimi, network güvenlik yönetimine kadar pek çok farklı kontrol noktaları var, dediğimiz alanda, bu kapsamda da müfettişler genellikle her sene DS5 sürecinde çalışırlar, işte ne yaparlar, baktığınız zaman, IPS, IDS yapılandırılmasını kontrol ederler. Intrusion Prevention veya Intrusion Detection denilen ağa bir saldırı çabası var mı bununla ilgili herhangi bir sorgulama var mı gibi cihazlar tanımlıdır. Herhangi birisi ağ ile keşif yapmaya çalıştı mı vesaire bununla alakalı alarmlar üretir. Bunların konfigürasyonlarının doğru yapılıp yapılmadığı ile ilgili kontroller yapar müfettişler veya herhangi bir uygulamada olsun ya da server 'da olsun tanımlı kullanıcıların gerçekten ihtiyacı olup olmadığını araştırırlar. Bunun haricinde, yine security, anti virus programlarının güncel olup olmadığını ve tüm işte hangi alanda denetim yapılıyorsa oradaki tüm makinalara dağıtılıp dağıtılmadığını doğru bir şekilde

kontrol ederiz. Bunların haricinde, temel olarak bunlar diyebilirim. Siber güvenlik ile alakalı temel olarak bu tarz önlemler alınabiliyor.

Panelist 8- Siber güvenlik denetimi kapsamında şimdi biz bankada çalıştığımız için ve banka, çalıştığım banka, Türkiye'deki diğer bankalar BDDK'nın çıkarttığı mevzuatlara tabi doğal olarak ve BDDK'nın bilgi sistemleri ile ilgili yönetmeliklerindeki gereksinimlere uyumlu faaliyet gösteriyor mu göstermiyor mu bunu denetliyoruz daha çok. Burada da siber güvenlik anlamında baktığımız zaman COBIT diye bir metodoloji var, bilmiyorum biliyor musunuz, COBIT'de bilgi güvenliği süreci ile ilgili DS5 süreci altındaki kontrol maddelerine bakılıyor, yani siber güvenlik anlamında işte buradaki maddeler neleri içeriyor, bankanın siber güvenlik programı var mı siber güvenlik politikası var mı, siber güvenlik ile ilgili olarak işte gerekli uygulama ve kontroller uygulanıyor mu, yani anti virüs yazılımları kuruluyor mu, yama programları var mı, işte sistemlerde sunucularda. Daha sonra kullanıcı hesaplarının yönetimi ile ilgili kontroller var yetkilendirmeler ile ilgili kontroller var bir de veri tabanı güvenliği ve ağ cihazları güvenliğine yönelik kontroller var bunlara yönelik bankada hem bilgi sistemleri iç kontrol tarafında hem de teftiş kurulu tarafında kontroller yapılıyor.

Panelist 9- Bankamız bünyesinde teftiş kurulu tarafından yapılıyor iç denetimler. Bir de üç seviyeli bir güvenlik kontrol mekanizması mevcut. Birinci safha dediğimiz en çok bilgi güvenliği operasyonlarını yerine getiren ekibimiz var. Hemen ikinci hat olarak bilgi teknolojileri kontrol ve biz varız bilgi güvenliği risk ekibi ve son noktada üçüncü hat olarak da denetim ekibimiz var. Denetim ekibimiz de yapılan işlere dair yönetim kuruluna güvence vermek ile sorumlu. Teknik olarak yetkinler, mevzuatlar kapsamında bizim denetimlerimizi yapıp yönetim kuruluna güvence veriyorlar.

Panelist 11- Bankacılık kanunu, BDDK bilgi sistemleri yönetmeliği, KVKK vb. regülasyonlar çerçevesinde kontroller yapılmaktadır. Alanım dışı olduğu için çok fazla detay ekleyemiyorum. Ancak incedent kontrolü , yetki kontrolü , erişim gözden geçirme gibi rolleri bulunmaktadır. Ayrıca üçüncü tarafların süreçleri de gözden geçirilmektedir.

Panelist 14- Türk Bankacık Sektöründe (TBS) bankalar Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmeliği kapsamında iç denetim sistemlerini kurmak ve yürütmekle yükümlüdürler. İç denetim sisteminin amacı, üst yönetime banka faaliyetlerinin Kanun ve ilgili diğer mevzuat ile banka içi strateji, politika, ilke ve hedefler doğrultusunda yürütüldüğü ve iç kontrol ve risk yönetimi sistemlerinin etkinliği ve yeterliliği hususunda güvence sağlamak olarak belirtilmiştir. Ayrıca, bu yönetmelik kapsamında bankalarda iç denetim birimi

Madde 21, 3. fıkra kapsamında;

"...

b) Elektronik bilgi sistemi ile elektronik bankacılık hizmetleri de dahil olmak üzere ve 13/1/2010 tarihli ve 27461 sayılı Resmî Gazete'de yayımlanan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmeliğin, Bilgi Sistemleri ve Bankacılık Süreçleri Denetimine İlişkin Esaslar başlıklı beşinci bölümünde belirlenen usul ve esaslar çerçevesinde bilgi sistemleri gözden geçirilir."

Hükmüne istinaden yasal bir zorunluluğu bulunmaktadır.

Ayrıca siber güvenlik daha üst bir kavram olarak değerlendirilebilecek bilgi güvenliği olarak ifade edilerek bankalardaki sorumluluk nihai olarak Yönetim Kurulunda olduğu belirtilmiştir.

Ayrıca bilgi güvenliği kapsamında ayrı bir iç denetim yaklaşımı bulunmaktadır.

Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik (Bilgi Sistemleri Yönetmeliği), Madde 8:

"Banka bünyesinde bilgi güvenliğinin sağlanmasında nihai sorumluluk yönetim kuruluna aittir. Yönetim kurulu, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi hususunda gerekli kararlılığı göstermekle ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis etmekle yükümlüdür."

Yukarıdaki madde değerlendirildiğinde konunun sorumluluktan daha öte bir kavram olarak gerekli kaynağın tahsis edilmesi şeklinde sadece yükümlülük boyutuyla değil aynı zamanda işlerliğinin sağlanmasının da göz önünde bulundurulduğu şekliyle değerlendirilebilir.

Ayrıca, bankalar Bilgi Sistemleri Yönetmeliği uyarınca Bilgi Sistemleri (BS) iç denetim faaliyetlerini ayrıca yerine getirme yükümlülükleri bulunmaktadır.

"Madde 31: Banka ve bankanın dış hizmet sağlayıcıları nezdindeki BS yönetimine ilişkin faaliyetler, bu faaliyetleri destekleyen süreçler ve tesis edilen BS kontrollerinin mevzuata ve banka içi politika, prosedür ve standartlara uyumlu olduğu ve bilgi sistemlerine ilişkin

iç kontrol ve risk yönetimi faaliyetlerinin etkinliği ve yeterliliği hususunda yönetim kuruluna güvence sağlamak üzere BS iç denetim fonksiyonu oluşturulur, BS iç denetim sorumlusu atanır ve BS iç denetim faaliyetleri bu kişinin sorumluluğunda yürütülür."

Soru 2- Kurumunuzda, iç denetimin, siber güvenlik kapsamında yürütülen fonksiyonlarının yeterlilik düzeyini nasıl ifade edersiniz?

Panelist 1- Bankamız bir şubeler ve bankacılık süreçlerini denetleyen müfettiş arkadaşlar var bir de bt müfettişi dediğimiz IT fonksiyonlarını denetleyen müfettiş arkadaşlar var, şu anda yaklaşık 12 kişilik IT müfettişi dediğimiz kadro var bankamızda bunların tamamı bilgisayar mühendisliği mezunu, denetim perspektifinden bakıldığında herhangi bir siber güvenliğe dokunan işte böyle penetration test veya certified ethical hacker yada OSCP (offensive security certified professional) dediğimiz sertifikasyonları yok, ama hepsi bunların 12 kişinin de tamamı CISA sertifikasına sahip, yeterlilikleri hem bilgisayar mühendisleri olmaları hem de uluslararası sertifikasyonlara sahip olmaları nedeni ile yeterli diyebiliriz, biraz zafiyet bulma yönünde birtakım eksiklikler var, ama zaten onu da bağımsız bir kuruluşa yaptırıyoruz düzenli periyodik olarak, yeterli düzeyde diyebiliriz teftişteki arkadaşlar için.

Panelist 2- En son yapmış olunan denetimde yapılan kontroller sonucunda açıkçası denetim kapsamında yapılan çalışmaların yeterli olduğunu düşünüyorum.

Panelist 3- Öncelikle, güvenlik tarafında aslında baktığımız çok farklı konular bizim, farklı alanlar olarak ilerliyoruz, alan ayrıştırmamız var öyle söyleyebilirim, öncelikle politikalardan başlıyoruz bilgi güvenliği politikasının kontrol edilmesi ve buna uyum çerçevesinde kontrollerimiz oluyor, onun haricinde ayrı ayrı mesajlaşma sistemleri gibi

denetimlerimiz oluyor ve bunların içerisinde de sistemlerin ve ekranların ne kadar güvenli tasarlandığının kontrolünü yapıyoruz, erişim kontrollerini, ağ kontrollerini gerçekleştiriyoruz, daha sonra yetkilendirmeye çok önem veriyoruz, bizim açımızdan büyük önem taşıyor, izinsiz kullanıcılar var mı yetkiler neye göre belirlenmiş yetki sınırları nelerdir bunlar bizim açımızdan çok önemli sistemin dışarıdan ulaşılabilir mi ulaşılabilir değil mi, VPN kontrolleri, antivirüs kontrollerimiz var, firewall kontrollerimiz var bu çerçevede sistem nasıl manipüle edilebilir bunların kontrolünü yapmaya çalışıyoruz veya doğru çalışıp çalışmadığını ve sistemin yeterince korunup korunmadığının kontrolünü yapmaya çalışıyoruz, genel anlamda bunlar.

Panelist 4- Siber güvenlik birimi, iş birimleri tarafında konuşacak olursak, bankalar diğer kuruluşlara göre diğer sektördeki kuruşlara göre bir adım önde bu konuda, bizim kuruluşumuzda da bilgi güvenlik müdürlüğü ile başlamıştı bu iş daha sonra siber güvenlik alanında ayrı bir birim kuruldu, eğer bir olgunluk şeması verecek olursak beşli bir skala üzerinden size dört diyebilirim, ama neler yapılması gerekiyor işte siber güvenlik tarafında takımların oluşturulması daha fazla kullanıcı eğitimleri, müfettişler tarafında bu yeni yönetmelikle birlikte uyum tarafları, açık bankacılık tarafları var, açık bankacılığa başladık bunla ilgili hususlar, KVKK ile ilgili çalışmalar, bazen de bizi regülasyonun zorladığı durumlar da oluyor mesela swift denetimi çıkıyor ortaya bazen bankalar ile ilgili büyük şeyler duyuyoruz problemler duyuyoruz mesela swift alanında bir sızıntı oluyor ya da farklı bir su istimal ortaya çıkıyor bu gibi durumlarda biz müdahil oluyoruz ben seviyesini dört olarak söyleyebilirim tekrardan.

Panelist 5- Biraz önce de bahsettiğim üzere biz banka olarak BDDK regülasyonlarına tabi olduğumuz için bu işler zaten mecburiyet kapsamında da olsa yeterlidir, çünkü yapılan işlerin hem iç kontrol hem de teftiş başkanlığı denetçileri kapsamında denetlenmesi

raporlanması ve aynı zamanda da BDDK tarafından da bağımsız denetçilerle denetlendiğimiz için bu süreç yeterlidir, yeterli olup olmadığı bulgularla da kanıtlanabiliyor, bağımsız denetim firmaları BDDK'nın belirlediği bağımsız denetim firmaları gelip bankaları denetleyip siber güvenlik anlamında veya bilgi güvenliği anlamında da bu süreçlerin de gerçekten doğru işlediğini inceleyip, kanıtları görerek, bu şekilde süreçlerini tamamlıyorlar.

Panelist 6- Çok yeterli değil, neden çok yeterli değil, şimdi belki sadece bizde de değil Türkiye deki diğer bankalarda da olabilir, bizim güvenlik alanında kaynak sıkıntımız var, bu kaynak sıkıntısı hem bizim gibi bilgi güvenliği fonksiyonları için az oluyor, denetim kısmında bankaların bt denetim ekiplerindeki kaynaklarda yeterlilik çok fazla olmuyor dolayısıyla bir ya da iki denetçi ile ilerliyoruz, o denetçi arkadaşların da çok fazla denetleyecek kısmı olduğu için haliyle çok sağlıklı ve çok derinlemesine denetimler yapamıyorlar, ayrıca sirkülasyon çok fazla oluyor bt denetim ekiplerinde, iç kontrol ve teftiş tarafında, sirkülasyonun fazla olması şu anlama geliyor, yeni gelen denetçi bankanın yapısını anlamak için zaman kazanması gerekiyor çünkü anlayacak ki sorularını ona göre sorsun ve almış olduğu kanıtları ona göre inceleyebilsin, şimdi güvenlikte var 30, 40 tane uygulama, altyapıda var birçok uygulama her bankanın dünyası çok farklı altyapısı mimarisi işleyişleri çok farklı, denetçinin geldiği zaman ilk işe başladığı zaman sürecin zaten altı ay bir yılı bizim bu yapıyı anlamakla geçiyor, sonra kanıt istediğinde de benim ona verdiğim kanıtın yeterli olup olmadığı ile ilgili karşı tarafın bilgisi olması lazım daha önce bir denetim yapması sorgulama yapması lazım aksi takdirde benim verdiğim kanıt onun için yeterli olup geçiyor, birinci sorun, aslında iç denetim ekiplerindeki birinci sorun bence, yeterli bilgi ve tecrübeye sahip kaynak bulunmamasını söyleyebilirim, biz şimdi ne yapıyoruz bankada denetim ekiplerine aynı bilgi güvenliği çalışanıymış gibi

eğitimlerimize ya da uygulamalarımızı öğretme kısımlarına davet ediyoruz, anlatıyoruz bakın bu uygulamaların şöyle şöyle özellikleri var, biz bu kadarını yapıyoruz, bir de şuradan buna bakabilirsiniz diye, dediğim gibi bir kısmı öğreniyor bir kısmı da öğrenmeye bile fırsat bulamadan iş değişikliğine gidiyor, yine süreç sil baştan devam ederek gidiyor, sıkıntının birincisi bu aslında, ikincisi de bt denetimlerini yapan arkadaşlar daha önce bt de çalışmamış olan arkadaşlar oldukları için soru sormakta, anlamakta ve sonrasını incelemekte sıkıntı çekiyorlar, yani karşıdaki teknik ekip bir soru sorduklarında teknik ekip cevap verdiğinde bazen ikinci soruya bile gidemiyorlar ya da gittikleri sorular anlamsız olabiliyor teknik taraf için yani bir veri tabanını yönetmek bir network ü yönetmek bir sistem yönetmek, bilgi güvenliğindeki izleme kısımlarını yönetmek apayrı bir dünya, özellikle de yeni mezun arkadaşların burada zamana ihtiyacı var öğrenmek için, denetçi denetlenenden bir tık daha yukarıda olmalı ki denetlenenin kusurunu daha iyi bulabilmesi gerekiyor, orda genel de eksikler var sadece bizim bankamız için değil, genelde zaten güvenlik alanı yeni bir alan olduğu için kaynak sıkıntısı herkeste olduğu için çoğu yerde var, bizim bankaların da diğer bankaların da yetiştirdiği kaynağı içeride tutmak için çeşitli önlemler alması gerekiyor bence.

Panelist 7- Her şeyden evvel bankada IT müfettişliği tam anlamıyla yapılmıyor. Yani, örneğin, mesela, bizim, şu ana kadar siber güvenlik ile alakalı yetkin biri olunabilmesi için çok fazla kalifikasyona ihtiyaç var. Yani bir kişi bir kere yazılımdan anlayacak her şeyden önce, bunun üzerine sadece yazılım da değil network bilgisi olacak sistem yönetimi bilgisi de olacak, bunları kombine edip işte birtakım cihazları vesaire falan kullanacak. Programları veya toolları kullanacak, bu bağlamda, aslında bakarsanız biz çok yüzeysel kalıyoruz, o yüzden kötü diyebilirim yani, siber güvenlik yetkinliği genel anlamda, birkaç arkadaş haricinde mesela kötü diyebilirim, çünkü, gerçekten bu işe katkı

yapan, mesela Siber Olaylara Müdahele Ekibi (SOME) birimleri kadar detaylı bir şekilde onların yaptığı her işi denetleyemiyoruz çünkü o kadar hâkim değiliz konuya. Bu bağlamda denetim birazcık yapılan işin gerisinde kalıyor, banka örneğinde konuşursak. Şu ana kadar ben diğer bankalar ile kıyaslıyorum, mesela diğer bankalar bunlar direkt olarak müfettişlerini, denetçilerini belli konularda özellikle IT denetçilerini yetiştiriyorlar. Ama bankada bir IT denetçisi şube teftişi de yapıyor, süreç teftişi de yapıyor kalan zamanında da IT denetçiliği yapıyor. İşte bu dediğim COBIT süreçlerini falan denetliyor, bu üçünü birden yapmaya çalıştığı için, siber güvenliğe olan katkısı ve yetkinliği düşük düzeyde kalıyor, yani normalin üçte biri seviyesinde kalıyor diyebilirim. Olması gerekenin üçte biri seviyesinde kalıyor. Birincisi buradaki iç denetçilerin siber güvenlik konusunda bir denetim yapmaları ve bunu yeterli seviyede ortaya koyabilmeleri için, yani siber güvenlik alanında atılan adımların doğru olduğunu teyit edebilmek, eksiklikleri raporlayabilmek için bir kere dediğim gibi birden çok alanda kendilerini geliştirmiş olmaları gerekiyor. Bu alanlardan bir tanesi yazılım, orta seviyede yazılım yapabilecek seviyede bir IT müfettişi bilgi birikimine sahip olmalı, ikincisi bunlardan daha da önemlisi network bilgisi ve sistem yönetimi bilgisi, yani Windows veya Linux yönetimi bilgisi ile bu cihazların ağda birbiri ile nasıl haberleştiğine dair bilgilerin olması gerekiyor, bir IT müfettişinde ve de tabii ki de bunlara sahip olduktan sonra, siber güvenlik önlemlerini almak ve diğer oradaki araştırmaları yapmak artık daha kolay olur, böyle bir bilgi birikimine sahip birisi için. Bundan sonraki adım da oradaki toolların doğru kullanılıp kullanılmadığını denetlemek oluyor işte, SIEM denilen Security Incident Event Management araçları veya işte bunun haricinde yapılan taramalar, düzenli taramalar, örneğin bir server ‘da gerekli gereksiz materyallerin bulunup bulunmadığına dair birtakım taramalar yapılıyor farklı birimler tarafından. İşte bunların tam olarak yapılıp

yapılmadığını anlamak için gerekli sorgulamaları da yapacak konuma geliyor bu üç bileşeni de bildikten sonra, yazılım, network bilgisi ve sistem yönetimi bilgisi. Bunların olması gerekiyor, banka müfettişleri için konuşursak, bunlar yeterli seviyede öğretilmiyor. Yeterli seviyede ele alınmıyor, yani. Bunun da sebebi, müfettişlerin şube denetimi de yapması ve aynı zamanda süreç denetimlerine de yani bankacılık süreçleri ile alakalı denetimler de yapması oluyor.

Panelist 8- Türkiye'de yine BDDK deyim bankacılık sektörünün bilgi sistemleri alt yapısını ilk defa 2006 yılında bir düzenleme ile oluşturdu. 2006 yılından önceki Türkiye'deki Bankacılık sektöründe tabii bilgi güvenliği siber güvenlik konusundaki aksiyonlar kurumların kendi insiyatiflerine bırakılmıştı, bankaların kendi insiyatiflerine bırakılmıştı ama bankacılık sektörü özünde zaten müşteri gizliliği, banka sırrı gibi hususlar çok önemli konular olduğu için bankalarda siber güvenlik ve bilgi güvenliği 2006 yılında artık yasal zorunluluk nedeniyle zaten bir de düzenleme altına girdiler. Banka bu süreç içerisinde sürekli gelişim halindedir, tabi ki 2006 ile 2008, 2010 yılından önceki duruma baktığımız zaman bankanın içindeki tüm çalışanlar nezdinde bu bahsettiğim aslında Türkiye'deki bütün banka sektöründe geçerli. Biz başka bankalar ile karşılaştırdığımızda da konuşurken aynı şeyleri duyuyoruz, bilgi güvenliği farkındalığı düşüktü ama zaman geçtikçe işte BDDK düzenlemeleri nedeni ile de arttı, işte banka personellerine sürekli bilgi güvenliği konusunda eğitimler vermeye başladı. Sadece tabii banka çalışanlarına değil müşterilere bile bilgi güvenliği konusunda farkındalıklarını artıracak çalışmalar yapılıyor, yani 2006'dan günümüze kadar bu geldi. Bankanın kendi uyguladığı teknik kontroller anlamında siber güvenlik kontrolleri anlamında da tabii bankalar şöyle olmak zorunda siber güvenlik anlamında teknolojinin hep en ilerisinde olmak zorunda, bir adım gerisinde olsanız belki bir kötü niyetli saldırgan size zarar

verecektir, o yüzden her zaman bir adım önde olmalısınız o yüzden bankalarda sürekli kötü niyetli kişilerin bir adım önünde olmak için yatırım yapıyorlar, aksiyon alıyorlar, bizde de bu yatırımlar aksiyonlar alınıyor. Bizde de bu aksiyonlar alınıyor, şu ana kadar bir vaka olmadı zaten, bu şekilde özetleyebilirim.

Panelist 9- Biz şimdi, bütün bankalar gibi BDDK'ya tabiyiz. Onun yayınladığı bilgi sistemleri yönetmeliği var, biz de buna karşı sorumluyuz ve şu an teftiş kurulunun yaptığı denetimlerde bilgi güvenliği yönetimi mekanizmamız var. Yaptıkları denetimler sonucunda bulguları varsa bunları majörlüyorlar. Mutabık kaldıktan sonra biz o bulguların kapatılması için gerekli aksiyonları alarak onlara denetim bulgularının kapatıldığına dair dökümanlar sunuyoruz, ardından da yönetim kuruluna raporlama yapılıyor.

Panelist 11- Çalıştığım kurum Banka olduğu için regülasyonlar ve uyum açısından diğer sektörlere göre görev ve sorumluluklar daha belirgin durumdadır. Bu düzey "iyi" olarak ifade edebilirim.

Panelist 14- Bankaların siber güvenlik kapsamında yürütülen fonksiyonların yeterlilik düzeyi temel olarak ilgili mevzuata uyum olarak tanımlanabilir. Bu yeterlilik düzeyi ise en temel olarak bankanın içindeki süreçler, bağımsız denetim süreci ve kamu otoritesinin denetimi olarak kategorize edilebilir.

Yeterlilik düzeyi asgari mevzuata uyum olarak değerlendirilmesi, herhangi bir uyumsuzluk durumunda da idari yaptırımlarla karşılaştırılması olarak değerlendirilebilir. Bankaların bu kapsamda asgari olarak mevzuattaki tüm unsurları bağımsız denetim şirketlerince denetlenmektedir.

Bu konuda dikkat çekilebilecek bir başka husus da bankalarda bilgi güvenliğinin teknolojik gelişmeler de dikkate alındığında sadece bir zorunluluk olarak değil aynı zamanda bir gereklilik hatta rekabet avantajı sağlar yönünün olduğu söylenebilir.

Soru 3-Siber güvenlik ile ilgili sorunlarda, iç denetim ve yönetim kurulu arasındaki etkileşim mekanizması nasıl oluşturulmaktadır?

Panelist 1- İlk soruda bahsetmiştim, biz her yıl düzenli olarak, üç ayda bir sızma testi bulgularına yönelik aksiyonlarımızı yönetim kurulu onayına sunuyoruz, bu kapsamda yeni çıkan yönetmelik ile beraber bahsettiğim BDDK, bankada bilgi güvenliği müdürlüğü olarak bizler doğrudan genel müdüre bağlandık genel müdür ile beraber yılda minimum iki kere olacak şekilde bilgi güvenliği komitesini oluşturuyoruz teftiş kurulu başkanımız da bu komitenin üyesi ve sonrasında her yıl da düzenli olarak bilgi güvenliği faaliyetlerini yönetim kuruluna raporluyoruz teftiş kurulu başkanlığımız da sızma testi sonuçlarını yine eskiden olduğu gibi üç ayda bir yönetim kurulu onayına kendileri sunuyorlar doğrulamasını yaptıktan sonra bulgunun kapanıp kapanmadığı kapsamında bir de bahsettiğim yine ilk soruda bilgi güvenliğinin ve siber güvenliğin sağlanmasına yönelik kontroller sonucunda çıkan yönetim beyanı dediğimiz bir rapor var bu rapor da teftiş kurulu başkanlığımız tarafından hazırlanıyor ve yıllık olarak yönetim kurulu onayına sunuluyor.

Panelist 2- Yılın belli periyotlarında bilgi güvenliği komitesi toplanıyor, bu komitede alınan kararlar doğrultusunda, iç kontrol ekibi de katılıyor bu komite çalışmasına ve burada alınan kararlar doğrudan yönetim kuruluna iletiliyor bu şekilde bir süreç işlendiğini biliyorum, dolayısıyla iç kontrol ve üst yönetim arasında sürekli bir iletişim hali mevcut süreçlerin yönetilmesi noktasında.

Panelist 3- Bizim risk kontrol matrislerimiz hesaplanır bu risk kontrol matrislerimizde her riskin belli bir seviyesi vardır bu seviyeye göre alınan aksiyonların geçerliliği tartışılabilir, ama genel anlamda bizim bankada özellikle bilgi güvenliği konularına ciddi önem verilmekte açıkçası, zaten bankacılık sektörünün bir çoğunda da böyledir aslında bakarsanız, işin ucunda para olunca bayağı riskli sistemlerden oluşuyor bunlar, o sebeple bizim taraf için söylemek gerekirse yönetim tarafından pozitif bir şekilde bir yönlendirme yapılıyor öyle söyleyebilirim, ama her riskte anında çözüm üretilecek diye bir şey yok, risk matrisine göre sırasına göre dediğim gibi çözümlemeler sağlanır, burada tabi maddiyat da çok önemlidir bizim sisteme kazandıracağımız faaliyetler ile kazandırdığı değerin ilişkisi de alınacak kararlar ve aksiyonlar açısından önem teşkil ediyor diyebilirim yönetim için.

Panelist 4- Biz, İç Denetim Enstitüsü standartlarına göre kurumsal yönetim prensiplerimizi belirledik bizim periyodik olarak yönetim kurulunu ve denetim komitesini bilgilendirdiğimiz hususlar var, hızlıca bir organizasyon yapımızdan bahsedecek olursak biz öncelikle denetim komitesine bağlıyız ve tüm raporlarımızı denetim komitesine yapıyoruz akabinde de yönetim kuruluna sevk ediyoruz ayrıca teftiş kurulu başkanının üst yönetime erişiminde herhangi bir kısıt yok istediği zaman denetim komitesi ve yönetim kurulu ile iletişime geçebiliyor, herhangi bir siber güvenlik riski ortaya çıktığında biz doğrudan denetim komitesine bilgilendirme yapıyoruz ayrıca müfettişler de herhangi bir güvenlik açığı çıktığında iş birimlerine refakatçi oluyor büyük bir sistem değişimi olabilir bir olay çıktığında biz de danışmanlık rolümüzle incelemeye başlıyoruz, doğrudan denetim değil de, danışmanlık rolü ile güvence sağlamak için yanlarında yer alıyoruz, bizim raporlamalarımız şöyle üçer aylık raporlamalar yapıyoruz her çeyrekte raporlamalarımız var, ayrıca denetim komitesinin de toplanma sıklığı da dört

değil bu üç aylık periyotlarda ortalama yirmi kez denetim komitesi toplanıyor, risk yönetiminden tutunda tüm iç sistemler kapsamındaki birimler siber riskleri değerlendirebiliyor, bu durumlarda erişim sınırı yok, İç Denetim Enstitüsü standartlarına göre gerekli aksiyonlar alınıyor.

Panelist 5- Biz de şöyledir, biz bilgi güvenliği olarak, aslında siber güvenlik olarak soruyorsunuz ama bizdeki karşılığı bilgi güvenliğidir, bilgi güvenliği anlamında BDDK tarafından belirlenen regülasyonlar doğrultusunda doğrudan genel müdüre bağlanmış olduk, onun haricinde öncesinde de biz yılda üç veya dört defa bilgi güvenliği komitesini toplamaktaydık, dolayısıyla da hem denetçiler anlamında hem de bilgi güvenliğindeki süreçler anlamında üst yönetimi komite toplantıları ile yılda dört kez bilgilendirmekteyiz ve bulguları aktarmaktayız. İç denetimin de kendi süreçleri var, iç kontrol ve teftiş başkanlığı kapsamında sürdürdükleri ve onlar da tespit ettikleri bulguları kendi birimlerince üst yönetime raporluyorlar aynı zamanda biz de bilgi güvenliği olarak da komite toplantıları ile ilgili paydaş birimleri de bu şekilde bilgilendiriyoruz. Ama denetçi anlamında, kendi iç denetçilerimiz veya bağımsız denetçiler ile üst yönetimi düzenli olarak bilgilendiriyorlar.

Panelist 6- Bizim denetim komitesi ile yönetim kurulu toplantılarımız üç ayda bir yapılır, önceden de belirttiğim gibi yabancı sermayeli bir banka olduğumuz için, yabancı ortaklarımız her üç ayda bir bu toplantıları gerçekleştirirler bizim iç kontrol ve teftiş başkanlığımız da kendi yaptıkları denetimlerde tespit etmiş oldukları bulguları düzenli bir şekilde üst yöneticiler ile paylaşırlar, raporlarını oluştururlar ve etkin bir takip sistemimiz vardır.

Panelist 7- Bununla alakalı normalde, siber güvenlik konuları ile alakalı bir şu anki yönetmelik gereği, bilgi sistemleri yönetmeliği gereği birtakım mekanizmalar var yani

yönetim kuruluna direk bağlı olan, siber güvenlik konularını yönetim kuruluna taşıyan bir mekanizma var. Ama bu iç denetim ile alakalı değil tabii, iç denetim her sene düzenli olarak raporlamalarını yapıyor ve bu sayede siber güvenlik özelinde bir bildiğim kadarı ile bir şey yok, bir bağlantı yok. İç denetim ve yönetim kurulu arasında.

Panelist 8- Şimdi iç denetim birimleri olarak iç kontrol ve teftiş kurulları bankada zaten doğrudan yönetim kuruluna bağlı faaliyet gösteriyorlar, yani zaten biz bilgi sistemleri yönetiminden bağımsız bir göz olarak işte rutin, planlı denetimler, kontroller yapıyoruz, bu kontrollerin sonucunda hazırladığımız raporlarda resmi olarak direk yönetim kuruluna gidiyor. Denetim yönetim kurulunun içinde de küçük bir denetim komitesi kurulmuş durumda yönetim kurulu üyelerinden oluşan doğrudan biz onlara gönderiyoruz. Onlar raporlarımızı bulgularımızı inceliyorlar tespitlerimizi inceliyorlar ve ardından o raporu genel müdürlük nezdinde bilgi sistemlerinden sorumlu yöneticilere gidiyor ve onlar da bulguları gidermek için aksiyon alıyorlar. Yani, siber güvenlik alt yapısında bir aksaklık olumsuzluk küçük de olsa büyük de olsa bir şey tespit edildiyse zaten bizim muhatabımız iç denetim biriminin iç kontrol biriminin muhatabı yönetim kurulu doğrudan, yani bizi görevlendiren de yönetim kurulu, o yüzden zaten bizi onlar görevlendirdiği için raporumuzu da biz ilk onlara sevk ediyoruz ardından, onlar diğer birimlere gönderiyorlar ve aksiyon alınmasını talep ediyorlar.

Panelist 9- Bunu şöyle söyleyeyim şimdi, bilgi güvenliği fonksiyonu bankalarda ya genel müdür ile ya da yönetim kuruluna bağlı olabiliyor. Biz banka olarak yönetim kuruluna bağlı yönetim kurulu içinde denetim komitesi başkanının yönetiminde işlemlerimizi icra ediyoruz. Burada teftiş kurulu, iç kontrol ve bankadaki risk yönetimi ve bilgi güvenliği olarak, biz her üç ayda bir mevcut risklerimizi bunun içinde siber güvenlik de dahil teftiş kuruluna bildiriyoruz. Teftiş kurulu da yaptığı denetimlerde riskli gördüğü konular varsa,

onlar da her ay yönetim kuruluna bunları raporluyorlar. Bu şekilde riskler var siber güvenlik ile ilgili, ya da mesela değişen veya gelişen siber riskler biz değerlendirmeler yapıyoruz ve bu değerlendirmelerimizden sonra bizim yapmamız gereken varsa aksiyonlar çıkardığımız rapor dahilinde, bunların da bilgi teknolojileri projesine dönüştürülmesini sağlayarak, yapılmalarını takip ediyoruz. Ve bütün projeler yönetim kuruluna zaten raporlanıyor plan dahilinde ayrıca.

Panelist 11- Komiteler ve içeride belirlenmiş ekiplerin aracılığıyla, düzenli veya case bazlı toplantılar yapılmaktadır.

Panelist 14- Söz konusu mekanizması ilgili mevzuat uyarınca belirlenmiştir, nihai sorumluluk yönetim kurulunda olmakla birlikte bankaların bu konudaki denetim mekanizması ilgili mevzuat uyarınca bankanın gerçekleştirdiği faaliyetler çerçevesinde ve kendine uygun yöntemler geliştirmesini ve uygulamasını gerekli kılacak şekilde oluşturulmaktadır. Bu süreçteki banka içi tarafları; Yönetim Kurulu, Denetim Komitesi, iç denetim sistemi ve BS iç denetim sistemi olarak özetlemek mümkündür.

Soru 4-Organizasyonunuz değerlendirmeye alındığında, gizlilik, bütünsellik ve kullanılabilirlik kavramları sizde nasıl bir çağrışım yapmaktadır?

Panelist 1- Bütünü ile ele alındığında BDDK nın son çıkarmış olduğu yönetmelik sadece bizim bankamız için değil tüm bankalar için bir avantaj oluşturdu, orda adreslediği husus şuydu bankanın bilgi güvenliği sorumlusunun doğrudan genel müdüre veya yönetim kuruluna bağlı olması esastır şeklinde bir ibare vardı, biz de bu ibare kapsamında bilgi güvenlik müdürlüğümüzü doğrudan genel müdürümüze bağladık, bilgi güvenliğinin sağlanmasında gizlilik, bütünsellik ve kullanılabilirlik olarak sizin de belirttiğiniz üç temel unsur da eskiden sadece bilgi teknolojileri kapsamında değerlendirilen bilgi

güvenliği ve siber güvenlik fonksiyonunun organizasyon yapısının değişmesiyle birlikte banka bünyesine kurumsal bir şekilde yayılmasını sağladı, yaklaşık bir yıl önce organizasyon yapısında değişiklik oldu, bunun da faydasını her alanda hissediyoruz, bilgi güvenliği açısından bakıldığında.

Panelist 2- ISO 27001, COBIT süreçleri olsun ve diğer bilgi güvenliğinin denetimi ile alakalı sürekli olarak ekibimizde çalışmalar yürütülüyor, o yüzden özellikle bilgi güvenliği servisi bu bahsetmiş olduğum uluslararası denetim süreçlerine hakim, ikinci olarak bütünsellik kavramından bahsedersem eğer, şöyle belirteyim, bilgi güvenliği dediğimiz çok geniş bir kavram içinde birçok konuyu barındırıyor açıkçası, siber güvenlik de bilgi güvenliğine bağlı bir dal gibi düşünebiliriz, tabi bütün bu konuları değerlendirdiğimizde tüm ekibin birbirlerinin yapmış olduğu işler ile alakalı bir bütünsellik var, hem süreçlerin kontrol edilmesi hem de süreçlerin iyileştirilmesi noktasında bir bütünsellik mevcut. Kullanılabilirlik ile alakalı şunu belirtebilirim, biz mevcut süreci yönetirken birçok ürünler ve araçlar var bunları gerçekleştirirken tabi bir bilgi güvenliği ekibi bu işlemleri sağlarken, daha doğrusu şöyle oradaki kaynaklar da çok önemli, kullanılabilirlik olarak bunları örnek verebilirim daha doğrusu.

Panelist 3- Bankacılık sektörü için özellikle gizlilik tarafı çok büyük önem teşkil ediyor biliyorsunuz yasalar kapsamında BDDK nın vermiş olduğu sınırlamalar kapsamında bankada birinci öncelik özellikle gizliliktir, erişilebilirlik de aynı şekilde yüksek derecede önem verilen bir konu olarak bizim gündemimizde her zaman, çünkü kullanıcı deneyimi ve kullanıcıyı müşteriyi memnun etme açısından erişilebilirliğin yüksek olması gerekmekte, bütünsellik anlamında da banka genel anlamda bunu korunması ve sürdürülebilirliğin sağlanması yönünde çok dikkatli diyebilirim size, çünkü sürdürülebilirlik aslında bir sistemin tamamen yaşaması için gerekli olan bir sistem ve

ekip olarak düşünülmesi gerekli, bu nedenle bizim açımızdan üç konu kritik diyebilirim, ama özellikle gizlilik kavramının altını çizebilirim.

Panelist 4- Evet, gizlilik, bütünlük, ve kullanılabilirlik kuralları bizde çok önemli bizim denetimimizde de çok önemli, veriler bütün olmalı ki bizde kendi etik ilkelerimiz gereği dürüstlük kavramına yönelik düzgün bir denetim yapabilelim, biz İç Denetim Enstitüsü standartlarında belirtilen etik kuralları benimseyerek, bu yönetmeliğimize de uyarlanmış bulunmakta, biz denetimlerimizde bu hususlara şöyle dikkat ediyoruz tüm denetim kanıtları güvenilir, erişilebilir ve bütünsel olmalı, biz bu doğrultuda birçok denetim yapmaktayız, veri yönetişimi birimi kuruldu, bu birimin denetimleri ayrıca yine COBIT hedefleri kapsamındaki denetimlerimizde, bu üç şart sağlanmaz ise biz denetim kanıtını bile sunmuyoruz çünkü süreç tamamlanmamış oluyor ve eksik olarak belirtiliyor.

Panelist 5- Bilgi güvenliği temelde sizin de biraz önce bahsettiğiniz üzere gizlilik, bütünlük ve erişilebilirlik kavramları üzerine kurulmuştur. Bilgi güvenliği olarak bu üç kavramı kesinlikle uygulamanız veya uymanız gerekiyor, örneğin gizlilik dediğimiz şey, yetki prensibi çerçevesinde her kişinin veya her birimin kendi yetkisi olduğu sistemlere veya ortamlara erişmesi gerekiyor, öncelikle gizlilik kavramı bunları çağrıştırmaktadır. Erişilebilirlik anlamında da sürekli olarak bu alt yapıların erişilebilir olması gerekiyor, hem altyapısal olarak hem işleyiş süreç anlamında hem görev dağılımı konusunda, erişilebilirlik tarafını da sağlamanız gerekiyor, yani sistemlerin her zaman canlı ve sorunsuz bir şekilde çalışmasını sağlamanız gerekiyor, üçüncü diğer bir adım ise bütünsellik kavramıdır, bilgilerin hiçbir şekilde değiştirilmediğinin kanıtlanması veya o bilgilerin oluşturulma tarihine kadar verilerin kesinlikle değişmediğinin ve bütünselliğinin bozulmadığını ispatlamanız gerekiyor, bu unsur de izleme fonksiyonları ile gerçekleştirilebilmektedir, örneğin dosya sunucuları üzerinde veya herhangi bir dosya

dizininde ilgili bir dosya vardır, o dosyanın içerisindeki bütün dokümanları incelemeniz ve izlemeniz gerekiyor, orada herhangi bir değişiklik olursa hem dosya silme hem de ilgili dosya üzerinde değişiklik olursa, bunları loglamanız gerekiyor ve kayıt altına almanız gerekiyor, bunlar da bütünsellik anlamında yapılan işlemlerdir.

Panelist 6- ISO 27001'in üç temel başlığı var zaten gizlilik, bütünsellik, ve erişilebilirlik diye geçiyor biz bilgi varlıkları envanterimizi çıkartıp her bir varlık envanterinin sınıflandırılmasını yaparken bu üç unsur açısından değerlendirmeler yapıyoruz, dolayısıyla ISO 27001 sertifikamız olduğu için banka olarak bu konuya çok aşinayız hem 27001 denetimlerinde hem yönetmelik denetimlerinde hem de COBIT denetimlerinde bu varlık sınıflandırmasını zaten denetçi arkadaşlar ile de paylaşıyoruz, bir de bankadaki bilgi güvenliği içerisindeki politika prosedürlerimizi de bu üç unsur üzerine oluşturduğumuz bu sınıflandırmalarda çalışanların nasıl davranacağı kapsamında tasarlanmış kurallarımız da bulunmaktadır. Dolayısıyla, gizlilik derecesi yüksek olan bir veri bankanın kuralları çerçevesinde örneğin bir müşteri verisi ise dış aygıtlar ile farklı bir cihaza aktarılamaz, çünkü bu gibi işlemlere yetki verilmez veya elektronik posta yolu ile de gizlilik seviyesi yüksek olan verilerin transferi engellenir. Bankacılık işlemlerinde çok fazla veriye ihtiyaç duyulmakta, bunlar, müşterilerin ev adresleri, telefonları, hesap bakiyeleri, kart verileri veya kredi kartı ile ilgili harcamaları gibi. Ayrıca, BDDK verilerin korunması için bu üç temel unsuru gözeterek değerlendirmeler yapabiliyor, ancak bir de BDDK'nın belirlemiş olduğu şöyle bir sınıflandırma var hassas ve sır kapsamındaki veriler. Bunlara ilaveten, kişisel verilerin korunması kanunu da bu üç temel unsurun sağlanmasının yanında takip edilmektedir. Belirttiğim gibi, bu üç unsurla beraber KVKK kapsamında verilerin niteliği belirlenmekte. Bizim bankamızda veriler çok gizli, bankaya özel, hizmete özel ve genel olmak üzere dört sınıf içerisinde değerlendirilmektedir.

Panelist 7- Bu zaten güvenliğin en temel kavramları, gizlilik, bütünlük ve erişilebilirlik. Aslında bütünlük değil dürüstlük olarak çeviriyorum, çünkü bütünlük denilince tam olarak anlam içermiyor. Bir tanesi confidentiality, biri integrity, bütünlük, bütünsellik veya daha doğrusu aslına bakarsanız dürüstlük diğeri de availability. Bütünlük nedir, bu çok böyle bize yabancı olan bir kelime, bütünlük deyince bana hiçbir anlam ifade etmiyor açıkçası öyle söyleyeyim, ama bir şeyin bütünlük dediğinizde, bir verinin tam olarak doğru kişi tarafından değiştirildiğinden emin olunması, yani ben bir veriyi alıyorum ama bu verinin tam olarak kim tarafından değiştirildiğinden emin miyim, bunun için bir garanti vermek oluyor bütünlük. Aslına bakarsanız, yani bu veri evet bütündür, yani bu veri doğru kişi tarafından tanımlanmıştır ve değiştirildiği zaman da doğru kişi tarafından değiştirilmektedir. Yani sizin önünüze bir bütün halinde gelmektedir, şeklinde ifade ediliyor. İngilizce'de integrity deniliyor. Integrity dürüstlük demek aslında. Confidentiality için her şeyden evvel ilk zaten finart uygulaması, bizim ana bankacılık uygulamamızda anahtar veya finart olarak geçiyor, burada zaten, her sene düzenli olarak denetimler yapılıyor ve veriye yetkisi olan kişiler erişebiliyor. Bu yapılması teknik olmayan daha böyle ilk etapta insanın dikkatini çeken denetim noktalarından bir tanesi olduğu için çok düzgün bir şekilde ilerletiliyor. Yani gerçekten, biz veriye doğru kişinin eriştiğini görebiliyoruz ve aynı şekilde integrity de buna bağlı, bütünlük dediğimiz şey, o veri değiştirilirken, örneğin mesela bir yerdeki faiz oranı, ekrandaki faiz oranı değiştirilecek bu da çok sıkı bir şekilde kimler tarafından değiştirildiği her sene mutlaka denetleniyor. Hatta, birden çok kez farklı zamanlarda denetleniyor. Availability de genellikle zaten banka sistemleri için kesinti zamanları bellidir, çoğunlukla ulaşılabilirdir her sistem, availability 'nin tanımı zaten gerektiğinde bir veriye ulaşabilmek olarak yapıldığı için gerek internet bankacılığı için olsun gerekse şubedekilerin o an müşterilerin

ihtiyaçlarını görebilmesi için erişmeleri gereken servisler olsun bunlar available bir şekilde her zaman servisler sunulabiliyor. Bazen yılda bir falan belli bir zaman belli bir kapasitenin üzerinde kesinti olabiliyor, mesela, geçen geçtiğimiz senelerde bir zaman damgası sunucusundan dolayı bir saatlik falan bir kesinti olmuştu. Böyle bir konudan dolayı mesela büyük bir sıkıntı çıktı onun haricinde availability de banka için sağlanan ve yeterince sağlanan konulardan birisidir diye düşünüyorum. Confidentiality, integrity ve availability kontrolleri öyle hadi biz bunun confidentiality'sine bakalım diye yapılacak denetimler değil baktığınız zaman, çünkü aslında bunlar bilgi güvenliğinin temeli, ben denetimlerimi bu üçü kapsamında yapmalıyım diye sizin içselleştirmeniz gereken şeyler. Sizin yaptığınız denetim çok farklı bir şey de olabilir, ben dediğim gibi bankacılık sürecine gidiyorum, kredi kartları ile alakalı, kredi kartları charge back konusunda yani geri iade konusunda bir kontrol listem var onunla alakalı kontroller yapıyorum ama benim aklımda her zaman şu bulunuyor, buradaki ekrana bu arkadaş her zaman erişebiliyor mu, yani erişemediği belli bir zaman periyodu var mı, onu mesela sorguluyor mu, kullanamadığı bir zaman dilimi olmuş mu veya işte önüne gelen veri kaynaktan sonra kimler tarafından değiştirilebiliyor kimler bu veriye erişim sağlamış gibi şeyleri sorgulayarak ben confidentiality, integrity ve availability kavramlarını denetimimin içine yedirmek zorundayım, yoksa bunlar somut olarak tek başına denetimleri yapılabilecek şeyler değil. Bunlar dediğim gibi bilgi güvenliğinin temelidir, sizin yaptığınız her türlü denetimde aslında bunları bir bilgi teknolojileri uzmanı olarak sorgulamanız gerekir. Nereye elinizi atarsanız atın ve orada bir bu alanlarda bir confidentiality, integrity veya availability de bir açık varsa bunu da raporlamanız gerekir. Dediğim gibi ama işte confidentiality denetimi diye bir şey ben şu ana kadar görmedim şahsen, confidentiality denilen şey veya integrity, availability denilen şey denetim içerisindeki sizin uymanız

gereken dikkat etmeniz denetlemeniz gereken konu ile alakalı bir sorun var mı diye denetlemeniz gereken kavramlardır diyebiliriz.

Panelist 8- Gizlilik, bütünlük ve kullanılabilirlik çok ciddi uygulamalar var bankada zaten en başta dediğim gibi bankacılık sektörü özünde banka ve müşteri sırrı konusunda çok ciddi aksiyonlar alınması gereken kurumlar yani bankalar bir güven kurumlarıdır ve müşteri gizliliği çok önemlidir. BDDK düzenlemelerinde de bu var, müşteri sırrı konusu çok önemli, müşterinin bilgisi dışında bir dışarıya bilgi sızması olduğu zaman onun hapis cezasına kadar yolu var, dolayısıyla bankada gizlilik konusunda aksiyonlar alıyor, işte veri tabanlarında müşteri bilgilerinin şifreli tutulmasından tutun kurum içi kurum dışı veri transferlerinde tüm altyapının şifrelenmesi gibi tüm bunlar hatta internet bankacılığı mobil bankacılık uygulamaları bile protokoller üzerinden şifreli olarak işletilmekte, dolayısı ile şifreleme konusunda çok ciddi aksiyonlar var. Bütünlük konusunda da verinin kötü niyetli kişilerde manipüle edilmesi konusunda aslında bu şifreleme ile de yakından ilişkili, siz hareket halindeki bir veriyi ne kadar korursanız bütünlüğünü de o kadar korumuş oluyorsunuz, burada da tabii ilave olarak bu hash algoritmaları NB5 gibi SHA gibi hash algoritmaları kullanılıyor yani bütünlüğün kontrolünün sağlanması amacıyla. Kullanılabilirlik anlamında da kullanılabilirliği erişilebilirlik olarak kastettiğinizi düşünüyorum ben, çünkü Türkçe'deki ifadesi ile usability kelimesi var o da kullanılabilirlik anlamına geliyor ama sizin kastettiğiniz erişilebilirlik. Hizmet sürekliliği politikaları olsun bu politikalar kapsamında bayağı ciddi şeyler var uygulamalar var hani veri merkezinin yedekte tutulmasından tutun işte veri merkezi yedek kopyalarının iki farklı lokasyonda tutulmasına kadar çeşitli risklere karşı bertaraf edilmek üzere önemli aksiyonlar var.

Panelist 9- Şimdi orda şöyle bir şey var, normalde bunlar gizlilik, bütünlük ve erişilebilirlik değerlendirilirken artık Kişisel Verilerin Korunması Kanunu'ndan (KVKK) sonra bir de privacy işin içine girdi. Bu da mahremiyet olarak değerlendiriliyor, artık CIA kavramlarının yanına bir de gizlilik, bütünlük ve erişilebilirlik kavramlarının yanına mahremiyet değerlerine göre biz değerlendirme yapıyoruz. Mesela, siz, bankamız müşterisi iseniz, mobil bankacılıktan bakıp da gördüğünüz 100 TL'lik mevduatınız, o sizin aslında, yüz liranız varken yetmiş gösterilmemesi, bu verinin bütünlüğü ile ilgilidir. Verinin gizliliği de sadece sizin görebileceğiniz user name, parola ve One time Password (OTP) ile sağlarken yetkisiz kişilerin veriyi görmesini engellemek için de Service Set Identifier (SSID) kullanarak güvenliği bütüncül olarak temin ederek o veriye erişmenizi sağlıyoruz. Availability bacağı da bu sizin yedi yirmi dört bu sistemlere erişmenizle ilgili bir şey.

Panelist 11- Kurumsal veri ofisi ve bilgi riski yönetimi ekiplerimiz süreçleri bu süreçleri yazılı hale getirmiştir.

Panelist 14- Bu hususu bankacılık sektörü olarak değerlendirirsek, bu kavramları mevzuat olarak ve uygulama pratiği açısından ilk gerçekleştiren kurumlardan birisi olan BDDK ve Türk Bankacılık Sektörü için bilgi güvenliği hususunun sadece bir güvenlik unsurundan öte gerek sektör gerek banka bazında rekabet avantajı sağlar nitelikte bir özellik kazandığından bahsedebiliriz.

Gizlilik, bütünlük ve kullanılabilirlik kavramlarını genel literatür açıklamaları zaten bu konuyla ilgili herkesin malumudur. Şahsi olarak ise bunların ötesinde oldukça detaylı açıklamalar ve farklı boyutları ile ele alabilmek mümkündür. Kısaca bu kavramların banka, kamu, müşteri, banka tarafları vb. boyutları ile değerlendirilebilir.

Soru 5- Etik kurallar, iç denetim ve siber güvenlik kavramları ile birlikte değerlendirildiğinde, sizde neleri çağrıştırmaktadır?

Panelist 1-

Bankamızın çıkardığı etik ilkeler bulunmakta, bu da bizim kurumsal yapıda yer alan komitelerde sadece güvenlik fonksiyonu açısından değil tüm yapılan çalışmalarda temel alınıyor, burada bütünsellik olarak değerlendirdiğimizde bankamızdaki etik ilkeleri her alanda sadece güvenlik fonksiyonunda değil diğer her alanda bütün iş yapış biçimlerimizde, bu ilkelere uymakla zorunluyuz zaten, orda da herhangi bir olağan dışı gözlemlenmemekte.

Panelist 2- Hem iç denetim hem de siber güvenlik süreçlerinin yönetilmesinde, bilgi güvenliği departmanı ve iç denetim fonksiyonları sürekli olarak koordineli bir şekilde çalışması gerekiyor, çünkü takdir edersiniz ki siber güvenlik dünyası her geçen gün büyüyen, gelişen ve yenilenen bir sektör, böyle de olunca iç denetimdeki kişilerin bilgi güvenliğindeki kişiler kadar konulara vakıf olmalarını bekleyemeyiz tabi ki, bilgi güvenliği servisi burada iç denetim tarafına danışmanlık noktasında yardımcı olabilir, onların hangi süreçleri takip edeceğini ve şu şekilde açıklanacak olursa iç denetim bilgi güvenliği servisini denetledikten sonra ortaya çıkan bulgular ile ilgili siber güvenlik yani bilgi güvenliği ekibine raporlama sağlar sonrasında da bilgi güvenliği ekibi de bu konu ile alakalı kendi eksik olduğu noktalarda zayıflıkları giderir ve daha sonrasında da bu sürecin bir bütün halinde ilerletilmesi için iç denetim ekibine yardımcı olur. Bu süreçler yönetilirken etik kuralların olması gerekiyor.

Panelist 3-

Biraz önce yetkilendirmeden bahsetmiştim, etik kurallar anlamında, bizim kurumumuzda etik kurallara uyum çok önemlidir, bu nedenle de yetkilendirmeye çok dikkat ederiz herkesin her veriye erişimi sağlanmaz ve bu kurallara uyulması için de iç denetim tarafında dikkat edilmekte. Bir teknoloji şirketi ile konuşuyor olsaydınız, belki bu çok daha fark edebilirdi, ancak özellikle denetim tarafını sorduğunuz için, denetim tarafı bu belirttiğiniz unsurlara özellikle dikkat etmekte, bunu denetlediği şeylerde görmeye çok dikkat ediyor, yetkilendirmeler olsun, gizliliğin sağlanması olsun, sınırlar zaten İç Denetim Enstitüsü'nün belirtmiş olduğu standartlara göre belirleniyor ve bu hususlara dikkat ederek denetimleri gerçekleştiriyoruz. Sınırlandırıldığımız kısımlar var, BDDK tarafından oluşturulan yasalar var ve onun haricinde yasa kapsamındaki kurallarımız var, hepsini de geçtim, ISACA kapsamında bizim kontrol ettiğimiz şeyler var.

Geçen seneye kadar BDDK tarafından kabul edilen bize referans olarak gösterilen COBIT 4.1'di, geçen sene BDDK tarafından yeni bir yönetmelik çıkartıldı, bilgi sistemlerine dair, yeni çıkarılan yönetmelikle birlikte COBIT'in değerlendirdiği alanlar temel alınarak bir yasal çerçeve oluşturuldu. Aslında, yasa yapıcılar etik kuralların oluşumunda da önemli rol oynamakta. Bankacılık sektöründe etik kurallar daha net ve bariz olarak uygulanmaktadır.

Panelist 4-

Önceden de bahsettiğim üzere, IIA etik kurallarına tabiyiz ve onları tamamı ile benimsemiş durumdayız, siber güvenlik tarafında mesela yeterlilik kavramı var, biz yeterli olmalıyız, yetkin olmalıyız, bir siber olay ortaya çıktığında nasıl yaklaşacağımızı belirlemek için eğitimli olmamız lazım ve kendimizi geliştirmeliyiz, eğer biz bu uğurda ya da bu denetimleri yaparken iyi değilsek, bu denetimleri gerçekleştiremeyeceğimizi görüyorsak biz o görevden çekilmek zorundayız, dış kaynak kullanımına gitmek

zorundayız, eğer yeterli kaynağımız yoksa, orayı denetleyecek bilgi birikime müfettiş sahip değilse, biz o görevi yapmıyoruz, çekiliyoruz, dış kaynak kullanımına gidiliyor, ama biz bunu, yönetmeliğimizde var dış kaynak kullanımı, alternatifi ama biz bunu şöyle yapıyoruz, öncesinde denetçilerimiz eğitiyoruz, zaten denetim planımız var her şey planlı programlı, bu uğurda öncelikle müfettişleri eğitmekle başlıyoruz olaya, siber güvenlik veya diğer konular ile ilgili tecrübe kazanmalarını sağlıyoruz, bu şekilde yedekli çalışıyoruz daha sonra da denetimlerimizi bu şekilde planlamış oluyoruz, yani dış kaynak kullanımına doğrudan gitmiyoruz genellikle eğitim oluyor, yeterlilik kısmını yani etik ilkelerdeki yeterlilik unsurunu bu şekilde sağlıyoruz, dürüstlük kavramı ya da diğer etik davranış ilkelerine de bakacak olursak da denetim kanıtlarımızı tüm bütün taraflara sunabilecek şekilde elektronik olarak kaydediyoruz, bütün denetlenenlerde açık oluyor, bulgularımızı izlerken tüm sonuçlarımızı paylaşıyoruz, yine kanıtlarını onlar da görebiliyor, kapanış toplantıları yapıyoruz yani etik ilkeler ile bu şekilde eşleştirebilirim.

Panelist 5-

Biraz önce aslında bahsettiğimiz konu ile eşdeğer bir konu, bilgi güvenliğinin temel ilkesi olan gizlilik, bütünlük, ve erişilebilirlik kavramları, aslında burada en büyük şey gizlilik tarafı ile ilgili bilgi vermek gerekirse, şimdi etik kurallar dediğimiz çerçevede bazı ortamlar vardır, örneğin veri tabanları, örneğin sistemler, örneğin uygulamalar, uygulama sürücüleri, bunlara ilgili ekiplerin erişip o uygulamalar üzerinde çalışma yapmaları gerekmektedir, bu da aslında etik kavram olarak düşünülebilir, çünkü, yapması gereken iş listesinde olması sebebiyle, o ortamlara, örneğin, kimsenin erişmemesi gerekirken, ilgili ekipler erişebiliyor, çünkü o iş sürecini işletebilmeleri için, aynı şekilde bilgi güvenliği tarafında da yönetilen uygulama ve sunucuları veya altyapısal olarak da bu kavramları söyleyebiliriz, her ekip kendi yetki ve görevler ayrılığı matrisine göre kendi

etik kavramı ya da bizdeki karşılığı şudur etiğin, kendi izole veya sınırlayıcı kapsamı içerisinde işleyişini sürdürebilirler, burada zaten herhangi bir sıkıntı yoktur. İç kontrol ve bağımsız denetimlerinde örneğin bir veri tabanı sunucusuna, veri tabanı ekibi dışında bir admin'in erişmemesi gerekiyor, bilgi güvenliğindeki herhangi bir uzmanın veri tabanı sunucusuna erişmemesi gerekiyor, bu da bir kontroldür, o sistemlere veya sunuculara veri tabanı yöneticileri yani yetkili olan kişiler erişmektedir. Bunu genel olarak bankadaki tüm altyapılar için söyleyebilirim.

Panelist 6-

Olmazsa olmazı çağrıştırıyor Etik Kurallar, yani etik kurallar bir çalışanın bulunmuş olduğu kurumda, kurumun bünyesindeki politikalara ve kurallara uygun şekilde davranmasını tetikleyecek şeyler, siber güvenlik ve iç denetim fonksiyonlarında oldukça önemli, siber güvenlik tarafında sürekli yeni saldırılar, yeni oltalamalar, sıkıntı oluşturabilecek durumlar ortaya çıkabiliyor. Eğer içerdeki çalışanlar bizim etik kurallarımıza uymadan bilerek veya bilmeyerek bir şekilde siber güvenlik alanındaki zayıf halka oldular ise eğer, yani bankaya ait bilgileri bir başka kişinin eline verdiler ise bu durumda bir bizim bunu biliyor ve ölçüyor yani takip ediyor olmamız gerekli, iki bu veri çıktıktan sonra, bu olayın üzerine gidip neden nasıl kim yapmış hangi kanalla yapmış bunu biliyor olmamız lazım, biz bilgi güvenliği olarak, bu olayın tekrar etmemesi için ne yapılabilir de bu bilgi dışarı çıkamaz diye işte farkındalık eğitimi ise farkındalık eğitimi, sistemsel düzenleme ise onu yapıyor olmamız lazım, denetim ekipleri de burada herhangi bir olay olmadan düzenli kontroller olabilecek açıklıkları bulup raporlamaları ve iyileşmeyi takip etmeleri, bir taraftan da böyle bir olay olduğunda bir çalışan siber güvenlik olayına etik kurallara uymadı, bir bilgi sızıntısı yaptıysa, iç denetim ekipleri bunun peşine düşüp, araştırması ve çalışana da gerekiyorsa disiplin cezalarını işletiyor

olması gerekiyor, çünkü biz yapıyoruz yani, oltalama maili atıyoruz, önce eğitim veriyoruz ardından oltalama maili atıyoruz, kişiye parolasını paylaşma diyoruz ama bakıyoruz parolasını paylaşmış, sonra tekrar farkındalık eğitimi veriyoruz, tekrar oltalama maili atıyoruz, bir daha paylaşmış, o zaman diyoruz ki bir de paylaştın tamam, iki de de paylaştın o zaman sen bizim zayıf halkamızsın diyoruz. Ne oluyor, artık burada, insan kaynakları disiplin süreci devreye girmeye başlıyor, eğitim veriyorsanız, öğretiyorsanız, bir sürü şeyden bahsediyorsanız, bir iki üç senaryoda hala size oltalamada parolayı veriyorsa, bu benim zayıf çalışanımdır, siz de zaten banka olarak, zayıf çalışanınız kadar zayıfsınız, yarın öbür gün o kişi şube çalışanı ise, ben işte Ahmet müşterisiyim benim şu hesabımdan şunu aktar dediğimde buna da inanabilecek potansiyelde olmuş oluyor. Etik kurallar şirketimizde mevcut, disiplin politikamız var, etik kurallarımız var, prosedürlerimiz var ve birçok kuralımız var ve engelleyici kontrollerimiz de var, etik kurallar da ama, yine de yazılı olan politika ve prosedürleri her zaman sistemsel kontroller ile takip edemiyoruz. Burada da iç kontrolün gidip denetimler yapması bizim gidip çeşitli senaryolar ile kontroller ile yapmamız gibi şeyler devreye giriyor, oltalama da bunlardan bir tanesi. Parolanı paylaşma, bizim bilgi güvenliği politikamızda yazıyor mesela. İşe giriş sözleşmesinde imzaladığı sözleşmede de yazıyor, bankanın bilgilerini kimseyle paylaşma, işte bankaya ait sistem bilgilerini paylaşma, bu da yazıyor. Gizlilik taahhütnamesi de imzalatıyoruz orada da yazıyor, eğitimler veriyoruz her sene mutlaka her çalışana eğitim veriyoruz ama bütün bunlara rağmen, bakıyoruz ki paylaşmış, burada bir daha uyarıyoruz, bir daha bir eğitim veriyoruz, bir daha çalışma yapıyoruz, yine paylaştıysa artık burada farklı bir yola gidiyoruz. Geçen seneler de bu kadar önemli değildi ama şimdi artık pandemiden sonra evden çalışma düzenine girdik, biliyorsunuz çağrı merkezleri bile artık evden çalışıyorlar, eskiden binanın içerisinde işte

kameralar var, ofis içerisinde kartlı geçiş sistemleri var, işte sistemler zaten internet çıkışları, bilgisayarlar hepsi zaten bankanın bünyesinde korunuyordu ama şimdi evinde belki evinde bile değil gittiği bir misafirlikte başka bir lokasyonda belki de dışarıda bir yerde dolayısıyla burada bağlanmış olduğu ekran ve bilgiler daha kritik hale gelmiş oluyor o yüzden hiç oltalanmamasını ve bu konular da daha dikkatli olmasını bekliyoruz.

Panelist 7-

Bir siber güvenlik denetçisi veya bu alanda çalışan biri, aslına bakarsanız her türlü yetkiye sahiptir, özellikle denetim açısından bizim erişemediğimiz herhangi bir veri yok ve bu bağlamda da gidip insanların gizli bilgilerini sorgulayabilirsiniz. İşte bu yüzden, bu noktada belli bir etik ahlaka sahip olmak gerekiyor veya size verilen yetkiler, yapabileceğiniz tasklar söz konusu olduğunda mesela öyle birtakım bağlantılar yapabilirsiniz ki belki mesela o noktada kendinize kişisel bir menfaat sağlamanız söz konusu olur altyapı ile alakalı bir yerden bir yere para aktarabilmeniz söz konusu olur mesela. Bu noktada etik kurallar net olarak belirlenmeli ve bu bir kurum politikası olarak da herkese sunulmalı, çünkü eğer kurum politikası olarak sunulmazsa insanlar elinde bulunan yetkiler ile kişisel olarak baktığınız zaman hani ben abimin kredi miktarına bakmış mıyımdır evet veya işte eşim ile alakalı bazı şeylere bakmış mıyımdır şu ana kadar evet, ama bunun çok daha ileri versiyonları da yapılabilir. Bunların çok net bir biçimde ortaya konması lazım etik kurallar çerçevesinin, bir disiplin yönetmeliğine bağlanması gerekir diye düşünüyorum, çünkü yoksa önünüzde çok geniş bir alan ve geniş yetkiler ile insanlar baş başa kalıyor ve sanki herhangi bir sorgulama yaptığında hiçbir şey olmayacakmış gibi düşünüyor. Bir tek benim gördüğüm çok kesin kurallar cumhurbaşkanının hesaplarına falandı yani hani onunla alakalı herhangi bir şekilde girilemez diye insanlara uyarı yapılıyordu sakın elinizde böyle bir veri var, böyle bir

imkan var sakın böyle bir şey yapmayın veya işte herhangi bir kimse bunu yaptığı zaman anında alarmlar üretiliyordu vesaire falan, sadece cumhurbaşkanı demiyim de yani milletvekilleri ve belli bir VIP listesinde ama onun haricinde sanki ben diyelim ki x kişisinin hesabını sorguladığım zaman kendi müfettişlik konumum dışında sorguladığım zaman bunun bana sorulmayacağını biliyordum hiçbir şekilde, bu bağlamda da etik kavramı bence baktığınız zaman birincisi insan bir kişinin kendi öz değeri olarak onun içerisinde var olmalı, ikincisi de bir kurum politikası olarak o kişiye dayatılmalı, baktığımız zaman, yoksa işin sonu bir şekilde alınamıyor, yani bu bizim dediğimiz gibi veri tabanındaki veriler üzerinde böyle ama bir de diğer taraftan denetçiler olsun veya o siber güvenlik adımlarını atan insanlar olsun onlar altyapı ile alakalı da çok daha fazla yetkiye sahipler ve oradan gerçekten bir menfaat sağlamaları da söz konusu. Yapılabilir mi evet bir şekilde yapılabilir, bunlara ilişkin kontroller falan var ama, bir şekilde orada menfaat sağlanması söz konusu olabilir. Etik değerlerin herkes tarafından benimsenmesi ve kurum politikaları ile belirlenmesi gerekmektedir.

Panelist 8- Siber güvenlik aslında bir kurumun alacağı uygulamalar aksiyonlar, kontroller, hani iç denetimde etik konusu tabi iç denetim standartlarının bir parçası etik, hani burada sizin siber güvenlik ile ilgili yaptığınız denetimde denetçi bakış açısıyla sizin çıkarınıza olan bir durum var ise, örnek vereyim, siber güvenlikten sorumlu yönetici veya siber güvenlik ile ilgili kontrolleri uygulayan bir personel sizin samimi olduğunuz yakın bir arkadaşınız ise, sizin kalkıp orayı denetlemeniz etik olmaz, iç denetim standardıdır bu etik, ya da sizin mesela bir açık vardır siber güvenlik alt yapısında o açığın bir takım kişiler tabii banka bundan zarar görecektir ama bazı kişiler de o açıktan faydalanıyordur orayı suiistimal ediyorlardır bu açıktan faydalanan tarafta sizsiniz, sizin orada denetim yapıp o açık konusunda yorumda bulunmanız yine etik olmaz. Bu genel denetim etiğidir.

Bu konuda da bizim bankada tüm denetçilere etik konusunda çok sıkı eğitimler veriyoruz yani işe yeni başlayan herkese. Etik konusunda kesinlikle taviz verilmemesi gerektiği konusunda sürekli eğitimler alıyoruz, iş başında eğitim verirken etik konusunu çok önemsiyoruz. Denetim konusundaki etik anlayışla alakalı siber güvenlik etiği.

Panelist 9- Etik kurallar derken, banka olarak bizim banka çalışanlarına imzalattığımız bir gizlilik taahhütnamesi var. Gizlilik taahhütnamesi banka ve müşteri verilerinin hiçbir şekilde ifşa etmemek, görev tanımı dışındaki zaten verilere erişmemesini zaten biz sağlıyoruz, bilgi teknolojileri olarak limit koyuyoruz. Onun dışında bankamızda etik hattı var, bir yönetici bağlı olan personeline bankacılık kanununa aykırı, bankamızın yayınladığı etik ilkelere aykırı bir işlem yaptırmak isterse bu personel doğrudan bu hattı arayarak sadece kendi bağlı olduğu bölümü belirtecek şekilde bu bildirimlerini yapabilir. Onun dışında zaten bizim de banka bünyesinde yapılan birçok etik kontrol var, internal fraud dediğimiz yapmaması gereken işlemleri yapan personelimiz varsa ya da yapmaya çalışan, onları da zaten biz takip ediyoruz ve disiplin komitesine onları gönderiyoruz.

Panelist 10- Şimdi bu soru aslında, şunu gösteriyor yaptığınız çalışmada da evet siber güvenlik alanında yapılan çalışmalar, benim de doktora tezim siber güvenlik alanındaydı, siber güvenlik alanında yapılan çalışmalar biraz zor çalışmalardır çünkü kaynak eksiği çok olur özellikle Türkiye'de. Gelişmiş ülkelerde yine bir takım bilgi ve belgelere ulaşabilirsiniz ama Türkiye'de daha bu belgeler oluşmadığı için bir ulaşma sıkıntısı var, kaynak sıkıntısı da ön plana çıkmakta siber güvenlik alanına girildiğinde. Şimdi biz siber güvenliğin daha bana göre yeni politika oluşturma yani sıfırdan politika oluşturma siber güvenlik kavramlarını tanımlama ve bu tanımlamaları özümseme safhasındayız. Etik meselesini biliyorsunuz, birçok alanda yani daha yeni alanlarda değil de daha köklü eski alanlarda bile etik meselesi daha yeni yeni tartışılır hale geldi. Yani bir işletme alanında

düşünürsek meslek etiği, iş etiği dediğimiz şey aslında daha yeni yeni literatürü oluşmakta ve gelişmekte yani doyum noktasına henüz ulaşılmadı. Siber güvenlik gibi çok yeni bir alanda daha kavramlar yeni özümsenmeye başlamışken, daha ortaya konacak ve literatüre eklenecek yeni kavramlar bile varken, etik kurallar kısmı daha yolun çok başında, yani daha filizlenmiş bir tohum gibi diyebiliriz bu etik kurallar için. İç denetimin kendisindeki etik kurallar oturmuştur, evet bir denetleme mekanizması bizim gibi işte bir imparatorluk döneminden cumhuriyete geçmiş köklü bir devlet geleneği olan Türkiye'de iç denetimin etik standartları oluşmuştur, buna kimsenin bir lafı olamaz zaten ama, işin içine siber güvenlik girdiğinde siber güvenlik ile etik kuralları şu an daha tam olarak oturtamadık yani çok başlarındayız bu işin, öyle söyleyeyim. O yüzden etik kurallar yavaş yavaş yani bizim çalışmalar sizin gibi bizim gibi akademisyenler, araştırmacılar bunları çalıştıkça önce siber güvenliği bir yere oturtacağız, daha sonra politikaları bir yere oturtacağız, işte bilgi güvenliği, bunlarla ilgili bizim elimizde bir sürü işte kurumların, üniversitelerin uyguladığı politikalar olacak, belgeler olacak, daha sonra işte kamu kurumlarının uyguladığı politikalar, siber güvenlik politikaları sonra özel sektörde şirketlerin uyguladıkları siber güvenlik politikaları elimizde olacak ki biz şu politikada eksik var, burada etik bir eksiklik var, şu uygulamada etik bir sorun var diye tartışacağız daha sonra etik kuralları artık yavaş yavaş oturtmaya başlayacağız ama bizim etik kurallardan konuşabilmemiz için şu an elimizde bir uygulama, bir belge, bir kaynak yok daha onların oluşması lazım diye düşünüyorum.

Panelist 11- Hepsi bir bütündür. Yaptığımızı yazmalı, yazdığımızı da yapmalıyız.

Panelist 12- Burada değerlendirirken, biraz kurumsal manada değerlendirirsek, artık şirketler kurumsal kaynak planlaması (ERP) ortamlarında genelde işlemlerini takip

ediyorlar özellikle büyük ve kurumsal işletmeler. Dolayısıyla ben burada ERP ortamının ya da bilgisayar kullanımının işletme faaliyetlerinde birlikte değerlendirilmesi gerektiğini düşünüyorum. Dolayısıyla burada, öncelikle, doğal olarak etik kurallar çok önemli bir işletme için özellikle hileler ya da usulsüzlükler için ya da hatalar için etik kurallar oluşturulması lazım öncelikle şirketlerde bu etik kurallar yazılı olarak da çalışanlara bildirilmesi lazım. Bir de burada şöyle bir şey yapılması kanaatindeyim ben, etik kuralların etik kodlar adı altında kodlanıp, kodlarla ERP ortamına ya da işletmelerin kullandıkları programlara tanıtılması gerektiğini düşünüyorum bu etik kuralların iç denetim kapsamında.

Eğer, bu kurallar çok iyi şekilde saptanır, tespit edilir daha sonra da kodlanıp programlara aktarılırsa ve şirket çalışanlarına duyurulursa, çalışanların ERP ortamında ya da bilgisayar programları üzerindeki hile yapmalarının ya da hata yapmalarının ya da usulsüzlük olmasının önüne daha fazla geçilebilir diye düşünüyorum. Tabi bu durum siber güvenlik kapsamında da uygulanabilir, çünkü teknolojik ortamda sonuç olarak, bilgisayar ortamında, ERP ortamında dediğim gibi işlemler takip edildiğine göre etik kurallar çerçevesinde yapılacak usulsüzlüklerden bir tanesi biliyorsunuz siber saldırılar, siber riskler dolayısı ile bu siber saldırılara veya siber risklere karşı etik kuralların kodlar haline dönüştürülmesini ve programlara kodlanmasını daha sonra da kodlandıktan sonra ERP ortamında yönetilmesini. Yani siz zaten kodladığınız zaman ERP ortamında ya da bilgisayar programı üzerinde kodladığınız zaman etik kuralları adam istese de yapamaz zaten. Mesela, şirketler artık elektronik imza falan kullanıyorlar elektronik yetkilendirmeler var biliyorsunuz, mesela her çalışan her programa her modüle ulaşamıyor, dolayısı ile mesela bu tür uygulamalar daha da genişletilebilir ve herkesin yetkileri sınırlandırılabilir şirketlerde, bunlar sayesinde dediğim gibi usulsüzlüklerin

önüne geçilebilir. Bir de burada yapılabilecek şeylerden bir tanesi de şu, loglar, log kayıtlarının takip edilmesi de burada önemli, log kayıtları biliyorsunuz her çalışanın yaptığı işlemin bilgisayar ortamında görülmesi, izlenmesi, eğer böyle yaparsanız siber saldırılara karşı da bir önlem almış olursunuz ve bunların hepsini etik kurallar çerçevesinde yazılı hale getirmek gerekmektedir. Daha sonra iç denetim prensipleri kapsamında bunların kodlanması gerekiyor ve kontrol edilmesi gerekiyor. Burada iç denetimin yanında iç kontrolü de değerlendirmek gerekiyor ve sürekli denetim metodolojisini de kullanmak gerekiyor. Biliyorsunuz sürekli denetim bilgisayar ortamında yapılan bütün işlemleri elektronik ortamda anlık olarak kontrol edilmesi ve denetlenmesi. Dolayısı ile, iç denetimin de burada kullanılması gerektiğini düşünüyorum. Özellikle, bankacılık sektörü sürekli denetim metodunun en sık kullanıldığı endüstriler arasındadır.

Panelist 13- Genel olarak, siber güvenlik konusu yakın zamana kadar sadece belli kişilerin profesyonel uzmanlığı ile düşünülürken, olsa iyi olur değil de mutlaka yetkinlikler arasına katılması gereken bir alan olarak ifade edilebilir. Yetkinlik seti içerisinde belki de ön sıralarda yer alması gereken konulardan biri olarak ifade edebiliriz. Yapmış olduğumuz özellikle de denetim sonucundaki tavsiyelerin gerçekçi ve geçerli uygulanabilir olması ve riskler karşısındaki gerekli korumayı sağlayabilmesi için konuya hâkim olmanız lazım, yoksa nasıl bir öneri yapabilirsiniz ki? Aslında şu şekilde ifade edilebilir, etik dediğimiz şey, zaten orada hiç toleransımız yok, bir denetçinin mutlaka ve mutlaka etik kurallara tam ve eksiksiz uyması ve belki de rol model özelliği taşıması lazım, orada hiç taviz veremeyiz zaten. O yüzden, bunu bir çatı olarak düşünürsek, temeli etiğe dayanmayan, ne kadar yetkinliği yüksek seviyede olursa olsun, profesyonel olarak, ama etik değilse, zaten daha riskli vakalara sebep olabilir. Etik olmayan birinin çok yetkin

olsa bile, denetçi olmasını bekleyemezsiniz. Bilgi eksiği giderilebilir ancak ama öbür tarafta çok yetkin ama etik ve ahlaki yönden zaafları varsa o kişi benim için makbul değildir zaten uluslararası standartların da çok temel bir tavsiyesidir. Mutlaka iç denetçilerin özellikle her yıl mutlaka etik ile ilgili beyanlarını, bunlar ile ilgili eğitimlerini ve görünür hale gelip rol modelliğini ortaya koyması beklenir, bu açıdan önemli. Meslek etiği, evrensel etik değerler yanında, her meslek için yok ama bizim denetim mesleği için çok net bir şekilde meslek etiği tarif edilmiş ve buna da eksiksiz bir biçimde uymamız beklenir. Örnek olarak, bir kişinin uluslararası standartlara göre siber konularda yeteri kadar bilgisi yok, standartlar derki eğer o alanda yetkin değilsen, dışarıdan bir uzman takviyesi ile bu işi denetleyebilirsin, bu konuda hiçbir sıkıntı yok. Ancak, etik konular ile ilgili dışarıdan danışmanlık alınması beklenemez. Kişinin etik olması ve etik rolü bizzat üstlenmesi gereklidir. Onun dışındaki her konuda danışmanlık alabilir. Etik kurallara uygun davranmak, denetçinin teknik özelliklerinden çok daha önemli ve esas unsur olarak denetimin temelini oluşturmaktadır, eğer denetim yapacak kişide etik veya ahlaki değerler yoksa diğerlerinin hiçbir önemi yok. Eğitimlerin zorunlu olarak organize edilmesi gerekir, ben biliyorum bir daha bakmama gerek yok değil, sürekli farkındalığı yüksek seviyede ve uyanık tutmak lazım, hiçbir şekilde gündemden düşmemesi gerekiyor. Konu, banka sektörü çerçevesinden değerlendirilecek olunursa, bankalardaki denetimler bütünüyle teknoloji tabanlı altyapılar vasıtasıyla sürdürülmektedir ve tüm işlemler gerçek zamanlı olarak yürütülmekte. Ayrıca, verilerin yapısı itibari ile de finansal piyasalar yüksek frekanslı zaman serisine dayalı olduğu için sürekli denetim (continuous audit) teknikleri olmadan zaten gerçekleştirilmesi zor. Siber konular ile ilgili süreçlerin denetimini yaparken, siber risklere açık olan süreçler ve insanlar, kritik varlıklar olarak da değerlendirilen, yetki anlamında, onların etik ikilem ya da etik ihlale

yatkınlıklarının testini yapabilirsiniz. Bu bağlamda, siber güvenlik denetimleri ile birlikte etik denetimi de yapılması gereklidir. Etik davranış standartlarının kurum kültürüne entegre olması ve organizasyonun geneline yayılması gereklidir. Etiğin en çok ihlal edildiği yer çıkar çatışmaları, burada kişisel çıkarlar ve kurum menfaati dediğimizde, o kişi herhangi bir bilgiye eriştiğinde kurumsal bir amaç için mi kullanacak yoksa şahsi menfaat elde edebilir mi? Önlenmesi için şeffaflık veya hesap verebilirlik gibi birtakım çareler aranıyor. Özellikle bankacılık sektöründe çok hassas bir konu, ben banka teftiş kurulundan geliyorum, mutlaka aradığımız şey ikili kontrol mekanizması ve üçlü mutabakat dediğimiz şey de fiziksel olarak sanal ortamda ve üçüncü taraflar işin içine girdiğinde kredi alanlar açısından bunların haberinin olması olası hırsızlık vakalarının önlenmesi, kayıpların önlenmesi açısından önem taşımaktır. Kurum kültürü içerisinde ahlaki yönden kişilerin farkındalıkları artırılırsa, siber güvenlik açısından risklerin indirgenmesi sağlanabilir. Etik liderlik, kurum kültürünün yaygınlaştırılması, güçlendirilmesi bunun göstergeleri var tabii. Etik konusu öyle bir konu ki, yokluğunda dediğim gibi diğerlerinin hiçbir önemi kalmıyor, milyonun önündeki bir gibi düşünülebilir, o biri aldığın anda o kadar çok sıfırın olsa o kadar çok yetkinliğin olsa da hiçbir kıymeti yok. Kurumsal yapı itibari ile bu temeli sağlayanlar ve bunu da bir güçlendirici etki olarak sosyal sorumluluk projeleri ile faaliyetleri ile destekleyenlerin çok başarılı olduğu yönünde literatürde bulgular var.

Panelist 14- Etik kuralların her bir iş kolunda ve organizasyon türünde önemli ve gerekli olduğu bilenen bir gerçektir. Bununla birlikte, özellikle kritik, karmaşık ve büyük organizasyonel yapılarda en küçük operasyon biriminden en üst yönetsel birime kadar iş süreçlerinde kontrol aşamalarının olabildiğince bağımsız, şeffaf ve hesap verebilir şekilde tasarlanmasına ihtiyaç bulunmaktadır.

Bankalar, bu hususlarda normal ticari işletmelerden daha sıkı bir şekilde mevzuatsal olarak düzenlenmiş ve birçok ilave yasal yükümlülüklere tabi kılınmışlardır. Bunun en önemli sebeplerinden birisi bankaların ticari bir kuruluş olmalarının yanında kamusal nitelikte kritik bir hizmeti yerine getirmelerinden kaynaklanmaktadır. Bu nedenle, bir güven kuruluşu olan bankaların etik kurallar ile organizasyonel faaliyetlerine ek olarak gerek iç denetim gerek bağımsız denetim ve kamu denetimi anlamında birçok farklı tarafça denetlenmektedir. Bankacılık sektöründe siber güvenlik işlemlerinin ayrı bir mevzuat ve detaylı kural setlerinin bulunması da bu konuda ülkemiz açısından konunun ne kadar hassas olarak ele alındığının bir göstergesi olarak değerlendirilebilir.

Panelist 15- Etik pratik bir tanım olarak şu demek, haklıyı, doğruyu, iyiyi ve adil olanı yapmak demek. Etik kurallar dediğimiz zaman, üç sistem vardır en tepede değerler vardır, değerlerin altında ilkeler vardır, ilkelerin altında kurallar vardır. Etik kurallar dediğimiz zaman temelde değerlerinizi belirlerseniz ne olabilir bu dürüstlük olabilir, değerler de çeşitli şekilde sınıflandırılabilir, kurumsal yönetim değerleri vardır, temel değerler vardır, bu değerlerden de birtakım ilkeler çıkar, mesela dürüstlük değerdir, bunun altında örneğin yalan söylememek bir ilkedir. Bunun altında da davranış kuralları çıkar, bu mantık içinde zaten çerçeve oluşur, temelde tepede bir değer vardır, bir kurumun örneğin yedi sekiz tane değeri vardır, bunun altında da ilkeler vardır, bunun altında da yap yapma şeklindeki davranış kuralları, mesela hırsızlık yapma, buradan da değerler ilkeler bu şekilde oluşur. İç denetim temelde bir kuruma değer katmak amacı ile o kurumun başta ilkeleri, prosedürleri, kurumsal yapısı ve her şeyden önce kontrol mekanizması, çünkü kontrol mekanizmasını iç denetim kontrol eder, ikisi birbirinden farklı müesseselerdir, kontrol mekanizmasının çalışıp çalışmadığını, kuruma değer katmak amacıyla sistematik bir şekilde incelemek olarak tanımlanır. Burada önemli kavramlardan bir tanesi değer

katmak, diğeri de sistematik inceleme. İç denetimin içinde güvenlikte var, siber güvenlik de çok önemli alanlardan bir tanesi, siber güvenlik de çok kaba bir tanım ile bir kurumun bilgi işleme ilişkin, bilgi güvenliğine ilişkin sistemlerini kontrol edilmesini, tehditlere karşı korunmasını sağlayacak bir sistem olarak tanımlayabilirim. Burada sızma testleri örnek verilebilir. Kritik bilgilerin korunmasına temelde siber güvenlik denilebilir. Bilgi teknolojileri güvenliği aslında, iç denetimin kontrol etmesi gereken alanlardan bir tanesi. Bilgi teknolojileri tarafında da denetim kısmı var, yeni gelişen bir alan, dolayısıyla çok bilinen bir alan olmadığı için denetlenmesi zor. Ancak, çok detayların bilinmesi de gerekmiyor, bilgi teknolojilerinde nelerin denetleneceğini bilmeniz yeterli olabilir. Benim kendi açımdan kontrol listem var, örneğin şifreler güvenli bir şekilde nerede saklanıyor, şimdi yedek alınıyor mu, bunların hepsi bilgi teknolojileri güvenliği ile ilgili kısımlar. Sonuçta, denetleyecek kişinin yedeklemenin nasıl yapıldığını bilmesi gerekmiyor, ama denetçinin şifre güvenliğinin sağlam olup olmadığını veya yedeklemenin yapılıp yapılmadığını bilmesi gerekir ya da firewall kullanılıyor mu. Kısaca, bilgi güvenliğini denetleyecek kişinin bu konularda çok uzman birisi olması gerekmiyor, yalnızca bu konularda doğru soruları sorması gerekiyor. Yani, önemli olan doğru soruların sorulmasıdır. Tabi bu aldığınız yanıtlarda sizi yanıltıyor olabilirler, bunları da kontrol etmek için bir takım teknik bilgilere de sahip olmak lazım. Aslında özetle, denetçiye bilgi işlem konusunda yetkinlik kazandırılabilir ya da bilgi işlem konusunda yetkin bir kişiye denetçi rolü verilebilir. İki yöntem de kullanılabilir, bana göre bir iç denetim ekibinde hem bilgi işlem konusuna vakıf iç denetçiler olmalı hem de iç denetim konusunu bilen bilgi işlem alanında uzman kişiler olmalıdır. Bilgi teknolojileri denetimi bir uzmanlık alanı ama dediğim gibi ille bilgi işlem konusunda uzman olmak gerekmiyor, siz bir denetçi olarak, denetçilik çünkü bir tekniktir, neyi, nasıl

denetleyeceğinizi sorular ile mantık ile kapsayabilirsiniz, uzmanlık gerektiren kısımlarda konunun uzmanına da gidebilirsiniz, ama genel çerçeve ile bilgi teknolojileri konusunda sorular ile alanı kapsamanız mümkün. Etik açıdan bakıldığında ise, örnek olarak denetim sırasında elde edilen bilgilerin gizliliğinin sağlanması, ya da bilgileri elde edilme yöntemleri etik sorunlara neden olabilir. Aslında, konu, iç denetimin etiği ve etiğin denetimi şeklinde iki kısma ayrılabilir. Daha sonra, etiğin siber güvenliği ve siber güvenliğin etiği, iç denetimin siber güvenliği kullanması ve siber güvenliğin iç denetimden yararlanması olarak incelenebilir. Ayrıca, bir de üç öğenin kesiştiği nokta var, yani burada hem etik hem siber güvenlik hem de iç denetim var. Genel teknik hep aynıdır, iç denetim siber güvenlik ile ilgili fonksiyonlarını gerçekleştirirken risk haritasını çıkartırsınız, risk konusunu belirlersiniz bunun olma olasılığını belirlersiniz ve bunun etkisini belirlersiniz. Örneğin sisteme oltalama saldırıları oluyor, bunun zararı ne kadar ya da bazı vakalar bir defa olur ancak etkisi çok büyük olur, bunlara kara kuğu riskleri de denir. Siber güvenlik açısından depremin olması çok nadir bir olaydır, olduğu zaman da çok büyük zarar görebilirsin, bu nedenle yedekleme ve bölge çeşitlendirmesi yapmak gereklidir. Her bir konu için risk haritası belirlenir, ondan sonra bunların testi yapılır.

Soru 6-Size göre, organizasyonunuzda, etik kurallar, iç denetimin siber güvenlik süreçlerinde üstlendiği rolü gerçekleştirirken takip ettiği yöntemler açısından nasıl tanımlanmaktadır?

Panelist 1-

Bu etik kurallara uyum konusunda bir de bizim teftiş kurulu başkanlığımızdan hariç, iç kontrol müdürlüğümüz var aslında bizim günlük olarak güvenlik tarafında yer alan fonksiyonlarımızda günlük, haftalık, aylık kontroller ile devamlı kontrol ediliyor zaten,

bunların tamamen aslında herhangi bir icrai faaliyette bulunmayan kişilerden oluşan organizasyon, bir sıkıntı olması halinde de bulgu olarak raporluyorlar, onlar da kendi raporlamalarını yönetim kurulu seviyesinde yapıyorlar.

Panelist 2-

Bir iç denetim ekibi, siber güvenlik ve bilgi güvenliği kapsamında faaliyetlerini sürdürürlerken, etik kurallara bağlı olmak zorunda, biz denetimler gerçekleştirilirken de raporlama aşamasında da yine bu etik kurallardan faydalanarak bir rapor oluşturulmakta, sonrasında siber güvenlik ekibi de bu konular ile alakalı o ekibe geri bildirim vermekte, bu işlemleri yaptık, bu konular hakkında çalışma sağladık, eksik olan noktaları belirledik şeklinde bilgilendirme yapılarak, tabi ki bu süreç, işletilirken her zaman etik kurallara bağlı olmak gerekiyor.

Panelist 3-

Denetçilerin aslına bakarsanız birçok faktöre bakma ve görme hakları vardır, ama banka tarafı gereksiz olan unsurların denetlenmesini engellemek için, bizim de güvenlik tarafında bazı unsurları denetlememiz kısıtlanmakta veya şu şekilde de açıklanabilir, bir denetime başladınız o denetim ile alakalı alanlara giriş yapmanız gerekti, bunların hepsinde belli süreler dahilinde operasyon yapabilirsiniz. Örneğin, bir denetimin süresi iki gündür veya üç gündür sadece süre kısıtları dahilinde denetimi gerçekleştirebilirsiniz. Siber güvenlik açısından, bizlere ekstradan sorumluluk yüklememek açısından kontrol noktaları organize edilmektedir. Yasalar çoğunlukla teknolojideki gelişmelerin arkasında kalıyor. BDDK'nın bilgi sistemleri üzerine oluşturduğu yönetmeliğin daha önceden tasarlanması ve icra edilmesi gerekmekteyken, bu yönetmelik ancak geçen sene yayınlanabildi. Bu durumlarda ne oluyor öncelikle size şu şekilde açıklayabilirim, her

denetime başladığınızda ilk olarak değişen ve gelişen sistemin araştırmasını yapıyorsunuz, yani neler değişmiş ve neler yapılabilir, bazı temeller bulunmakta, ancak bu temellerin üzerinde değişiklikler meydana gelmekte, yeni yazılımlar gelebiliyor, bu çerçevede tekrardan incelemeler ve araştırmalar yapılıyor, ilk başta denetim süreci bu şekilde başlamakta. Ondan sonra sisteme tekrardan yeni öğrenilen kavramlar üzerinden kontrollere başlanıyor. Sadece yasal mevzuat anlamında değil, yasalar sadece belli bir çerçeveyi çizebilir, yasaların temeline girilmesi gerekmektedir.

Panelist 4-

Şöyle, biz aslında, biraz daha proaktif olmaya çalışıyoruz bu konuda, siber güvenlik ile ilgili işlemleri denetlemeden önce, bilgi güvenliği ile alakalı denetlemeden önce, biz risk değerlendirme çalışmaları yapıyoruz bu risk değerlendirme çalışmasında da aslında bir kontrol öz değerlendirme yöntemi kullanıyoruz, bu kontrol öz değerlendirme yönteminde tüm üst düzey yöneticiler ile görüşülüyor ayrıca, GRC modülü var Archer GRC modülü, bunla da bir yöneticilere anket gönderiyoruz, bu anketlerde tüm paydaşlar bize risk değerlendirmesi öncesi bilgi sunuyor, bu bilgileri biz değerlendiriyoruz ve bu bilgileri değerlendirdikten sonra yapacağımız denetimleri, hangisine öncelik vereceğimizi mesela siber güvenlik olayı biz de hep riskli çıkıyor neden belli organizasyon yapımızın ya da bunla ilgili kontrollerin zayıf olduğu için değil, gelişmekte olan büyük bir alan olduğu için, biz organizasyon içerisinde buna öncelik veriyoruz, yüksek risk alanı olarak ifade ediyoruz bu kısmı, hem paydaşlardan bilgi alıyoruz, hem geçmiş denetim kanıtları hem bilgi sistemlerinin alt yapısını kullanarak, bu şekilde bir planlama gerçekleşiyor.

Panelist 5-

Aslında olması gereken bir süreç bir prosestir bu ve her kurum veya her altyapıya göre bu değişiklik gösterebilir, ancak biraz önce bahsetmiş olduğum çerçeve kapsamında, her ilgili ekip veya her ilgili birimin kendi görevler ayrılığı matrisine göre süreçlerin işletilmesi olması gereken ve sürecin de genel olarak tüm süreçlerin de ilerlemesi aşamasında olmazsa olmazdır veya zorunludur diyebiliriz. Tabi ki iyileştirme konusunda eksikler olabilir, bu her kurumda da vardır, bunlar da o sorunları görüp analiz edip, gerekli aksiyonları alıp bu etik kavramını daha da genişletip ve kontrollü bir şekilde denetlenebilir hale getirmektir.

Panelist 6-

Aslında biraz insan kaynakları (İK) biraz iç denetim tarafına sormak daha faydalı olabilir ama, şimdi bizim etik kurallarımızdan kastım politika ve prosedürlerimiz İK'nın hazırlamış olduğu etik kurallar ile ilgili dokümanlarımız. İç denetim de zaten bunlara uyulup uyulmadığı ile ilgili çalışmalar ve incelemeler yapıyor. Herhangi bir ihlal olayında da gidiyor kişiye özel soruşturma yapıyor ve dediğim gibi disiplin süreci buna göre işliyor. Yeterli mi değil mi derseniz eğer, ben bilgi güvenliği olarak baktığımda benim açımdan yeterli. Ama, yani dış dünyanın, siber güvenlik anlamında sağladığı her geçen gün arttığı, çalıştığım bankayı düşündüğümde, çalıştığım banka çok insancıl bir banka, hatta biz de insan kaynakları müdürlüğü değil insan kıymetleri müdürlüğü yer almakta. Orada belki, ilerleyen zamanlarda daha sert yaptırımlar yapılmakta fayda olabilir. Yani benim etik kurallarıma uymayan çalışanların, uymama durumunda, iç denetim ekiplerimin yaptığı incelemeler sonucunda yapması gereken çalışmalar belki işten çıkartmaya kadar gidebilecek şeyler olabilir diye düşünüyorum. Bu benim yorumum, ama. Ben yani hani, işten çıkarmak çok acımasız bir şey ama, yani etik kurallar birçok senaryoyu atlatıyorsa kişi, uymuyorsa, yapacak bir şey yok. Yani etik kurallar iç kontrol

için yeterli midir değil midir sorusu, yani tabi iç kontrolün buna cevap vermesi lazım ama, yeterli diyebiliriz. Takip edemiyor tam olarak çünkü kaynakları yok, benim şu anki zaman diliminde, bugün yaptığım bir toplantıyı örnek verecek olursam, iç denetçiler de bu dediğiniz çalışmayı yapacak BT gözüyle bakıyorum, süreç denetçisi gözüyle bakmıyorum, kaynak yetersiz olduğu için, sizin dediğiniz bu kadar kapsamlı bir çalışma maalesef yapılamıyor. Eksikler var. Kaynak olsa zaman olsa, konsantre olsalar belki daha çok yapacaklar. Birini yapıyorlar, diğerini bırakıyorlar. Benim BT denetçilerim şu anda, sizin demiş olduğunuz gibi bütünsellik şudur budur vesaire, bunu yapmaktan ziyade, BDDK'nın uy demiş olduğu COBIT yönetmelikleri ve yeni yayınlamış olduğu yönetmeliği uyumla ilgileniyor o uyumla da ilgilenirken siber güvenlik tarafında geliyor bana, o bütünsellik kısmında belki şey olabilir, benim zaman damgalı bir şekilde logları tutuyor olmam gerekiyor ya, kim ne zaman sisteme bağlanmış, kim ne zaman veri tabanına girerek veriyi değiştirmiş, bunları ben tutuyorum bilgi güvenliği olarak. Ya da işte, Ahmet kullanıcısı yetkili bir kullanıcı değilken, gitmiş bir sisteme bağlanmaya çalışmış, bunu da ben tutuyorum, burada benim tuttuklarımı kontrol ediyor. Ama dediğim gibi, bu böyle her gün iç denetçiler mükemmel denetimler yapıyor anlamında da değil. Düzenli ve yapabildikleri kadar yapıyorlar kaynak sıkıntısından dolayı. Bütçenin düzenlenmesi lazım, Türkiye'deki güvenlik alanındaki kaynakların hem denetçi kaynaklarının hem bilgi güvenliği kaynaklarının artması lazım, çok yeni bir alan, yani bu alanlar, eleman alındıktan sonra, elemanın içeride tutulması için tecrübesinin artması için gerekli iyileşmelerin yapılıyor olması lazım, yani mesela bir tane denetçiniz varsa BT süreç denetiminde bütün iş onun üzerine yüklendiyse, istenilen kalitede denetim yapılamayacaktır. Dolayısıyla, kaynak sayısı artmalı, kaynak sayısı arttıktan sonra, o kaynağın eğitimleri ile ilgili çalışmalar yapılmalı, kendini geliştirme kısmında, eğitim

aldırmalı, belki gelip denetleyeceği ekiplerin kullanmış olduğu uygulamalar ile yapmış olduğu çalışmaları gidip belki aylarca onların yanında durarak inceleyerek öğrenmeli. Sonra da bu çalışanlar olgunlaştıktan sonra, piyasa avantajından dolayı başka yerlere gitmemeli, işte daha iyi maaş daha iyi şart vesaire gibi, bankada kalmasına yönelik çalışmalar yapılmalı. Etikler yeterli mi diyorsunuz, evet etikler de sürekli bir döngü içerisinde ilgili paydaşlar ile birlikte konuşularak düzenlenmeli. Yani içerideki veri dışarı çıkmasın ve kötü niyetli kişiler bu veriye ulaşmasın, çalışanlar da rollerini ve sorumluluklarını bilsinler, bu farkındalıkta olsunlar, bankanın bütün bunları koruyacak bir etik kuralları diyorsunuz siz, ben biraz daha geniş açıyorum, etik deyince de işte bir firmayla çalışırken ahbabın olmasın hediye kabul etme gibi şeyler akla gelir ama, sizin anlatmaya çalıştığınız şey bizim politika ve prosedürlerimiz bilgiyi paylaşma, paylaşırken yetkiyi araştır gibi şeyler, bunların yeterli olması. Denetçi arkadaşların belki manuel kontroller değil de sistemsel kontrolleri daha çok yapıyor olması fayda sağlar.

Panelist 7- Aslına bakarsanız organizasyonumuzda etik kurallar tanımlanmıyor, yani eksik taraflardan bir tanesi de bu, çok sözlü bir şekilde tanımlanıyor ve de insanlar da zaten yapacakları denetçiler özellikle bankadaki en güvenilir kesim gibi görüldüğünden ve gerçekten de öyle olduğundan dolayı hani bu etik kuralların üzerinden tek tek geçmeye ihtiyaç duyulmamakta. Ama, yani biz tam olarak hangi şartlarda oluştuğunu bilmiyorum tabi ama yurtdışında insanlar bu sebeplerden işlerini kaybediyorlar. Yani yapmaması gereken bir sorgulamayı yaptığı için veya doğrudan işi ile alakalı olmadığı için fazladan bir satır olduğu için mesela işlerini kaybedebiliyorlar. Bu bağlamda, bu kadar kesin bir etik kurallar tanımı yok, bankada.

Panelist 8- Siber güvenlik ile ilgili aksiyon alınırken mesela bir bankanın siber güvenlik ile ilgili görevli birimleri aksiyon alırken mutlaka şey yapmalılar kişisel çıkarları göz ardı

etmeliler mesela burada siber güvenlik ile ilgili karar alacak olan iş birimleri ile mesela kurumun içinde IT'den sorumlu bir bölüm var, ekip var, yönetici var, iş birimleri var bir de siber güvenlik birimi var. Şimdi, her birimin aslında hedefleri farklı, siber güvenlik birimi istiyor ki bankanın, kurumun, şirketin ya da bilgileri çalınmasın, hacklenmeyelim, güvenli olalım ama diğer iş birimleri şunu istiyor, sürekli biz dışarıya açılalım, yeni müşteri alalım, hani onlarda şirketin para kazanması için birtakım aksiyonlar almak istiyorlar, yeni yeni kapılar açıyorlar belki dış dünyaya, dış internete bu karlılığı artırabilmek için şimdi burada karşılıklı bir çatışma oluyor aslında, yani diğer iş birimleri mümkün olduğunca farklı risk alırken, siber güvenlik tarafı da mümkün olduğunca riski azaltmaya çalışıyor, şimdi bu iki fonksiyon aynı kişiye bağlı olursa yani hem risk üstlenmek isteyen IT tarafı, iş birimleri, hem de riskleri bertaraf etmek isteyen bilgi güvenliği tarafı aynı kişiye bağlı olursa bir çıkar çatışması olur o zaman ilgili yönetici daha çok kar elde edebilmek için belki daha yüksek siber risklere maruz kalıp şirketin ileride siber güvenlik anlamında kötü bir şey gelmesine neden olabilir, bu yüzden, siber güvenlik birimlerinin de bağımsız, özerk yapıda olması lazım kurum içinde. Yani doğrudan, işte pazarlama, satış faaliyetlerini yürüten ekiplere bağlı değil, IT operasyonlarından sorumlu ekiplere bağlı değil de bağımsız olmalı etik olarak. Bunu söyleyebilirim.

Panelist 9- Bizde şimdi şöyle bir şey var, zaten bizde bilinmesi gereken diye bir prensip var, biz ona need to know diyoruz, bu görev tanımı dışında tanımlanmış yetkileri gösteren uygulamalarda da kullandığımız rol bazlı sistemimiz var. Zaten hiçbir personelin yetkisi olmayan bir role atanması söz konusu olmuyor, yetki verilirken onay alınması gerekiyor. Onun dışında yapılan zaten ne kadar işlem varsa bunların yolları mevcut ve bunlar devamlı gözden geçiriliyor. Eğer biraz önce bahsettiğim gibi yetkisi olmadığı halde

verilere erişmeye çalışan ya da bir şekilde anormal işler yapan varsa personelimiz bunlar ile ilgili etik olmadığı değerlendirildiğinden bunlarla ilgili inceleme başlatılıyor. Bunun içinde siber güvenlik de var, bütün banka personeli bir şube çalışanı da olsa siber güvenlikteki müdür de olsa yetkisini aşan aktivitenin içinde yer alıyorsa, Bankanın etik politikasına uygun olmayan faaliyetlerde bulunuyorsa zaten onları tespit edip teftiş kuruluna bildiriyoruz. Zaten teftiş kurulunun da yaptığı bu tür rutin denetimler var. Bir de teftiş kurulu iç denetim demektir.

Panelist 11- İçsel bir bilgi olduğu için net bir bilgi paylaşamamaktayım.

Panelist 14- Bir önceki soru cevabının içerisinde belirtilmiştir.

Soru 7- Kurumunuzda, siber güvenlik yönetiminde yer alan yasal çerçevenin ve uluslararası standartların gözetilmesi süreçlerinde iç denetim nasıl bir rol üstlenmektedir?

Panelist 1-

Mevzuat anlamında, yasal standart, içeride, Türkiye'deki düzenleyici kurumlar anlamında mevzuatı bilgi güvenliği müdürlüğü olarak biz takip etmekteyiz. İşte en son Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin yayınlamış olduğu bilgi güvenliği ve iletişim rehberi var, dediğim gibi BDDK'nın bankaların bilgi sistemleri ve elektronik bankacılık hizmetleri hakkında yönetmelik var, zaten bu yönetmelikler ilk çıktığı anda bize mevzuat ve uyum başkanlığımızdan gelmekte, biz oradaki kontrol noktalarını iş süreçlerimize yansıtmaya çalışıyoruz, denetim fonksiyonu açısından bakıldığında teftiş kurulu başkanlığımız da bu iç standartlara ve uluslararası mevzuatlardan baz alınarak oluşturulmuş olan kontrol listeleri üzerinden denetimlerini gerçekleştiriyorlar, denetimler sonucunda ortaya çıkan bulgular varsa da bunları yıllık olarak yönetim kuruluna raporluyorlar, altı aylık periyotta da izleme fonksiyonunu gerçekleştiriyorlar.

Panelist 2-

Hem ulusal hem de uluslararası anlamda siber güvenlik süreçlerinin değerlendirilmesi ile ilgili birçok kurum ve prosedür var, bunlara örnek olarak bahsetmem gerekirse, bankacılık sektörü için konuşacak olursam, sonuçta çalıştığımız kurum bir banka ve katılım bankası, BDDK'nın süreçlerine tabi olan bir banka, BDDK'nın bankalar ile ilgili yayınlamış olduğu yönetmelik var, bu yönetmelik genelde, yıldan yıla veya çeşitli dönemlerde güncellenebiliyor, bizim bu yönetmeliğe tümü ile uymamız gerekiyor banka olarak aksi takdirde BDDK'nın çok ciddi yaptırımları var kurumlara, çok ciddi cezaları var, özellikle bu yıl itibari ile herhangi bir bulgu tespit ederse BDDK bankaların siber güvenlik açıkları ile ilgili, çok ciddi cezai yaptırımlar uygulayabiliyor, sonrasında şöyle bir şey belirteyim, bir de uluslararası anlamda bilgi güvenliği ekibinin ve iç denetimin sorumlu olduğu süreçler var, örneğin COBIT süreci, PSIDSS dediğimiz, ISO 27001 dediğimiz bilgi güvenliğini çerçeveleyen kural kümeleri var, bunlar gibi birçok politika ve prosedür yer almakta bunlara tüm bankalar ve finansal kuruluşlar uymak zorunda olduğu regülasyonlar, bu şekilde açıklanabilir.

Panelist 3-

Uluslararası standartları karşılamazsanız eğer bankaların beraber çalıştığı birçok uluslararası bankalar ve finansal kuruluşlar mevcut ve hepsi sizden o yeterliliği bekliyor sonuçta, bu sebeple de bunu sağlamak açısından dikkatli olmanız gerekiyor, ISACA tarafından oluşturulan COBIT çerçevesinin otuz dört ayrı kriteri var, bu kriterlerin her biri ayrı ayrı denetlenmekte, ITIL ve ISO 27001 çerçevelerine göre de sistemin denetlenmesi gerekebiliyor. Ayrıca, biraz önce bahsettiğim gibi bunların haricinde, bizim ayrı denetimlerimiz de bulunmakta, sistem bazında gerçekleştirilen, aktif dizin denetimi ayrı yapılmakta, mesajlaşma sistemi denetimi ayrı yapılmakta, bunlarla beraber sızma

testleri yapılmakta ve ayrıca güvenlik açıklarının tespit edilmesi için de denetimler icra edilmektedir. DS5 açısından ayrı ve bilgi teknolojileri açısından ayrı olmak üzere yapılan denetimlerimiz mevcut. Bizim yıl içerisinde denetimlerimiz gerçekleşir, bilgi güvenliği ile alakalı olarak ve diğer bankacılık süreçleri ile ilgili olarak, bunların haricinde tekrardan gözden geçirme sürecimiz bulunmakta, tekrar süreç ve bulgular kontrol edilir, düzeltmelerin yapılıp yapılmadığı, düzeltmelerin hangi aşamalarda olduğu, bulgunun kritikliğine göre alınan aksiyonlar, bunlar tekrar kontrol edilir, tekrar birimler ile görüşülür, tekrar cevaplar istenir, bütün bunların sonunda da üst yönetime ve yönetim kuruluna raporlama işlemi yapılır. Yönetim kuruluna raporlamamız yetmiyor bizim için bankalar tarafında, ayrıca bağımsız denetçilerimiz oluyor, bağımsız denetçiler ile öncelikle kendi denetimlerini yapıyorlar hem bankacılık süreçleri hem bilgi sistemleri tarafında, kendi denetimlerini yaptıktan sonra, bizim yapmış olduğumuz denetimlerin kontrollerini yapıyorlar ve ayrıca BDDK murakıpları tarafından da banka gözden geçiriliyor diyebilirim, son olarak bütün bu denetim bulguları yönetim beyanı olarak BDDK'ya sunulmakta. Önceden de bahsettiğim gibi, risk matrislerimizde risklerin derecelendirilmesi yapılır, ikinci olarak da sadece bizim gözetimimiz altında değil banka, bağımsız denetçiler de ayrı denetimler gerçekleştirmekte, bu sebeple kendinize göre bizim sistemimiz çok iyi bizim sistemimiz mükemmel diyemezsiniz hiçbir şekilde çünkü, bağımsız bir gözetim de yapılmakta, bu sebeple elinizden geldiğince o sistemin en iyisini ortaya koymak zorundasınız, zaten bankacılık sektörü çok riskli bir sektördür, yani dediğim gibi parayla oynadığı için, çok katı da bir sektördür, bu konuda kesinlikle affı da yoktur böyle şeylerde, ister istemez zaten belli bir düzeyin üstünde denetim sağlamak zorundasınız, çalıştığım banka Türkiye'nin en büyük bankası, en köklü de bankası, öyle

olunca yılların da bir deneyimi var burada yani sade birden oluşan bir sistem değil, hepsi aşama aşama kaydedilerek gelinen sistemler.

Panelist 4-

Swift denetiminden bahsetmiştim size, mesela bu swiftin bir şeyi var, swift kurumunun getirmiş olduğu müşteri güvenliği ile ilgili bir çerçeve var, mesela biz bunu duyduğumuzda ya da bununla ilgili bir aksiyon alınması gerektiğinde iç denetim olarak hemen aksiyon alıyoruz, bunun öncelikle bir eğitimi alındı, sonra swiftin çerçevesi alınıyor, bunun hemen bir anda kontrol noktalarını oluşturup denetimine başlıyoruz, yine uluslararası çerçeveler anlamında, biz COBIT standartlarına yönelik denetim yapıyorduk, şimdi COBIT standartlarını yine bir kenarda da tutuyoruz, çünkü bilgi sistemleri yönetmeliği ile birlikte yeni maddeler geldi, COBIT 4.1 ile denetimlerin yapılması istenmekteydi, BDDK bu şekilde belirtmekteydi, ancak şimdi yeni maddelere göre otuz adet, eskiden otuz dört COBIT alanıydı şimdi otuz alana inmiş oldu, biz şunu yaptık, COBIT standartları ile BDDK yönetmeliklerini de eşleştirdik, böylelikle bütünleşik bir denetim ortaya çıkardık, hem standartlar ile iç içeyiz hem de BDDK'nın kurallarını kabul ediyoruz, böyle bir uyum aşaması yaptık, bunu denetim planımıza entegre ettik, akabinde de yine bu yönetmelik kavramını, yönetmelik içerisinde denetçilerimiz CISA sahibi bizim neredeyse tüm denetçilerimiz on tane bilgi sistemleri denetçisi var hepsi uluslararası sertifika sahibi, biz zaten yıllık eğitim planlarını düzenleyip onlara eğitimler verdiriyorduk şimdi yönetmelikte üç yılda bir yüz yirmi saat geldi, hani bu tür olaylar bizi etkilemedi çünkü uluslararası standartlar nezdinde zaten kurmuştuk sistemimizi, bu yönde de devam ediyoruz.

Panelist 5-

Toplantının başında da belirttiğim üzere, biz banka olarak öncelikle BDDK regülasyonlarına tabiyiz ek olarak aynı şekilde ISO 27001 kapsamında sertifikasyonumuz olduğu için ISO 27001 kapsamına da dahiliz, aynı zamanda COBIT DS5 maddesindeki altyapı operasyonlarının işletilmesi maddesine de tabiyiz, bir bağımsız denetim veya iç denetimler, siber güvenlik veya bilgi güvenliğini denetlediği esnada bu kabul görmüş kontroller üzerinden bizi denetlemektedir. BDDK'nın bankalar birliği kapsamında var olan regülasyonları ve maddeler kapsamında bağımsız firmalar gelip bizi denetlemektedirler. Tabi olduğumuz genel olarak Türkiye'deki bankaları örnek verecek olursak, BDDK'nın regülasyonlarıdır, ek olarak da ISO 27001 kapsamı veya COBIT'in DS5 maddesindeki kontrol noktasını adresleyebiliriz. Buna ek olarak da, teknik olarak da biraz daha detaylı bilgi vermem gerekirse, biz teknik olarak, her alanın global olarak da kabul görmüş platformlarından beslenmek zorundayız, örneğin bir güvenlik testi, penetrasyon testi yapıldığı zaman Open Web Application Security Project (OWASP) Top 10 üzerindeki kontrolleri uygulamak gerekir, bu aynı zamanda SysAdmin, Audit, Network and Security (SANS) veya diğer global olarak kabul görmüş kontrol listelerini uygulamamız gerekiyor ki gerçekten yapılan test hem küresel olarak hem de ulusal olarak da kabul görebilsin. Bir de aynı zamanda log tarafında da küçük bir örnek verecek olursak, bunların mesela bizim hali hazırda Security Incident and Event Management (SIEM) tarafında regülasyonlar kapsamında çalışmaları yürütüyoruz ancak teknik olarak bazı aksiyonların veya bazı kural korelasyonlarının bazı standartlar çerçevesine veya regülasyonlara tabi tutulmasında büyük fayda vardır, çünkü bunu adresleyip, referans gösterebilmek için bunlar çok önem arz etmekte. Örnek verecek olursak SIEM tarafı için, Mitre Attack çerçevesi mevcuttur, orada belirlenen bir çerçeve vardır, bunu global olarak da tüm bankalar veya tüm kurum kuruluşlar bu tür çerçevelerden beslenerek kendi

altyapısını daha güvenli ve güçlü hale getirirler. SIEM aslında log management değildir, log management kısmı sadece logların yönetildiği kısım. SIEM ise sadece log management olarak kabul edilemez, çünkü orada analizlerin yapıldığı, loglarla eşleştirildiği, pars edildiği ve onlarla birden fazla yerde eşleştirme yaparak, kural korelasyonlarının oluşturulduğu bir yapıdır. Örneğin, bir sunucu üzerinde herhangi bir yazılım ulaştığı anda, ben bu zararlı yazılımın kaynağını bulup, bütün banka altyapısında loglarına bakarak bununla ilgili bir isim eşleşmesi olduğu zaman analiz üret, bunun tespitini yap veya örneğin bir sunucuda beşten fazla yanlış deneme olduğu zaman bunun alarmını üret ve bunda brute force attack gibi olaylar gibi değerlendirilebilen çok büyük bir mekanizmadır. Ben şahsen bir bilgi güvenliği uzmanı olarak da SIEM log management denmesine karşıyım, çünkü SIEM çok büyük bir dünyadır, log management onun sadece küçük bir parçasıdır, aslında birleşenlerinden biridir. IBM Q Radar, Splunk ve Microfocus R side en çok bilinen SIEM ürünleridir. Ulusal Siber Olaylara Müdahele Ekibi var, burada tüm bankalar ile ilgili bilgileri toplayıp aslında bilgi toplamak değil de örneğin şimdi siz bir bankasınız, siz bir banka olarak kendi kapsamınızda analiz yapıyorsunuz, siber istihbarat platformlarından besleniyoruz, ve bunlar için gerekli aksiyonları alıyorsunuz, ancak USOM, SOME dediğimiz taraf ise birçok bankanın entegre olduğu bir yer, USOM tarafının bir uygulama aracı bir platform vardır, o platform üzerinde de gerekli bildirimleri yapabiliyorsunuz ve gerçekten de onlar gerekli durumlarda hızlı bir şekilde aksiyon alıyorlar, şöyle daha rasyonel bir ifade verebilirsem, örneğin size bir oltalama saldırısı olduğu zaman siz o oltalama saldırılarının gelen mail adreslerinin Türkiye'de veya globalde engellenmesini istiyorsunuz, var olan kendi hizmet aldığınız platformlarda da bunu engellemeye çalışıyorsunuz ama ek olarak da Siber İstihbarat Platformu (SİP) dediğimiz bir ara platform var oraya kullanıcı bilgilerinizle

giriyorsunuz, USOM'a diyorsunuz ki böyle bir oltalama yapıldı benim bankamda bankamın domain adresi var, lütfen bunu kaldırın diye, USOM'da bu şekilde aksiyonlar alıyor. Tabi, bu süreç pandemiden dolayı bayağı geride durdu, pandemiden önceki durumlarda yılda iki veya üç defa toplantı oluyordu ama, bu toplantıların ben şahsen o toplantılarda bunu izah etmiştim, bu toplantıların daha sık olması gerekiyor ve gerçekten bilgi alışverişinde bulunulması gerekiyor. Şöyle bir şey oluyor, örneğin herhangi bir bankada zafiyet oluyor veya bilgisayar korsanlığı durumu oluyor, tabi doğal olarak da USOM'a bildirilmiyor hem prestij hem de diğer çekincelerden dolayı, bu tür bildirimlerde hemen hemen tüm bankalar biraz daha geri planda duruyor, kendi içinde çözmeye çalışıyorlar bu gibi durumları, tabi kimse istemez böyle durumların olmasını, bu konu ile kendi görüşüm ise, USOM ve bankalar arasındaki bu ilişkinin daha sıkı ve sürekli olması gerekiyor. Bu bağlamda, banka, USOM ve Bilgi Teknolojileri İletişim Kurumu (BTK) tarafının daha güçlü olması gerekiyor.

Panelist 6-

İç denetim COBIT 4.1'e uyum kapsamında denetim çalışmaları yapıyor, çünkü BDDK bizim COBIT 4.1'e uymamızı istiyor, COBIT 4.1'de uluslararası bir standart, biliyorsunuzdur belki bir çerçeve, COBIT 5 çıktı, COBIT 2019 çıktı ama BDDK hala bize bankalara COBIT 4.1'e uyacaksın diyor. IT'nin süreçlerinin oluşturulması ve kontrol edilmesi için oluşturulmuş olan bir standart, iç kontrol ekiplerimiz bizi COBIT 4.1'e göre her sene denetliyorlar. COBIT 4.1'in otuz dört tane süreci var, en az on yedi tane yirmi tane süreci mutlaka iç kontrolcüler denetliyor ve burada bulgu yazıp, bulgular ile ilgili aksiyonları takip ediyorlar onun dışında bizim bankamız ISO 27001 sertifikası var, iç kontrol ekibindeki arkadaşlar ISO 27001 kapsamında da kontroller yapıyorlar, bir de

BDDK'nın yönetmelikleri var, iç kontroldeki arkadaşlar BDDK yönetmeliklerine uyum kapsamında da çalışmalar yapıyorlar.

Panelist 7-

Dediğim gibi daha evvelden de konuştuğumuz gibi, burada gözetim süreci dediğimiz şey, var olan adımların iş adımlarının siber güvenlik ile alakalı atılması gereken iş adımlarının ve bu adımların nasıl kontrol edildiğinin uluslararası kurallara Türkiye mevzuatına ve kurum kültürüne uyumu ile alakalı bir çalışma, denetim yapmak oluyor ve bu bağlamda da biz herhangi bir şey olursa tabi belli bir seviyenin üzerinde çok küçük şeyler bazen göz ardı edilebiliyor ama, belli bir seviyenin üzerinde bir kontrol eksikliği varsa yapılan işte bunları raporlamak, yönetim kuruluna raporlamak şeklinde bir gözetim yapıyoruz ve iç denetim aslına bakarsanız tüm altyapıya hakim durumda tüm altyapı ile alakalı denetimleri her sene belli bir düzeyde yerine getiriyor diyeyim burada hani IT müfettişlerinin iş tanımlarının birazcık sadece IT ile alakalı olmaması söz konusu olduğu için biraz işgücü kaybı var orada ama, genellikle tüm BDDK isteklerini yapmaya çalışıyoruz ve bu kapsamda da gözetim fonksiyonu dediğimiz şey tüm yapılan denetimlerdeki eksiklikleri yönetim kuruluna raporlamak şeklinde gerçekleşiyor. Bizzat zaten, ISO 27001, ISO 22301 yani iş sürekliliği, sistem sürekliliği, bilgi güvenliği ve COBIT, NIST gibi referanslar olsun bunların bizzat kontrollerini ilgili denetim gerçekleşiyorsa eğer ilgili müfettiş yapıyor, denetim tarafı yapıyor ve direkt olarak gözetimi biz yapmış oluyoruz, yani hangi müfettiş oraya gittiyse o konu ile alakalı alınan kararların ve yapılan uygulamanın uluslararası kurallara uygunluğunu Türkiye'deki mevzuata uygunluğunu bizzat biz gözetliyoruz, bu anlamda bu işin tek mercii de IT müfettişliği gözetim anlamındaki tek mercii IT müfettişleri oluyor bizim yaptığımız rapor da direk olarak yönetim kuruluna sunulduğu için çok etkili oluyor o bakımdan yani hani

herhangi bir şubede yaptığınız rapor yönetim kurulu tarafından direk olarak bakılmıyor, sadece tüm raporlar birden faaliyet kapsamında onların önüne sunuluyor yönetim kurulunun önüne şubelerde yapılan üç aylık çalışmalar geliyor, ama siz gidip firewall denetiminde bir şey bulduysanız direkt olarak yönetim kurulunun önüne sunuluyor bu yüzden de siber güvenlik ile alakalı gözetim bizzat bizim tarafımızdan bizim kanalımızda yönetim kuruluna aktarılmış oluyor. Bizde bir iç kontrol var bir müfettiş var, müfettiş iç denetçi oluyor, iç kontrol BDDK kavramları kapsamında, müfettiş gibi farklı bir birim oluyor. Dediğim gibi, belli bir temeli var bu işin, çünkü özellikle IT müfettişlerinin konumlandırılması yani süreç teftişi denilen şey, bizde süreç teftişi ile IT müfettişi sanki aynı şeymiş gibi algılanmış, onun için 2007'den beri on dört yıldır süreç müfettişi olarak adlandırılıyoruz biz ben 2015'ten beri buradayım ama, daha evvelinde de o şekildeymiş, süreç müfettişi eşittir IT müfettişi diye bakıyorlar, birincisi bu yanlış ama bankada süreç teftişleri her zaman herhangi bir şube denetiminin daha üstünde olmuştur ve de buradaki süreç teftişinde direk olarak birimler ile kurulan iletişim olsun kendi genel müdür yardımcımız da teftiş kurulu başkanı ve yönetim kurulu ile kurulan ilişki doğru çalışıyor bankada. Aslına bakarsanız konumlandırma doğru yani oradaki mekanizma doğru tanımlanmış ben diğer bankalarda bunun özel bankalarda özellikle daha da güçlü olduğunu düşünüyorum. Genel olarak BDDK'nın kurmaya çalıştığı bu fonksiyon yerinde yani böyle birtakım müfettişlerin olması gidip bizzat IT denetimi ve siber güvenlik ile alakalı kontrolleri yerinde yapmaları ve bununla alakalı raporlarını direk olarak yönetim kuruluna sunabilmeleri tam olarak bence olması gerektiği gibi tanımlanmış ve de diğer iç denetçiler de zaten sizin varlığınızı biliyor ekiple beraber çalışıyorsanız karma yani entegre bir denetim yapıyorsanız birbirinize dediğim gibi yani. Diyelim ki kurumsal krediler ile alakalı bir denetim yapılıyor siz altyapı ile alakalı sorgulamalar yapıyorsunuz

IT müfettişi olarak diğer iç denetçiler de süreç ile alakalı kontrol eksikliklerine bakıyor, burada tanımlanmış bir temel var ama her zaman bankada doğru işliyor mu o noktada da işte IT müfettişinin sadece IT'ye odaklanması süreç müfettişinin veya idari müfettişin ise sürece odaklanması ve bu ikisinin işlerini ayrı ayrı yaparak sonucu beraber raporlamaları daha doğru bir yöntem olurdu, bankada anlaşılmayan şey bu oluyor yani IT'nin süreçten ayrılması gerektiğini bir yerde yapılan iş bakımından, rapor olarak olmasa da yapılan iş bakımından ayrılması gerektiğini anlamaları lazım tabi hangi bankada bu şekilde ise eksik ise bu şekilde anlaşılması lazım ki IT müfettişleri kendi bilgi birikimlerini de hem geliştirebilsinler hem de tam olarak ilgili alanda siber güvenlik alanında denetimlere daha iyi odaklanabilsinler. Bilgi teknolojileri müfettişleri sadece siber güvenliğe odaklı bir denetim yapıyorlarsa siber güvenlik konularından bir tanesi ile alakalı bir denetim yapıyorlarsa zaten diğer bankacılık süreçlerine hiç karışmıyorlar bu yüzden yaptıkları tek şey kendi birikimlerini ve bilgilerini tek bir alanda işlemek oluyor yani siber güvenlik alanında artık hangi siber güvenlik alanı ise o bu alanda çalışmak oluyor ve bu bağlamda da bizim yazdığımız şey direk olarak ilgili mekanizma tarafından tanınıyor ve doğru şekilde doğru kanalla doğru yere ulaşıyor o konudan tamamen belki Türkiye'de en iyi yapan bankalardan bir tanesidir. Devlet bankası olmasından dolayı bulgunun doğru makama iletilmesi hususunda çok hassas davranılmaktadır. Konu ile alakalı şey hiçbir zaman kişisel algılanmaz mesela bir bulgu veya yapılan bir şey herkes o şeyin çözülmesine yardımcı olmaya çalışır ve de bu raporlandığı zaman da bu yönetim kurulu tarafından da bilinir yani muhakkak ki yönetim kuruluna sunulur, bu mekanizmanın doğru çalıştığını düşünebiliriz. Ama buradaki eksik dediğim gibi siber güvenlik ve IT konuları ile alakalı yeterli denetimin yapılmamasında, bence bana kalırsa, bankada bu konu ile alakalı yeterli denetim yapılmıyor, eksik bir tek burada yani. Yoksa, mekanizma

konusunda her şey BDDK'nın kurmaya çalıştığı gibi ve uluslararası kurallara da uygun bir şekilde işliyor. Diğer bankalar için konuşacak olursak, bazı özel bankalarda bu dediğim gibi daha da güçlü bir şekilde çalışır ama çalışmayan banka bu şekilde yapılmayan banka ve sadece BDDK böyle bir şey istemiş biz de geçiştirelim bir denetim yapalım diyen banka muhakkak vardır yani elli beş tane banka var onların içlerinden muhakkak bu işi tamamen basit bir oyun gibi yapan bir banka çıkacaktır muhakkak ki. BDDK'nın sizin yaptığınız raporlamalar üzerindeki incelemesi daha iyi olabilir ve daha sık olabilir veya daha detaylı olabilir. Ama ben buna dair yazdığım raporun daha böyle kapsamlı olmasına dair bir eleştiri almadım, BDDK bu noktada belki biraz daha kurduğu sistemi daha iyi denetliyor olsa belki daha faydalı bir sonuç alınabilir. Bu bağlamda BDDK'nın yaptığı şeyin birazcık daha yüzeysel olduğunu düşünüyorum. Diğer bankalarda mesela çok detaylı sızma testçisi gibi müfettişler denetim raporlarını yazarken bizim bankamızda vaktinin yüzde otuzunu ayırmakta. Bizim açımızdan IT tarafında diğer birkaç banka ile aramızda çok fark var çünkü dediğim gibi onlar sadece IT tarafına odaklanıyor biz ise IT müfettişi olarak sadece IT'ye odaklanmıyoruz birden çok iş yapıyoruz bu da tabii doğal olarak yıllar içerisinde birikimli olarak bir fark oluşturuyor, yani yetişen müfettiş ve denetim kapasitesi dediğinizde onlarda daha detaylı olarak sızma testi yapabilecek uzmanlar yetiştirilirken bizde daha yüzeysel ama bankacılıktan daha iyi uzmanlar yetişmiş oluyor. Bunu özel sektör ve devlet bankası şeklinde ayırmak doğru mu bilmiyorum, ben sadece kendi deneyimlerimle yani özel sektörün birkaç büyük bankasından bahsediyorum, yani diğer bazı bankalarda buraya göre IT alanında daha çok niteliğe sahip müfettişler yetiştirilmek isteniyor yani politikaları bu şekilde. Bazı bankalarda özellikle söylüyorum biz sızma testçisi yetiştirmek istiyoruz diye çıkıyorlar yola yani genel politikaları bu şekilde. Bu bankanın politikası ise biz müfettiş dediğin

müfettiştir, müfettiş her alanda her işi yapar, mantığı var, ben şahsen şube denetimine de gidiyorum dediğim gibi soruşturmaya da gidiyorum süreç denetimine de gidiyorum, kalan vaktimde IT denetçiliği de yapıyorum, şimdi bu ikisi böyle bir kurumla diğer ben sadece sızma testlerini yetiştiriyorum diyen kurum arasında bir birikim farkı oluşuyor. O adam beş sene boyunca sürekli sistem güvenliği olsun işte Certified Ethical Hacking, OSCP vesaire falan bunlarla alakalı hem sertifikalar almaya çalışıyor hem de bunlarla alakalı kavramlar ile uğraşıyor sürekli, biz ise bankacılık ile ilgili kavramlar ile uğraşıyoruz, uğraştık şu zamana kadar daha ziyade, temel fark aramızdaki fark bu. Ama zaten CISA bu işin temeli bankadaki BDDK'nın vakti zamanında getirdiği şey CISA sertifikasının alınmasıydı. CISA sertifikası da bunların arasındaki alınması en kolay sertifikadır yani öyle söyleyeyim. Hiçbir zorluğu yoktur tamamen para tuzağı diye de adlandırabilirim yani bunu bana eğer samimi görüşümü sorarsanız, bir insan birazcık o konu ile alakalı çalışsın, CISA'yı alır muhakkak yani, illa bunun için dört sene beş sene onların belirttiği kadar IT alanında çalışmak lazım falan filan diye bir şey yok, biraz aşina olun konulara birazcık da sorularını çözün yaparsınız yani herkes yapar. Bunun için mühendis olmaya da gerek yok, bunun için IT denetimi alanında çalışmış olmaya da gerek yok, he muhakkak çalışmalarınız size katkı sağlıyor yani sürekli o COBIT'teki o kontrol noktalarına bakıp bir takım denetimler yapmaya çalıştığınız için CISA sertifikasını almak daha kolay oluyor tabii ki, ama ben o kadar da zor bir sınav olduğunu düşünmüyorum ama Certified Ethical Hacking, OCSP gibi sertifikalar daha uzman sertifikalardır, mesela belirttiğim bankalarda bunların alınması için belli bir çaba sarf ettiriliyor insanlara ama bu bankada ve diğer devlet bankalarında gördüğüm kadarı ile bu yok. İlk on banka içerisinde devlet bankaları ve özel bankaları ayırıp böyle bir genelleme yapabiliriz, evet, özel bankalarda uzmanlık daha çok ön plana çıkarılmak isteniyor, kişilerin, devlet

bankalarında ise özellikle denetim kademesi için denetçi her şeyden anlasın gibi bir mantık güdülüyor.

Panelist 8-

İç denetim birimleri zaten kontrol çerçeveleri, hem yasal çerçeveyi, siber güvenlik ile ilgili kontrolleri tamamı ile esas alıyoruz ve oradaki kontrol hedeflerine banka uygun faaliyet gösteriyor mu göstermiyor mu oradaki işte siber güvenlik kontrollerini uyguluyorlar mı uygulamıyorlar mı tamamen zaten bunları esas alıyoruz ayrıca BDDK'nın da çizdiği bilgi güvenliği ile ilgili kontroller var düzenlemelerinde onları da esas alıyoruz, hepsi iç denetim, iç kontrol fonksiyonlarının kapsamında olan konular.

Panelist 9-

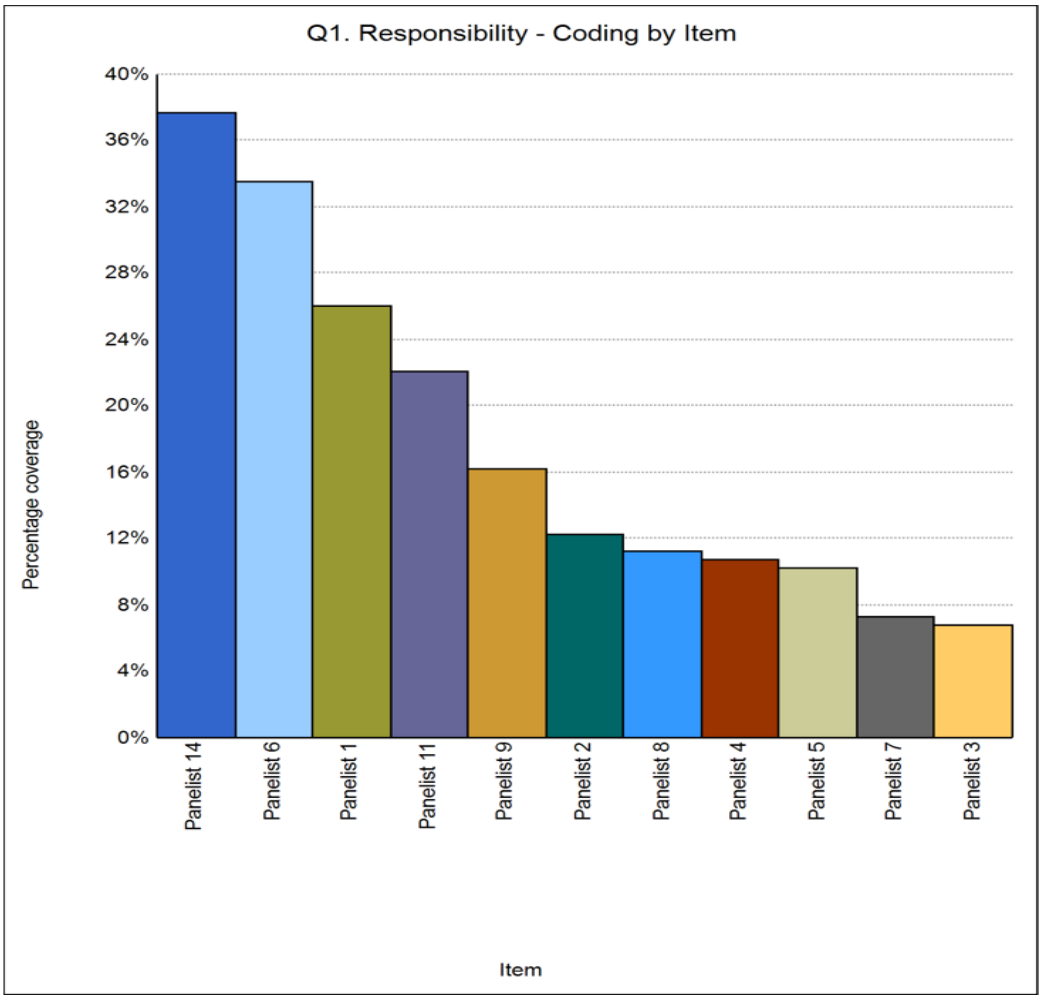
Biraz önce söylediğim gibi işte bizim tabi olduğumuz mevzuatlara göre yapıyorlar denetimlerini ve kontrollerini. Biz banka olarak, BDDK'nın 5411 sayılı bankacılık kanununa tabiyiz, bilgi sistemleri olarak da yeni yayınlanan bankacılık süreçleri ve elektronik bankacılık yönetmeliğine biz tabiyiz. Yapılan denetimlerde zaten mevzuatlardaki kontrollerin varlığı ve etkinliği değerlendiriliyor iç denetim tarafında. Varsa yetkin olmayan ya da hiç olmayan kontrol varsa o majör yazılıyor, var olan bir kontrol yeterince etkin değil ise de gerekli yönlendirmeler yapılıyor. Onun dışında yurt dışı ortaklığımız var bizim, bizim Dubai Emirates'te hissedarımız ve siber güvenlik ile ilgili bir standart var. Biz oradaki kontrol listelerini de banka bünyesinde yapıyoruz.

Panelist 11- İç denetim bağımsız bir gözle süreçlerin işletilip işletilmediği ile ilgili kontrol ve takibi gibi bir rolü bulunmaktadır.

Panelist 14- Türkiye'de bankacılık sektörünün bilişim sistemleri güvenliği hususu bankacılık işlemleriyle sıkı sıkıya ilişkili bir şekilde düzenlenmiş olup, hizmeti alan vatandaşların güvenliğinin sağlanması, bankacılık sektörünün gerek banka bazında gerek sektörel olarak güvenirliliğini artırıcı olması da amaçlanarak oluşturulmuştur. Bununla birlikte, bankacılık sektöründeki siber güvenlik çalışmaları kapsamlı bir şekilde uluslararası uygulamaları da göz önünde bulundurarak ve daha da önemlisi ülkemiz ekosistemine uygun olarak geliştirilmiş mevzuat, yöntem ve uygulamalarla güncelliği sağlanmaktadır.

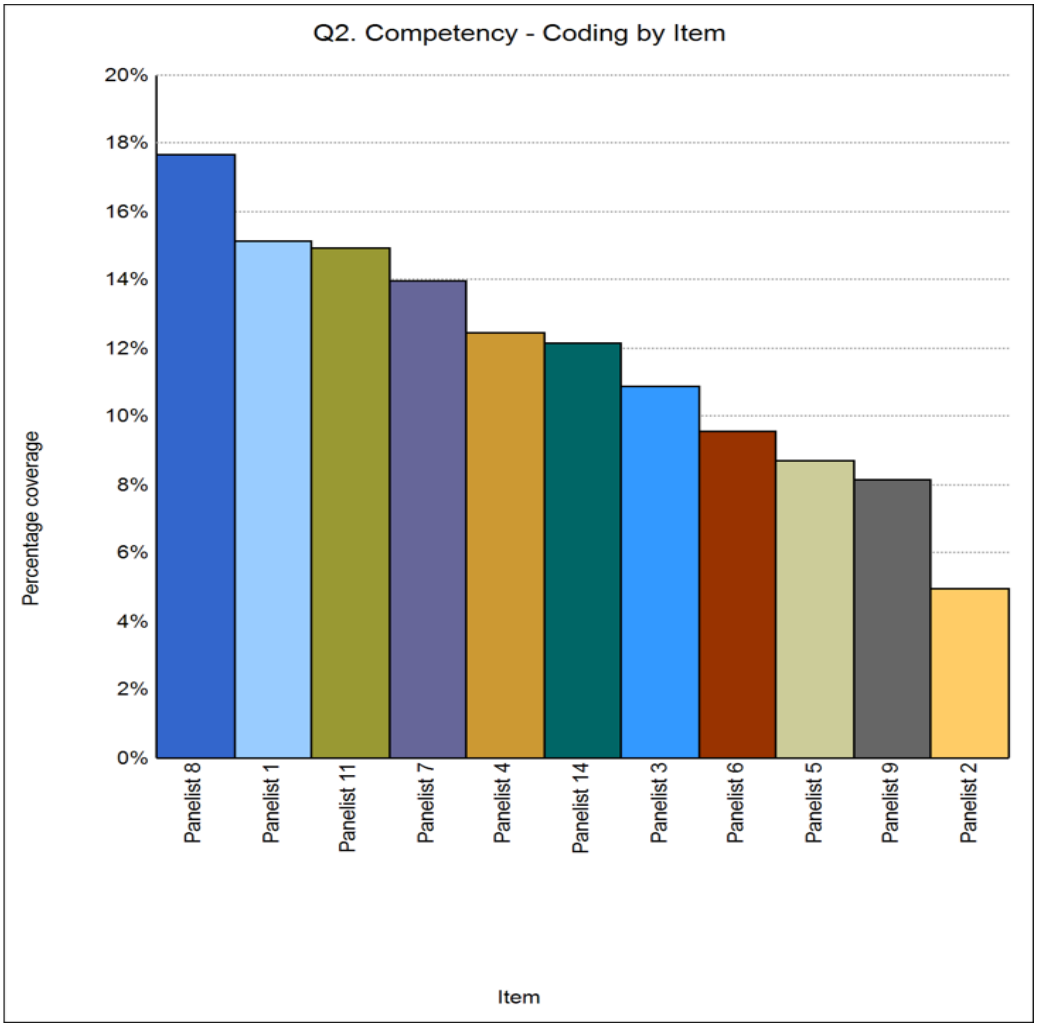
Appendix-7.Gauges of the Panelist Responses for the First Round of Delphi in Nvivo

- Which processes do internal auditors take responsibility for in your organization within the cyber security services?



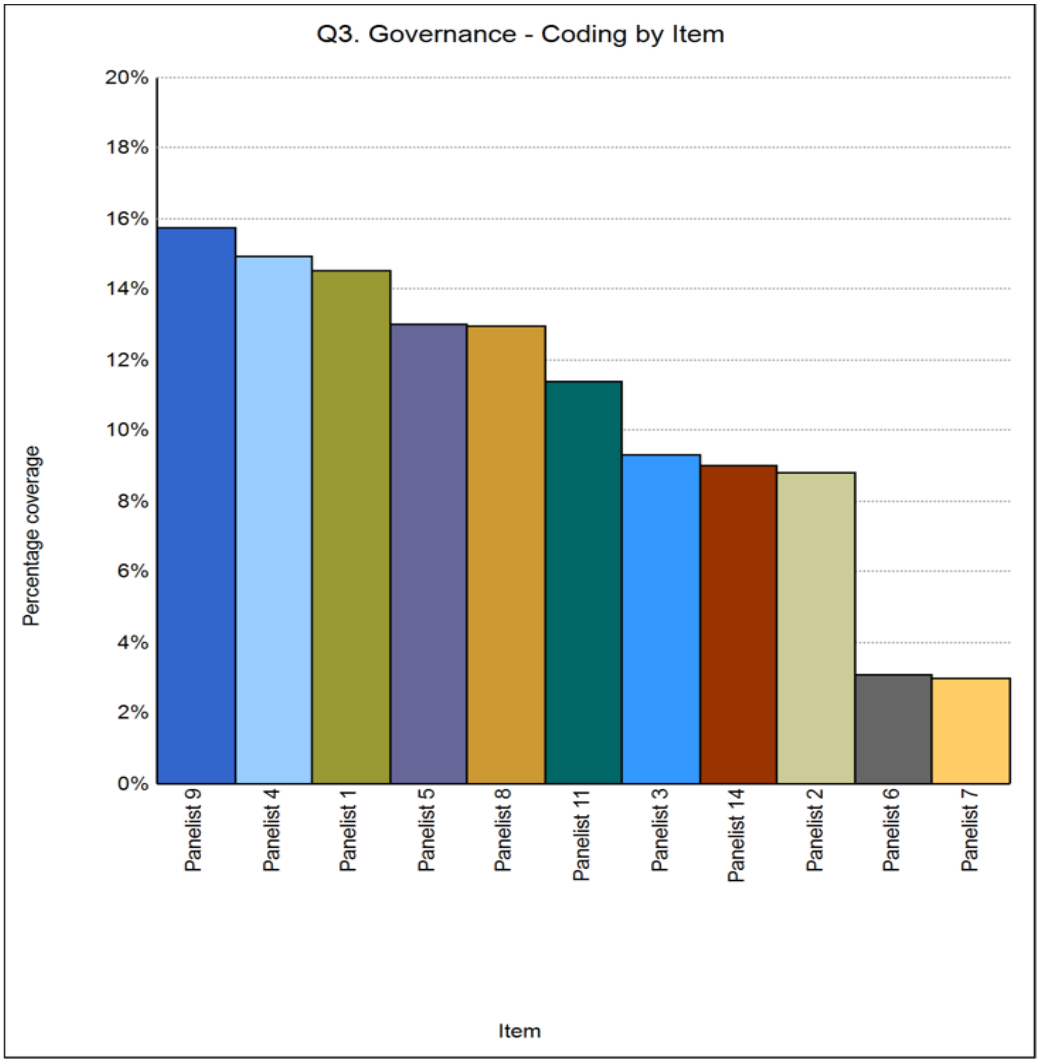
Type	Name	In Folder	References	Coverage
Document	Panelist 1	Files\\Semi Structured Interviews Textual Data	1	26,05%
Document	Panelist 11	Files\\Semi Structured Interviews Textual Data	1	22,12%
Document	Panelist 14	Files\\Semi Structured Interviews Textual Data	1	37,70%
Document	Panelist 2	Files\\Semi Structured Interviews Textual Data	1	12,27%
Document	Panelist 3	Files\\Semi Structured Interviews Textual Data	1	6,76%
Document	Panelist 4	Files\\Semi Structured Interviews Textual Data	1	10,73%
Document	Panelist 5	Files\\Semi Structured Interviews Textual Data	1	10,26%
Document	Panelist 6	Files\\Semi Structured Interviews Textual Data	1	33,57%
Document	Panelist 7	Files\\Semi Structured Interviews Textual Data	1	7,31%
Document	Panelist 8	Files\\Semi Structured Interviews Textual Data	1	11,20%
Document	Panelist 9	Files\\Semi Structured Interviews Textual Data	1	16,22%

- How do you explain the competency of internal audit functions which are being conducted as part of cyber security?



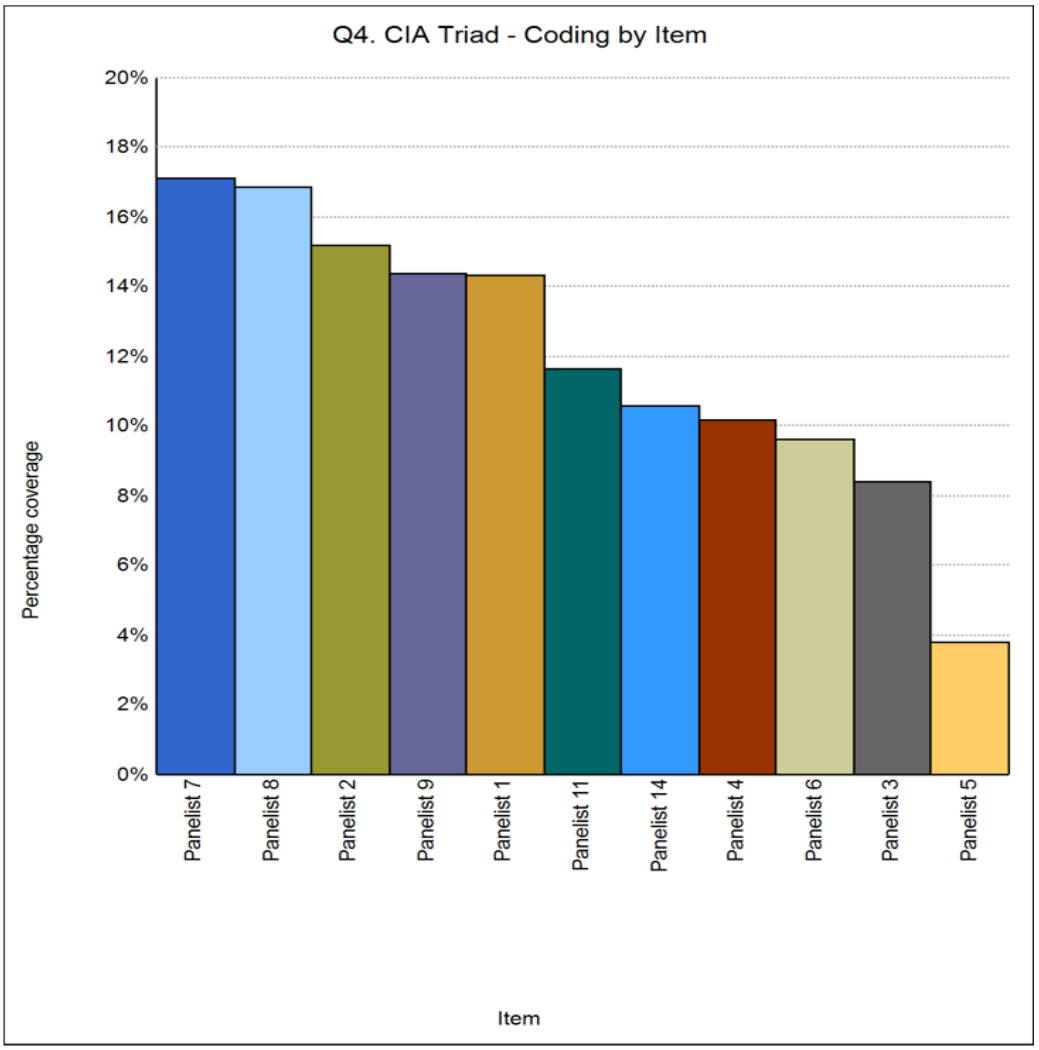
Type	Name	In Folder	References	Coverage
Document	Panelist 1	Files\\Semi Structured Interviews Textual Data	1	15,15%
Document	Panelist 11	Files\\Semi Structured Interviews Textual Data	1	14,92%
Document	Panelist 14	Files\\Semi Structured Interviews Textual Data	1	12,15%
Document	Panelist 2	Files\\Semi Structured Interviews Textual Data	1	4,95%
Document	Panelist 3	Files\\Semi Structured Interviews Textual Data	1	10,90%
Document	Panelist 4	Files\\Semi Structured Interviews Textual Data	1	12,47%
Document	Panelist 5	Files\\Semi Structured Interviews Textual Data	1	8,69%
Document	Panelist 6	Files\\Semi Structured Interviews Textual Data	1	9,59%
Document	Panelist 7	Files\\Semi Structured Interviews Textual Data	1	13,98%
Document	Panelist 8	Files\\Semi Structured Interviews Textual Data	1	17,68%
Document	Panelist 9	Files\\Semi Structured Interviews Textual Data	1	8,14%

- How is the interaction mechanism between internal audit and management board formed for the issues which are related to cyber security?



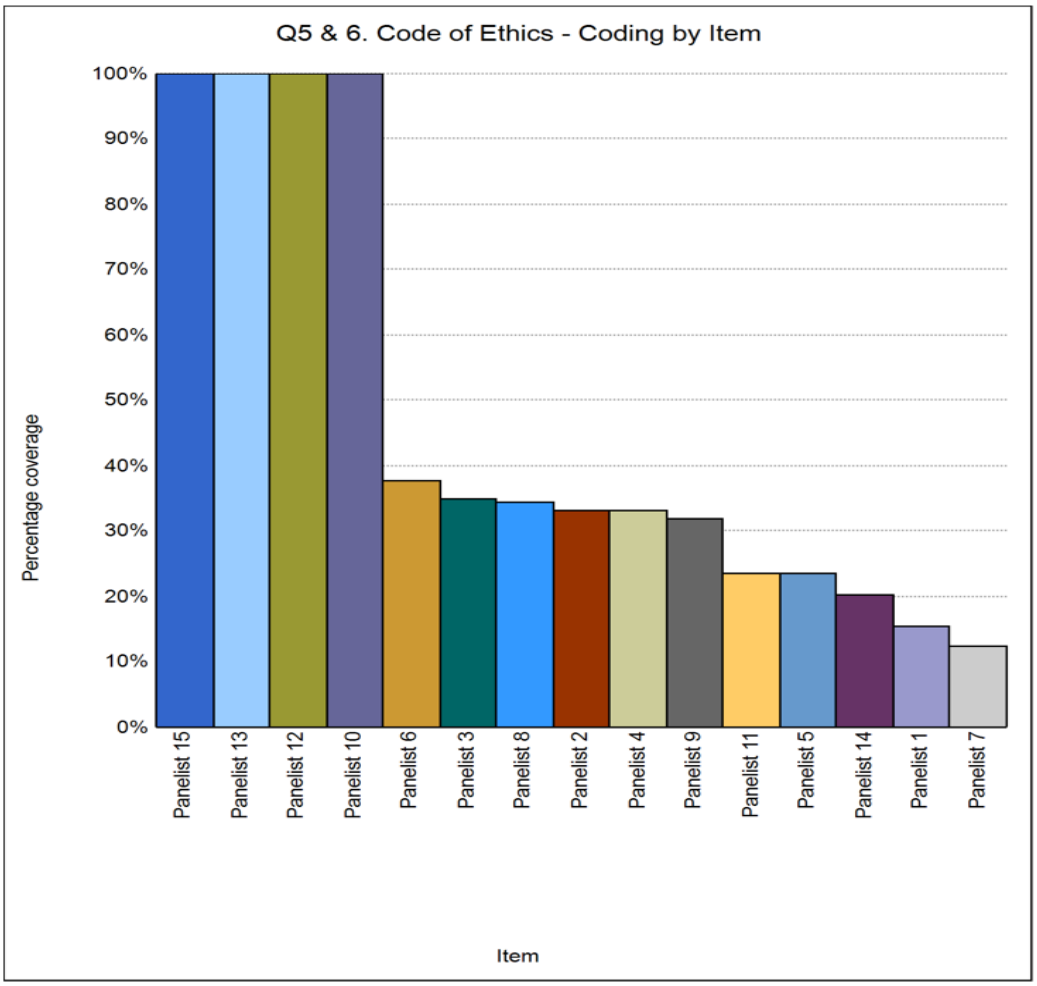
Type	Name	In Folder	References	Coverage
Document	Panelist 1	Files\\Semi Structured Interviews Textual Data	1	14,51%
Document	Panelist 11	Files\\Semi Structured Interviews Textual Data	1	11,37%
Document	Panelist 14	Files\\Semi Structured Interviews Textual Data	1	9,02%
Document	Panelist 2	Files\\Semi Structured Interviews Textual Data	1	8,83%
Document	Panelist 3	Files\\Semi Structured Interviews Textual Data	1	9,31%
Document	Panelist 4	Files\\Semi Structured Interviews Textual Data	1	14,96%
Document	Panelist 5	Files\\Semi Structured Interviews Textual Data	1	13,03%
Document	Panelist 6	Files\\Semi Structured Interviews Textual Data	1	3,08%
Document	Panelist 7	Files\\Semi Structured Interviews Textual Data	1	2,98%
Document	Panelist 8	Files\\Semi Structured Interviews Textual Data	1	12,94%
Document	Panelist 9	Files\\Semi Structured Interviews Textual Data	1	15,77%

- How do the confidentiality, integrity, and availability concepts remind you within the context of your organization?



Type	Name	In Folder	References	Coverage
Document	Panelist 1	Files\\Semi Structured Interviews Textual Data	1	14,34%
Document	Panelist 11	Files\\Semi Structured Interviews Textual Data	1	11,67%
Document	Panelist 14	Files\\Semi Structured Interviews Textual Data	1	10,60%
Document	Panelist 2	Files\\Semi Structured Interviews Textual Data	1	15,17%
Document	Panelist 3	Files\\Semi Structured Interviews Textual Data	1	8,39%
Document	Panelist 4	Files\\Semi Structured Interviews Textual Data	1	10,19%
Document	Panelist 5	Files\\Semi Structured Interviews Textual Data	1	3,80%
Document	Panelist 6	Files\\Semi Structured Interviews Textual Data	1	9,62%
Document	Panelist 7	Files\\Semi Structured Interviews Textual Data	1	17,12%
Document	Panelist 8	Files\\Semi Structured Interviews Textual Data	1	16,87%
Document	Panelist 9	Files\\Semi Structured Interviews Textual Data	1	14,38%

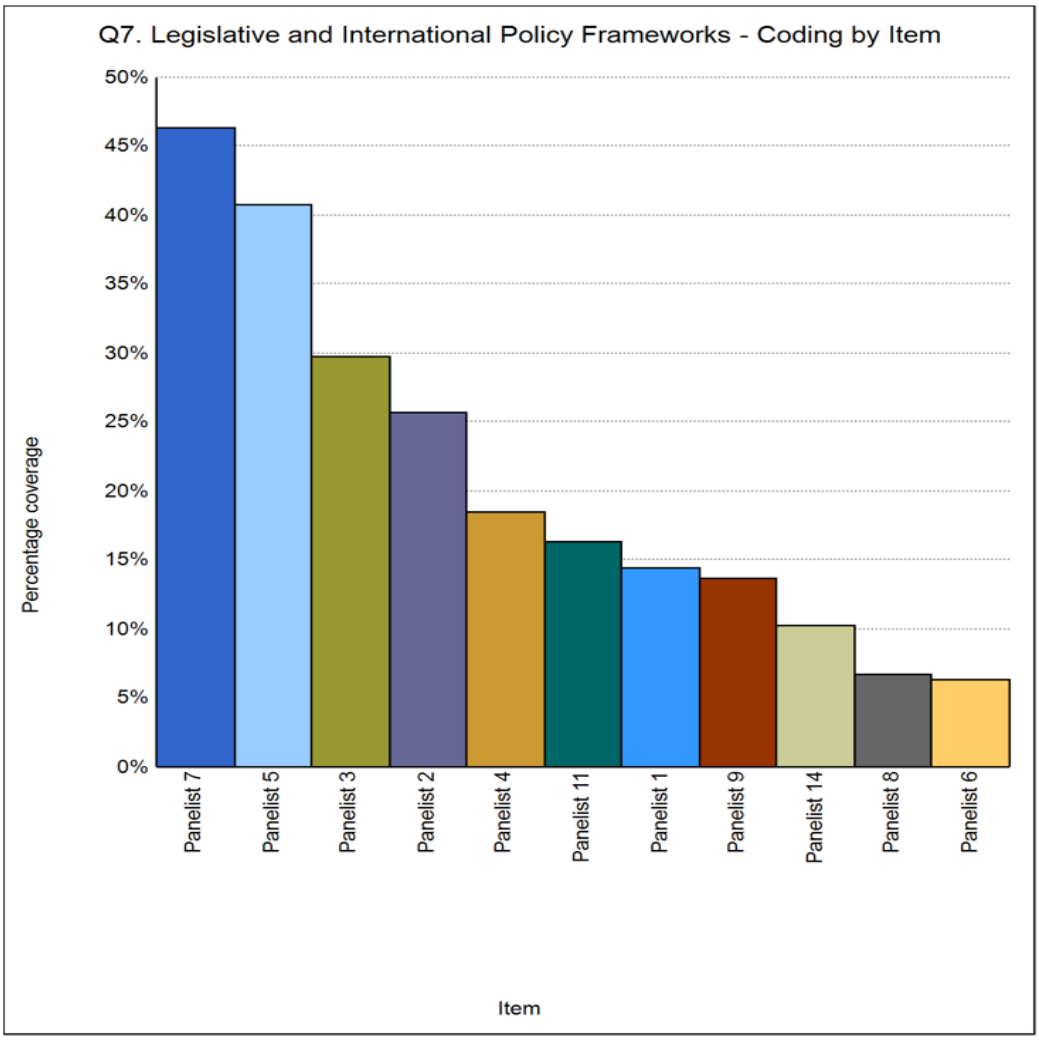
- What does the code of ethics recall you of when the internal audit and cyber security principles are discussed simultaneously?
- How are the ethical rules defined inside your organization, in terms of the methodologies which are tracked by the internal auditors for performing the role of internal audit in cyber security processes?



Type	Name	In Folder	References	Coverage
Document	Panelist 1	Files\\Semi Structured Interviews Textual Data	1	15,54%
Document	Panelist 10	Files\\Semi Structured Interviews Textual Data	1	100,00%
Document	Panelist 11	Files\\Semi Structured Interviews Textual Data	1	23,56%
Document	Panelist 12	Files\\Semi Structured Interviews Textual Data	1	100,00%
Document	Panelist 13	Files\\Semi Structured Interviews Textual Data	1	100,00%
Document	Panelist 14	Files\\Semi Structured Interviews Textual Data	1	20,29%
Document	Panelist 15	Files\\Semi Structured Interviews Textual Data	1	100,00%
Document	Panelist 2	Files\\Semi Structured Interviews Textual Data	1	33,14%
Document	Panelist 3	Files\\Semi Structured Interviews Textual Data	1	34,86%
Document	Panelist 4	Files\\Semi Structured Interviews Textual Data	1	33,11%
Document	Panelist 5	Files\\Semi Structured Interviews Textual Data	1	23,47%

Document	Panelist 6	Files\\Semi Structured Interviews Textual Data	1	37,77%
Document	Panelist 7	Files\\Semi Structured Interviews Textual Data	1	12,32%
Document	Panelist 8	Files\\Semi Structured Interviews Textual Data	1	34,55%
Document	Panelist 9	Files\\Semi Structured Interviews Textual Data	1	31,78%

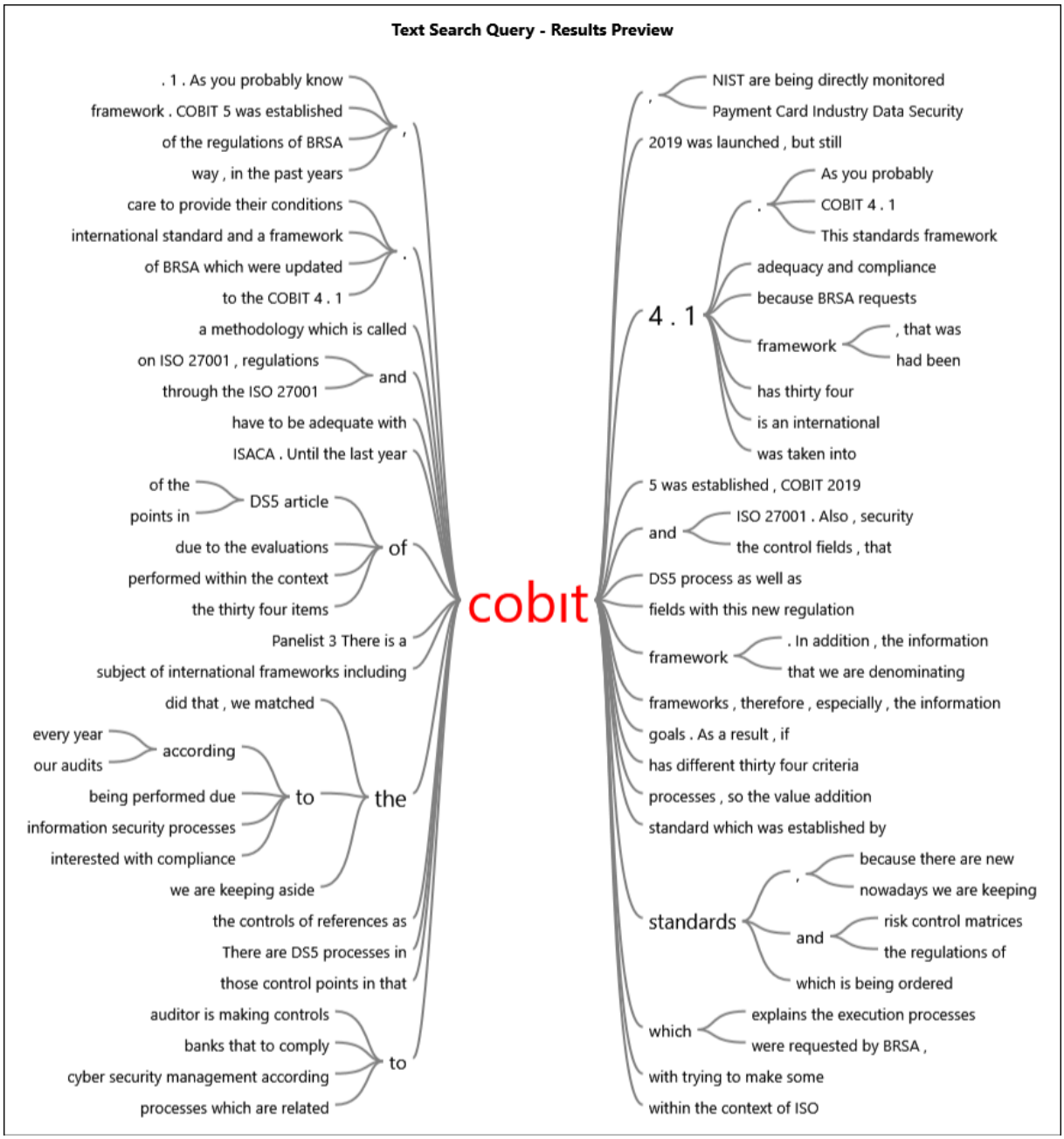
- How does the internal audit take part in cyber security management relative to the monitoring activities of the legislative framework and international standards?

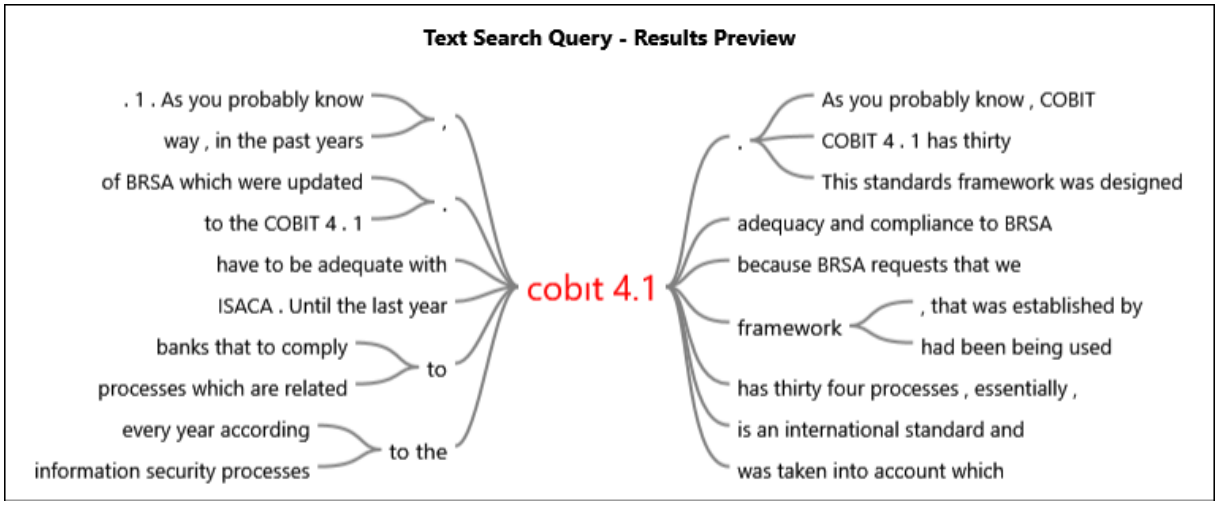


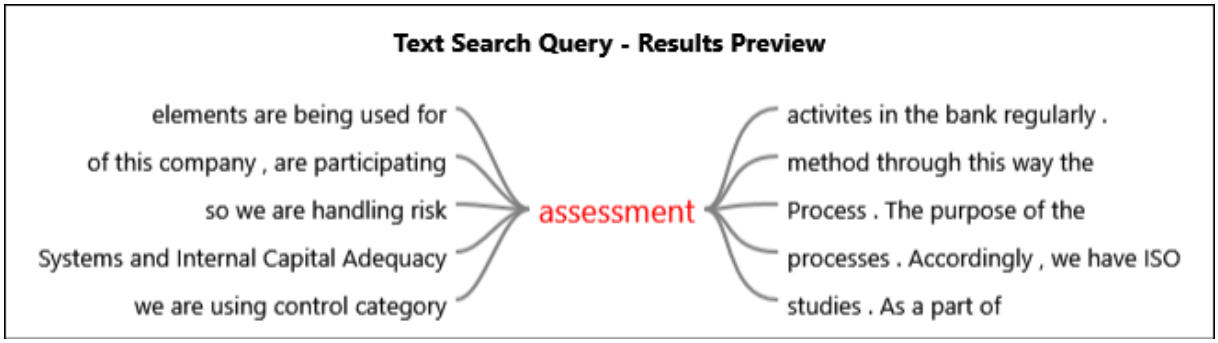
Type	Name	In Folder	References	Coverage
Document	Panelist 1	Files\\Semi Structured Interviews Textual Data	1	14,41%
Document	Panelist 11	Files\\Semi Structured Interviews Textual Data	1	16,36%
Document	Panelist 14	Files\\Semi Structured Interviews Textual Data	1	10,24%
Document	Panelist 2	Files\\Semi Structured Interviews Textual Data	1	25,64%
Document	Panelist 3	Files\\Semi Structured Interviews Textual Data	1	29,78%
Document	Panelist 4	Files\\Semi Structured Interviews Textual Data	1	18,54%
Document	Panelist 5	Files\\Semi Structured Interviews Textual Data	1	40,75%
Document	Panelist 6	Files\\Semi Structured Interviews Textual Data	1	6,38%

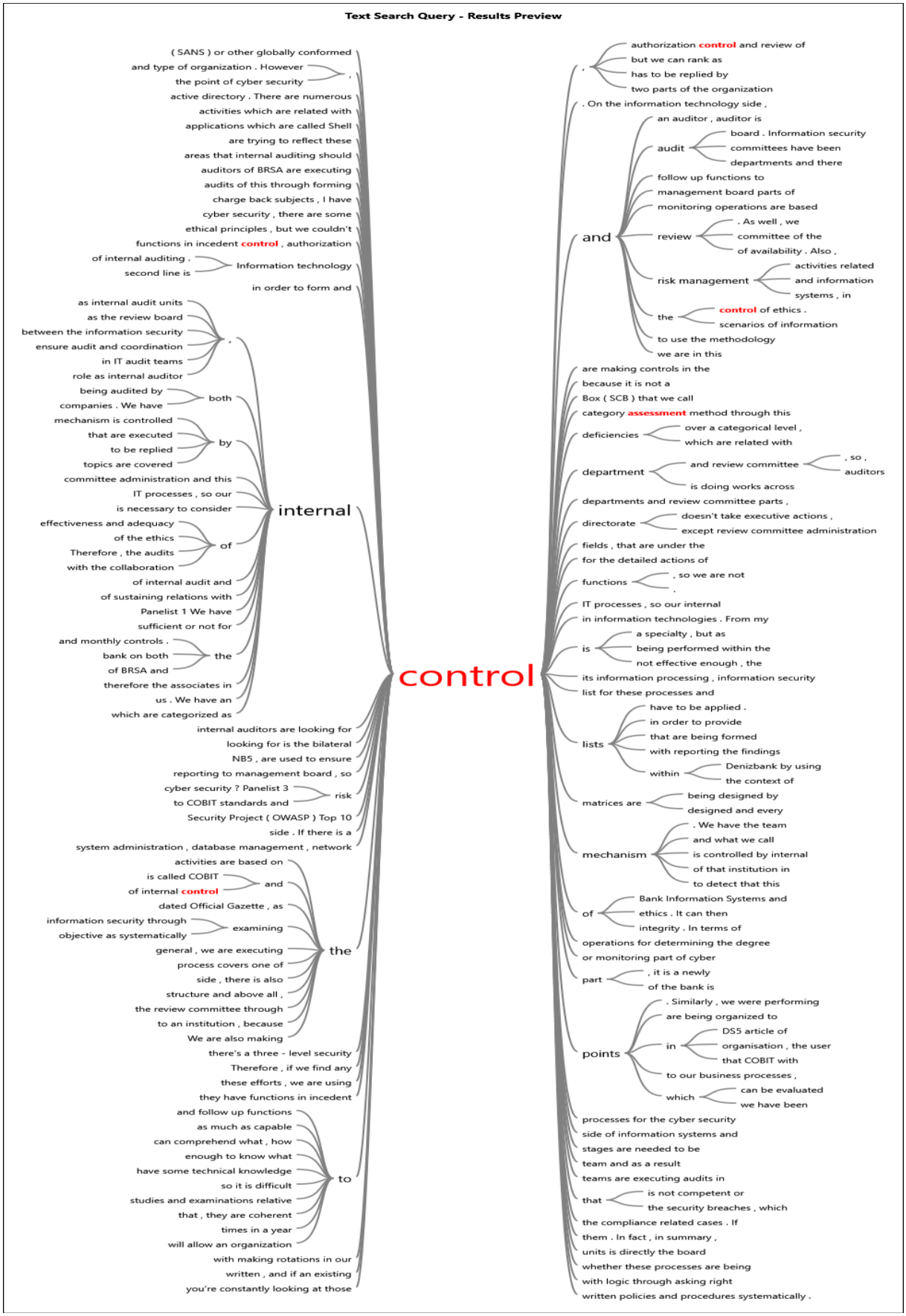
Document	Panelist 7	Files\\Semi Structured Interviews Textual Data	1	46,29%
Document	Panelist 8	Files\\Semi Structured Interviews Textual Data	1	6,76%
Document	Panelist 9	Files\\Semi Structured Interviews Textual Data	1	13,72%

Appendix-8.Text Search Query Results




Text Search Query - Results Preview
. 1 . As you probably know
way , in the past years
,
of BRSA which were updated
to the COBIT 4 . 1
.
have to be adequate with
ISACA . Until the last year
banks that to comply
processes which are related
to
every year according
information security processes
to the
cobit 4.1
.
As you probably know , COBIT
COBIT 4 . 1 has thirty
This standards framework was designed
adequacy and compliance to BRSA
because BRSA requests that we
framework
, that was established by
had been being used
has thirty four processes , essentially ,
is an international standard and
was taken into account which

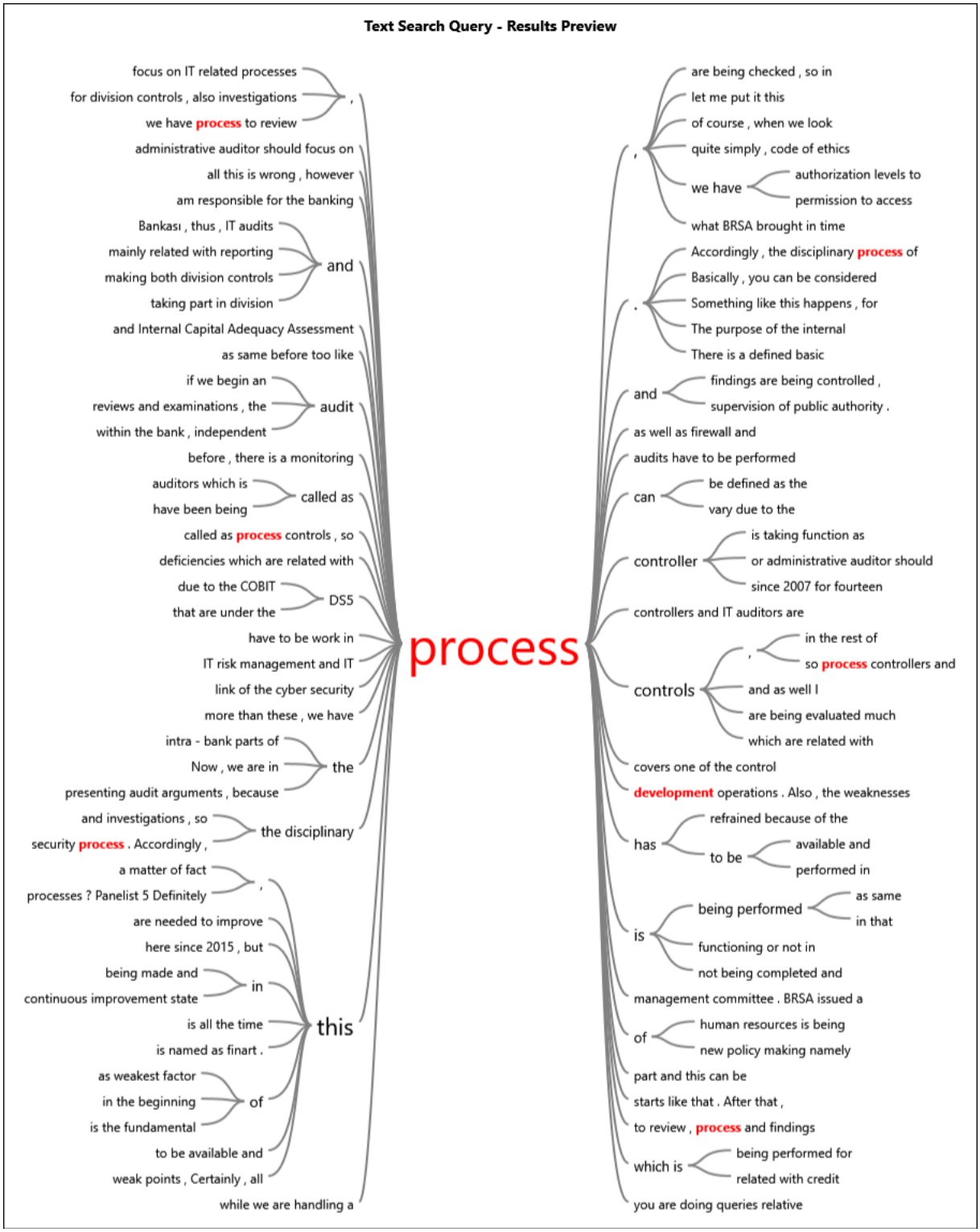

Text Search Query - Results Preview
elements are being used for
of this company , are participating
so we are handling risk
Systems and Internal Capital Adequacy
we are using control category
assessment
activites in the bank regularly .
method through this way the
Process . The purpose of the
processes . Accordingly , we have ISO
studies . As a part of

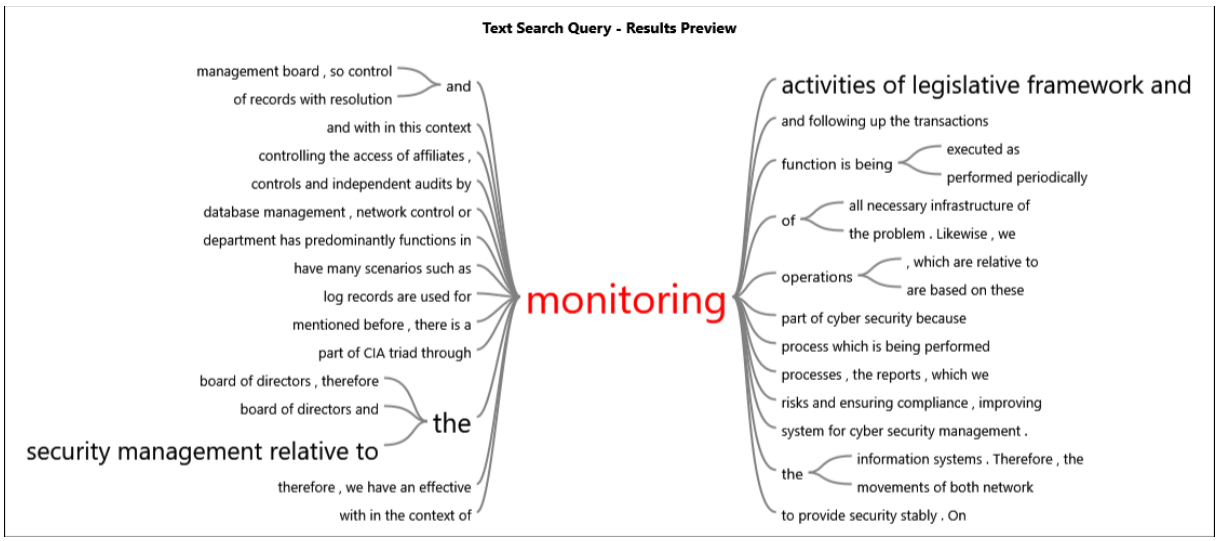

Text Search Query - Results Preview
control
internal
(SANS) or other globally conformed
and type of organization . However
the point of cyber security
active directory . There are numerous
activities which are related with
applications which are called Shell
are trying to reflect these
areas that internal auditing should
auditors of BRSA are executing
audits of this through forming
charge back subjects , I have
cyber security , there are some
ethical principles , but we couldn't
functions in incedent control , authorization
of internal auditing .
second line is
Information technology
in order to form and
as internal audit units
as the review board
between the information security
ensure audit and coordination
in IT audit teams
role as internal auditor
being audited by
companies . We have
both
mechanism is controlled
that are executed
to be replied
topics are covered
by
committee administration and this
IT processes , so our
is necessary to consider
effectiveness and adequacy
of the ethics
Therefore , the audits
with the collaboration
of
of internal audit and
of sustaining relations with
Panelist 1 We have
sufficient or not for
and monthly controls .
bank on both
of BRSA and
the
therefore the associates in
us . We have an
which are categorized as
internal auditors are looking for
looking for is the bilateral
NB5 , are used to ensure
reporting to management board , so
cyber security ? Panelist 3
to COBIT standards and
risk
Security Project (OWASP) Top 10
side . If there is a
system administration , database management , network
activities are based on
is called COBIT
of internal control
and
dated Official Gazette , as
information security through
objective as systematically
examining
general , we are executing
process covers one of
side , there is also
structure and above all ,
the review committee through
to an institution , because
We are also making
the
there's a three - level security
Therefore , if we find any
these efforts , we are using
they have functions in incedent
and follow up functions
as much as capable
can comprehend what , how
enough to know what
have some technical knowledge
so it is difficult
studies and examinations relative
that , they are coherent
times in a year
will allow an organization
to
with making rotations in our
written , and if an existing
you're constantly looking at those
authorization control and review of
but we can rank as
has to be replied by
two parts of the organization
. On the information technology side ,
an auditor , auditor is
board . Information security
audit
committees have been
departments and there
follow up functions to
management board parts of
monitoring operations are based
. As well , we
review
committee of the
of availability . Also ,
activities related
risk management
and information
systems , in
control of ethics .
the
scenarios of information
to use the methodology
we are in this
and
are making controls in the
because it is not a
Box (SCB) that we call
category assessment method through this
deficiencies
over a categorical level ,
which are related with
, so ,
department
and review committee
auditors
is doing works across
departments and review committee parts ,
directorate
doesn't take executive actions ,
except review committee administration
fields , that are under the
for the detailed actions of
functions
, so we are not
.
IT processes , so our internal
in information technologies . From my
a specialty , but as
is
being performed within the
not effective enough , the
its information processing , information security
list for these processes and
have to be applied .
in order to provide
that are being formed
lists
with reporting the findings
Denizbank by using
within
the context of
matrices are
being designed by
designed and every
. We have the team
and what we call
mechanism
is controlled by internal
of that institution in
to detect that this
Bank Information Systems and
of
ethics . It can then
integrity . In terms of
operations for determining the degree
or monitoring part of cyber
, it is a newly
part
of the bank is
. Similarly , we were performing
are being organized to
DS5 article of
in
organisation , the user
that COBIT with
points
to our business processes ,
can be evaluated
which
we have been
processes for the cyber security
side of information systems and
stages are needed to be
team and as a result
teams are executing audits in
is not competent or
that
the security breaches , which
the compliance related cases . If
them . In fact , in summary ,
units is directly the board
whether these processes are being
with logic through asking right
written policies and procedures systematically .

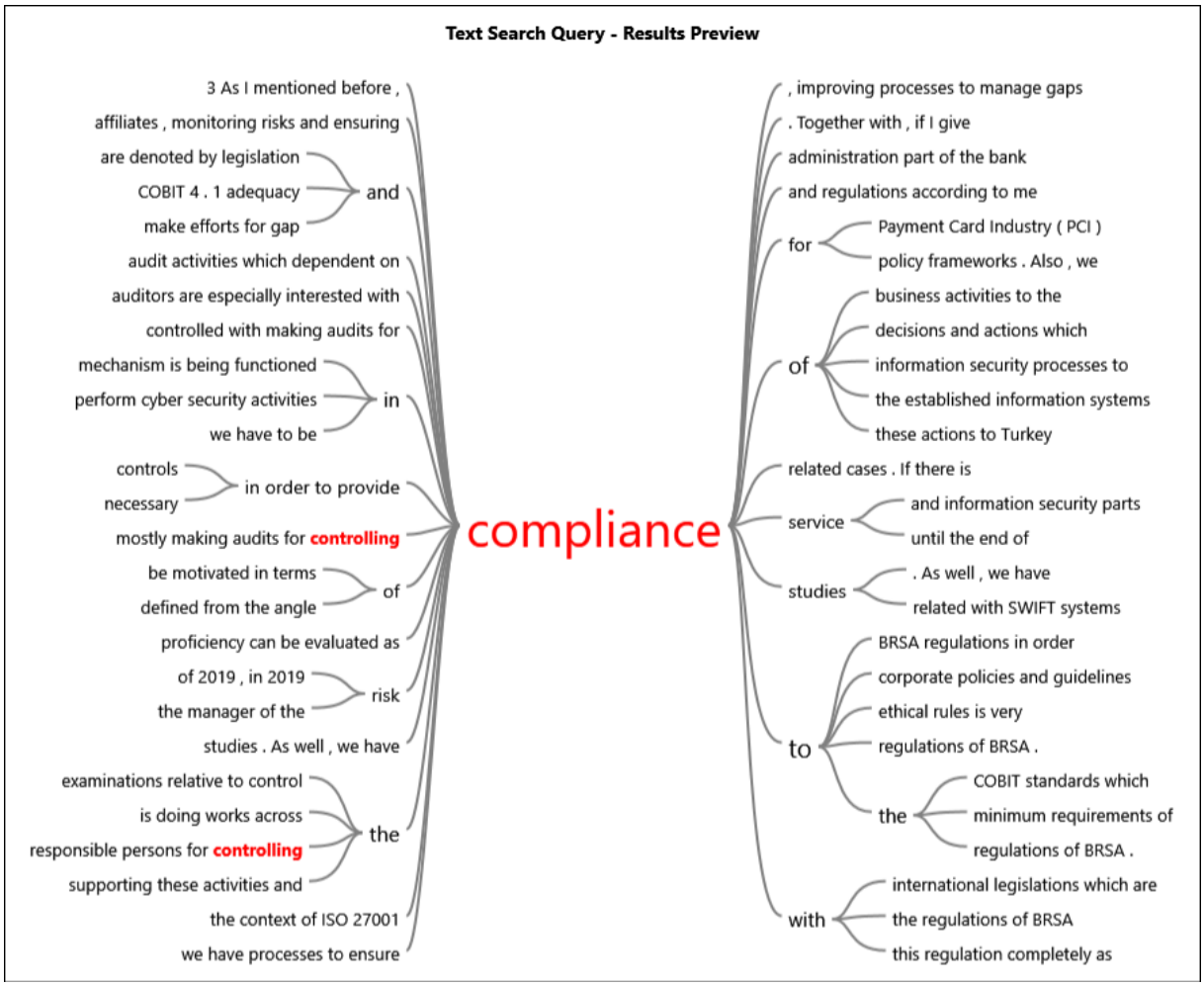
Text Search Query - Results Preview

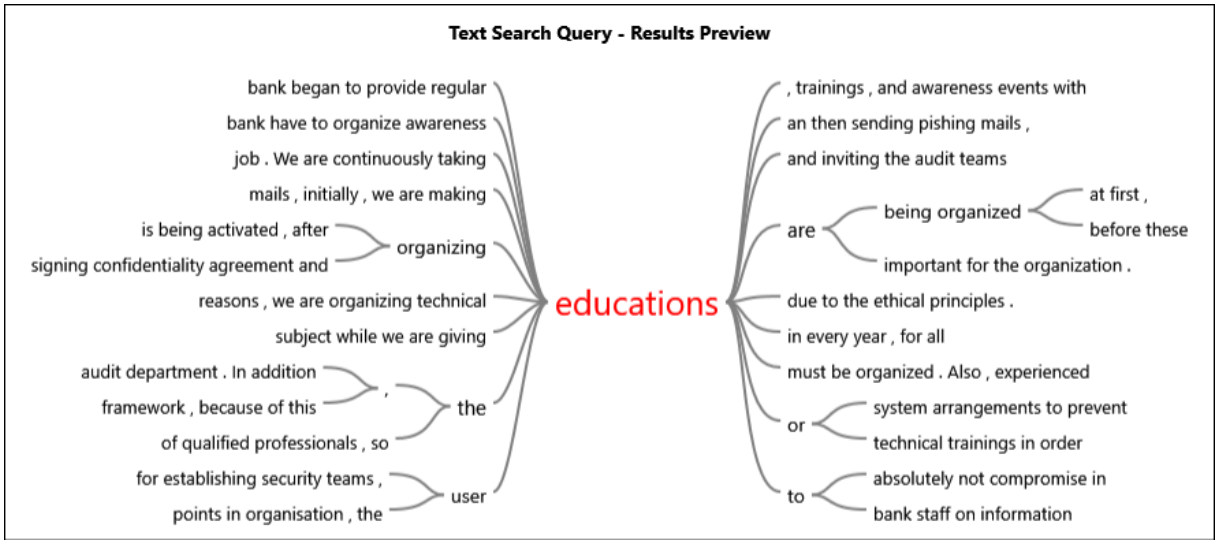
Text Search Query - Results Preview

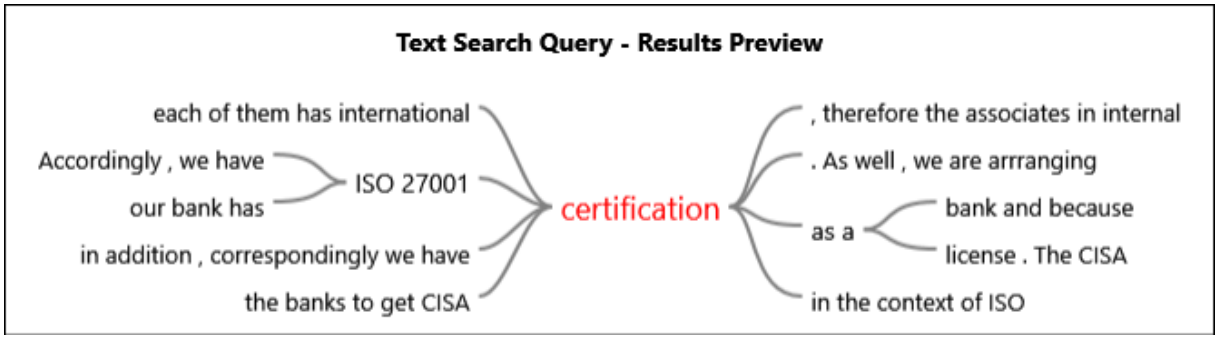
Text Search Query - Results Preview

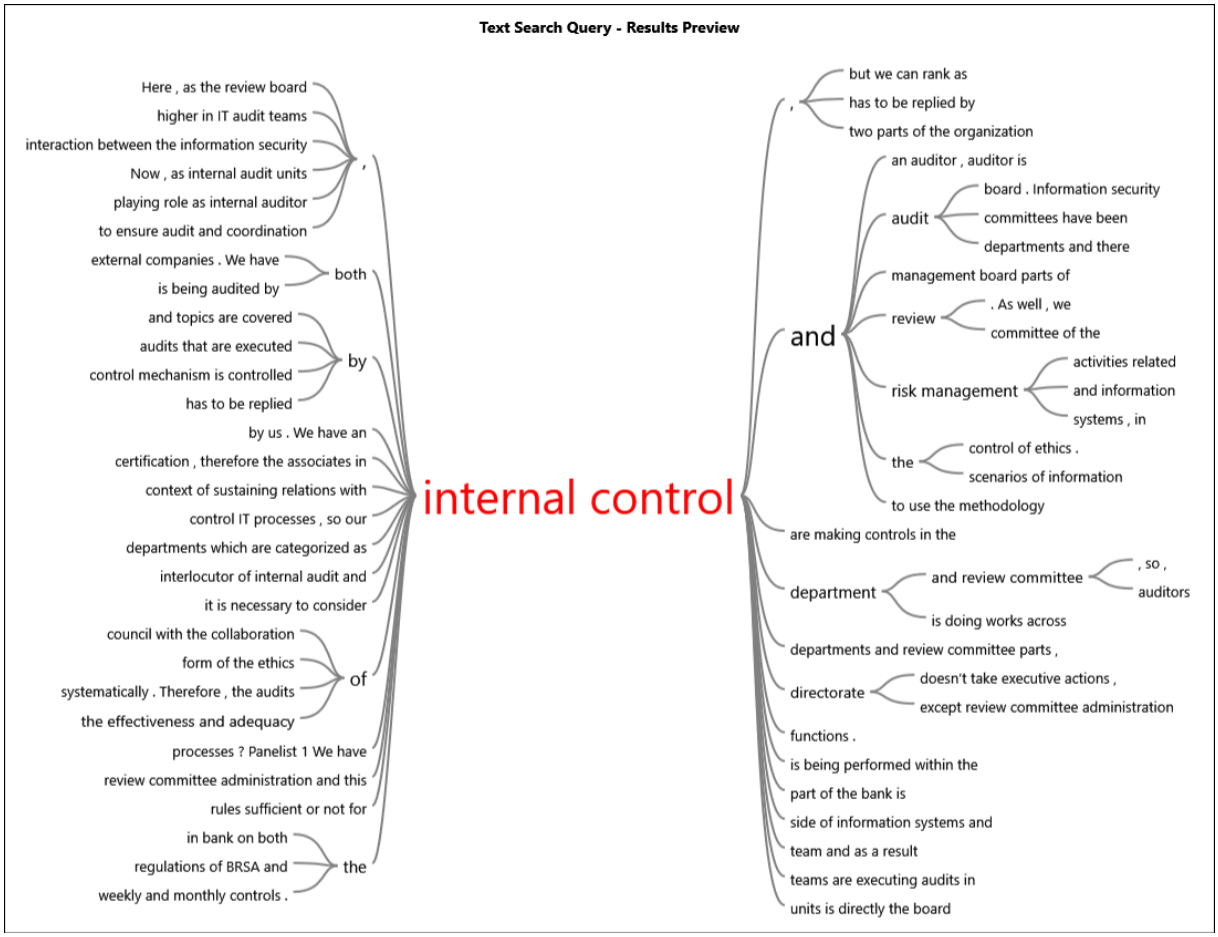

Text Search Query - Results Preview
process
focus on IT related processes
for division controls , also investigations
we have process to review
,
administrative auditor should focus on
all this is wrong , however
am responsible for the banking
Bankası , thus , IT audits
mainly related with reporting
making both division controls
taking part in division
and
and Internal Capital Adequacy Assessment
as same before too like
if we begin an
reviews and examinations , the
within the bank , independent
audit
before , there is a monitoring
auditors which is
have been being
called as
called as process controls , so
deficiencies which are related with
due to the COBIT
that are under the
DS5
have to be work in
IT risk management and IT
link of the cyber security
more than these , we have
intra - bank parts of
Now , we are in
presenting audit arguments , because
the
and investigations , so
security process . Accordingly ,
the disciplinary
a matter of fact
processes ? Panelist 5 Definitely
,
are needed to improve
here since 2015 , but
being made and
continuous improvement state
in
is all the time
is named as finart .
this
as weakest factor
in the beginning
is the fundamental
of
to be available and
weak points , Certainly , all
while we are handling a
,
are being checked , so in
let me put it this
of course , when we look
quite simply , code of ethics
we have
authorization levels to
permission to access
what BRSA brought in time
.
Accordingly , the disciplinary process of
Basically , you can be considered
Something like this happens , for
The purpose of the internal
There is a defined basic
and
findings are being controlled ,
supervision of public authority .
as well as firewall and
audits have to be performed
can
be defined as the
vary due to the
controller
is taking function as
or administrative auditor should
since 2007 for fourteen
controllers and IT auditors are
,
in the rest of
so process controllers and
controls
and as well I
are being evaluated much
which are related with
covers one of the control
development operations . Also , the weaknesses
has
refrained because of the
to be
available and
performed in
is
being performed
as same
in that
functioning or not in
not being completed and
management committee . BRSA issued a
of
human resources is being
new policy making namely
part and this can be
starts like that . After that ,
to review , process and findings
which is
being performed for
related with credit
you are doing queries relative

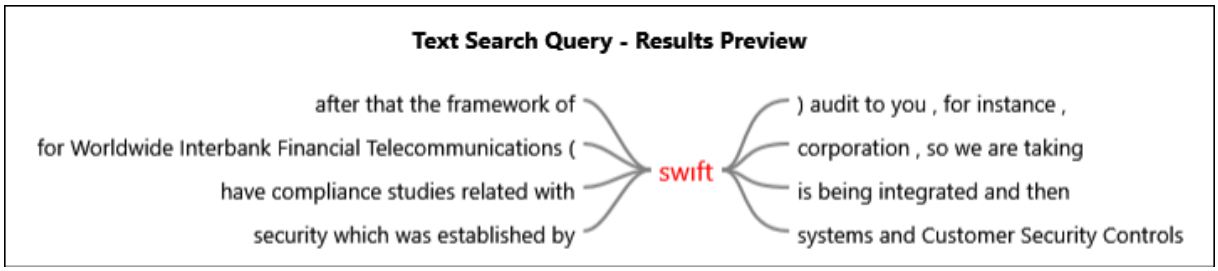

Text Search Query - Results Preview
management board , so control
of records with resolution
and
and with in this context
controlling the access of affiliates ,
controls and independent audits by
database management , network control or
department has predominantly functions in
have many scenarios such as
log records are used for
mentioned before , there is a
part of CIA triad through
board of directors , therefore
board of directors and
the
security management relative to
therefore , we have an effective
with in the context of
monitoring
activities of legislative framework and
and following up the transactions
function is being
executed as
performed periodically
of
all necessary infrastructure of
the problem . Likewise , we
operations
, which are relative to
are based on these
part of cyber security because
process which is being performed
processes , the reports , which we
risks and ensuring compliance , improving
system for cyber security management .
the
information systems . Therefore , the
movements of both network
to provide security stably . On

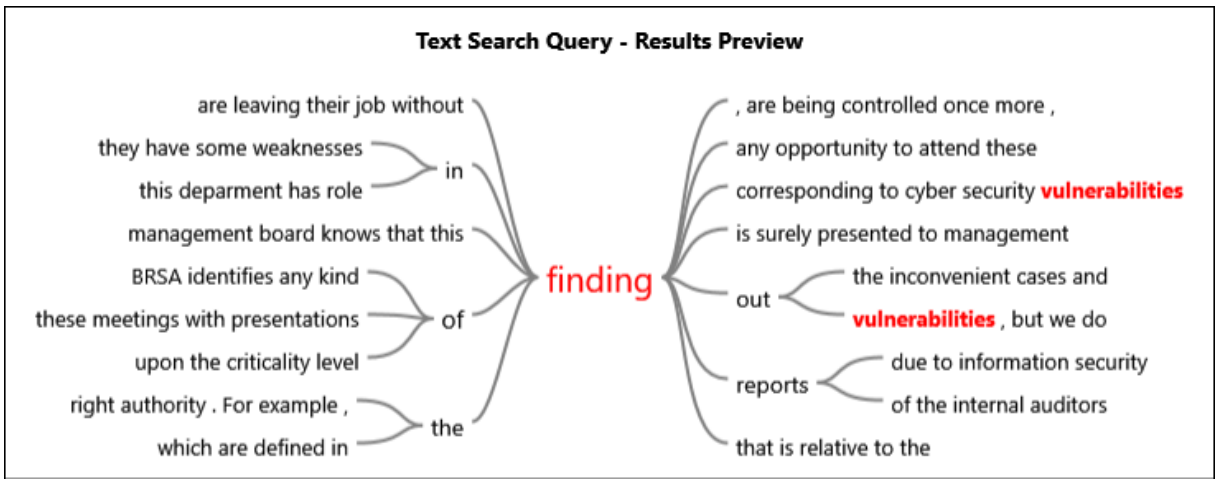

Text Search Query - Results Preview
3 As I mentioned before ,
affiliates , monitoring risks and ensuring
are denoted by legislation
COBIT 4 . 1 adequacy
and
make efforts for gap
audit activities which dependent on
auditors are especially interested with
controlled with making audits for
mechanism is being functioned
perform cyber security activities
in
we have to be
controls
necessary
in order to provide
mostly making audits for controlling
be motivated in terms
defined from the angle
of
proficiency can be evaluated as
of 2019 , in 2019
the manager of the
risk
studies . As well , we have
examinations relative to control
is doing works across
responsible persons for controlling
supporting these activities and
the
the context of ISO 27001
we have processes to ensure
compliance
, improving processes to manage gaps
. Together with , if I give
administration part of the bank
and regulations according to me
for
Payment Card Industry (PCI)
policy frameworks . Also , we
of
business activities to the
decisions and actions which
information security processes to
the established information systems
these actions to Turkey
related cases . If there is
service
and information security parts
until the end of
studies
. As well , we have
related with SWIFT systems
to
BRSA regulations in order
corporate policies and guidelines
ethical rules is very
regulations of BRSA .
the
COBIT standards which
minimum requirements of
regulations of BRSA .
with
international legislations which are
the regulations of BRSA
this regulation completely as


Text Search Query - Results Preview
bank began to provide regular
bank have to organize awareness
job . We are continuously taking
mails , initially , we are making
is being activated , after
signing confidentiality agreement and
organizing
reasons , we are organizing technical
subject while we are giving
audit department . In addition
framework , because of this
,
of qualified professionals , so
the
for establishing security teams ,
points in organisation , the
user
educations
, trainings , and awareness events with
an then sending pishing mails ,
and inviting the audit teams
are
being organized
at first ,
before these
important for the organization .
due to the ethical principles .
in every year , for all
must be organized . Also , experienced
or
system arrangements to prevent
technical trainings in order
to
absolutely not compromise in
bank staff on information


Text Search Query - Results Preview
each of them has international
Accordingly , we have
our bank has
ISO 27001
in addition , correspondingly we have
the banks to get CISA
certification
, therefore the associates in internal
. As well , we are arrranging
as a
bank and because
license . The CISA
in the context of ISO

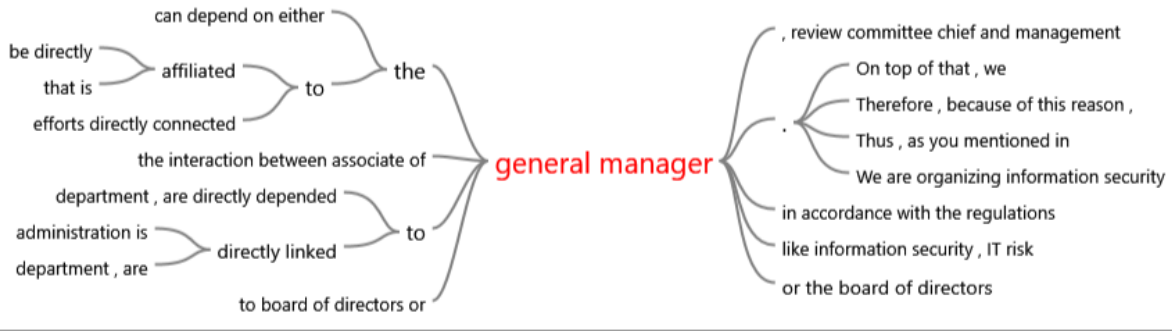

Text Search Query - Results Preview
internal control
Here , as the review board
higher in IT audit teams
interaction between the information security
Now , as internal audit units
playing role as internal auditor
to ensure audit and coordination
,
external companies . We have
is being audited by
both
and topics are covered
audits that are executed
control mechanism is controlled
has to be replied
by
by us . We have an
certification , therefore the associates in
context of sustaining relations with
control IT processes , so our
departments which are categorized as
interlocutor of internal audit and
it is necessary to consider
council with the collaboration
form of the ethics
systematically . Therefore , the audits
the effectiveness and adequacy
of
processes ? Panelist 1 We have
review committee administration and this
rules sufficient or not for
in bank on both
regulations of BRSA and
weekly and monthly controls .
the
but we can rank as
has to be replied by
two parts of the organization
,
an auditor , auditor is
board . Information security
committees have been
departments and there
audit
management board parts of
. As well , we
committee of the
review
activities related
and information
systems , in
risk management
control of ethics .
scenarios of information
the
to use the methodology
and
are making controls in the
, so ,
auditors
and review committee
is doing works across
department
departments and review committee parts ,
doesn't take executive actions ,
except review committee administration
directorate
functions .
is being performed within the
part of the bank is
side of information systems and
team and as a result
teams are executing audits in
units is directly the board


Text Search Query - Results Preview
swift
after that the framework of
for Worldwide Interbank Financial Telecommunications (
have compliance studies related with
security which was established by
) audit to you , for instance ,
corporation , so we are taking
is being integrated and then
systems and Customer Security Controls

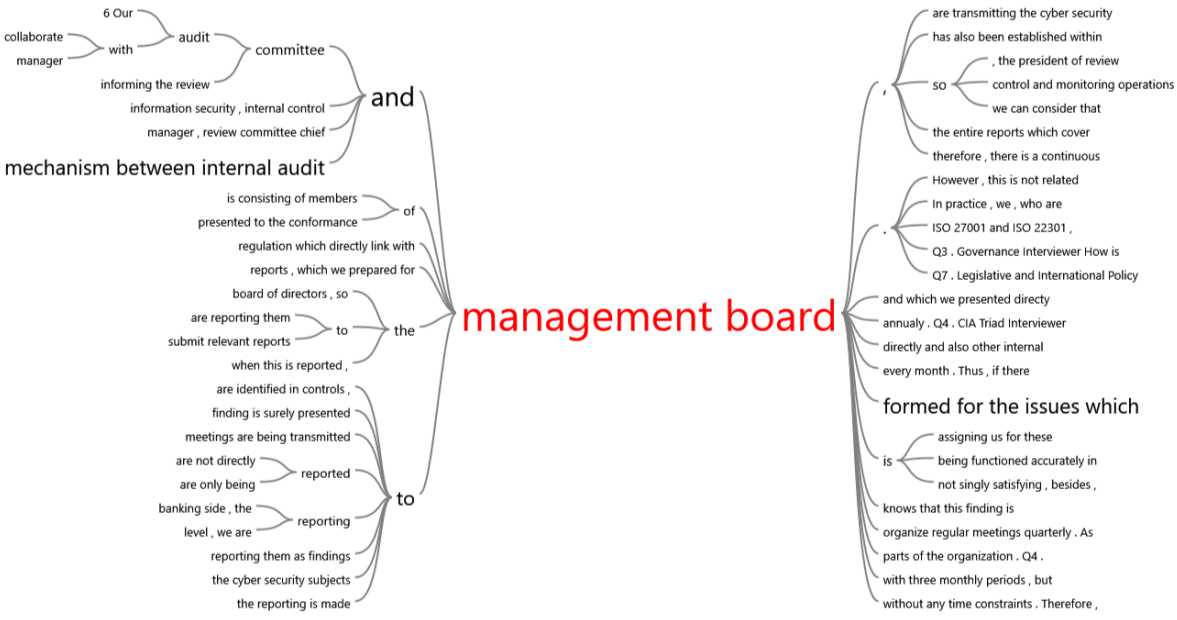

Text Search Query - Results Preview
finding
are leaving their job without
they have some weaknesses
this deparment has role
in
management board knows that this
BRSA identifies any kind
these meetings with presentations
upon the criticality level
of
right authority . For example ,
which are defined in
the
, are being controlled once more ,
any opportunity to attend these
corresponding to cyber security vulnerabilities
is surely presented to management
out
the inconvenient cases and
vulnerabilities , but we do
reports
due to information security
of the internal auditors
that is relative to the

Text Search Query - Results Preview

Text Search Query - Results Preview



Text Search Query - Results Preview



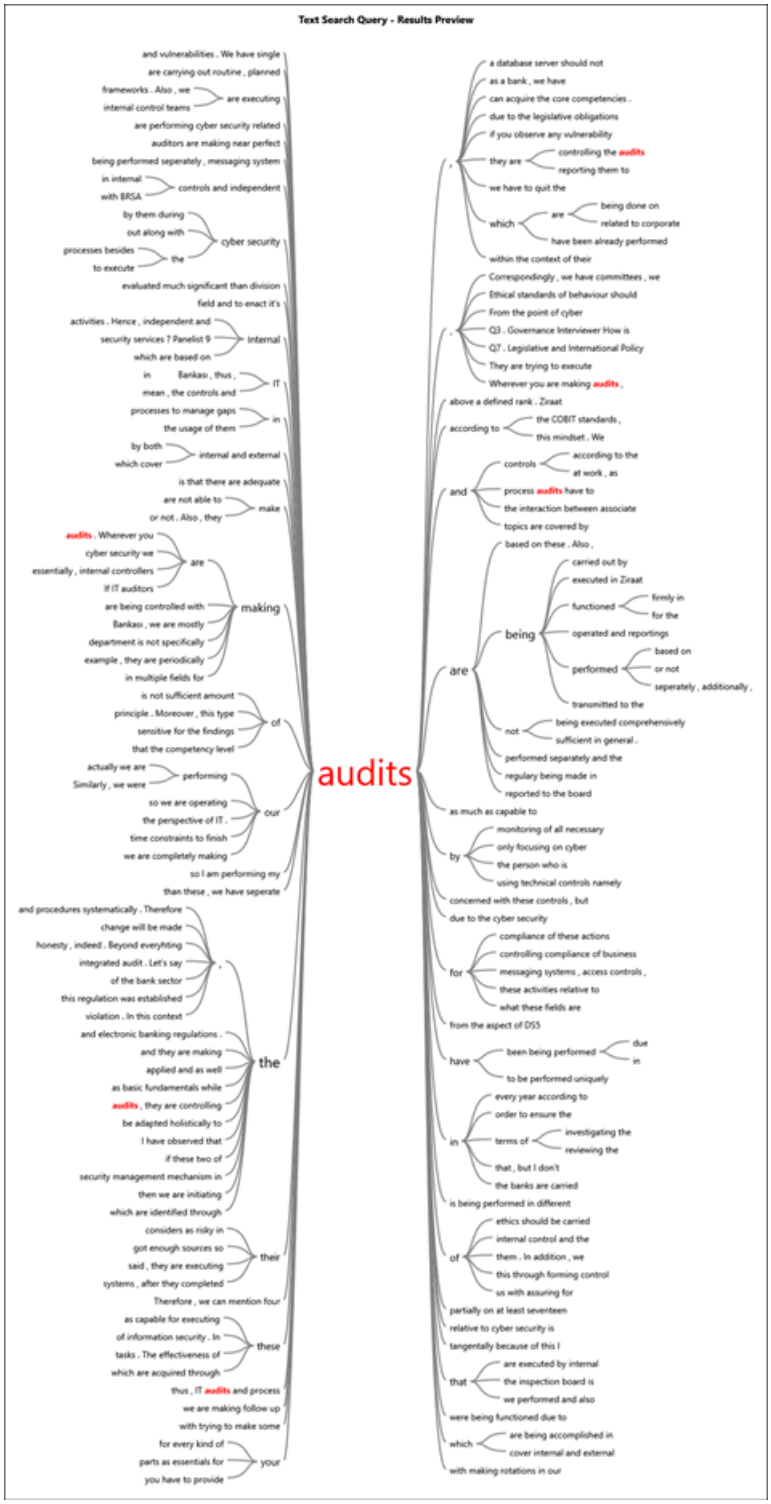
Text Search Query - Results Preview

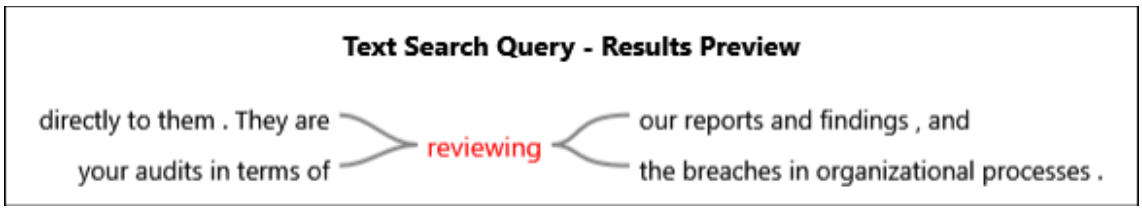
Text Search Query - Results Preview

data and then we are
infrastructure of information systems , the
their transactions in enterprise resource

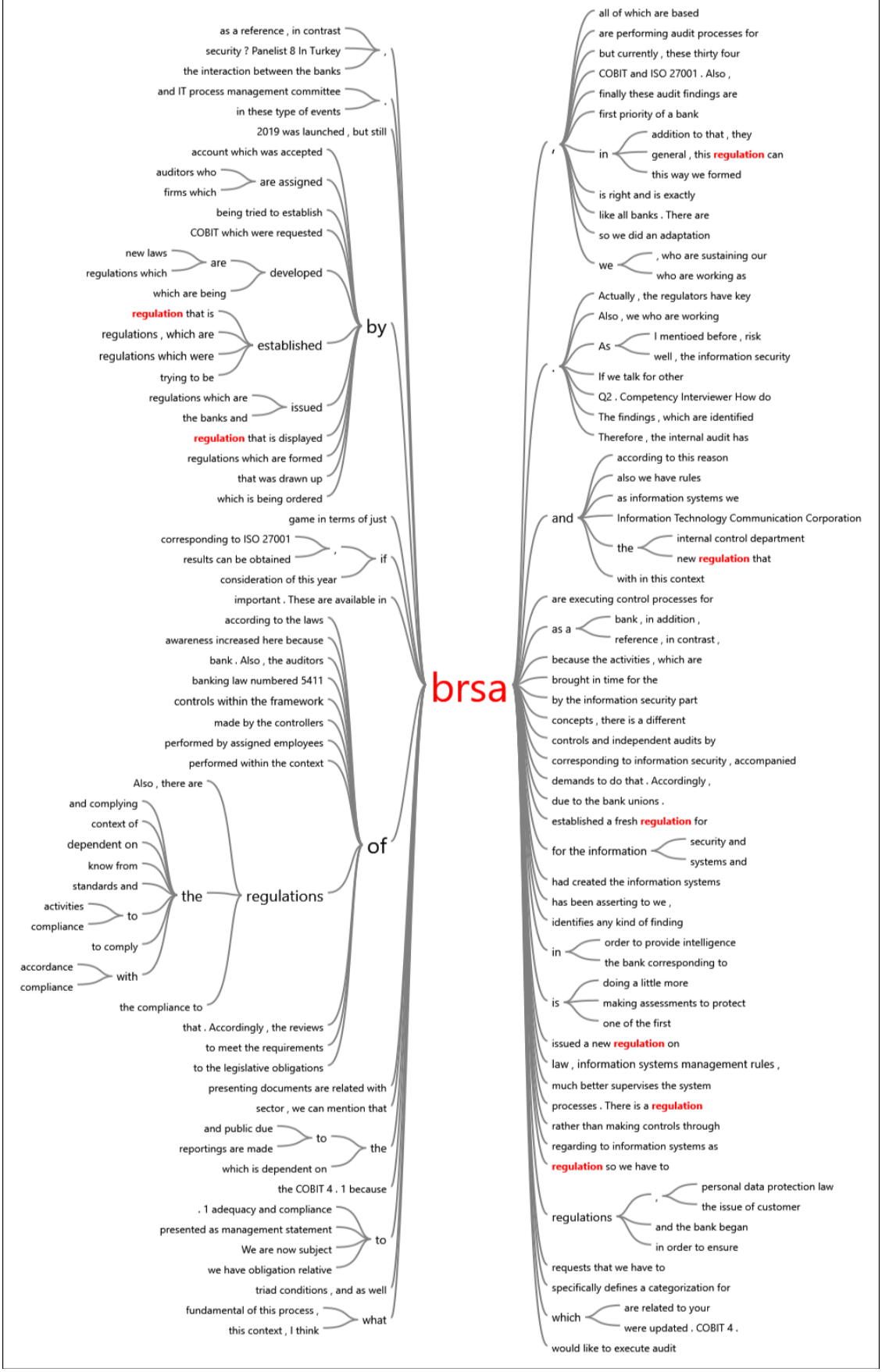
planning

(ERP) platforms . Therefore , I think
activities are being realized like
our audit operations according to

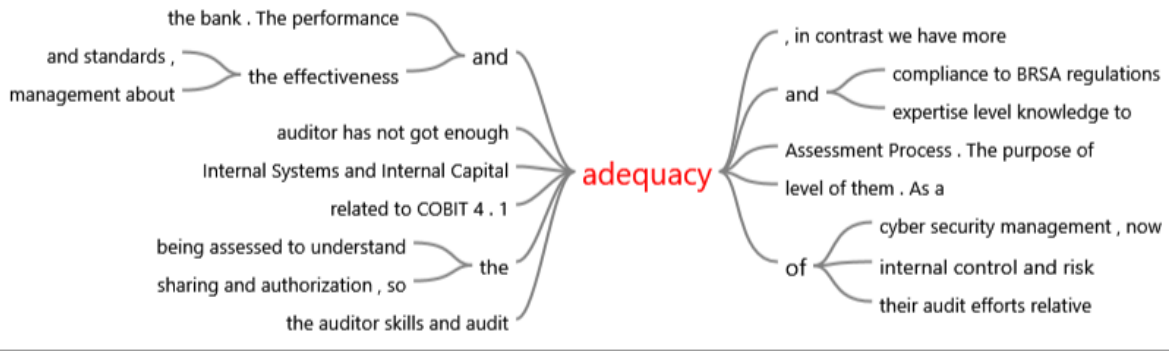



Text Search Query - Results Preview
directly to them . They are
your audits in terms of
reviewing
our reports and findings , and
the breaches in organizational processes .

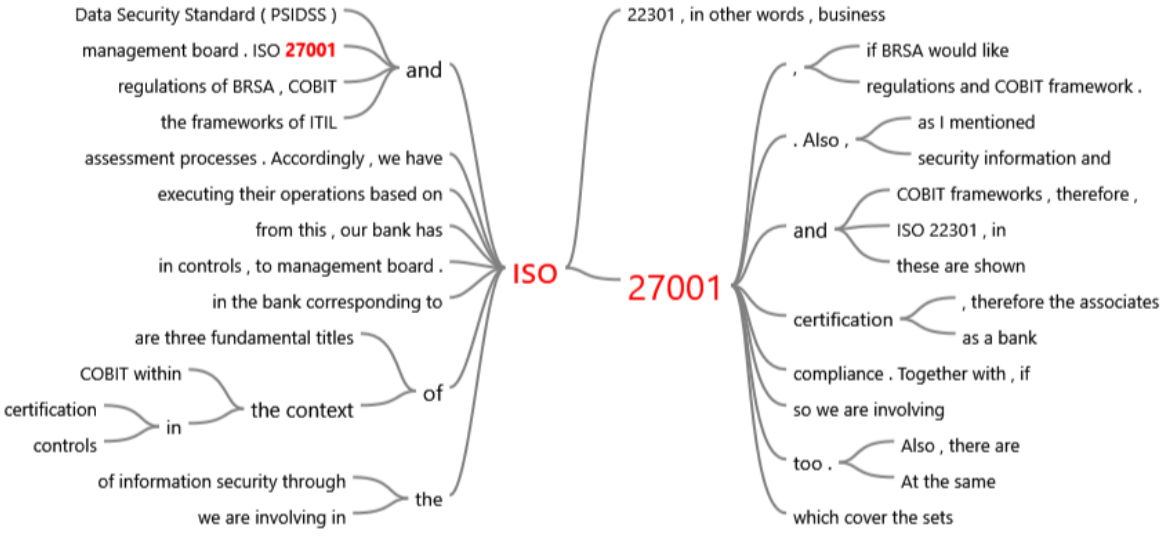
Text Search Query - Results Preview



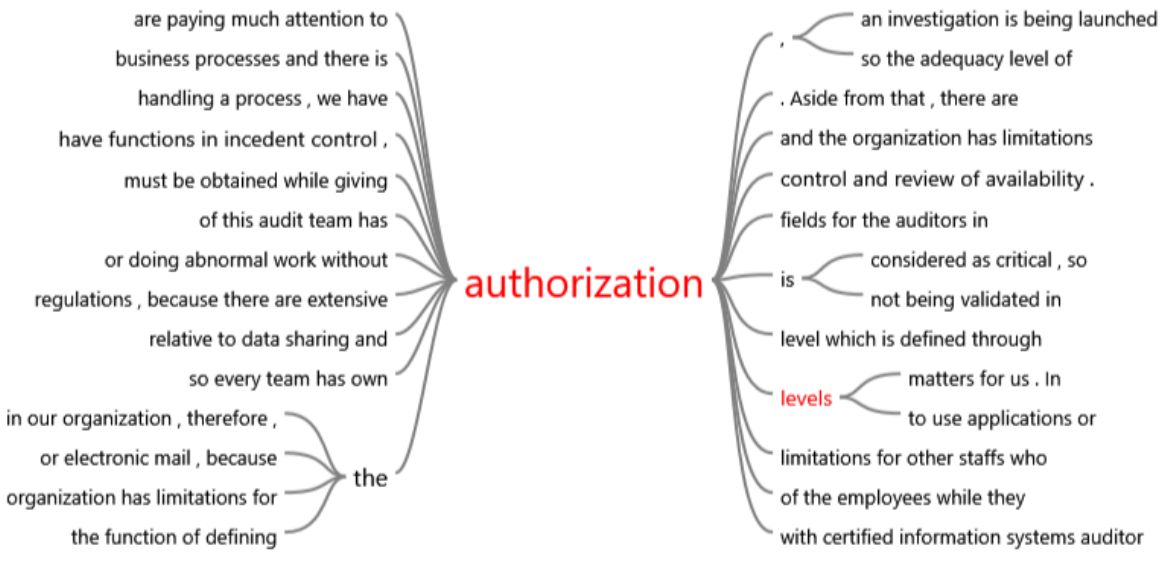
Text Search Query - Results Preview



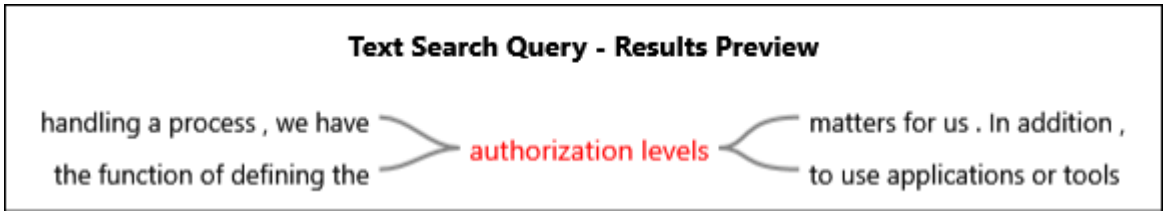
Text Search Query - Results Preview



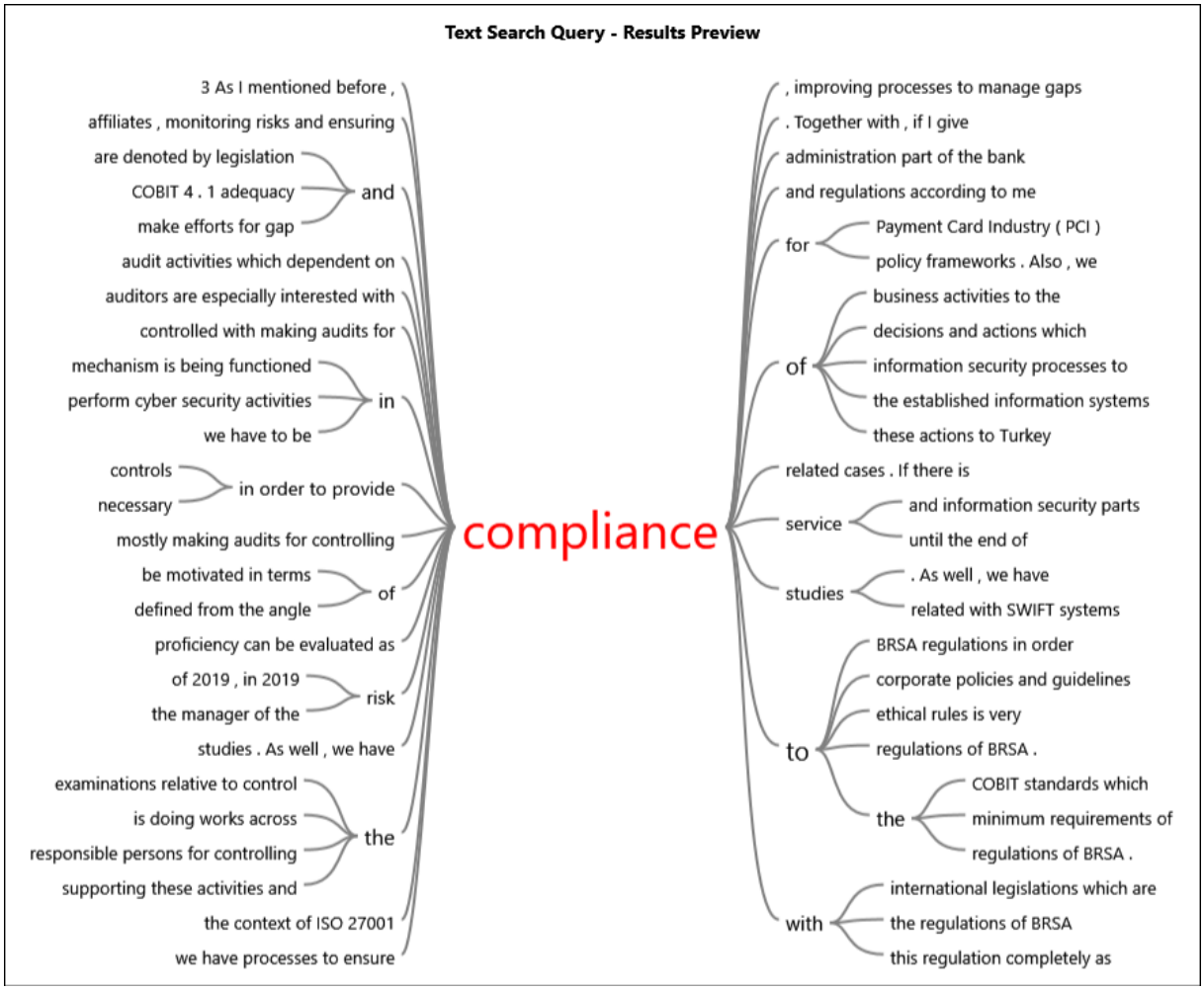
Text Search Query - Results Preview



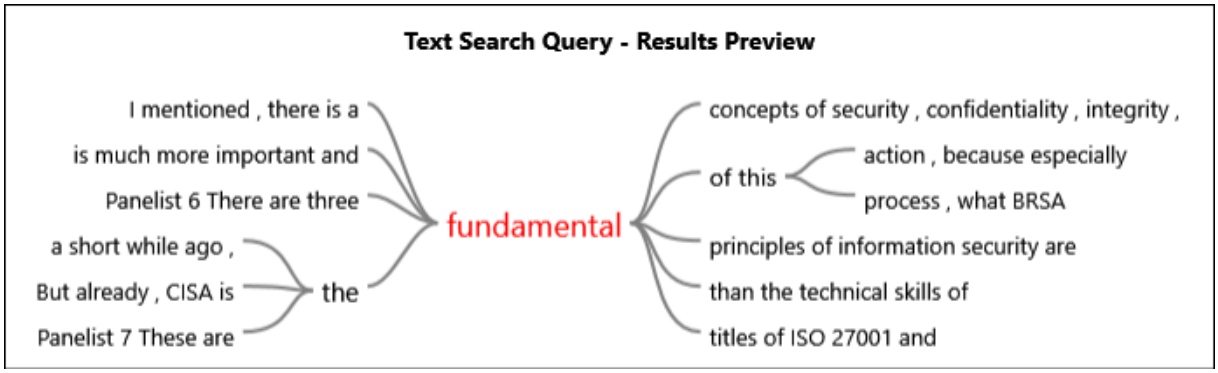
Text Search Query - Results Preview

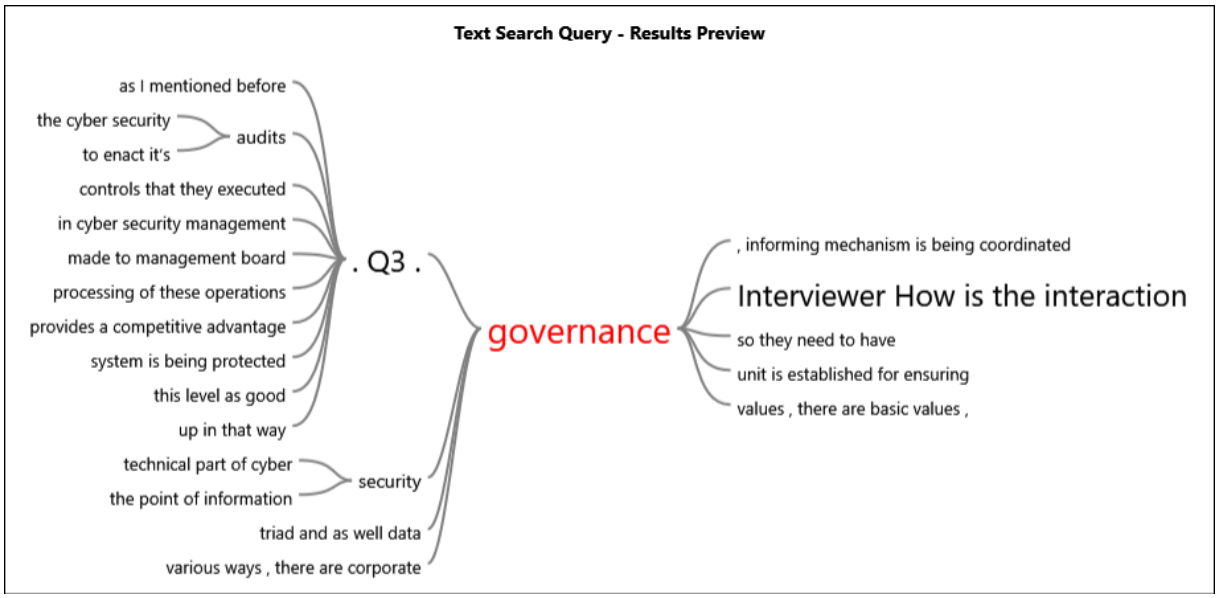


Text Search Query - Results Preview

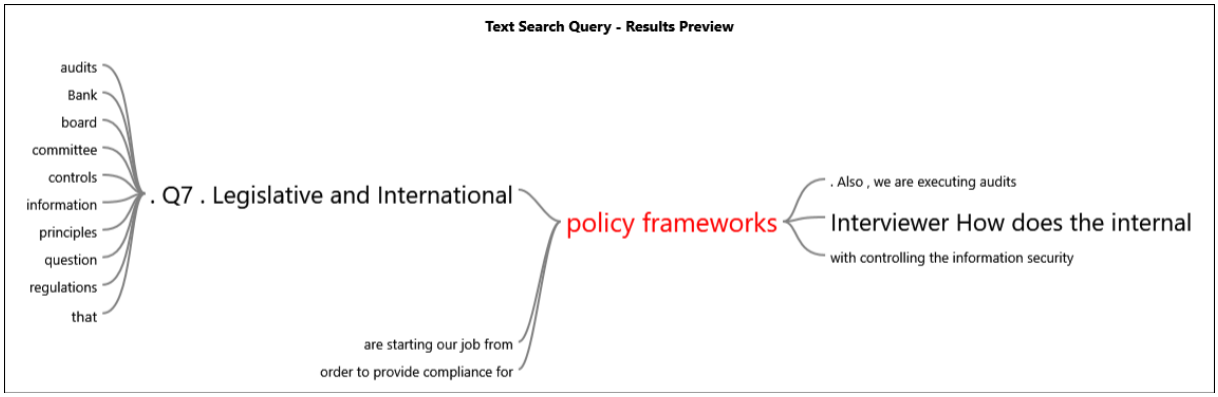


Text Search Query - Results Preview


Text Search Query - Results Preview
I mentioned , there is a
is much more important and
Panelist 6 There are three
a short while ago ,
But already , CISA is
Panelist 7 These are
the
fundamental
concepts of security , confidentiality , integrity ,
of this
action , because especially
process , what BRSA
principles of information security are
than the technical skills of
titles of ISO 27001 and

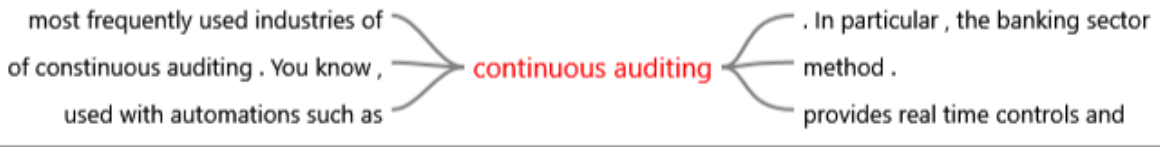

Text Search Query - Results Preview
as I mentioned before
the cyber security
to enact it's
audits
controls that they executed
in cyber security management
made to management board
processing of these operations
provides a competitive advantage
system is being protected
this level as good
up in that way
. Q3 .
technical part of cyber
the point of information
security
triad and as well data
various ways , there are corporate
governance
, informing mechanism is being coordinated
Interviewer How is the interaction
so they need to have
unit is established for ensuring
values , there are basic values ,


Text Search Query - Results Preview
condition of one hundred hours
organized as both in person
well , we are arrranging annual
education
and distance learning as we
for every three year was
plans for IT auditors and


Text Search Query - Results Preview
audits
Bank
board
committee
controls
information
principles
question
regulations
that
. Q7 . Legislative and International
are starting our job from
order to provide compliance for
policy frameworks
. Also , we are executing audits
Interviewer How does the internal
with controlling the information security

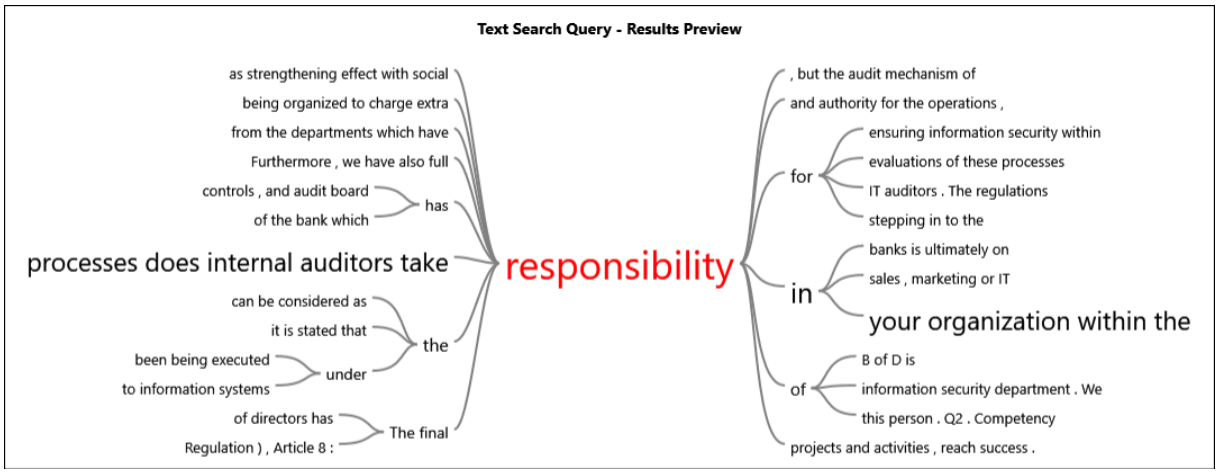
Text Search Query - Results Preview

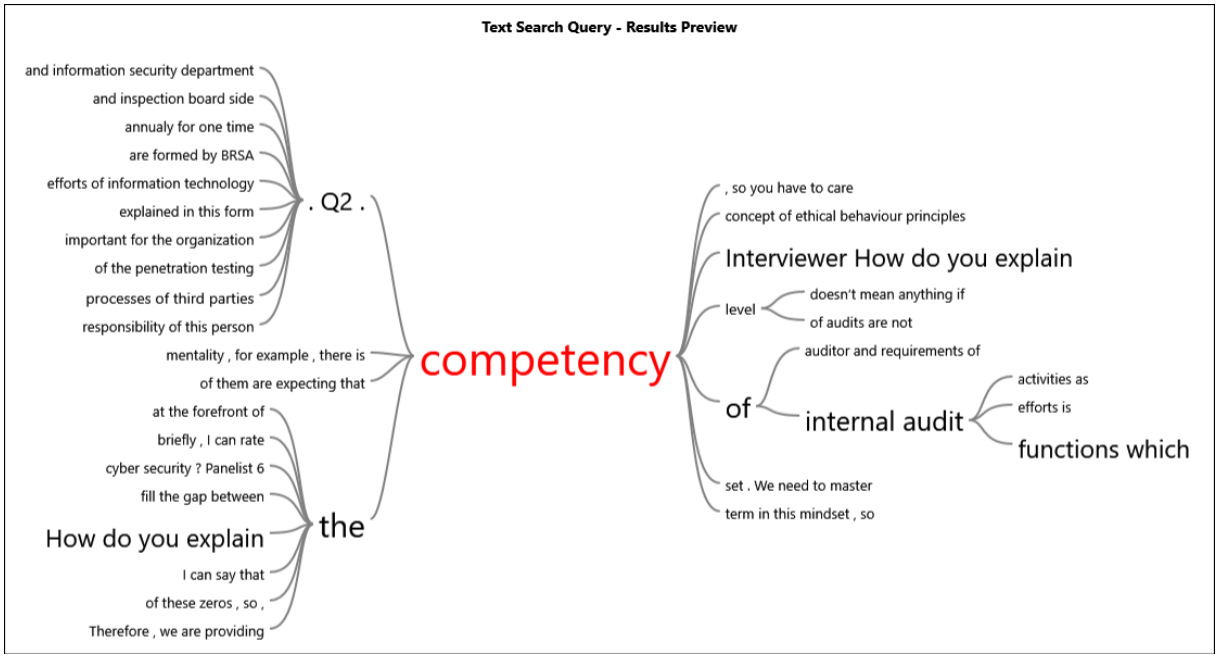
Text Search Query - Results Preview

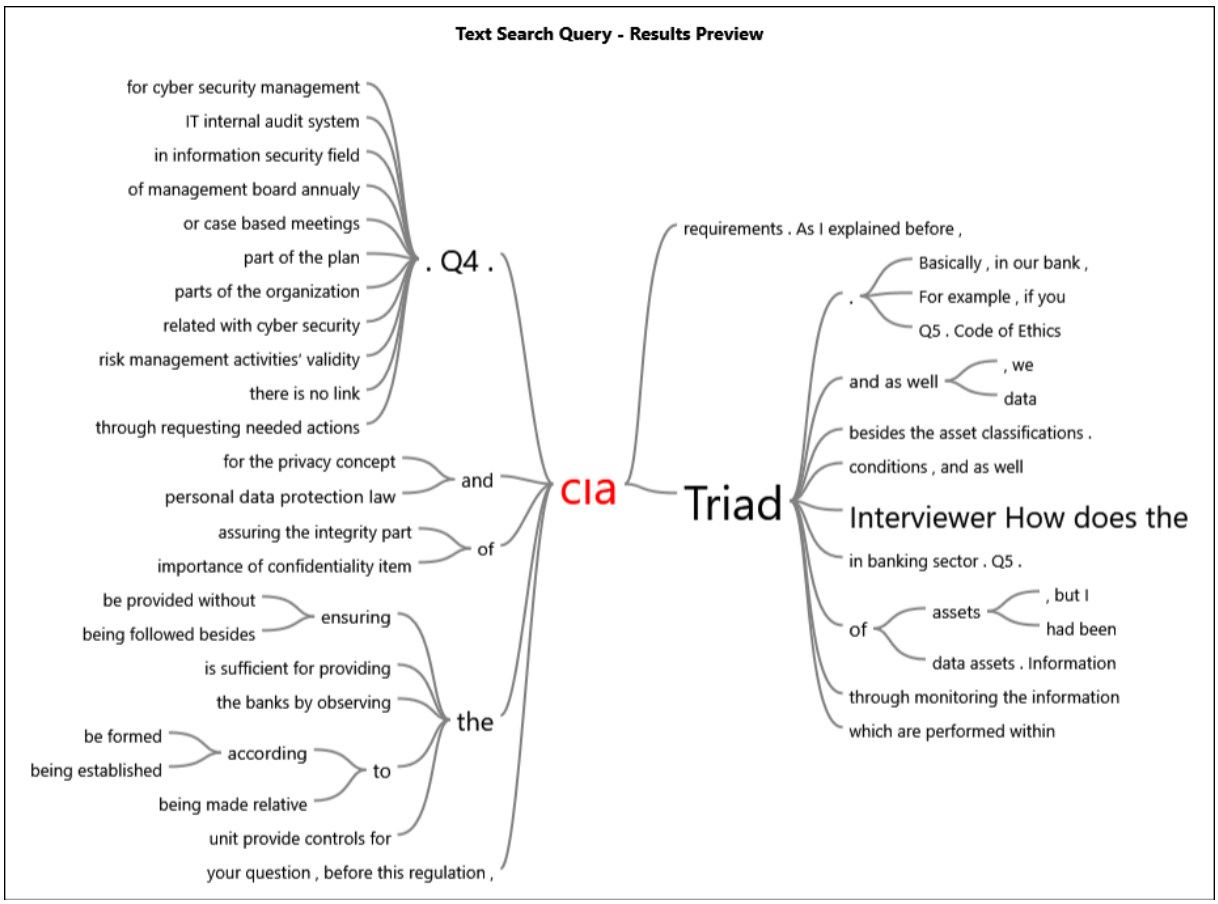


Text Search Query - Results Preview

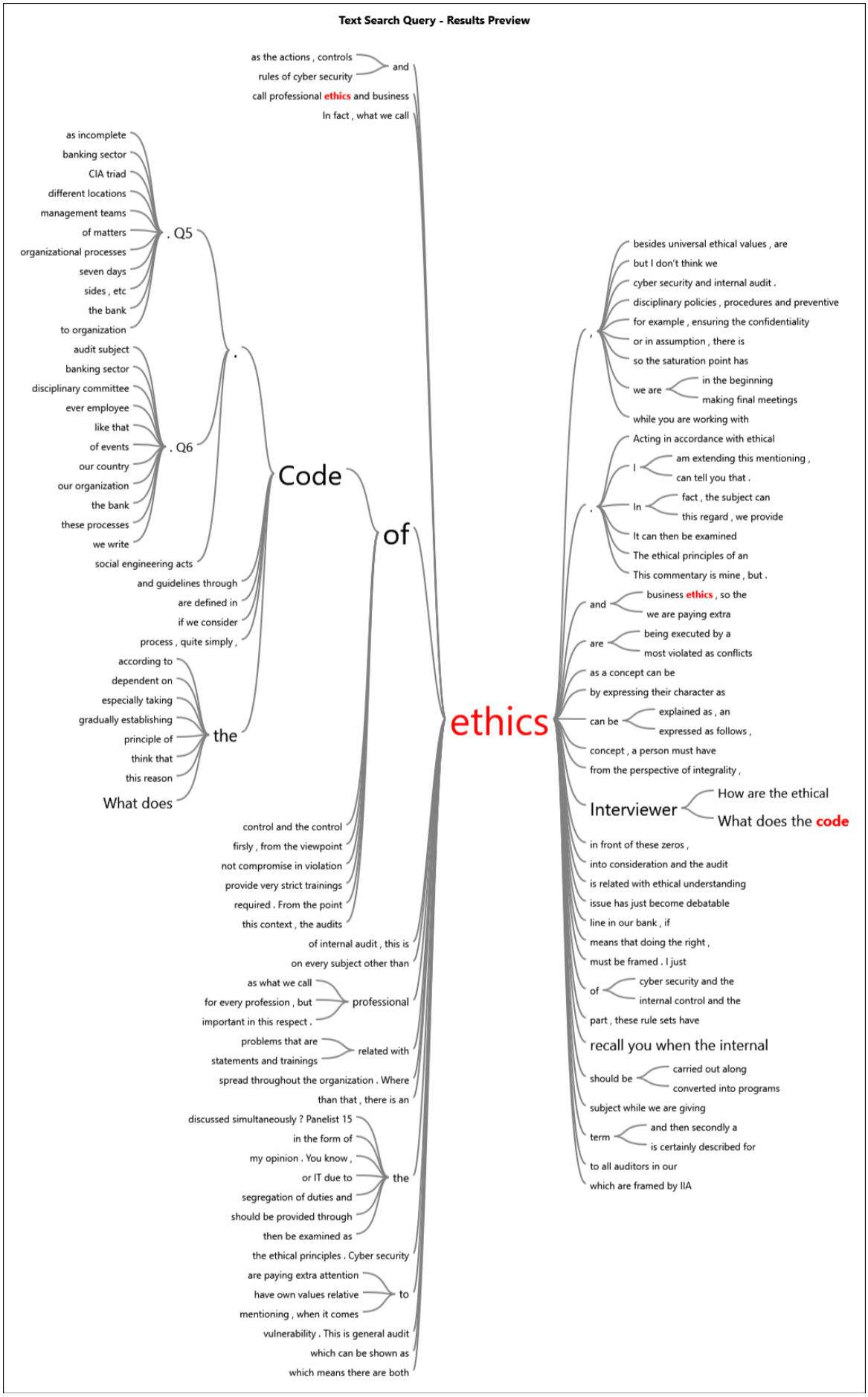

Text Search Query - Results Preview
activities , so we are handling
according to COBIT standards
adequacy of
internal control
review board ,
and
review , security architecture evaluations
applications where we can make
are being made in our
BRSA . As I mentioed before ,
corporate data office and information
diversify the region . Therefore , a
end of 2019 , in 2019
I explained before , we have
Also , we are executing
IT
Manager like information security ,
level , so according to these
matrices are designed and every
periods in order to evaluate
any kind of cyber
being performed by
information
security
line as an
first you must define
IT teams with practicing
is trying to reduce
then you must map
the
through these questionnaires before
was the manager of
we can track our own
with cyber security ? Panelist 3
risk
as much as possible , if
assessment studies . As a part
assessments with external companies . We
by the determination of the
compliance service
and information security
until the end
control matrices are
being designed
designed and
evaluations . After that , we are
field , while the functions of
has it's own level , so
levels the actions are taken
, as well , we have
activities related to information
activities' validity . Q4 . CIA
management
and
IT process management
information security in
projects of the bank ,
systems , in which bank
teams . Q5 . Code of
map is created for each
matrices , secondly , the bank is
matrixes for cyber security decisions
occurs in the bank , we
ratings are being made in
records and where we can
sessions as definitions of threat ,
team
, to the board of
and at the last

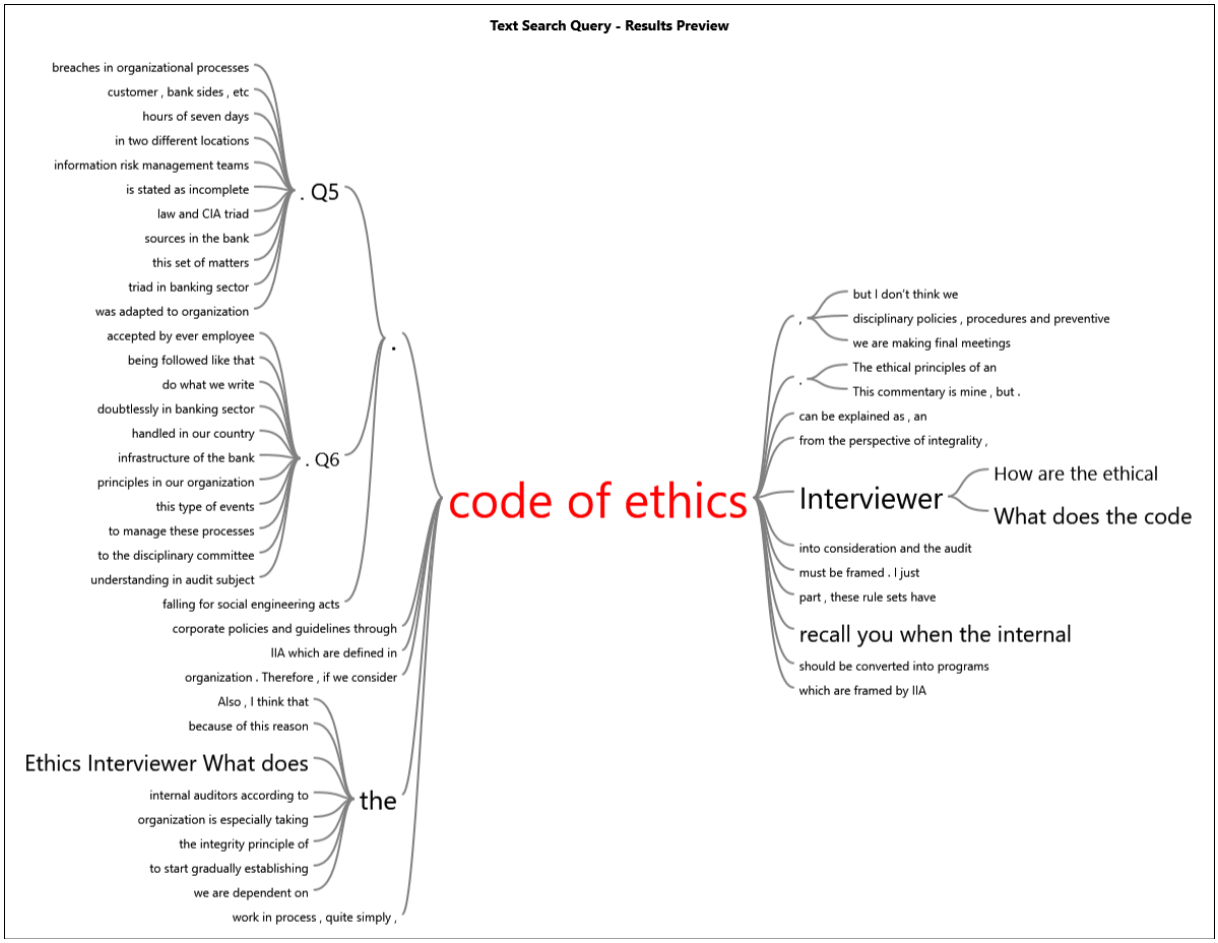

Text Search Query - Results Preview
as strengthening effect with social
being organized to charge extra
from the departments which have
Furthermore , we have also full
controls , and audit board
has
of the bank which
processes does internal auditors take
can be considered as
it is stated that
the
been being executed
under
to information systems
of directors has
The final
Regulation) , Article 8 :
responsibility
, but the audit mechanism of
and authority for the operations ,
for
ensuring information security within
evaluations of these processes
IT auditors . The regulations
stepping in to the
banks is ultimately on
in
sales , marketing or IT
your organization within the
B of D is
of
information security department . We
this person . Q2 . Competency
projects and activities , reach success .

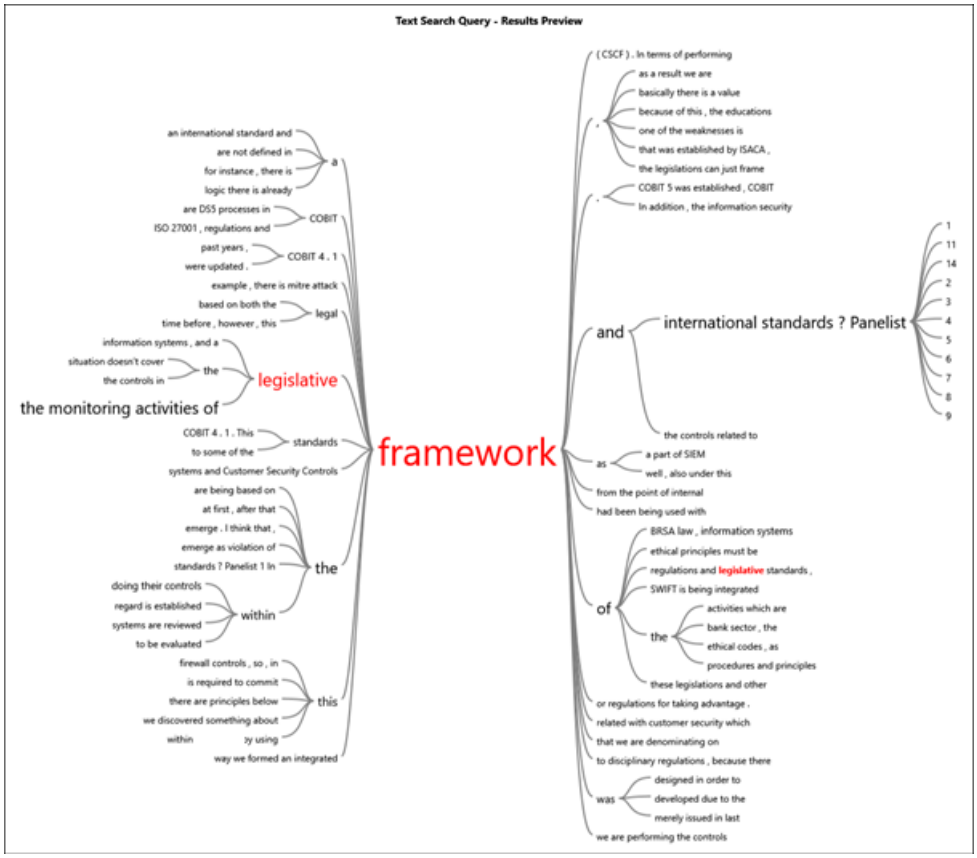

Text Search Query - Results Preview
and information security department
and inspection board side
annualy for one time
are formed by BRSA
efforts of information technology
explained in this form
important for the organization
of the penetration testing
processes of third parties
responsibility of this person
. Q2 .
mentality , for example , there is
of them are expecting that
at the forefront of
briefly , I can rate
cyber security ? Panelist 6
fill the gap between
How do you explain
I can say that
of these zeros , so ,
Therefore , we are providing
the
competency
, so you have to care
concept of ethical behaviour principles
Interviewer How do you explain
level
doesn't mean anything if
of audits are not
auditor and requirements of
of
internal audit
activities as
efforts is
functions which
set . We need to master
term in this mindset , so

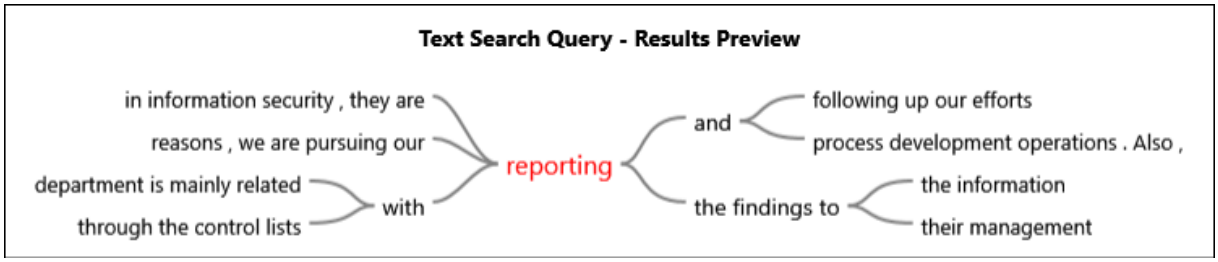

Text Search Query - Results Preview
for cyber security management
IT internal audit system
in information security field
of management board annualy
or case based meetings
part of the plan
parts of the organization
related with cyber security
risk management activities' validity
there is no link
through requesting needed actions
. Q4 .
for the privacy concept
personal data protection law
and
assuring the integrity part
importance of confidentiality item
of
be provided without
being followed besides
ensuring
is sufficient for providing
the banks by observing
be formed
being established
according
being made relative
to
unit provide controls for
your question , before this regulation ,
the
cia
requirements . As I explained before ,
Triad
.
Basically , in our bank ,
For example , if you
Q5 . Code of Ethics
and as well
, we
data
besides the asset classifications .
conditions , and as well
Interviewer How does the
in banking sector . Q5 .
of
assets
, but I
had been
data assets . Information
through monitoring the information
which are performed within

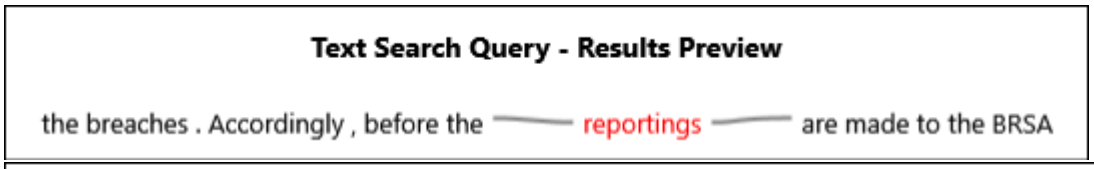
Text Search Query - Results Preview



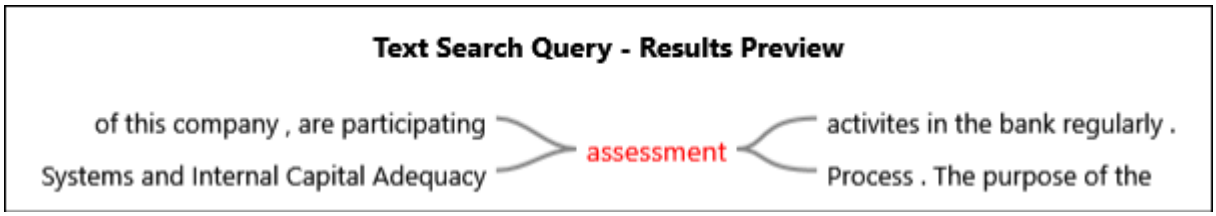

Text Search Query - Results Preview
breaches in organizational processes
customer , bank sides , etc
hours of seven days
in two different locations
information risk management teams
is stated as incomplete
law and CIA triad
sources in the bank
this set of matters
triad in banking sector
was adapted to organization
. Q5
accepted by ever employee
being followed like that
do what we write
doubtlessly in banking sector
handled in our country
infrastructure of the bank
principles in our organization
this type of events
to manage these processes
to the disciplinary committee
understanding in audit subject
. Q6
falling for social engineering acts
corporate policies and guidelines through
IIA which are defined in
organization . Therefore , if we consider
Also , I think that
because of this reason
Ethics Interviewer What does
internal auditors according to
organization is especially taking
the integrity principle of
to start gradually establishing
we are dependent on
the
work in process , quite simply ,
code of ethics
but I don't think we
disciplinary policies , procedures and preventive
we are making final meetings
The ethical principles of an
This commentary is mine , but .
can be explained as , an
from the perspective of integrality ,
Interviewer
How are the ethical
What does the code
into consideration and the audit
must be framed . I just
part , these rule sets have
recall you when the internal
should be converted into programs
which are framed by IIA


Text Search Query - Results Preview
framework
the monitoring activities of
legislative
the controls in
information systems , and a
situation doesn't cover
the
COBIT 4 . 1 . This
to some of the
systems and Customer Security Controls
standards
COBIT
are DS5 processes in
ISO 27001 , regulations and
COBIT 4 . 1
past years ,
were updated .
example , there is mitre attack
based on both the
time before , however , this
legal
an international standard and
are not defined in
for instance , there is
logic there is already
a
are being based on
at first , after that
emerge . I think that ,
emerge as violation of
standards ? Panelist 1 In
the
doing their controls
regard is established
systems are reviewed
to be evaluated
within
firewall controls , so , in
is required to commit
there are principles below
we discovered something about
within
ty using
way we formed an integrated
this
(CSCF) . In terms of performing
as a result we are
basically there is a value
because of this , the educations
one of the weaknesses is
that was established by ISACA ,
the legislations can just frame
,
COBIT 5 was established , COBIT
In addition , the information security
.
and
international standards ? Panelist
1
11
14
2
3
4
5
6
7
8
9
the controls related to
as
a part of SIEM
well , also under this
from the point of internal
had been being used with
BRSA law , information systems
ethical principles must be
regulations and legislative standards ,
SWIFT is being integrated
of
the
activities which are
bank sector , the
ethical codes , as
procedures and principles
these legislations and other
or regulations for taking advantage .
related with customer security which
that we are denominating on
to disciplinary regulations , because there
was
designed in order to
developed due to the
merely issued in last
we are performing the controls

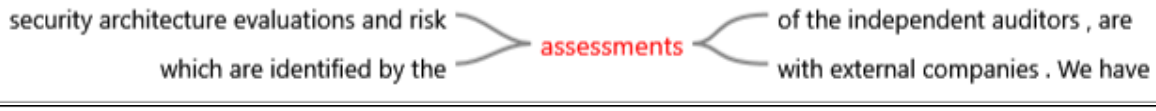

Text Search Query - Results Preview
in information security , they are
reasons , we are pursuing our
department is mainly related
through the control lists
with
reporting
and
following up our efforts
process development operations . Also ,
the findings to
the information
their management


Text Search Query - Results Preview
the breaches . Accordingly , before the
reportings
are made to the BRSA


Text Search Query - Results Preview
of the independent auditors , are
reported
to the information security department


Text Search Query - Results Preview
of this company , are participating
Systems and Internal Capital Adequacy
assessment
activites in the bank regularly .
Process . The purpose of the

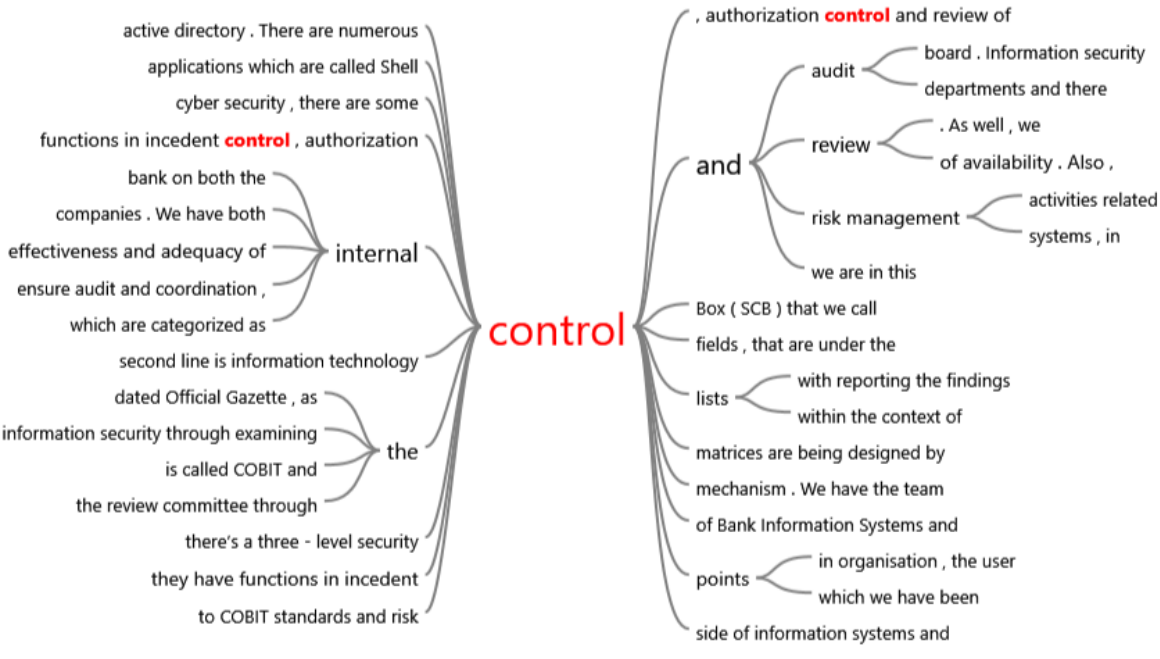
Text Search Query - Results Preview



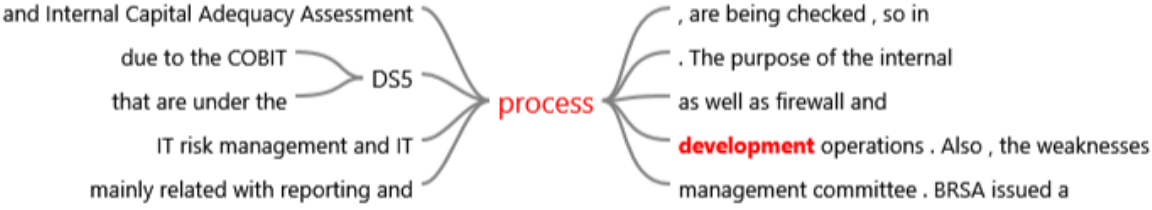
Text Search Query - Results Preview

Text Search Query - Results Preview

Text Search Query - Results Preview

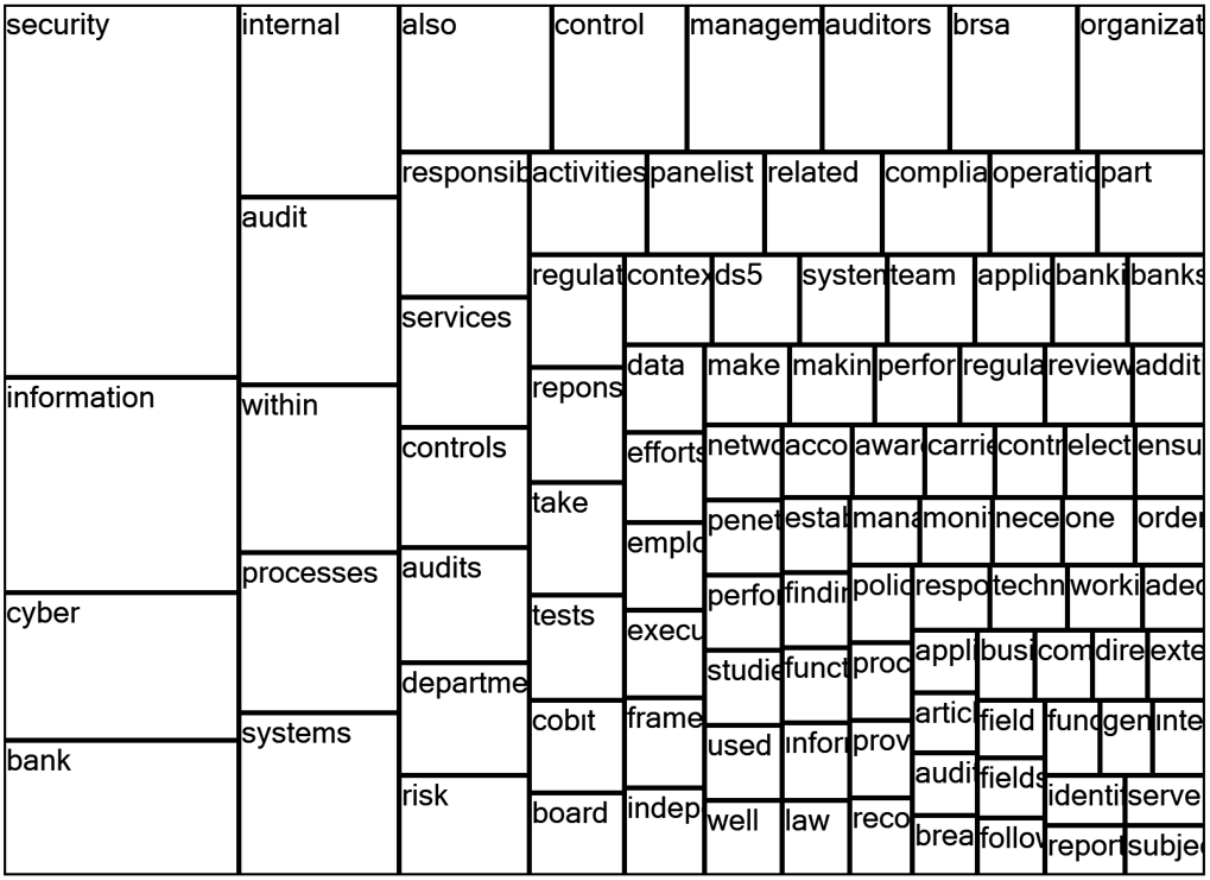


Text Search Query - Results Preview

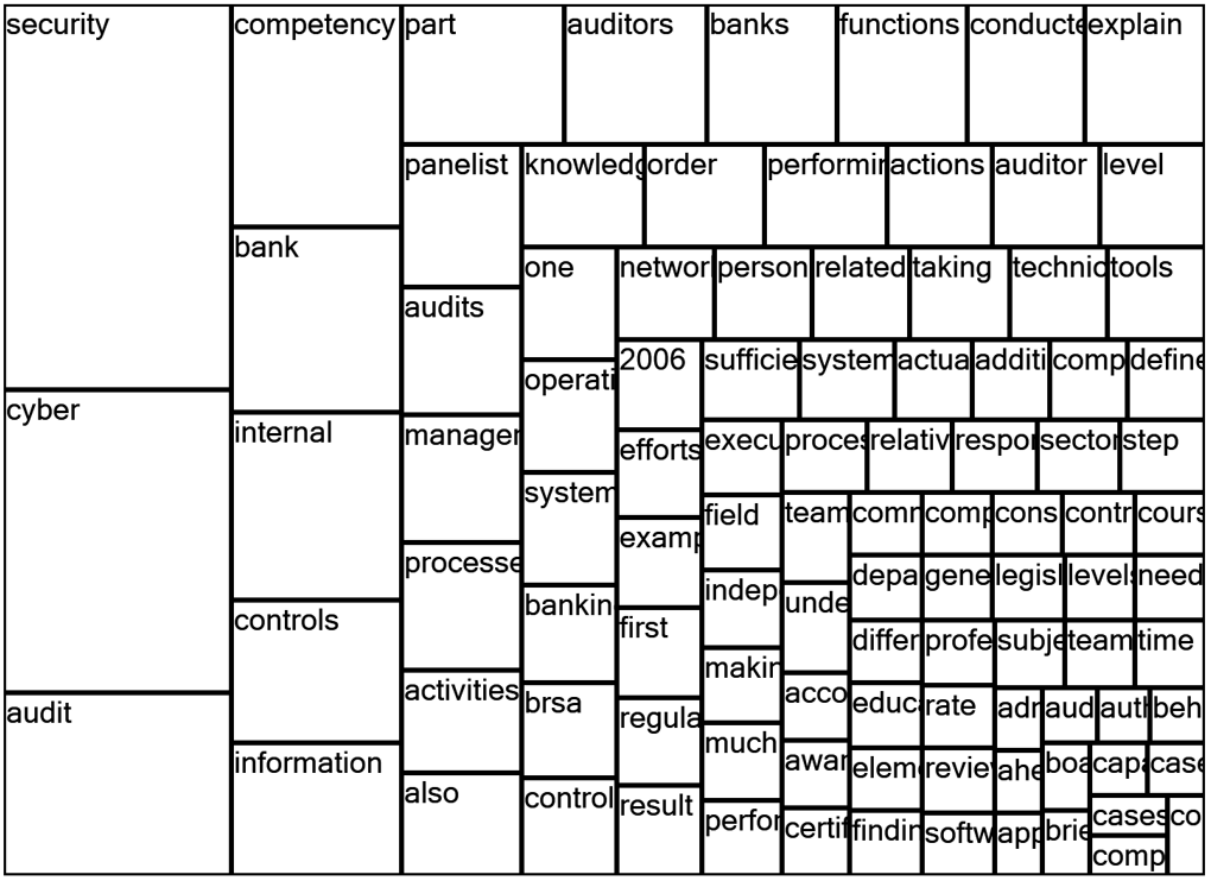


Appendix-9.Tree Maps

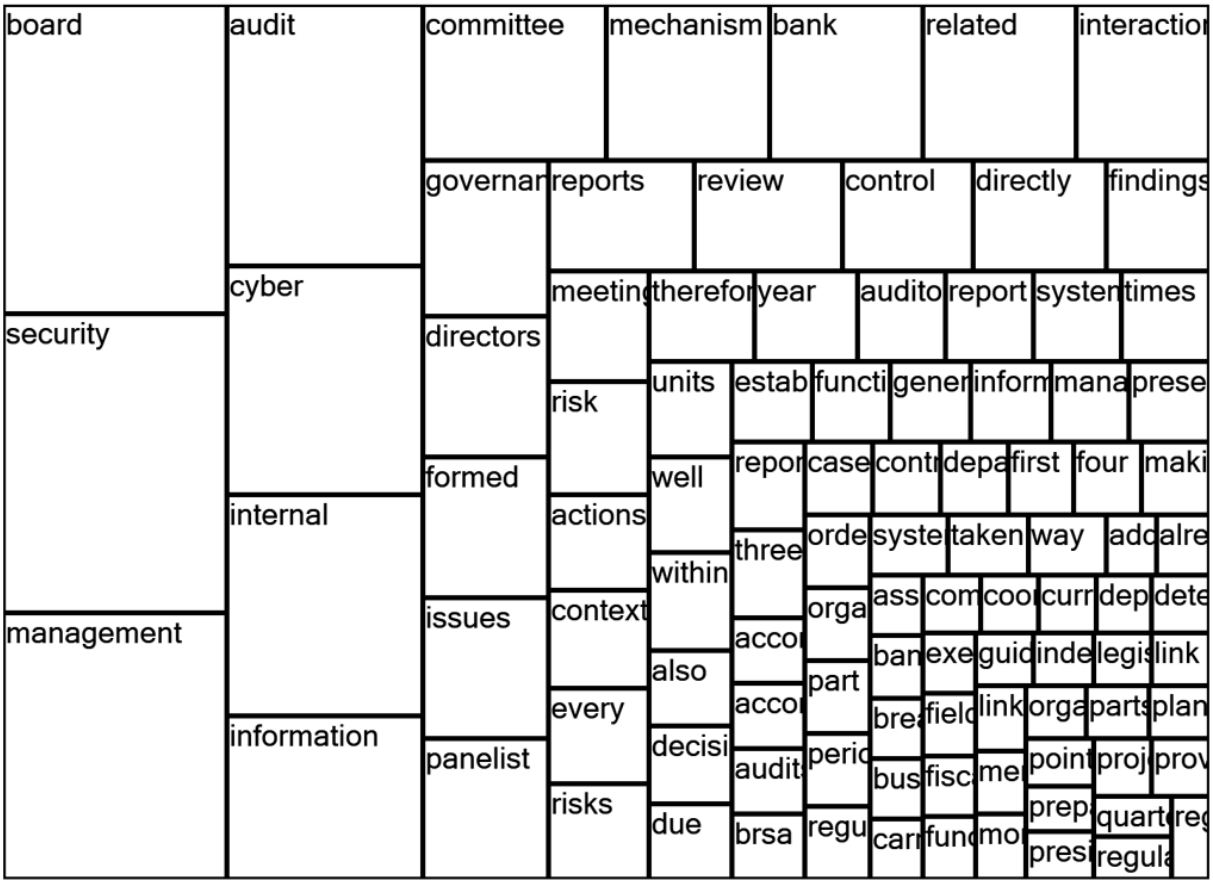
Responsibility



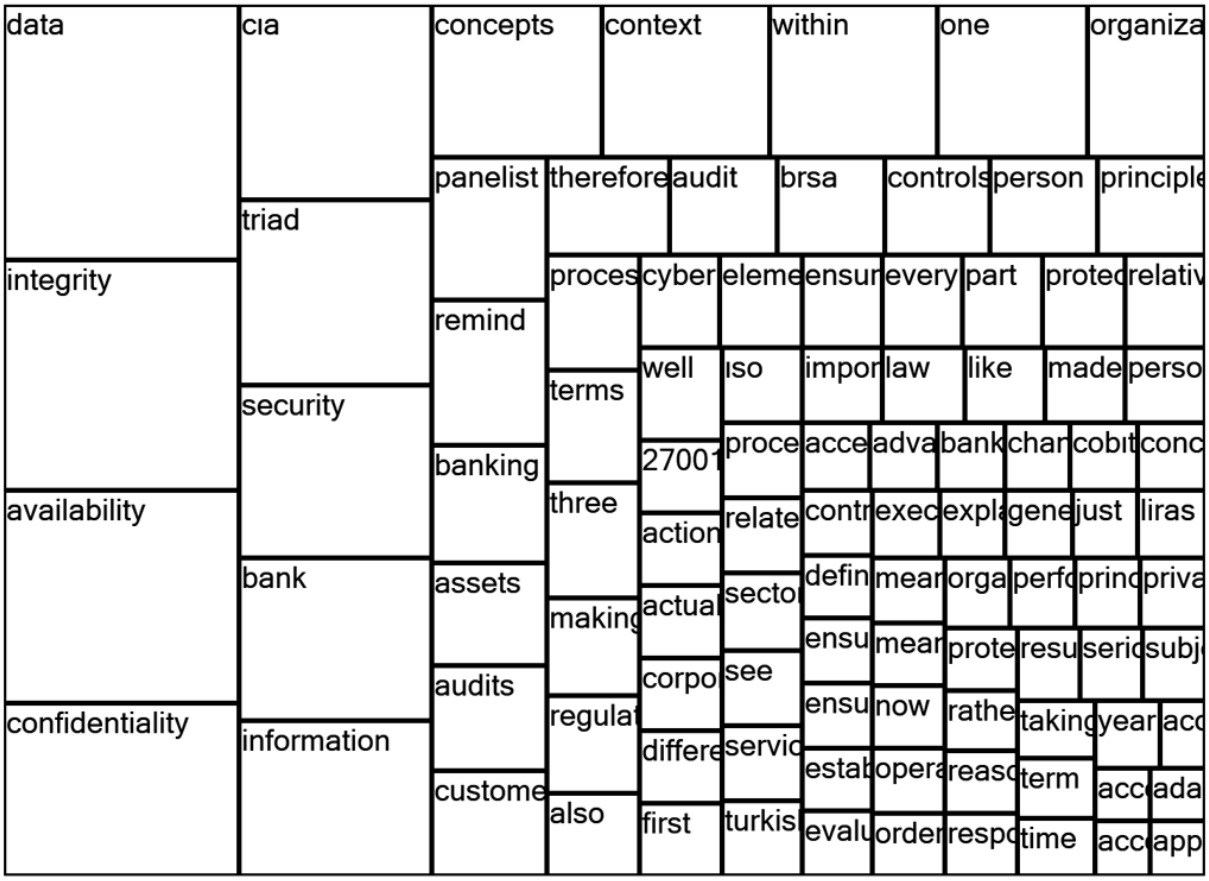
Competency


security
competency
part
auditors
banks
functions
conducte
explain
panelist
knowledg
order
performi
actions
auditor
level
bank
one
networ
person
related
taking
technic
tools
audits
operati
2006
sufficie
system
actua
additi
compl
define
cyber
internal
manager
efforts
execu
proces
relativ
respon
sector
step
system
field
team
comm
comp
cons
contr
cours
examp
depa
gene
legisl
level
need
processe
indep
unde
controls
bankin
first
differ
profe
subje
team
time
makir
acco
activities
brsa
regula
audit
educ
rate
adm
aud
auth
beh
much
awar
information
elem
revie
ahe
boa
capa
case
also
control
result
perfor
certif
findin
softw
app
brie
cases
comp
co

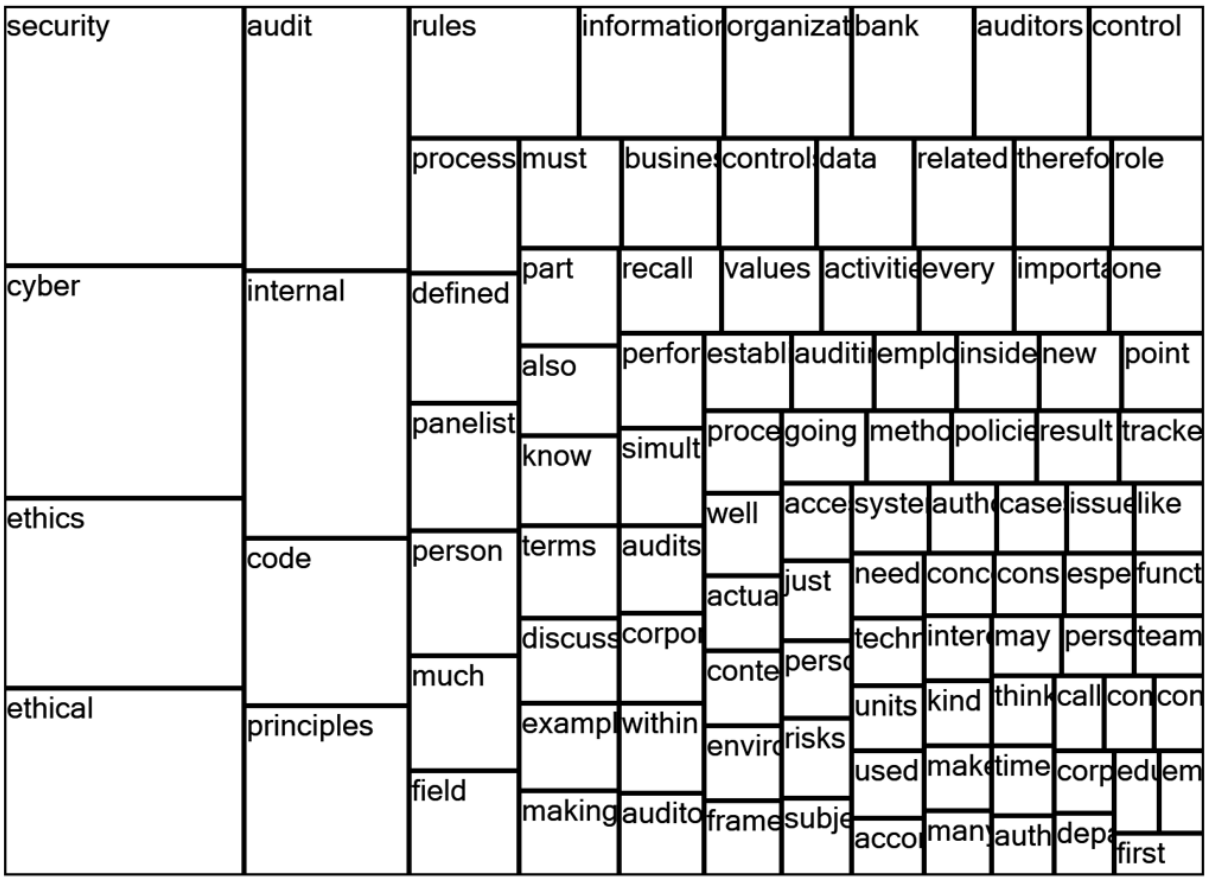
Governance


board
audit
committee
mechanism
bank
related
interactio
governan
reports
review
control
directly
findings
cyber
meeting
therefor
year
audito
report
system
times
security
directors
risk
units
estab
functi
gener
inform
mana
prese
repor
case
contr
depa
first
four
maki
formed
well
internal
actions
three
orde
syste
taken
way
add
alre
within
ass
com
coor
curr
dep
dete
management
issues
context
orga
acco
ban
exe
guid
inde
legis
link
also
part
acco
bre
field
link
orga
parts
plan
every
decisi
peric
point
proj
prov
information
panelist
audit
bus
fisc
mer
prep
quart
risks
due
regu
brsa
carr
func
mor
presi
regula

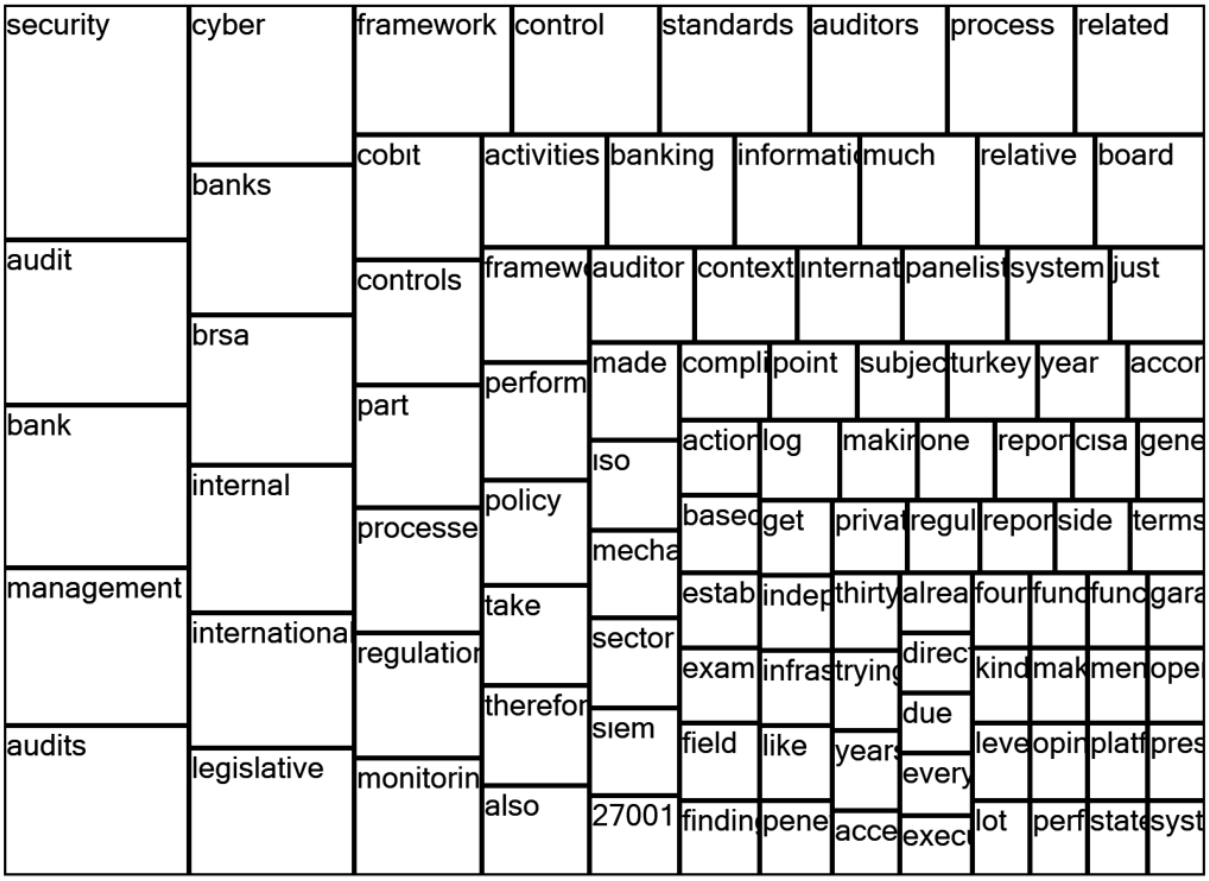
CIA Triad


data
cia
concepts
context
within
one
organiza
panelist
therefore
audit
brsa
controls
person
principle
triad
integrity
proces
cyber
eleme
ensur
every
part
protec
relativ
remind
well
iso
impor
law
like
made
perso
terms
security
proce
acce
adva
bank
char
cobit
conc
banking
27001
three
relate
contr
exec
expla
gene
just
liras
availability
action
defin
mean
orga
perfo
princ
priva
bank
assets
making
actual
secto
ensu
mean
prote
resu
serio
subj
audits
corpo
see
ensu
now
rathe
taking
year
acc
confidentiality
information
regulat
differe
servic
estab
opera
reaso
term
acc
ada
custome
also
first
turkis
evalu
order
respo
time
acc
app

Code of Ethics



Legislation and Policy Framework

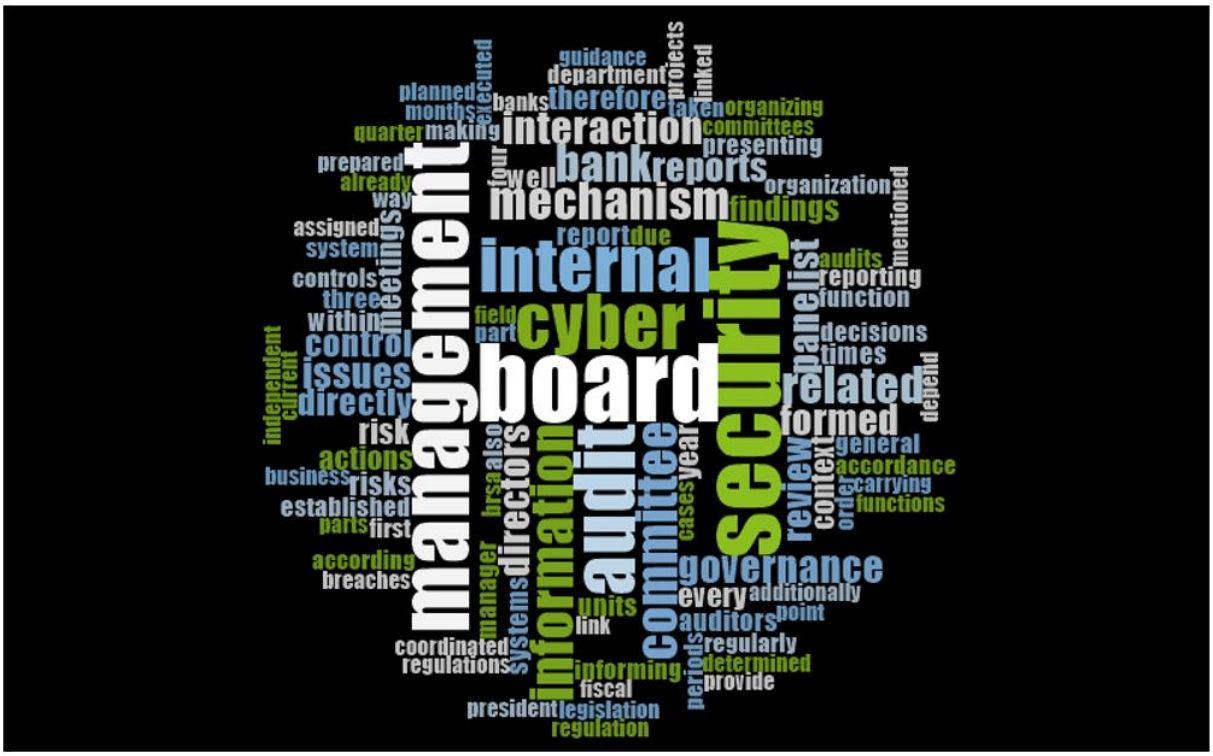


Appendix-10.Word Clouds

Responsibility

Competency

Governance


management
board
internal
security
cyber
audit
committee
information
governance
mechanism
interaction
bank
reports
therefore
related
formed
panelist
review
issues
control
directly
risk
actions
risks
established
according
breaches
meetings
assigned
system
controls
three
within
field
part
report
due
findings
organization
audits
reporting
function
decisions
times
depend
mentioned
independent
current
directors
also
brs
manager
systems
units
link
every
auditors
additionally
point
regularly
determined
provide
periods
informing
fiscal
president
legislation
regulation
coordinated
regulations
cases
year
context
order
carrying
functions
general
accordance
parts
first
business
already
prepared
way
four
well
quarter
making
planned
months
selected
banks
guidance
department
projects
linked
taken
organizing
committees
presenting

CIA Triad

Code of Ethics

Legislation and Policy Framework

Appendix-11.Questionnaire for Second Round of Delphi

1. Sorumluluk	Kesinlikle Katılmıyorum(1)	Katılmıyorum (2)	Kararsızım (3)	Katılıyorum (4)	Kesinlikle Katılıyorum (5)
İç denetim, siber güvenlik kapsamında elde edilen bulguların kapanmasından sonra, gerekli kontrollerin yapılmasında rol alır.					
İç denetim, BDDK'nın 15 Mart 2020'de yayınlamış olduğu yönetmelik çerçevesinde siber güvenliğe ilişkin yıllık kontrollerde bulunmaktadır.					
İç denetim, bağımsız denetim firmalarının gerçekleştirmiş oldukları sızma testi bulgularının kapatıldıktan sonra teyit edilmesi fonksiyonuna sahiptir.					
İç denetim, siber güvenlik kapsamındaki güvenlik açıklarının tespit edilmesinde fonksiyona sahiptir.					
İç denetim, siber güvenlik ile ilgili bulguların genel müdüre veya yönetim kuruluna doğrudan raporlanmasında sorumluluk sahibidir.					

2. Yetkinlik	Kesinlikle Katılmıyorum(1)	Katılmıyorum (2)	Kararsızım (3)	Katılıyorum (4)	Kesinlikle Katılıyorum (5)
İç denetim, BDDK'nın tasarladığı yönetmelikler kapsamında bilgi güvenliğine yönelik hazırlanan kontrol listelerinin denetlenmesi sürecini bilgi teknolojisi denetçilerinden destek alarak yürütmelidir.					
İç denetim, BDDK'nın bilgi sistemleri yönetmeliği doğrultusunda icra etmekte olduğu denetim faaliyetlerini sürdürmek için temel seviyede yazılım bilgisine sahip olmalıdır.					
İç denetim, bağımsız denetim firmalarının gerçekleştirmiş oldukları sızma testi bulgularının kapatıldıktan sonra kontrol edilmesi ve onaylanması süreçlerinde etkin olmak için sistem ve ağ yönetimi bilgisine sahip olmalıdır.					
İç denetim, BDDK'nın tasarladığı yönetmelikler kapsamında bilgi güvenliğine yönelik hazırlanan kontrol listelerinin denetlenmesi					

sürecinde etkin olmak için bilgi güvenliği mimarisi ve altyapısı üzerine teknik düzeyde bilgiye ve yeterli tecrübeye sahibi olmalıdır.					
İç denetim, siber güvenlik kapsamında sürdürdüğü gözetim faaliyetlerinde etkin rol almak için SIEM araçlarını kullanmaya hâkim olmalıdır.					
3. Yönetişim	Kesinlikle Katılmıyorum(1)	Katılmıyorum (2)	Kararsızım (3)	Katılıyorum (4)	Kesinlikle Katılıyorum (5)
İç denetim, yönetim kurulu, genel müdür ve bilgi teknolojileri departmanı arasındaki yönetişimde danışmanlık rolüne sahiptir.					
Siber güvenlik kapsamında faaliyetlerini sürdüren iç denetçilere gerekli eğitimler organize edilmelidir.					
İç denetim, siber güvenlik denetimlerinde doğrudan yetkiye sahip olmalıdır.					
İç denetim, siber güvenlik denetimlerinde danışmanlık rolü ile destekleyici konumundadır.					
İç denetim, siber güvenlik ile ilgili					

vakalarda gerekli bilgilendirmeyi düzenli aralıklar ile üst yönetime yapmakta sorumluluğa sahiptir.					
4. Gizlilik, Bütünlük, Erişilebilirlik	Kesinlikle Katılmıyorum(1)	Katılmıyorum (2)	Kararsızım (3)	Katılıyorum (4)	Kesinlikle Katılıyorum (5)
İç denetim, siber güvenlik kapsamındaki süreçlerde rol alırken denetim kanıtlarını gizlilik, bütünlük ve erişilebilirlik prensiplerine uygun olarak kayıtlara almalı, muhafaza etmeli ve raporlamalıdır.					
İç denetim, siber güvenlik kapsamındaki faaliyetlerini yetki prensibine göre yürütmelidir.					
İç denetim, siber güvenlik kapsamında gerçekleştirdiği faaliyetler sonucu elde ettiği bulguların erişiminin aksamadan gerçekleşmesini sağlamalıdır.					
İç denetim, siber güvenlik kapsamında sürdürdüğü aktivitelerin sonucunda elde ettiği bulguların herhangi bir şekilde değiştirilmediğine					

dair güvence sağlamalıdır.					
İç denetim, siber güvenlik kontrollerinde elde edilen bulguların yetkisi olmayan kişilere iletilmiyor olduğuna dair güvence sağlamalıdır.					
5. Kurumsal Yönetim İlkeleri	Kesinlikle Katılmıyorum(1)	Katılmıyorum (2)	Kararsızım (3)	Katılıyorum (4)	Kesinlikle Katılıyorum (5)
İç denetim, siber güvenlik kapsamındaki fonksiyonlarını gerçekleştirirken yasal çevreyi takip ederek, gerekli bilgilendirmeleri yapmalıdır.					
İç denetim, siber güvenlik kapsamındaki faaliyetlerini sürdürürken yasa dışı herhangi bir sürece dahil olmadan meslek ahlakına uygun biçimde aktivitelerde bulunmalıdır.					
İç denetim, siber güvenlik kapsamındaki faaliyetlerini gerçekleştirirken kurumun etik prensiplerine ve yönetim ilkelerine saygılı bir biçimde işlemlerini yürütmelidir.					
İç denetim ekipleri, siber güvenlik dahilindeki					

süreçlerde rol alırlarken bilgilerine, yetkinliklerine ve tecrübelerine uygun görevleri üstlenmelidirler.					
İç denetim ekipleri, siber güvenlik dahilindeki süreçlerde rol alırlarken kabiliyetlerini, etkinliklerini ve ürettikleri hizmetin kalite seviyesini gelişme sürecindeki teknolojiler doğrultusunda sürekli iyileştirmelidirler.					
6. Etik Kurallar	Kesinlikle Katılmıyorum(1)	Katılmıyorum (2)	Kararsızım (3)	Katılıyorum (4)	Kesinlikle Katılıyorum (5)
Kurumlarda, etik kuralların kesin ve net olarak tanımlandığı ve belirtildiği yazılı dokümanlar olmalıdır.					
Etik kuralların işlerliğinin denetlenmesinde etkin olarak işleyen bir raporlama mekanizması mevcut olmalıdır.					
Etik kuralların, ihlal edilmesi durumunda raporlamanın doğrudan genel müdüre veya yönetim kuruluna yapılması gereklidir.					
İç denetim ve siber güvenlik ekipleri etik kuralların ihlal edilmesine ilişkin					

durumlarda koordineli bir yaklaşımla bulgular elde etmelidirler.					
İç denetim ekipleri kurumların mevzuata uyumluluğunu kontrol ederlerken, yasaların neden yenilendiğini de araştırmalıdırlar.					
7. Yasal ve Uluslararası Politika Çerçevesi	Kesinlikle Katılmıyorum(1)	Katılmıyorum (2)	Kararsızım (3)	Katılıyorum (4)	Kesinlikle Katılıyorum (5)
İç denetim, BDDK'nın oluşturduğu yönetmelik ve uluslararası standartlar kapsamında oluşturulan kontrol listelerinin uyumluluğunu takip etmektedir.					
Türkiye'deki bankacılık sektöründe bilgi güvenliği bağlamında mevzuata uyum çerçevesinde BDDK yönetmeliği, ISO 27001 ve COBIT 4.1 DS5 süreci dikkate alınmaktadır.					
İç denetim, mevzuata uyum çerçevesindeki, gözetim faaliyetlerini sürdürürken tanımladığı kontrol eksikliklerini üst yönetime raporlamaktadır.					

İç denetim ekipleri mevzuata uyumluluğa ilişkin sürdürdükleri faaliyetlerde süreç teftişlerinde bulunmaktadırlar.					
Türkiye'de faaliyet gösteren tüm bankalar BDDK'nın 5411 sayılı bankacılık kanununa göre bilgi sistemlerini yapılandırmaktadırlar.					

1. Responsibility	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
Internal audit has a role in performing necessary controls after the findings are ensured within the context of cyber security.					
The internal audit makes annual controls relating to cyber security in accordance with the regulation which was issued by BRSA on 15 March 2020.					
Internal audit has a function in confirming penetration test findings after the findings are secured.					
Internal audit has a function in the identification of security breaches within the context of cyber security.					
Internal audit has the responsibility of reporting findings directly to the general manager or management board.					
2. Competency					
Internal audit should carry out the auditing process of control lists which are prepared for information security within the scope of the regulations that are designed by BRSA with the support of information technology auditors.					
Internal audit must have a basic level of software knowledge in order to maintain the audit activities which are carried out by BRSA in accordance with the information systems regulation.					
Internal audit must have system and network management knowledge to be effective in the process of controlling and					

confirming the penetration test findings which are carried out by independent audit firms after they are ensured.					
Internal audit must have technical level knowledge and sufficient experience on information security architecture and infrastructure to be effective in the auditing process of control lists that are prepared for information security within the scope of the regulations that are designed by BRSA.					
Internal audit should be a master of using SIEM tools to take an active role in monitoring and surveillance activities within the scope of cyber security.					
3. Governance					
Internal audit has a consultancy role in the governance between the board of directors, general manager, and information technology department.					
Required training events should be organized for internal auditors who are performing specifically in cyber security processes.					
Internal audit must have direct authority for cyber security controls.					
Internal audit has a supportive position in cyber security controls with its advisory role.					
Internal audit has the responsibility for informing the senior management necessarily with regular interval periods in cases related to cyber security.					
4. Confidentiality, Integrity, and Availability					
Internal audit must record, maintain and report audit evidence in accordance with the principles of confidentiality, integrity, and availability when taking part in cyber security processes.					
Internal audit should carry out its activities within the scope of cyber security according to the principle of authority.					
Internal audit should ensure that the access of the findings which are obtained as a result of its activities within the scope of cyber security is realized without disorganization.					
Internal audit should provide assurance that the findings of its activities within the scope of cyber security haven't been modified or altered in any way.					
Internal audits should assure that the findings of cyber security controls are not being transmitted to unauthorized persons.					
5. Corporate Management Principles					

Internal audit should follow the legal environment and provide the necessary reportings while performing its functions within the scope of cyber security.					
Internal audit must act accordantly with the professional ethics of being not involved in any of the illegal actions while sustaining its activities within the scope of cyber security.					
Internal audit should carry out its operations in a manner that respects the ethical principles and management principles of the corporation when performing its activities within the scope of cyber security.					
Internal audit teams must engage tasks in line with their knowledge, competencies, and experiences when they are taking part in cybersecurity-related processes.					
Internal audit teams must continuously improve their capabilities, effectiveness, and quality level of service consistent with emerging technologies while they are taking part in cyber security processes.					
6. Code of Ethics					
Institutions should have written documents in which the ethical rules are defined and specified precisely and clearly.					
There should be a reporting mechanism that effectively operates in the auditing of the functioning of ethical rules.					
In case of violation of the code of ethics, reporting must be made directly to the general manager or the board of directors.					
Internal audit and cyber security teams should get findings through a coordinated approach in cases of violation of ethics.					
Internal audit teams should evaluate why the laws have been being reframed while they are controlling the compliance of institutions with the legislative framework.					
7. Legislative and International Policy Framework					
The internal audit follows the compliance of the control lists which are established within the scope of the regulations that are framed by BRSA and international standards.					
BRSA regulation, ISO 27001, and COBIT 4.1 DS5 processes are taken into consideration within the framework of compliance with legislation in the context of information security for the banking sector of Turkey.					
Internal audit reports the control deficiencies to the senior management which are defined according to the compliance framework while they are performing their monitoring activities.					

Internal audit teams carry out process controls in their activities that are related to compliance with the regulation.					
All banks, which are sustaining their businesses in Turkey, structure their information systems in compliance with the banking law no. 5411 of BRSA.					

Appendix-12.Panelist Responses to Second Round of Delphi

Panelist ID	10	7	2	5	13	12	8	6	1	9	15	3	14	4	11
Statement 1	4	4	4	4	4	5	5	5	5	5	5	4	5	4	4
Statement 2	3	4	4	5	4	5	5	5	4	5	3	5	5	4	4
Statement 3	4	4	3	5	4	3	5	5	5	5	4	5	5	5	5
Statement 4	4	3	4	5	4	5	4	5	4	3	4	5	5	4	4
Statement 5	4	5	4	5	3	5	5	5	5	4	4	5	5	5	4
Statement 6	4	5	5	5	4	5	5	5	4	4	4	5	5	5	4
Statement 7	5	5	3	5	3	5	4	3	4	4	4	3	5	4	4
Statement 8	5	5	3	5	3	5	5	2	4	4	4	3	4	4	4
Statement 9	3	5	4	5	3	5	4	3	4	4	4	3	4	4	4
Statement 10	4	5	3	4	3	5	4	2	4	4	4	2	4	4	5
Statement 11	4	5	4	4	4	4	3	3	3	4	4	5	3	3	2
Statement 12	5	5	4	5	4	5	5	5	4	5	4	5	5	5	4
Statement 13	4	5	4	3	4	4	5	4	2	4	3	3	2	5	4
Statement 14	4	5	4	4	4	4	5	2	4	4	4	3	2	4	4
Statement 15	4	5	4	4	4	5	5	2	2	4	4	4	3	3	4
Statement 16	5	5	5	4	3	5	5	3	5	4	4	4	5	5	4
Statement 17	4	5	5	5	3	5	5	3	4	4	4	4	5	5	4
Statement 18	4	3	4	5	4	5	5	3	4	4	4	4	4	4	4
Statement 19	4	4	4	4	4	5	5	3	5	4	4	4	4	5	4
Statement 20	4	4	5	4	3	5	5	3	5	4	4	4	4	5	4
Statement 21	4	4	4	5	4	5	5	3	4	4	4	4	5	4	4
Statement 22	4	4	5	5	5	5	5	3	5	5	5	4	5	5	4
Statement 23	4	4	5	5	5	5	5	3	5	5	5	4	5	4	4
Statement 24	5	4	4	4	5	5	5	3	4	5	4	4	5	4	4
Statement 25	5	4	4	5	5	5	5	3	4	5	4	4	5	4	4
Statement 26	4	4	5	4	5	5	5	3	4	5	5	4	4	4	4
Statement 27	5	4	5	4	4	5	3	3	4	5	5	4	4	4	4
Statement 28	4	4	5	5	4	5	4	3	4	5	4	4	3	4	4
Statement 29	4	4	4	4	4	5	4	3	4	5	4	4	4	4	4

Statement 30	4	4	4	5	3	5	2	2	2	5	4	4	5	3	4
Statement 31	4	4	4	4	5	5	4	5	4	5	4	4	5	4	4
Statement 32	4	2	4	5	4	5	4	5	4	5	4	4	5	5	4
Statement 33	4	3	4	5	4	5	5	5	4	5	4	4	5	5	4
Statement 34	3	3	4	4	3	5	5	4	4	5	4	4	5	4	4
Statement 35	3	1	5	4	5	5	5	4	4	5	4	4	5	4	4

Appendix-13.Questionnaire for Third Round of Delphi

Yetkinlik	Kesinlikle Katılmıyorum(1)	Katılmıyorum (2)	Kararsızım (3)	Katılıyorum (4)	Kesinlikle Katılıyorum (5)
İç denetim, BDDK'nın bilgi sistemleri yönetmeliği doğrultusunda icra etmekte olduğu denetim faaliyetlerini sürdürmek için temel seviyede yazılım bilgisine sahip olmalıdır.					
İç denetim, bağımsız denetim firmalarının gerçekleştirmiş oldukları sızma testi bulgularının kapatıldıktan sonra kontrol edilmesi ve onaylanması süreçlerinde etkin olmak için sistem ve ağ yönetimi bilgisine sahip olmalıdır.					
İç denetim, BDDK'nın tasarladığı yönetmelikler kapsamında bilgi güvenliğine yönelik hazırlanan kontrol listelerinin denetlenmesi sürecinde etkin olmak için bilgi güvenliği mimarisi ve					

altyapısı üzerine teknik düzeyde bilgiye ve yeterli tecrübeye sahibi olmalıdır.					
İç denetim, siber güvenlik kapsamında sürdürdüğü gözetim faaliyetlerinde etkin rol almak için SIEM araçlarını kullanmaya hâkim olmalıdır.					
Yönetişim					
İç denetim, yönetim kurulu, genel müdür ve bilgi teknolojileri departmanı arasındaki yönetişimde danışmanlık rolüne sahiptir.					
İç denetim, siber güvenlik denetimlerinde doğrudan yetkiye sahip olmalıdır.					
İç denetim, siber güvenlik ile ilgili vakalarda gerekli bilgilendirmeyi düzenli aralıklar ile üst yönetime yapmakta sorumluluğa sahiptir.					
Etik Kurallar					
İç denetim ekipleri kurumların mevzuata uyumluluğunu					

kontrol ederlerken, yasaların neden yenilendiğini de araştırmalıdırlar.					

Competency	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
Internal audit must have a basic level of software knowledge to maintain the audit activities which are carried out by BRSA in accordance with the information systems regulation.					
Internal audit must have system and network management knowledge to be effective in the process of controlling and confirming the penetration test findings which are carried out by independent audit firms after they are ensured.					
Internal audit must have technical level knowledge and sufficient experience on information security architecture and infrastructure to be effective in the auditing process of control lists that are prepared for information security within the scope of the regulations that are designed by BRSA.					
Internal audit should be a master of using SIEM tools to take an active role in monitoring and surveillance activities within the scope of cyber security.					
Governance					

Internal audit has a consultancy role in the governance between the board of directors, general manager, and information technology department.					
Internal audit must have direct authority for cyber security controls.					
Internal audit has the responsibility for informing the senior management necessarily with regular interval periods in cases related to cyber security.					
Code of Ethics					
Internal audit teams should evaluate why the laws have been being reframed while they are controlling the compliance of institutions with the legislative framework.					

Appendix-14.Panelist Responses to Third Round of Delphi

Panelist ID	10	7	2	5	13	12	8	6	1	9	15	3	14	4	11
Statement 7	5	5	4	5	3	5	4	4	4	4	4	3	5	4	4
Statement 8	5	5	4	5	3	5	5	2	4	4	4	3	4	4	4
Statement 9	4	5	4	5	3	5	4	4	4	4	4	3	4	4	4
Statement 10	4	5	4	4	3	5	4	4	4	4	4	2	4	4	5
Statement 11	4	5	4	4	4	4	4	4	3	4	4	5	3	4	2
Statement 13	4	5	4	3	4	4	5	4	2	4	3	3	2	5	4
Statement 15	4	5	4	4	4	5	5	4	2	4	4	4	4	4	4
Statement 30	4	4	4	5	3	5	2	4	2	5	4	4	5	4	4

Panelist ID	Statement 7	Statement 8	Statement 9	Statement 10	Statement 11	Statement 13	Statement 15	Statement 30
10	1	1	0	1	1	1	1	1
7	1	1	1	1	1	1	1	1
2	0	0	1	0	1	1	1	1
5	1	1	1	1	1	1	1	1
13	1	1	1	1	1	1	1	1
12	1	1	1	1	1	1	1	1
8	1	1	1	1	0	1	1	1
6	0	1	0	0	0	1	0	0
1	1	1	1	1	1	1	1	1
9	1	1	1	1	1	1	1	1
15	1	1	1	1	1	1	1	1
3	1	1	1	1	1	1	1	1

14	1	1	1	1	1	1	0	1
4	1	1	1	1	0	1	0	0
11	1	1	1	1	1	1	1	1

(Note: 0 values are showing that changing panelist opinions for the statements in third round. For example, the panelist who has second identity document changed the response from three (neutral) to four (agree) for seventh statement.)