

**BİLGİ TEKNOLOJİLERİNİN İÇ DENETİMDE
YARATTIĞI DEĞİŞİMLER VE İÇ DENETİM
BİRİMLERİNİN DEĞİŞİMLERİ
DEĞERLENDİRMESİNE YÖNELİK İMKB-100
İŞLETMELERİNDE BİR UYGULAMA**

Burcu İŞGÜDEN

(Doktora Tezi)

Eskişehir, 2012

**BİLGİ TEKNOLOJİLERİNİN İÇ DENETİMDE YARATTIĞI DEĞİŞİMLER
VE İÇ DENETİM BİRİMLERİNİN DEĞİŞİMLERİ DEĞERLENDİRMESİNE
YÖNELİK İMKB-100 İŞLETMELERİNDE BİR UYGULAMA**

Burcu İŞGÜDEN

DOKTORA TEZİ

Muhasebe Bilim Dalı

Danışman: Prof. Dr. Saime ÖNCE

Eskişehir

Anadolu Üniversitesi Sosyal Bilimler Enstitüsü

Mart, 2012

JÜRİ VE ENSTİTÜ ONAYI

Burcu İŞGÜDEN'in "Bilgi Teknolojilerinin İç Denetimde Yaratdığı Değişimler ve İç Denetim Birimlerinin Değişimleri Değerlendirmesine Yönelik İMKB-100 İşletmelerinde Bir Uygulama" başlıklı tezi 15 Mart 2012 tarihinde, aşağıdaki jüri tarafından Lisansüstü Eğitim Öğretim ve Sınav Yönetmeliğinin ilgili maddeleri uyarınca, **İşletme (Muhasebe)** Anabilim Dalında Doktora tezi olarak değerlendirilerek kabul edilmiştir.

İmza

Üye (Tez Danışmanı) : Prof.Dr.Saim ÖNCE

Üye : Prof.Dr.Yılmaz BENLİGİRAY

Üye : Prof.Dr.Melih ERDOĞAN

Üye : Doç.Dr.Elif DAĞDEMİR

Üye : Doç.Dr.Hasan ABDİOĞLU

Prof.Dr.B.Zafer ERDOĞAN
Anadolu Üniversitesi
Sosyal Bilimler Enstitüsü Müdürü

Doktora Tez Özü**BİLGİ TEKNOLOJİLERİNİN İÇ DENETİMDE YARATTIĞI DEĞİŞİMLER VE İÇ
DENETİM BİRİMLERİNİN DEĞİŞİMLERİ DEĞERLENDİRMESİNE YÖNELİK
İMKB-100 İŞLETMELERİNDE BİR UYGULAMA****Burcu İŞGÜDEN****Muhasebe Bilim Dalı, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Mart 2012****Danışman: Prof. Dr. Saime ÖNCE**

Gelişen bilgi teknolojileri ortamında gerçekleştirilen işlemlerin güvenilirliğinin sağlanması ve işletmedeki faaliyet alanlarına ilişkin çalışmalara yön verilmesi iç denetimin işlevlerini etkilemiş ve güvence ve danışmanlık hizmetinin ön plana çıkmasına yol açmıştır. İşletmelerde bilgi teknolojilerinin yaygın bir şekilde kullanılması, bu teknolojilerin denetimini de gündeme getirdiğinden, bu yöndeki çalışmalar bağlamında iç denetim birimlerince gerçekleştirilen güvence ve danışmanlık hizmetlerine ihtiyaç daha da artmıştır. Bilgi teknolojilerinde yaşanan gelişmeler iç denetimin etkinliğini artırma çabalarını da ön plana çıkarmıştır. Bu çabalar sayesinde iç denetim faaliyetleri geleneksel denetim yaklaşımından uzaklaşarak bilgi teknolojilerine dayalı çalışma ortamlarının gerektirdiği sürekli denetim, risk odaklı iç denetim ve kontrol özdeğerlendirme gibi yeni yaklaşımlara yönelmiştir. Bilgi teknolojilerindeki gelişmeler işletmenin gerçekleştirdiği faaliyetlerde değişmelere neden olmuş ve işletmenin risklerden korunma ihtiyacını arttırmıştır. Bunun sonucunda iç denetimin faaliyet alanları risk yönetimi, iç kontrol ve kurumsal yönetim alanlarını kapsayacak şekilde genişlemiştir.

Çalışmanın ilk bölümünde, bilgi teknolojileri ve bilgi teknolojileri uygulamalarının iç denetim ile ilişkisi üzerinde durulmaktadır. İkinci bölümde, iç denetim ile ilgili temel bilgilerin yanı sıra güvence ve danışmanlık hizmeti işleviyle birlikte, iç denetim sürecinde uygulanan yaklaşımlar ve iç denetimin gelişen faaliyet alanları ele alınmıştır. Üçüncü bölümde, bilgi teknolojilerindeki değişimlerin iç denetimin işlevlerinden güvence ve danışmanlık hizmetleri ve iç denetim sürecinde yarattığı etkiler incelenmiştir. Dördüncü bölümde bilgi teknolojilerinin iç denetimde yarattığı değişimlerin iç denetim birimleri tarafından değerlendirilmesi amacıyla İMKB-100 işletmelerinde yapılan araştırmanın sonuçlarına yer verilmiştir. Araştırmanın sonuçları, iç denetimin bilgi teknolojilerindeki gelişmelerden etkilendiğini desteklemektedir. Bilgi teknolojilerindeki gelişmeler, iç denetim birimlerinin bu teknolojilerin etkisiyle ortaya çıkan güvence ve danışmanlık işlevini yerine getirmelerini, yeni yaklaşımları benimsemelerini ve faaliyet alanlarının genişlemesini sağlamıştır.

Anahtar Kelimeler: Bilgi Teknolojileri Denetimi, İç denetim, Güvence ve Danışmanlık Hizmetleri, İç Denetim Yaklaşımları, İç Denetimin Faaliyet Alanları.



Abstract

CHANGES IN INTERNAL AUDITING THAT CAUSE INFORMATION TECHNOLOGY AND AN APPLICATION IN ISE-100 BUSINESSES FOR ASSESSING THE CHANGES BY INTERNAL AUDITING DEPARTMENTS

Burcu İŞGÜDEN

Accounting Discipline, Anadolu University, Institution of Social Science, March 2012

Adviser: Prof. Dr. Saime ÖNCE

Ensuring reliability of operations that are performing in the developing information technology environment and conducting studies about areas of activity in the business have effected functions of internal auditing and caused to services of assurance and consulting to loom large. Widespread use of information technology in business because of control of these technology are on the agenda, in the context of studies in this direction, demand of assurance and consulting services performed by internal audit units have increased. Development in information technologies has highlighted the effects of increased effectiveness of internal auditing, too. Through these efforts, internal auditing activities are away from traditional auditing approaches, it has directed towards the new approaches such as continuous auditing, risk based internal auditing and control self-assessment that are necessary for work environment based on information technology. Developments in information technologies have caused changes in the activities carried out by the business and increased the need for protection against business risks. As a result, activity areas of internal auditing have expanded to include areas of risk management, internal control and corporate governance.

In the first part of the study it is focused on information technology and relationship between information technology application and internal auditing. In the second part, it is discussed as well as basic information about internal auditing with assurance and consulting services, approaches applied to internal auditing process and growing activity areas of internal auditing. In the third part, it is examined the effects of changes of information technology in assurance and consulting services of internal auditing functions and internal auditing process. In the fourth part, it is included the result of study that is focused on ISE-100 enterprises for changes internal auditing that cause information technology is assessed by internal auditing department. The results of the study has supported that internal auditing is influenced by developments in information technologies. Developments in information technologies provided to fulfill the function of assurance and consulting, that is emerged with the impact of these technologies, by internal audit units and adopt new approaches. At the same time, activity areas of internal auditing have expanded in businesses that widely use information technologies.

Key Words: Information Technology Auditing, Internal Auditing, Assurance and Consulting Services, Approaches of Internal Auditing, Activity Areas of Internal Auditing.

Önsöz

Bilgi teknolojilerinin iç denetimde yarattığı değişimleri ve iç denetim birimlerinin değişimlere uyumunu incelediğimiz çalışmamızda bilgi, tecrübe ve anlayışıyla yardımlarını esirgemeyen değerli Hocam Sayın Prof. Dr. Saime ÖNCE'ye; çalışmamıza ilişkin anketlerin uygulama aşamasında yardım ve desteklerini esirgemeyen Türkiye İç Denetçiler Enstitüsü Akademik İlişkiler Komitesi Başkanı Ali Kamil UZUN'a ve Türkiye İç Denetçiler Enstitüsü Yayın Kurulu Başkanı Gürdoğan YURTSEVER'e, ayrıca anlayış ve desteklerinden ötürü aileme teşekkürlerimi sunarım.

Burcu İŞGÜDEN

İçindekiler

Jüri ve Enstitü Onayı	ii
Öz	iii
Abstract	iv
Önsöz	v
Özgeçmiş	vi
Tablolar Listesi	xvi
Şekiller Listesi	xxiv
Kısaltmalar Listesi.....	xxv
Giriş	1

Birinci Bölüm

Bilgi Teknolojileri İle Muhasebe Bilgi Sistemi ve İç Denetim İlişkisi

1. Bilgi Teknolojileri	9
1.1. Bilgi Teknolojileri Kavramı.....	9
1.2. Bilgi Teknolojilerinin Yarattığı Uygulamalar.....	10
1.2.1. Elektronik ticaret.....	10
1.2.2. İnternet.....	12
1.2.3. Elektronik veri değişimi	14
1.2.4. Kurumsal kaynak planlaması	14
1.2.5. Elektronik veri işleme	15
1.3. Bilgi Teknolojisi Kontrolleri	15
1.3.1. Genel kontroller.....	16
1.3.2. Uygulama (işlem) kontrolleri.....	17
1.4. Bilgi Teknolojilerinin ve Bilgi Teknolojisi Kontrollerinin İşletmeler Üzerine Etkileri	19

2. Bilgi Teknolojilerinin Yarattığı Uygulamaların Muhasebe Bilgi Sistemi İle İlişkisi	20
2.1. Elektronik Ticaret ve Muhasebe Bilgi Sistemi İlişkisi	23
2.2. İnternet ve Muhasebe Bilgi Sistemi İlişkisi	24
2.3. Elektronik Veri Değişimi ve Muhasebe Bilgi Sistemi İlişkisi	25
2.4. Kurumsal Kaynak Planlaması ve Muhasebe Bilgi Sistemi İlişkisi...	26
2.5. Elektronik Veri İşleme ve Muhasebe Bilgi Sistemi İlişkisi	27
3. Bilgi Teknolojilerinin Yarattığı Uygulamaların İç Denetim İle İlişkisi.....	29
3.1. Elektronik Ticaret ve İç Denetim İlişkisi	31
3.1.1. Elektronik ticaret görevinin anlaşılması ve planlanması...	32
3.1.2. Elektronik ticaret riskleri ve kontrol sorunları	33
3.1.3. Elektronik ticaret faaliyetlerinin denetlenmesi	33
3.2. İnternet ve İç Denetim İlişkisi	35
3.3. Elektronik Veri Değişimi ve İç Denetim İlişkisi	37
3.4. Kurumsal Kaynak Planlaması ve İç Denetim İlişkisi	37
3.5. Elektronik Veri İşleme ve İç Denetim İlişkisi	38

İkinci Bölüm

İç Denetim ve İç Denetimin Değişen Faaliyet Alanları

1. İç Denetim İle İlgili Genel Bilgiler	40
1.1. İç Denetim Kavramı	40
1.1.1. İç denetimin tarihsel gelişimi ve tanımı	41
1.1.2. İç denetimin amaçları	45
1.1.3. İç denetimin önemi	46
1.1.4. İç denetimin faydaları	49
1.2. İç Denetimin İşlevleri	49
1.2.1. Güvence hizmetleri	50
1.2.1.1. Güvence hizmetlerinin tanımı	51
1.2.1.2. Güvence hizmetlerinin türleri	53

1.2.2. Danışmanlık hizmetleri	55
1.2.2.1. Danışmanlık hizmetlerinin tanımı	55
1.2.2.2. Danışmanlık hizmetlerinin alanları	57
1.3. İç Denetimin İlkeleri	60
1.4. İç Denetimin Türleri	60
1.4.1. Finansal denetim	61
1.4.2. Uygunluk denetimi	61
1.4.3. Faaliyet denetimi	62
1.4.4. Bilgi teknolojisi denetimi	62
1.4.5. Sistem denetimi	63
1.5. İç Denetim Planı, Uygulama Süreci ve Raporlama	64
1.6. İç Denetçiler ve Uluslararası İç Denetim Standartları	68
1.6.1. İç denetim mesleğinin kapsamı ve örgütlenmesi	68
1.6.2. İç denetçilerin görevleri	69
1.6.3. İç denetçilerin nitelikleri	71
1.6.4. Uluslararası iç denetim standartları	72
2. İç Denetim Sürecindeki Yaklaşımlar	73
2.1. Geleneksel İç Denetim Yaklaşımı	74
2.2. Sürekli Denetim Yaklaşımı	75
2.2.1. Sürekli denetimin tanımı ve unsurları	76
2.2.2. Sürekli denetimin uygulama süreci	77
2.3. Risk Odaklı İç Denetim Yaklaşımı	79
2.3.1. Risk odaklı iç denetimin tanımı ve unsurları	79
2.3.2. Risk odaklı iç denetimin uygulama süreci	80
2.4. Kontrol Özdeğerlendirme Yaklaşımı	82
2.4.1. Kontrol özdeğerlendirmenin tanımı ve unsurları	82
2.4.2. Kontrol özdeğerlendirmenin uygulama süreci	83
3. İç Denetimin Değişen Faaliyet Alanları	85
3.1. Risk Yönetimi	86
3.1.1. Risk yönetiminin tanımı ve bileşenleri	86

3.1.2. Risk yönetimi ve iç denetim ilişkisi	91
3.2. İç Kontrol Sistemi	93
3.2.1. İç kontrol sisteminin tanımı ve amaçları	93
3.2.2. İç kontrol sisteminde yönetimin ve iç denetçinin sorumluluğu.....	95
3.2.3. İç kontrol sisteminin bileşenleri ve iç denetim ilişkisi	96
3.2.3.1.Kontrol çevresi ve iç denetim ilişkisi	97
3.2.3.2.Risk değerlemesi ve iç denetim ilişkisi	98
3.2.3.3.Kontrol eylemleri ve iç denetim ilişkisi	99
3.2.3.4.Bilgi-iletişim ve iç denetim ilişkisi	99
3.2.3.5.İzleme-gözlem ve iç denetim ilişkisi	100
3.3. Kurumsal Yönetim	101
3.3.1. Kurumsal yönetimin tanımı ve ilkeleri	101
3.3.2. Kurumsal yönetim ve iç denetim ilişkisi	103
3.3.3. Kurumsal yönetim bağlamında yıllık faaliyet raporları ve iç denetim ilişkisi	105

Üçüncü Bölüm

Bilgi Teknolojilerindeki Değişimlerin İç Denetimin İşlevlerindeki ve İç Denetim Sürecindeki Etkileri

1. Bilgi Teknolojilerindeki Değişimlerin İç Denetimin İşlevleri Üzerine Etkileri	107
1.1. Güvence Hizmetlerindeki Değişimler	108
1.1.1. Bilgi teknolojileri ile ilgili güvence hizmetleri	109
1.1.1.1.Webtrust hizmetleri	111
1.1.1.2.Systrust hizmetleri	111
1.1.1.3.Diğer bilgi teknolojileri türlerine ilişkin güvence hizmetleri	111

1.1.2. Güvence hizmetlerinin yerine getirilmesindeki değişimler.....	112
1.1.2.1.Güvence derecesi	112
1.1.2.2.Kanıt türleri ve güvence hizmetleri arasındaki ilişki.....	113
1.1.2.3.Hile araştırmalarında güvencenin yapısı	115
1.2. Danışmanlık Hizmetlerindeki Değişimler	116
1.2.1. Bilgi teknolojilerinin danışmanlık hizmet alanlarına etkisi.....	116
1.2.2. Danışmanlık hizmetlerinin yerine getirilmesindeki değişimler.....	117
1.2.2.1.Güvence ve danışmanlık hizmetlerinin dengelenmesi.....	118
1.2.2.2.Danışmanlık hizmetlerinin beraberinde getirdiği riskler ve ödüller	118
2. Bilgi Teknolojilerindeki Değişimlerin İç Denetim Sürecindeki Etkileri.....	118
2.1. Sürekli Denetim Sürecindeki Etkiler	119
2.1.1. Sürekli denetimin uygulama sürecindeki etkiler	120
2.1.1.1.Sürekli denetim yeteneğinin oluşturulması	122
2.1.1.2.Sürekli denetim uygulamasının planlanması	123
2.1.1.3.Sürekli denetim –gerçek zamanlı muhasebe ilişkisi...	124
2.1.2. Denetim çevresinde meydana gelen değişiklikler	126
2.1.2.1.Sürekli denetimde bilgi güvenliği	126
2.1.2.2.Sürekli denetimin teknolojik uygulanabilirliği	128
2.1.3. Sürekli denetim ve bilgi teknolojileri denetimi	128
2.1.3.1.Bilgisayar destekli denetim teknikleri	129
2.1.3.1.1. Bilgisayar destekli denetim tekniklerinin yapısı ve kullanımı	129
2.1.3.1.2. Bilgisayar destekli denetim tekniklerinin çeşitleri	130

2.1.3.2.Sürekli denetimde kullanılan raporlama dilleri ve bilgi teknolojileri yazılımları	135
2.1.3.2.1. Raporlama dilleri	135
2.1.3.2.2. Bilgi teknolojileri yazılımları	139
2.1.3.3.Bilgi teknolojileri denetimi	139
2.1.3.3.1. Bilgi teknolojileri kontrolleri	140
2.1.3.3.2. Bilgi teknolojilerinin uygulama süreci	143
2.2. Risk Odaklı İç Denetim Sürecindeki Etkiler	144
2.2.1. Risk odaklı iç denetimin uygulama sürecindeki etkiler.....	145
2.2.2. Bilgi teknolojileri riskleri ve etkileri	145
2.2.3. Risk yönetimi ve kurumsal yönetim ile olan ilişkilere etkisi	148
2.2.3.1.Risk yönetimi ile ilişkilere etkisi	148
2.2.3.2.Kurumsal yönetim ile ilişkilere etkisi	150
2.3. Kontrol Özdeğerlendirme Sürecindeki Etkiler	151
2.3.1. Kontrol özdeğerlendirmenin uygulama sürecindeki etkiler	152
2.3.2. İç denetim faaliyetinde kontrol özdeğerlendirmenin rolü...	153

Dördüncü Bölüm

Bilgi Teknolojilerinin İç Denetimde Yarattığı Değişimlerin İç Denetim Birimleri Tarafından Değerlendirilmesi: İMKB-100 Araştırması

1. Araştırmanın Amacı	155
2. Evren ve Örneklem	155
3. Araştırma Yöntemi	156
3.1. Verilerin Toplanması	156

3.2. Anketin Hazırlanması ve Anket Sorularının İçeriği	157
3.3. Araştırma Kısıtları	158
4. Araştırma Soruları	159
5. İstatistiksel Analiz Bulguları ve Yorumlar	159
5.1. Güvenilirlik Analizi ve Verilerin Dağılımı	160
5.2. Demografik Sorular İle İlgili Frekans Analizleri	160
5.3. Çapraz Tablo Analizleri ve Non-Parametrik Testler	161
5.3.1. İç denetim birimi ile ilgili çapraz tablo analizleri ve non-parametrik testler	162
5.3.1.1.İç denetim birimi ile ilgili çapraz tablo analizleri	162
5.3.1.2.İç denetim birimi ile ilgili non-parametrik testler	169
5.3.2. İç denetimin güvence ve danışmanlık hizmetleri ile ilgili çapraz tablo analizleri ve non-parametrik testler	170
5.3.2.1.İç denetimin güvence ve danışmanlık hizmetleri ile ilgili çapraz tablo analizleri	170
5.3.2.2.İç denetimin güvence ve danışmanlık hizmetleri ile ilgili non-parametrik testler	177
5.3.3. İç denetim yaklaşımları ile ilgili çapraz tablo analizleri ve non-parametrik testler	178
5.3.3.1.Sürekli denetim ile ilgili çapraz tablo analizleri ve non-parametrik testler	178
5.3.3.1.1. Sürekli denetim ile ilgili çapraz tablo analizleri.....	178
5.3.3.1.2. Sürekli denetim ile ilgili non-parametrik testler.....	192
5.3.3.2.Risk odaklı iç denetim ile ilgili çapraz tablo analizleri ve non-parametrik testler.....	193

5.3.3.2.1. Risk odaklı iç denetim ile ilgili çapraz tablo analizleri	193
5.3.3.2.2. Risk odaklı iç denetim ile ilgili non-parametrik testler	196
5.3.3.3.Kontrol öz değerlendirme ile ilgili çapraz tablo analizleri ve non-parametrik testler	198
5.3.3.3.1. Kontrol öz değerlendirme ile ilgili çapraz tablo analizleri	198
5.3.3.3.2. Kontrol öz değerlendirme ile ilgili non-parametrik testler	201
5.3.3.4.İç denetim yaklaşımları doğrultusunda iç denetim sürecinde kullanılan araç ve gereçlerle ilgili çapraz tablo analizleri	202
5.3.4. İç denetimin faaliyet alanları ile ilgili çapraz tablo analizleri ve non-parametrik testler	206
5.3.4.1.Risk yönetimi ile ilgili çapraz tablo analizleri ve non-parametrik testler	207
5.3.4.1.1. Risk yönetimi ile ilgili çapraz tablo analizleri	207
5.3.4.1.2. Risk yönetimi ile ilgili non-parametrik testler.....	210
5.3.4.2.İç kontrol ile ilgili çapraz tablo analizleri	213
5.3.4.3.Kurumsal yönetim ile ilgili çapraz tablo analizleri ve non-parametrik testler	215
5.3.4.3.1. Kurumsal yönetim ile ilgili çapraz tablo analizleri.....	215
5.3.4.3.2. Kurumsal yönetim ile ilgili non-parametrik testler	217
5.3.5. Bilgi teknolojileri uygulamaları ile ilgili çapraz tablo analizleri ve non-parametrik testler	220
5.3.5.1.Bilgi teknolojileri uygulamaları ile ilgili çapraz tablo analizleri.....	220

5.3.5.2.Bilgi teknolojileri uygulamaları ile ilgili non-parametrik testler	238
5.3.6. Bilgi teknolojileri denetimi ile ilgili çapraz tablo analizleri ve non-parametrik testler	242
5.3.6.1.Bilgi teknolojileri denetimi ile ilgili çapraz tablo analizleri.....	242
5.3.6.2.Bilgi teknolojileri denetimi ile ilgili non-parametrik testler	249
Genel Değerlendirme ve Sonuç	251
Ekler	258
Kaynakça	303

Tablolar Listesi

Tablo-1. WebTrust ve SysTrust Hizmetlerine İlişkin İlkeler	55
Tablo-2. Bilgi Teknolojisi Denetiminin Yapısı	63
Tablo-3. Diğer Güvence Hizmetleri	112
Tablo-4. Elektronik Bilginin Denetim Kanıtı Olarak Güvenilirliğinin Belirlenmesi	114
Tablo-5. Genel Kontroller ve Uygulama Kontrollerinin Sınıflandırılması.....	142
Tablo-6. Ankete Katılanların İşletmedeki Konumları*Güvence Hizmetlerinin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler	162
Tablo-7. Ankete Katılanların İşletmedeki Konumları*Danışmanlık Hizmetlerinin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler.....	163
Tablo-8. Ankete Katılanların İşletmedeki Konumları*İç kontrol Sistemini İzleme ve İncelemenin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler	163
Tablo-9. Ankete Katılanların İşletmedeki Konumları*Risk Yönetimin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler	164
Tablo-10. Ankete Katılanların İşletmedeki Konumları*Kurumsal Yönetimin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler	164
Tablo-11. Ankete Katılanların İşletmedeki Konumları*Finansal Denetimin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler	165
Tablo-12. Ankete Katılanların İşletmedeki Konumları*Uygunluk Denetiminin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler	166
Tablo-13. Ankete Katılanların İşletmedeki Konumları*Faaliyet Denetiminin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler	166
Tablo-14. Ankete Katılanların İşletmedeki Konumları*Bilgi Teknolojileri Denetiminin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler	167

Tablo-15. Ankete Katılanların İşletmedeki Konumları*Sistem Denetiminin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler	167
Tablo-16. Ankete Katılanların Konumları*İç Denetim Görevini Yerine Getirirken Karşılaşılan Zorluklar	168
Tablo-17. Ankete Katılanların Konumları*Yerine Getirilen Güvence Hizmetlerinin Türleri	170
Tablo-18. Ankete Katılanların Konumları*Güvence Sağlamada Kullanılan Yöntemler	172
Tablo-19. Ankete Katılanların Konumları*İç Denetim Biriminin Güvence Hizmetlerini Verebilmesi İçin Yerine Getirmesi Gereken Faaliyetler..	173
Tablo-20. Ankete Katılanların Konumları*Yerine Getirilen Danışmanlık Hizmetleri.....	174
Tablo-21. Ankete Katılanların Konumları ile İç Denetim Biriminin Danışmanlık Hizmetlerini Verebilmesi İçin Yerine Getirmesi Gereken Faaliyetler..	176
Tablo-22. Ankete Katılanların İşletmedeki Konumları*Sürekli Denetimin Uygulama Durumu	178
Tablo-23. Bilgi Teknolojileri Denetiminin Uygulandığı Süre*Sürekli Denetim Uygulama Durumu	179
Tablo-24. İç Denetim Biriminin Faaliyette Bulunduğu Süre*Sürekli Denetim Uygulama Durumu	179
Tablo-25. Ankete Katılanların İşletmedeki Konumları*Sürekli Denetim Yaklaşımının Uygulanmama Nedenleri.....	180
Tablo-26. Ankete Katılanların İşletmedeki Konumları*Sürekli Denetim Yaklaşımının Uygulanmasındaki Temel Amaçlar	181
Tablo-27. Ankete Katılanların Konumları*Sürekli Denetimin Fayda Sağladığı Alanlar.....	183
Tablo-28. Ankete Katılanların İşletmedeki Konumları*Sürekli Denetimi Desteklemek Amacıyla İşletmedeki BT Kullanımının Yaygınlığı	184
Tablo-29. Ankete Katılanların İşletmedeki Konumları*Sürekli Denetimde Kullanılma BT'nin Kullanım Amacı	185
Tablo-30. Ankete Katılanların İşletmelerindeki Konumları*Sürekli Denetimde Veri Analizinin Kullanım Yeri	186

Tablo-31. Ankete Katılanların Konumları*Sürekli İzleme Faaliyetinde BT Kullanımı.....	187
Tablo-32. Ankete Katılanların Konumları*Sürekli İzleme Kontrollerinin Uygulama Durumları	187
Tablo-33. Ankete Katılanların İşletmedeki Konumları*Veri Bulma, Veri Analizi ve Sürekli Denetim Sürecinde Kullanılan Yazılımlar	189
Tablo-34. Ankete Katılanların İşletmedeki Konumları*XBRL Kullanımı	190
Tablo-35. XBRL kullananlar*İşletmede XBRL Kullanılan Süreçler	190
Tablo-36. Ankete Katılanların İşletmedeki Konumları*XBRL'nin Kullanmama Nedenleri	191
Tablo-37. Ankete Katılanların İşletmelerindeki Konumları*XBRL İle İlgili Bilmek İstenilen veya Bilinmesi Gereken Bilgiler	192
Tablo-38. Ankete Katılanların İşletmedeki Konumları*Risk Odaklı İç Denetim Yaklaşımının Uygulanması	194
Tablo-39. Ankete Katılanların Konumları*Risk Odaklı İç Denetim Yaklaşımının Bileşenleri	195
Tablo-40. Ankete Katılanların İşletmedeki Konumları*Kontrol Özdeğerlendirme Yaklaşımının Uygulanması	198
Tablo-41. Ankete Katılanların Konumları*Kontrol Öz Değerlendirme Yaklaşımının Uygulanma Nedenleri	199
Tablo-42. Ankete Katılanların Konumları*Kontrol Öz Değerlendirme Yaklaşımı Uygulamama Nedenleri	200
Tablo-43. Ankete Katılanların Konumları*Kontrol Oz Değerlendirme Yaklaşımı Türleri	200
Tablo-44. Ankete Katılanların Konumları*İç Denetim Faaliyetinde Kullanılan Araç ve Teknikler (Şimdi)	203
Tablo-45. Ankete Katılanların Konumları*İç Denetim Faaliyetinde Kullanılan Araç ve Teknikler (Gelecekte)	205
Tablo-46. Ankete Katılanların Konumları*İşletmelerinde Risk Yönetimi Uygulama Durumu	207
Tablo-47. Ankete Katılanların Konumları*Risk Yönetimi Bileşenleri	208

Tablo-48. Ankete Katılanların Konumları*İç Kontrol Sistemlerinde BT Kontrollerinin Durumu	214
Tablo-49. Ankete Katılanların İşletmedeki Konumları*Kurumsal Yönetim Kapsamında İç Denetimin Rolü	216
Tablo-50. Ankete Katılanların İşletmedeki Konumları* BT Kullananlar	220
Tablo-51. Ankete Katılanların İşletmedeki Konumları*İnternetin Geçmişteki ve Şimdiki Kullanımı	221
Tablo-52. Ankete Katılanların İşletmedeki Konumları*İntranetin Geçmişteki ve Şimdiki Kullanımı	222
Tablo-53. Ankete Katılanların İşletmedeki Konumları*Extranetin Geçmişteki ve Şimdiki Kullanımı	222
Tablo-54. Ankete Katılanların İşletmedeki Konumları*Elektronik Veri Değişiminin Geçmişteki ve Şimdiki Kullanımı	223
Tablo-55. Ankete Katılanların İşletmedeki Konumları*Elektronik Ticaretin Geçmişteki ve Şimdiki Kullanımı	224
Tablo-56. Ankete Katılanların İşletmedeki Konumları*Kurumsal Kaynak Planlamasının Geçmişteki ve Şimdiki Kullanımı	224
Tablo-57. Ankete Katılanların İşletmedeki Konumları*Elektronik Veri İşlemenin Geçmişteki ve Şimdiki Kullanımı	225
Tablo-58. Ankete Katılanların İşletmedeki Konumları*E-ticaret-İç Denetim İlişkisi.....	226
Tablo-59. Ankete Katılanların İşletmedeki Konumları*İnternet-İç Denetim İlişkisi.....	228
Tablo-60. Ankete Katılanların İşletmedeki Konumları*Elektronik Veri Değişimi-İç Denetim İlişkisi	230
Tablo-61. Ankete Katılanların İşletmedeki Konumları*Kurumsal Kaynak Planlaması-İç Denetim İlişkisi	231
Tablo-62. Ankete Katılanların İşletmedeki Konumları*Elektronik Veri İşleme-İç Denetim İlişkisi	233
Tablo-63. Ankete Katılanların Konumları* BT'nin Değerlendirilmesi Sırasındaki Uygulamalar	235

Tablo-64. Ankete Katılanların İşletmedeki Konumları*BT Kontrollerinin Performansı.....	236
Tablo-65. Ankete Katılanların İşletmedeki Konumları*BT Kullanımının Artmasını Engellenen Durumlar	237
Tablo-66. Ankete Katılanların İşletmedeki Konumları*BT Denetiminin Uygulandığı Süre	242
Tablo-67. Ankete Katılanların İşletmedeki Konumları*BT Denetiminin Yapılma Gerekliliğine İlişkin Nedenler	243
Tablo-68. Ankete Katılanların İşletmelerindeki Konumları*İç Denetim Planlama Faaliyetlerinin BT Denetimini Kapsama Durumu	244
Tablo-69. Ankete Katılanların Konumları*BT Denetiminin Etkinliği	245
Tablo-70. Sürekli Denetimin Uygulanma Durumu*BT Denetim Faaliyetlerinin Etkinliği	246
Tablo-71. Sürekli İzleme Gerçekleştirmek Amacıyla BT Kullanımı*BT Denetimi Faaliyetlerinin Etkinliği	246
Tablo-72. Ankete Katılanların Konumları*BT Denetimini Etkileyen Konular	247
Tablo-73. Ankete Katılanların Konumları*BT Denetiminin Uygulanmasını Kolaylaştıran Teknolojik Yenilikler	248
Tablo-74. Ankete Cevap Verenlerin ve Çalıştıkları İşletmelerin Demografik Özellikleri.....	259
Tablo-75. Ankete Katılanların İşletmedeki Konumları ile İç Denetim Biriminin İç Denetimin İşlevleri, Faaliyet Alanları ve Türleri Açısından Gelecekteki Durumunda Meydana Gelen Değişimlerin Değerlendirilmesinin Kruskal-Wallis Testi Sonuçları.....	260
Tablo-76. Ankete Katılanların İşletmedeki Konumları ile Sürekli Denetimin Kullanımındaki Temel Amaçlar Arasında Kruskal-Wallis Testi Sonuçları	261
Tablo-77. Ankete Katılanların İşletmedeki Konumları ile Sürekli Denetimde Kullanılma BT'nin Kullanım Amacı Arasında Kruskal-Wallis Testi Sonuçları	261

Tablo-78. Ankete Katılanların İşletmedeki Çalışma Süreleri Ve Sürekli Denetimde BT Kullanım Amacı Spearman's Rank Order Korelasyonu	261
Tablo-79. BT Kullanan İç Denetim Personeli Sayısı ile Risk Odaklı İç Denetim Yaklaşımı Bileşenleri Arasında Kruskal-Wallis Testi Sonuçları.....	262
Tablo-80. İç Denetim Biriminin Faaliyet Gösterdiği Süre ve Risk Odaklı İç Denetim Yaklaşımı Bileşenleri Spearman's Rank Order Korelasyonu.....	263
Tablo-81. İşletmedeki Çalışma Süresi ve Kontrol Özdeğerlendirme Yaklaşımının Uygulanma Nedenleri Spearman's Rank Order Korelasyonu	263
Tablo-82. BT Denetiminin Uygulandığı Süre ile Risk Yönetimi Bileşenleri Arasında Kruskal-Wallis Testi Sonuçları	263
Tablo-83. BT Kullanan İç Denetim Personeli Sayısı ile Risk Bileşenleri Arasında Kruskal-Wallis Testi Sonuçları	264
Tablo-84. İç Denetim Biriminin Faaliyet Gösterdiği Süre ve Risk Yönetimi Bileşenleri Spearman's Rank Order Korelasyonu	265
Tablo-85. BT Kullanan İç Denetim Personeli Sayısı ve Risk Yönetimi Bileşenleri Spearman's Rank Order Korelasyonu	265
Tablo-86. BT Denetiminin Uygulandığı Süre İle Kurumsal Yönetim Kapsamında İç Denetimin Rolü Açısından Kruskal-Wallis Testi Sonuçları	266
Tablo-87. İç Denetim Biriminin Faaliyet Gösterdiği Süre ve Kurumsal Yönetim Spearman's Rank Order Korelasyonu	267
Tablo-88. BT Kullanan İç Denetim Personeli Sayısı ve Kurumsal Yönetim Spearman's Rank Order Korelasyonu	267
Tablo-89. BT Denetiminin Uygulandığı Süre ve Kurumsal Yönetim Spearman's Rank Order Korelasyonu	267
Tablo-90. Ankete Katılanların İşletmedeki Konumları İle Bilgi Teknolojilerinin Geçmişteki Kullanımı Arasında Kruskal-Wallis Testi Sonuçları	268

Tablo-91. Ankete Katılanların Yaşları ile E-ticaret ve İç Denetim İlişğine Yönelik Katılım Düzeyleri Arasında Kruskal-Wallis Testi Sonuçları...	269
Tablo-92. Ankete Katılanların Yaşları ile İnternet ile İç Denetim İlişğine Yönelik Katılım Düzeyleri Arasında Kruskal-Wallis Testi Sonuçları...	270
Tablo-93. Ankete Katılanların İşletmedeki Konumları ile Elektronik Veri Değişimi ile İç Denetim İlişğine Yönelik Katılım Düzeyleri Arasında Kruskal-Wallis Testi Sonuçları	271
Tablo-94. Ankete Katılanların İşletmedeki Konumları ile Kurumsal Kaynak Planlaması ile İç Denetim İlişğine Yönelik Katılım Düzeyleri Arasında Kruskal-Wallis Testi Sonuçları	272
Tablo-95. Ankete Katılanların İşletmedeki Konumları ile Elektronik Veri İşleme ile İç Denetim İlişğine Yönelik Katılım Düzeyleri Arasında Kruskal-Wallis Testi Sonuçları.....	272
Tablo-96. BT Kullanan İç Denetim Personeli Sayısı ve BT Uygulamaları Spearman's Rank Order Korelasyonu	273
Tablo-97. BT Denetiminin Uygulandığı Süre ve BT Uygulamaları Spearman's Rank Order Korelasyonu	273
Tablo-98. Ankete Katılanların İşletmedeki Konumları ile BT Denetiminin Yapılmasının Nedenleri Arasında Kruskal-Wallis Testi Sonuçları	273
Tablo-99. BT Denetiminin Uygulandığı Süre ile BT Denetiminin Yapılmasının Nedenleri Arasında Kruskal-Wallis Testi Sonuçları	274
Tablo-100. Ankete Katılanların Konumları ile Bilgi Teknolojileri Denetiminin Etkinliğinin Değerlendirilmesi Arasında Kruskal-Wallis Testi Sonuçları	274
Tablo-101. Bilgi Teknolojileri Denetimin Yapıldığı Süre ile Bilgi Teknolojileri Denetiminin Etkinliğinin Değerlendirilmesi Arasında Kruskal-Wallis Testi Sonuçları.....	274
Tablo-102. İç Denetim Biriminin Faaliyet Gösterdiği Süre ve BT Denetimi Etkinliği Spearman's Rank Order Korelasyonu	275
Tablo-103. BT Kullanan İç Denetim Personeli Sayısı ve BT Denetiminin Etkinliği Spearman's Rank Order Korelasyonu	275

Tablo-104. BT Denetiminin Uygulandığı Süre ve BT Denetiminin Etkinliği Spearman's Rank Order Korelasyonu	275
Tablo-105. Anket Sorularının Normal Dağılım Varsayımı Testi-Kolmogorov- Smirnov Testi	275

Şekiller Listesi

Şekil-1. Elektronik Veri İşleme	28
Şekil-2. Güvence Hizmetlerinde Taraflar ve İlişkiler	52
Şekil-3. Danışmanlık Hizmetinde Taraflar ve İlişkiler	56
Şekil-4. Risk Yönetimi Çerçevesi	87
Şekil-5. Kurumsal Yönetimde İç Denetimin Rolü	104
Şekil-6. XBRL Veri Akışı	137

Kısaltmalar Listesi

- AICPA:** American Institute of Certified Public Accountants (Amerika Mali Müşavirler Birliği)
- BDDT:** Bilgisayar Destekli Denetim Teknikleri
- COBIT:** Control Objectives For Information And Related Technology (Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri)
- COSO:** Committee of Sponsoring Organisations of the Treadway Comission (Treadway Komisyonu Sponsor Organizasyonlar Komitesi)
- ECIA:** European Confederation of Instituon of Internal Auditors (Avrupa İç Denetçiler Enstitüleri Konfederasyonu)
- EDI:** Electronic Data Interchange (Elektronik Veri Değişimi)
- ERP:** Enterprise Resource Planning (Kurumsal Kaynak Planlama)
- HTML:** HyperText Markup Language (Hareketli-Metin İşaretleme Dili)
- IIA:** The Instituon of Internal Auditors (İç Denetçiler Enstitüsü)
- INTOSAI:** International Organization of Supreme Audit Institutions (Uluslararası Yüksek Denetleme Kuruluşları Örgütü)
- OECD:** Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Gelişme Örgütü)
- SQL:** Structured Query Language (Yapısal Sorgulama Dili)
- TİDE:** Türkiye İç Denetçiler Enstitüsü
- UN-CEFACT:** The United Nations Centre for Trade Facilitation and Electronic Business (Birleşmiş Milletler Yönetim, Ticaret ve Ulaştırma Usullerini Kolaylaştırma Merkezi)
- WTO:** World Trade Organization (Dünya Ticaret Örgütü)
- XBRL:** Extensible Business Reporting Language (Genişletilebilir İşletme Raporlama Dili)
- XBRL FR:** XBRL Financial Reporting (Finansal Raporlama Taksonomisi)
- XBRL GL:** XBRL General Ledger (Büyük Defter Taksonomisi)
- XML:** Extensible Markup Language (Genişletilebilir İşaretleme Dili)

Giriş

Teknolojide meydana gelen değişiklikler günümüz dünyasını birçok açıdan dönüşümler içine sokmuştur. Gelişen ve değişen dünya içinde teknolojinin yaratmış olduğu imkanlar, küreselleşmeyle birlikte dünyayı daha küçültmekte, ticaret ağlarını genişletmekte ve işletmelerin çalışma şekillerini değiştirmektedir. İşletmeler bu değişim sürecinin içinde kaçınılmaz bir şekilde yer almakta, bu sürecin oluşumuna katkıda bulunmakta ve bu sürece uyum sağlamaktadırlar. Konu işletmeler açısından ele alındığında, yaratılan katma değer sonuçları paydaşlar açısından olduğu kadar bilgi kullanıcıları açısından da önem arz etmekte ve izlenmektedir. Duyarlılığın arttığı, etkileşimin ön planda yer aldığı ve neden-sonuç ilişkisinin geniş bir alanı etkilediği ortamda işletmelerin almış oldukları kararların izlenmesi ve değerlendirilmesi denetim açısından oldukça önem taşımaktadır.

Bilgi teknolojileri işletmelerin ticari faaliyetlerini elektronik olarak yönetmelerine ve finansal tablolarını gerçek zamanlı sistem üzerinden hazırlamalarına imkan sağlamaktadır. Gerçek zamanlı muhasebe sistemleri sayesinde birçok finansal bilgi ve denetimle ilgili kanıt elektronik biçimde saklanmaktadır. Günümüzde denetim süreci, fiziki belgeleme ile yapılan muhasebe sisteminin geleneksel olarak denetlenmesinden, bilgisayarla gerçekleştirilen denetim yöntemlerine doğru kaymıştır. Bilgi teknolojilerindeki yeni gelişmeler denetçilerin, meydana gelmiş finansal tablo hatalarını ortadan kaldırmaya yönelik düzeltici eylemler yerine, finansal tablolardaki hatalara karşı önleyici ve caydırıcı eylemlere yönelmesine ve hata olduğu anda müdahale edebilen sürekli denetim uygulamalarını yerine getirmelerine olanak sağlamaktadır.

Son yıllarda, giderek karmaşıklaşan ekonomik çevre, hızla gelişen teknoloji ve elektronik ticaretin oluşturduğu asıl riskler, işletmeleri iç denetim faaliyeti açısından çeşitli güçlüklerle karşı karşıya bırakmıştır. Özellikle bilgi teknolojilerinde yaşanan gelişmeler, iç denetçilerin iç kontrolün etkililiğini değerlendirme konusundaki bilgi ve becerilerini geliştirmesini gerektirmiştir. İç kontrol ise, faaliyetlerin verimliliğini sağlama ve finansal rapor hazırlama işleminin güvenilirliğine yönelik kalite güvencesinin sağlanması amacıyla iç denetim işlevinin odak noktası haline gelmiştir (Spira ve Page, 2003: 657).

Bilgi teknolojileri uygulamaları, denetim alanında meydana gelen değişimlerde etkili olmakta ve bu değişimleri çabuklaştırmaktadır. Bilgi teknolojilerindeki değişim özellikle elektronik ticaret, elektronik veri değişimi ve internet gibi uygulamalar vasıtasıyla işletmedeki işlem süreçlerini ve iç denetim alanını etkileyen önemli değişimler yaratmıştır (Rezaee, Elam ve Sharbatoghlie, 2001: 150). Elektronik veri değişimi sayesinde iş görünümü değişmiş, güvence olarak doğrulama ve gizlilik kaygıları çözülerek daha fazla işletme internet ortamına katılmıştır. İşletmelerin finansal bilgileri internet üzerinden yayınlamalarında meydana gelen artış, kağıt üzerindeki denetim politikalarını ortadan kaldırmakta ve denetçilerin yeni denetim teknolojilerini benimsemelerini gerektirmektedir. Bilgi teknolojilerindeki ilerlemeler, denetim sürecinin niteliğini, zamanlamasını ve kapsamını değiştirerek, sürekli denetim fikrini yapılabilir olmaktan çok gerekli olmaya doğru götürmektedir (Kurnaz ve Çetinoğlu, 2010: 192).

Bilgi teknolojileri ve elektronik ticaret ortamına ilişkin riskler ve bu risklerin tanımlanması, iç denetimin kapsamındaki ciddi kaygılar arasında yer almaktadır. İşletme eylemlerinin giderek daha fazla şekilde elektronik veri işlemeye (EDP–Electronic Data Processing) dayanması, iç denetim faaliyetinin çeşitli risklerle karşı karşıya kalmasına neden olmuştur. İşletme faaliyetleri, elektronik veri işleme ve çevrimiçi işlem gibi uygulamaların ortaya çıkmasına bağlı olarak değişim göstermiştir. Bu uygulamalar, yetkisiz ticari işlemleri ortaya çıkarmakta veya önemli derecede hatalı mali tabloların oluşmasına neden olarak asıl risk faktörlerini beraberinde getirmektedir. İç denetimin etkinliğini arttırmak açısından finansal duruma ve işletme faaliyetlerine ilişkin risklerin zamanında engellenmesini ya da tespit edilmesini sağlamak denetim planı stratejisinin daha fazla dikkate alınması ile mümkün olacaktır (Ahmed, 2007: 9). Bilgi teknolojileri ile ilgili geliştirilen yazılımlar iç denetçilerin birçok denetim prosedürünü çevrimiçi (on-line) olarak gerçekleştirmesine imkan sağlamakta ve bilgisayarların bellek kapasitelerinin yeterliliği sayesinde birçok işlem elektronik olarak gerçekleştirilebilmektedir. Özellikle elektronik veri değişimi gibi teknolojiler geleneksel denetim izlerini kaybetmekte ve kağıt çıktılarına dayalı denetim sürecini tamamen değiştirmektedir (Bierstaker, Burnaby ve Thibodeau, 2001: 159).

Çağdaş iç denetim uygulamalarında, iç denetimin sorumluluk üstlendiği alanları, danışmanlık ve güvence hizmetlerini ve son bir kaç yılda mesleki faaliyet alanını

genişleten değişimler yaşanmıştır. Profesyonel anlamda çağdaş iç denetim uygulamaları 1940'lı yılların başlarında ortaya çıkmıştır ve bu uygulamalar o zamandan günümüze kadar gelişimini sürdürmüştür. Finansal krizler ve bilgi teknolojileri dahil olmak üzere pek çok faktörden direkt olarak etkilenen iç denetimin faaliyet alanı, işlevleri ve iç denetçilerin nitelikleri açısından değişim geçirdiği görülmektedir. Geçen zamanı değerlendirdiğimizde, iç denetim geleneksel iç denetim işlevlerini yerine getirmenin ötesine geçmiştir. Bu değişim sürecinde, bilgi sistemlerindeki ve bilgi teknolojilerindeki gelişmelerin artmasının etkili olduğu yadsınamayacaktır. Bununla birlikte, iç denetimin odak noktasının değişmesi geleneksel iç denetim faaliyetlerinin ihmal edildiği anlamına gelmemekte aksine, iç denetim faaliyetlerinin sürekli denetim, risk odaklı iç denetim ve kontrol özdeğerlendirmesi yaklaşımlarıyla zenginleşmesine neden olmaktadır. Hangi yaklaşım benimsenirse benimsensin, iç denetim birimi çeşitli alanlarda güvence ve danışmanlık hizmetlerini yürütmektedir. Ancak küresel ölçekte iç denetim birimlerinin güvence ve danışmanlık hizmeti verdiği alanlar farklılık gösterebilmektedir. Bu farklılığa neden olan temel faktörler yasal mevzuat, üst yönetimin iç denetime bakışı, denetim komitesinin istekleri ve işletmenin risk yönetimi sisteminin olgunluk seviyesi olarak sıralanabilir.

Finansal kontrollerin, muhasebe kontrollerinin ve faaliyetlerle ilgili diğer kontrollerin yeterliliğinin ve uygulanmasının gözden geçirilerek değerlendirilmesini, etkin bir iç kontrol sisteminin geliştirilmesini ve uygulanmasını, varlıkların zararlara karşı korunmasını ve faaliyetlerin belirlenmiş politikalarla uyumlu bir şekilde yürütülmesini amaç edinen iç denetim; sorumluluk ve hesap verebilme, yönetime danışmanlık ve yardım, tasarruf ihtiyacı, vekalet teorisi ve hileli işlemlere karşı korunma ihtiyacı gibi nedenlerden ötürü gerekli hale gelmiştir. İç denetim ve iç denetçiler önceleri sadece muhasebe ve işletme varlıklarının korunması ile görevlendirilmiş iken, günümüzde finansal denetimde, uygunluk denetiminde, faaliyet denetiminde ve bunların yanı sıra bilgi teknolojileri denetiminde ve risk değerlendirme, kurumsal yönetim gibi faaliyet alanlarında görev alarak mesleğin çeşitliliğinin ve faaliyet alanının genişlemesini sağlamışlardır. Yaşanan gelişmeler sonucunda iç denetimde daha pro-aktif bir yaklaşım benimsenmiş, denetlenene “müşteri” gözüyle bakılmamış, risk yönetimi üzerinde yoğunlaşmış, denetim kalitesi süreklilik temeline oturtulmuş ve teknolojik olanaklardan daha fazla yararlanılmıştır.

İç Denetçiler Enstitüsü (The Institute of Internal Auditors-IIA), iç denetim faaliyetini ve niteliklerini, bir kuruluşun faaliyetlerine katma değer sağlamak ve iyileştirmek amacıyla tasarlanan, bağımsız, nesnel bir güvence¹ ve danışmanlık hizmeti² olarak tanımlamaktadır. İç denetim; risk yönetimi, iç kontrol ve kurumsal yönetim süreçlerinin etkinliğini değerlendirme ve artırma konusunda sistematik ve disiplinli bir yaklaşım getirerek kuruluşların hedeflerine ulaşmalarına yardım etmektedir (Hass, Abdolmohammadi ve Burnaby, 2006:836). İç Denetçiler Enstitüsü tarafından yapılmış olan bu tanım şimdiye kadarki en pro-aktif ve kapsamlı tanımdır. Bu yeni tanımda iç denetimin güvence ve danışmanlık hizmeti verme işlevlerinin yanı sıra risk yönetimi, iç kontrol ve kurumsal yönetim gibi faaliyet alanlarına da vurgu yapılmaktadır (Abdolmohammadi, Burnaby ve Hass, 2006: 816).

Tanımda yer alan “güvence” ve “danışmanlık” ifadeleri, günümüzde iç denetimin genişleyen işlevlerini yansıtmaktadır. Yapılan bu iç denetim tanımı “değerleme” fonksiyonunu dışlamamakta, fakat daha geniş olarak ele almaktadır. İç denetçilerin geleneksel değerleri zedelemeksizin, güvence ve danışmanlık hizmetleri vasıtasıyla katma değer yaratabileceği kabul edilmektedir. Ayrıca tanımda iç denetimin faaliyet alanı içinde risk yönetimine, iç kontrole ve kurumsal yönetime yer verilmesi sayesinde iç denetim biriminin sunacağı raporlar ve yapacağı çalışmalar vasıtasıyla denetim kuruluna ve üst yönetime önemli bir kaynak sağlamasına yardımcı olunmuştur (Demirbaş, 2005: 174).

İşletmelerdeki iş yapma ve bilgiyi işleme şekillerinin gösterdiği hızlı değişim ve gelişim süreci güvence hizmetleri açısından etkili olmuştur. Denetim sürecini gerçekleştiren ve güvence hizmetlerini yerine getiren denetçiler, bilgi teknolojileri ve elektronik ticaret hakkında temel bilgiye ve anlayışa sahip olmalıdırlar. Denetçilerin işletmeleri tüm yönlerden değiştiren ve sağladıkları hizmetleri etkileyen bu anahtar teknolojileri anlamaları gerekmektedir. Ayrıca denetçilerin bilgi sahibi olması gereken bir diğer konu da donanım, yazılım, iletişim ve internet gibi fonksiyonlarıyla birlikte

¹ **Güvence hizmetleri**, finansal ve faaliyetlerle ilgili bilginin güvenilir olması ve bütünlüğü ile ilgilidir (Ahmed, 2007:8). Mali yapıya, performansa, mevzuata ve düzenlemelere uyum gösterme, bilgi sistemleri güvenliğine ve ihtimam denetimine (ayrıntılı durum tespit çalışmasına) yönelik görevleri yerine getirme güvence hizmetleri kapsamındadır (TİDE, 2008:36).

² **Danışmanlık hizmetleri**, risk yönetiminin ve iç kontrolün etkinliğinin değerlendirilmesinde üst düzey yönetime yardımcı olmakla ilgilidir (Ahmed, 2007:8). Yol/Yöntem göstermek, tavsiyede bulunmak, işleri kolaylaştırmak ve eğitim vermek danışmanlık hizmeti kapsamındaki faaliyetlere örnektir (TİDE, 2008: 35).

karşımıza çıkan bilgi teknolojilerini güvence sağlamak için nasıl kullanacaklarıdır (Arens, Elder ve Beasley, 2008: 18).

İç denetim birimi tarafından sunulan güvence ve danışmanlık hizmetleri paydaşlar açısından da önemlidir. Çünkü paydaşlar açısından işletmede iç denetçilerinin varlığı, işletmede gerçekleştirilen denetimler ve bu denetimler sonucu hazırlanan denetim raporları doğru ve güvenilir bilgiye ulaşma açısından son derece önemlidir (Özoğlu, Mercan ve Çakıroğlu, 2010: 21).

İç denetçinin işletmeye kattığı değer, yöneticinin sorumluluk üstlenmesini ve iç denetimin iç kontrol sistemini kendi otoritesi altına almasını sağlamaktadır. İç denetçinin kolaylaştırıcı ve yenileştirici bir rol üstlenebilmesi için iş dünyasındaki süreçleri çok iyi anlamış olması gerekir. Geleneksel yaklaşımda iç denetim ve bununla ilgili risklerin analizi ve raporlanması görevleri temelde denetçiye verilmekte olup, diğer bölümlerde çalışanlar daha az sorumluluk taşımaktadırlar. Dolayısıyla bu yaklaşım, denetçilerin ve danışmanların iç denetimden sorumlu oldukları ve yöneticilerin ve diğer çalışma gruplarının yetkili olmadığı olgusu yaratabilmektedir. İşte “Kontrol Özdeğerlendirme (Control Self Assessment)” yaklaşımı sayesinde yönetim, gelişme sürecini takip etme ve iç denetimi oluşturma konusunda daha etkin rol almaya başlamıştır. (Nastase ve Nastase, 2007: 44-45). Kontrol Özdeğerlendirme yaklaşımı artan bilgi teknolojisi ortamının oluşturduğu yeni başlıklar arasında yer almaktadır. Kontrol Özdeğerlendirme, risk ve kontrollerin tanımlanması, değerlemesi, ölçülmesi ve izlenmesi süresince yönetim tarafından kullanılan bir yönetim aracıdır. Bu yaklaşım, çalışanların ve yöneticilerin kıdemli bir iç denetim çalışanı rehberliğinde bir araya geldiği, kurum hedeflerine ulaşılma olasılığını etkileyen her türlü faktörün değerlendirildiği bir etkinliktir (Pehlivanlı, 2010: 90). Kontrol özdeğerlendirme, iç kontrol sisteminin etkinliğinin incelendiği ve değerlendirildiği bir süreçtir. Amaç, tüm işletme amaçlarına ulaşılacağına dair makul bir güvence sağlamaktır (Moeller, 2004: 155).

Bilgi teknolojisi alanında yaşanan gelişmeler işletmelerin risk özelliklerini önemli ölçüde değiştirmiştir. Artık geleneksel risklerin yanı sıra yeni riskler oluşmuş ve riskler daha karmaşık bir hale gelmiştir. İşletmelerin hızlı değişim gösteren risk profillerini kavramaları geleneksel yöntemler kullanılarak yapılamamaktadır. Özellikle finansal ve bilgi teknolojileri denetimine odaklanan iç denetçiler, iç denetçinin değişen

rolüne paralel olarak risk odaklı iç denetime de gereksinim duymuşlardır. Risk odaklı iç denetim, işletmelerin risk profillerinin belirlenmesi, denetim sürecinin işletmenin risk profiline göre şekillendirilmesi ve denetim kaynaklarının buna göre tahsis edilmesi esasına dayanan ve denetimin etkinliğini artırmayı amaçlayan bir denetim yaklaşımıdır (Kurnaz ve Çetinoğlu, 2010: 84).

Düzenleyici ve denetleyici kurumların istekleri, halka açık işletmelerin ilgili taraflara karşı sorumlulukları finansal tabloların tam, doğru ve zamanında hazırlanmasını gerektirmekte ve üst yönetimin, düzenleyici ve denetleyici kurumların iç denetim birimlerinden beklentilerini arttırmaktadır. İç denetim birimlerinin beklentilere karşılık verebilmesi, hızlı ve anlamlı sonuçlar elde etmesi bilgi teknolojilerinden faydalanılmasını zorunlu kılmıştır. Artık birçok işletme belli dönemlerle hazırladıkları finansal tabloları kendi web sayfalarında yayınlamaktadır. Bilgi teknolojilerinin sağladığı bu dönüşüm, şeffaflığı ve bilgiye kolay erişimi sağlamaktadır. Bu nedenle sistemlerin işleyişinde karşılaşılabilecek risk ve tehlikelere karşı “Sürekli Denetim” önem kazanmıştır (Kurnaz ve Çetinoğlu, 2010: 152). Sürekli denetimde bilgi teknolojisi desteği yoğun olarak kullanılmaktadır. Sürekli denetim, teknolojik imkanlardan yararlanarak otomatik metotlarla belirli bir aralıkta düzenli ve sürekli olarak bilgi teknolojisi sistemlerinin, finansal verilerin oluşumunu sağlayan en detay işlemlerin ve süreçlerin izlenmesi, kontrol ve risk değerlendirmelerinin yapılması olarak tanımlanabilir. Finansal bilginin elektronik ortamda sürekli ve gerçek zamanlı üretilmesi elbette geleneksel denetim yaklaşımlarını değiştirmiştir; sürekli denetim yaklaşımı bunun bir sonucu olarak ortaya çıkmıştır (Selimoğlu, 2006a: 284). Sürekli denetim, iç kontrolün etkililiğini ve finansal bilginin doğruluğunu sağlamak amacıyla uygulanmakta, denetim prosedürlerine ilişkin değişen yöntem ve teknikleri kapsamaktadır (Sevimli, 2009: 30).

İç denetim biriminin denetim sürecindeki rolü, ortaya çıkan yeni yaklaşımlardan etkilenmiştir. Bu yaklaşımlar işletmelerde denetim anlayışını temelden değiştirmekte, ortaya çıkabilecek riskleri etkin bir şekilde izlemeyi amaçlamaktadır. Geleneksel denetim teknikleri işletme hakkında güvenilir bilgi verme konusunda yetersiz kalmaktadır. Denetim sürecinde geçmişe dönük finansal verilerin yanında işletmelerin karşılaşılabileceği risklerin de tahmin edilmesi gerekmektedir. Bu açıdan risk yönetimi ve risk odaklı iç denetim anlayışı ile işletme risklerinin belirlenmesi, ölçülmesi ve

yönetilerek minimize edilmesi gerekmektedir. Risk odaklı iç denetim yaklaşımı temelde kurumsal yönetime dayanmaktadır ve kurumsal yönetimin etkin bir şekilde uygulanıp uygulanmadığını belirlemeye çalışır. İç denetim birimi, gelecekte bilgi teknolojilerine hakim olmakla birlikte, risklerin yönetilmesi ve çeşitli yaklaşımlarla risk yönetimi ve kurumsal yönetim uygulamalarına daha fazla katkıda bulunulması konusunda da uzman olmak durumundadır.

Günümüzde denetim faaliyetinin katma değer sağlayan bir faaliyet haline gelmiş olmasından dolayı iç denetim önem kazanmaktadır. İç denetimin işletmede katma değer yaratması; işletmenin amaçlarının gerçekleştirilmesine, işletme faaliyetlerinin geliştirilmesine ve maruz kalınan işletme risklerinin azaltmasına güvence ve danışmanlık hizmetleri vasıtasıyla yardımcı olmasıyla gerçekleşmektedir (TİDE, 2008: 37). İç denetimin yarattığı katma değer; yönetimin karar alma ve iç kontrolün etkinliğini değerlendirme sürecinde iç denetçiler tarafından tavsiyelerde bulunulmasıyla ortaya çıkmaktadır (Ahmed, 2007: 8).

İç denetçinin bağımsızlığı da işletme bünyesinde katma değer sağlama açısından önemli bir niteliktir. Bağımsızlık olmazsa, iç denetçilerin görüşlerinin bütünlüğü ve tarafsızlığı konusunda şüpheye düşülebilir (Ahmed, 2007: 8). İç denetçilerin, denetledikleri müşteri ile iş birliği kurabilmesi ve denetim işini her türlü müdahaleden uzak tutabilmesi için üst yönetim, denetim komitesi ve yönetim kurulu tarafından desteklenmesi gerekir (Zakaria, Selvaraj ve Zakaria, 2006: 894). İç denetim yöneticisinin yönetim kurulu ve denetim komitesiyle doğrudan iletişiminin olması, iç denetimin bağımsızlığının güvence altına alınmasına yardımcı olacaktır (TİDE, 2008: 71-72). Bu nedenle İç Denetçiler Enstitüsü (IIA), gerekli kurum içi bağımsızlığın sağlanabilmesi için iç denetçilerin işlevsel olarak denetim komitesine veya dengi bir yönetim kademesine bağlı olması gerektiğini savunmaktadır.

Bu çalışmada işletmelerde iç denetimden sorumlu tarafların bilgi teknolojilerindeki değişimler sonucu iç denetimin işlevlerinde ve iç denetim sürecinde meydana gelen gelişmeleri değerlendirmeleri araştırılmaktadır. Çalışmanın amacı doğrultusunda oluşturulan araştırma sorularını incelemek üzere İMKB-100 endeksinde işlem gören işletmeler seçilmiştir.

Çalışmamızda, birinci bölümde bilgi teknolojileri ile muhasebe bilgi sistemi ve iç denetim ilişkisi incelenmiştir. Bu doğrultuda öncelikle bilgi teknolojileri ve bilgi

teknolojilerinin yarattığı uygulamalar ana hatlarıyla ele alınmış, sonrasında bilgi teknolojilerinin yarattığı uygulamaların muhasebe bilgi sistemi ve iç denetim ile ilişkilerine yer verilmiştir.

İkinci bölümde, iç denetim ve iç denetimin değişen faaliyet alanları ele alınmıştır. Öncelikle iç denetim ile ilgili temel bilgilere yer verilmiş, daha sonra iç denetim sürecindeki yaklaşımlar (geleneksel yaklaşım, sürekli denetim yaklaşımı, risk odaklı iç denetim yaklaşımı, kontrol özdeğerlendirme yaklaşımı) ve iç denetimin değişen faaliyet alanları (risk yönetimi, kontrol ve kurumsal yönetim) ele alınmıştır.

Üçüncü bölümde bilgi teknolojilerindeki değişimlerin iç denetimin işlevlerinde ve iç denetim sürecindeki etkileri ele alınmıştır. Öncelikle bilgi teknolojilerindeki değişimlerin yarattığı etkiler dikkate alınarak, iç denetimin işlevleri üzerinde ortaya çıkan etkiler incelenmiş ve bu kapsamda güvence hizmetlerindeki, güvence hizmetlerinin yerine getirilmesindeki ve danışmanlık hizmet alanlarındaki değişimler ele alınmıştır. Daha sonra bilgi teknolojilerindeki değişimlerin yarattığı etkiler dikkate alınarak, iç denetim sürecindeki etkiler ele alınmıştır. Bu kapsamda sürekli denetim, risk odaklı iç denetim ve kontrol özdeğerlendirmesi yaklaşımlarında meydana gelen etkiler incelenmiştir.

Dördüncü bölümde yukarıda belirtilen konulara ve çalışmamızın amacına uygun olarak, İMKB-100 endeksinde işlem gören işletmelerin iç denetim birimi yöneticilerine uygulanmış anket sonucu elde edilen bulgulara ve analiz sonuçlarına yer verilmiştir. Anket sonucu elde edilen veriler SPSS paket programında değerlendirilerek, niceliksel çoklu yöntem yaklaşımına göre istatistikî analizlere tabi tutulmuştur.

Birinci Bölüm

Bilgi Teknolojileri İle Muhasebe Bilgi Sistemi ve İç Denetim İlişkisi

1. Bilgi Teknolojileri

Bilgi teknolojilerinde meydana gelen değişimler, işletmelerin iş yapma biçimlerini derinden etkilemiştir. Bilgi teknolojilerindeki değişimler, işletmeleri rekabet avantajı sağlamak amacıyla, en gelişmiş teknolojileri kullanma ve doğru, güvenilir ve zamanlı bilgiye hızlı ve kolay yoldan ulaşma yönünde bir çaba içerisinde sokmuştur. Bu nedenlerle bilgi teknolojileri kavramından, yarattığı uygulamalardan, ilgili kontrollerden, bilgisayar destekli denetim tekniklerinden ve bilgi teknolojilerinin işletmeler üzerindeki etkilerinden ilerleyen kısımlarda bahsedilecektir.

1.1. Bilgi Teknolojileri Kavramı

Bilgi teknolojileri, verilerin kayıt edilmesi, saklanması, belirli bir işlem sürecinden geçirilerek bilgiler üretilmesi, üretilen bu bilgilere erişilmesi, saklanması ve nakledilmesi gibi işlemlerin etkili ve verimli yapılmasına olanak sağlayan teknolojileri ifade etmektedir (Aktaş, 2009: 9).

Bilgi teknolojileri donanım, yazılım ve veritabanı olmak üzere başlıca üç unsura sahiptir. Donanım, bilgisayarın fiziksel yapısını oluşturan araç ve teçhizattır. Donanım faaliyetlerini genel olarak yönlendiren komutlar ise yazılım olarak ifade edilir. Yazılımlar, sistem yazılımları ve uygulama yazılımları olmak üzere iki gruba ayrılmaktadır. Veritabanı ise uygulama yazılımları tarafından kullanılacak olan tüm verileri içermektedir (Bensghir, 1996: 39-40).

Bilgi teknolojileri, işletmelerde sinir sistemi vazifesi görerek etkin bir işleyiş sağlamaktadır. İşletmeler için uygun bilgi teknolojileri seçimi ve etkin bilgi teknolojileri yönetimi, hizmet kalitesi ve kurumsal etkinlik³ amaçlarına ulaşmak doğrultusunda önem arz etmektedir (Öğüt, 2003: 163).

³ Kurumsal etkinlik, kurumsal faaliyet ve çabaların amaca ulaşmasındaki isabet derecesidir.

Bilgi teknolojileri, örgüt yapısı ve bireyin işinin yeniden tasarımında önemli bir etkiye sahiptir. Bilgi teknolojisi, hem iş yapma biçimini hem de bu işlerin diğer insanlarla koordine edilme biçimini değiştirmektedir. Teknolojik gelişmeler farklı örgütleri birbirlerine bağlamakla kalmamakta, aynı zamanda ekonomik sonuçlar da bilgi teknolojilerinin tüm örgütte kullanılmasını gerektirmektedir. Bilgi teknolojisi örgütün çevre ile ilişkisini desteklemekte, geleneksel iletişimin yerine geçmekte ve iletişimi daha etkili yapmaktadır. İletişimde meydana gelen bu gelişmeler de örgütlerin uzaklık ve zaman farkı problemlerini gidermektedir. Bilgi teknolojilerinin kullanımı işletme içi iletişimi de hızlandırmaktadır (Ömürbek ve Altın, 2008: 110). İleri bilgi teknolojileri kullanımı sayesinde, elektronik ve eş zamanlı olarak verileri toplayan, özetleyen ve dağıtan yazılım programları kullanılmasıyla işletme yönetimi minimum maliyetle, doğru ve zamanlı bilgilere erişebilmektedir (Öğüt, 2003: 224).

1.2. Bilgi Teknolojilerinin Yarattığı Uygulamalar

Bilginin eş zamanlı olarak yeryüzündeki herkesle paylaşılabilmesi ve karşılıklı değişimini mümkün kılan pek çok teknolojik yenilik, günümüzde işletme faaliyetlerinin tamamen veya kısmen elektronik ortamda gerçekleşmesine yol açmıştır.

Bilgi teknolojisi ortamının artması işletmelerin hem iş yapma biçimini hem de bu işlerin diğer kişiler vasıtasıyla yürütülmesi biçimini değiştirmiştir (Karadal, 2007: 213). İşletmelerin iş süreçleri üzerinde yer alan kontrollerin tasarlanması, uygulanması ve depolanması bilgi teknolojileri ile gerçekleşmektedir. Bilgi teknolojileri, işletmelerin finansal tablolarında özetlenen ve raporlanan bilgilere ilişkin verilerin toplanması, işlenmesi ve depolanması açısından da kritik bir role sahiptir (Abu-Musa, 2008: 438).

Bilgi teknolojilerinin yarattığı uygulamalar arasında yer alan ve işletmelerde çok yaygın bir şekilde kullanılan elektronik ticaret, internet, elektronik veri değişimi, kurumsal kaynak planlama ve elektronik veri işleme teknolojileri kısaca ele alınacaktır.

1.2.1. Elektronik ticaret

Küresel ekonomi tartışmalarına bağlı olarak gelişen ve rekabetin bir başka enstrümanı olarak nitelendirilen elektronik ticaret, tüm dünyada hızla yayılmakta olan ve günümüzde sıkça telaffuz edilen bir kavramdır (Sevim, 2005: 95).

Elektronik ticaret ile ilgili tanımları incelediğimizde, çeşitli kuruluşların çeşitli tanımlamalar yaptığını görmekteyiz (Erdem ve Efiloğlu, 2002):

Dünya Ticaret Örgütü (World Trade Organization-WTO)'ne göre e-ticaret; mal ve hizmetlerin üretim, reklam, satış ve dağıtımlarının telekomünikasyon üzerinden yapılmasıdır.

Ekonomik İşbirliği ve Gelişme Örgütü (Organisation for Economic Co-operation and Development-OECD) tanıma göre e-ticaret; sayısallaştırılmış yazılı metin, ses ve görüntünün işlenmesi ve iletilmesine dayanan kişileri ve kurumları ilgilendiren tüm ticari işlemlerdir.

Birleşmiş Milletler Yönetim, Ticaret ve Ulaştırma Usullerini Kolaylaştırma Merkezi (The United Nations Centre for Trade Facilitation and Electronic Business-UN-CEFACT)'nin tanımına göre e-ticaret; iş, yönetim ve tüketim faaliyetlerinin yürütülmesi için yapılanmış ve yapılanmamış iş bilgilerinin, üreticiler, tüketiciler ve kamu kurumları ile diğer organizasyonlar arasında elektronik araçlar üzerinden paylaşılmasıdır.

Türkiye Elektronik Ticaret Koordinasyon Kurulu ise e-ticareti bireylerin ve kurumların internet veya intranet aracılığıyla yazı, ses, görüntü şeklindeki sayısal bilgilerin işlenmesi, iletilmesi, saklanması temeline dayanan bir değer yaratmayı amaçlayan ticari işlemlerin bütünü olarak belirlemiştir (Erdoğan, 2006: 189).

Elektronik ticaret, bilgi, hizmet ve ürünün internet üzerinden sağlanması suretiyle, hedef kitlede talep oluşturma, potansiyel tüketiciler bulma, ticari ve lojistik desteğin sağlanması ve pazarlama etkinliklerini kapsamaktadır. Elektronik ticaret, hem kısa vadeli bir taktik hem de uzun vadeli bir strateji olarak görülebilecek bir gelişmedir (Öğüt, 2003: 49-51).

Elektronik ticaret, internet üzerinden ticaret yapmak veya ticaretin elektronik ortamda yapılmasıdır. Elektronik veri değişimi, elektronik ticaretin temelini oluşturmaktadır. Elektronik veri değişimi sayesinde siparişler ve muhasebe verileri, güvenli ve doğru bir şekilde internet üzerinden elektronik ticaret işlemine taraf olan işletmelerin muhasebe bilgi sistemlerine transfer edilir. Bu sırada veri ve bilgi güvenliği konusunda da elektronik veri işleme teknolojilerinin sağladığı katkı yadsınamayacaktır. Ayrıca elektronik veri işleme teknolojileri tarafından elektronik ortamda kayıtlanıp saklanan kayıtlar sayesinde finansal tablolar eş zamanlı olarak hazırlanabilmektedir.

Gerçekleştirilen faaliyetlerde internetin kullanılması bilginin üretilmesine ve iletilmesine hız katmıştır.

Elektronik ticaret, verilerin doğruluğunun artmasını, yazım ve veri girişi hatalarının azalmasını, bilgiye daha hızlı ulaşılmasını ve yönetimin veri iletişimine daha az zaman ayırmasını sağlar. E-ticaretin bu faydalarına karşın donanım maliyetlerine, yazılım maliyetlerine, mevcut iş akışındaki değişikliklerin yarattığı maliyetlere, eğitim maliyetlerine, yönetim giderlerine ve iletişim giderlerine katlanmak gerekir.

1.2.2. İnternet

İnternet, dünyadaki bilgisayar ağlarının ağ sistem teknolojileri ile birbirine bağlanmaları ve bir IP-Bilişim Protokolü kullanarak anlaştıkları, haberleştikleri bilgi aktarım ve paylaşımında bulundukları bir iletişim ağıdır (Erol, Atmaca ve Şahin., 2004: 33). İnternet, birbirine bağlı bilgisayar ağlarının bütünleştirilmesidir. Bu bağlantılar tüm dünyayı kapsamakta ve pek çok faaliyetin gerçekleştirilmesi için kullanılan bir bilgi işlem merkezi alanı oluşturmaktadır (Sevim, 2009: 32).

Bilgi teknolojileri içerisinde en yoğun kullanılan ve güncelliğini yitirmeyen araç internettir. İnternet, farklı yerlerde bulunan bireyler, işletmeler ve toplumlar arasında kurulan elektronik bir etkileşim, paylaşma, bildirişme ve dayanışma ortamı olarak kullanılır (Öğüt, 2003: 47).

Bilgi paylaşımının getirdiği katkı ve bu katkının özellikle iktisadi alanda kullanıma sunulmasında sağladığı kolaylık nedeniyle internet, yeni ekonomi⁴ ile özdeşleşmiştir. Artık bilginin saklanması yerine paylaşılması ve paylaşıldıkça artacağı görüşü yaygın bir hale gelmiştir. İnsanların birbirleriyle iletişimini, bilgi alışverişini, öğrenme ve iş yapma süreçlerini etkileyen internet, ekonominin ve günlük yaşamın yeniden yapılanmasında etkin bir rol oynamaktadır. İnternet teknolojisi ve işletmelerdeki her türlü iş akışı günümüzde iç içe geçmiş durumdadır. Artık her işletme,

⁴ *Yeni ekonomi* sayısal bir ekonomidir. Bilginin sayısala kayması sayısal ağlar içinde sanal bir ekonomi yaratmıştır (Oktay, Balkanlı ve Salepçioğlu, 2004: 159). Bilgi, entelektüel sermaye, internet, maddi olmayan varlıklar, yeni organizasyon yapıları, network, küreselleşme gibi kavramlarla da açıklanabilen yeni ekonomi, eski ve ulusal tabanlı ekonomiden, farklı pazar ve endüstri yapılarıyla büyüyen küresel yeni ekonomiye dönüşümü ifade etmektedir. Yeni ekonomide işletmeler, maddi varlıklara yatırım yaparak büyümek yerine, bilgi, teknoloji ve insan gücüne yatırım yaparak büyümektedirler (Gürdal, 2004: 89-90).

internetin sağladığı olanakları kendi iş yaşamına yansıtmak zorundadır (Ömürbek ve Altın, 2008: 111-112).

İnternet teknolojisi içinde yer alan ve sıklıkla kullanılan diğer uygulamalar **intranet** ve **extranet**dir. İşletmeler içinde kişiler, bölümler ve özellikle coğrafi bakımdan dağınık durumda bulunan çeşitli birimler arasındaki iletişimi, bilgi akışını, bilgi alış verişini ve işbirliğini destekleyen en önemli sistemlerden birisi **intranet** teknolojisidir. Özetle, intranet, internet teknolojisinin yalnızca işletme dahilinde kullanılmak üzere uygulanmasıdır. Intranet teknolojisi, zengin içerikli ve çift yönlü bilgi transferini mümkün kılan, hızlı, etkili ve interaktif bir bilgi teknolojisidir. Intranet teknolojisi çok amaçlı bir teknolojidir ve bilgi transferinin dışında, bilgi depolaması, bilginin üretilmesi ve geliştirilmesi gibi farklı süreçler açısından da önemli fonksiyonlar göstermektedir. Geniş bir enformasyon tabanına erişim kolaylığı, hızlı bir basım yayın aracı olması, birebir diyalog imkanı vermesi, gelişmiş bir ağ ortamı oluşturması en önemli avantajları arasındadır (Zaim, 2005: 129-130). Tüm koruyucu önlemlere karşın yeterince denetlenemeyen bir olgu olarak internet bütün dünyanın erişimine açık durumdadır. Intranet ise, internetin en iyi özelliklerinden yararlanma ve sakıncalarını dışarıda bırakma temeli üzerine kurulmuştur. Bu açıdan intranetler daha güvenli, denetlenebilir ve belirli amaca yönelik olmaları açısından internetten ayrılırlar (Nakilcioğlu, 2002).

Intranet, salt belirli bir işletmeye özgü olan ve yalnız ilgili işletme üyeleri için erişime açılmış içsel iletişim ağı iken, intranete işletme dışından kişilerin erişimine kısmen dahi izin verildiği takdirde oluşturulan yeni ağ **extranet** olarak adlandırılır (Öğüt, 2003: 48). Extranet, işletmeyi kendi tedarikçileri, müşterileri veya ortak hedefleri paylaştığı diğer işletmelerle bağlayan, bunu yaparken de internet teknolojilerini kullanan işbirliğine açık bir ağıdır (Erol vd., 2004: 33). Extranet uygulaması söz konusu olduğunda güvenlik konusu intranete göre daha fazla önem kazanmaktadır. Çünkü extranetler, kurum intranetlerinin dış ortama açık hale gelmesini gerektirir (Hepkul, 2008: 159).

İnternet, elektronik ticaret açısından en etkin araç olarak kabul edilmektedir. İşletmelerin diğer işletmeler ve bireyler ile düşük maliyetlerle bağlantı kurmalarını kolaylaştırması ve işletmelerin kullanmakta oldukları bilgi teknolojisi standartlarından bağımsız olarak, evrensel olması ve kullanımının kolay olması gibi bir takım avantajları

sunması nedeniyle, internet elektronik ticaret için hızla yaygınlaşan ve tercih edilen bir altyapı haline gelmiştir (Sevim, 2009: 12). Ayrıca elektronik ticaret, işlemlerin gerçekleştiği ortam açısından internet ve intranet ile yakın ilişki içindedir. Elektronik ticaret hem internet gibi açık ağlarda gerçekleştirilebilir hem de intranet gibi işletmelerin kendi faaliyetlerini yürütebilmek amacıyla bayileri ile veya belli sayıdaki müşterileri ile oluşturdukları kapalı ağlarda gerçekleştirilebilmektedir (Güneş, 2002).

1.2.3. Elektronik veri değişimi

Elektronik Veri Değişimi (Electronic Data Interchange-EDI), ticaret yapan iki kuruluş arasında insan faktörü olmaksızın bilgisayar ağları aracılığıyla belge ve bilgi değişimini sağlayan bir sistemdir (Özbay ve Akyazı, 2004: 21). Elektronik veri değişimi kullanımı, özel bir telekomünikasyon altyapısı ve standart formlar gerektirmektedir. Sadece kayıtlı kullanıcılara açık olduğu için çok güvenli olan bu sistemin, donanım ve bağlantı maliyetleri yüksektir (Yürütücü, 2002).

Elektronik veri değişimi uygulamasıyla, zamandan ve işlem maliyetlerinden tasarruf sağlanmasının yanı sıra, bilgilerin elektronik ortamda değişimi nedeniyle insan faktöründen kaynaklanan hatalar da ortadan kalkmış olacaktır (Gökçen, 2007: 261-262).

Elektronik veri değişimi kamu ve özel sektör kuruluşlarının etkin bir biçimde iletişim kurma ihtiyaçlarından doğmuş olup hızlı ve doğru veri akışının sağlanması, daha etkin denetim yöntemlerinin geliştirilmesi, üretkenliğin ve kârın artırılması, rekabet gücünün yükseltilmesi gibi konularda sağladığı avantajlar nedeniyle giderek daha fazla kullanım alanı bulmuştur (Erdem ve Efiloğlu, 2002).

Elektronik veri değişimi, elektronik ticaretin temeli olarak değerlendirilmektedir (Öğüt, 2003: 51). Elektronik ticarete konu olan işlemlerin sayısı ve boyutu gün geçtikçe artmaktadır. Yakın bir zamanda kağıdın yerini elektronik belgeler alacaktır. Dolayısıyla günümüzde elektronik veri değişiminin internet ve elektronik ticaret ile uyumlu olarak çalışması gerekmektedir (Sevim, 2009: 59).

1.2.4. Kurumsal kaynak planlaması

Kurumsal Kaynak Planlaması (Enterprise Resource Planning-ERP), bir kurumun tüm süreç ve verilerini tek bir geniş kapsamlı ve bütünlük yapı altında toplayan gelişmiş bir sistemdir (Sevim, 2005: 97). Kurumsal kaynak planlamasının en önemli

özelliği, firmanın bütün bölüm ve fonksiyonlarını tek bir sistem içinde birleştirmeye çalışmasıdır. İhtiyaç ve beklentileri birbirinden farklı olan çok sayıda bölümün aynı bilgisayar sistemi içinde bir araya getirilmesi ve aynı bilgi tabanını paylaşması güç, ancak çok faydalıdır (Alptürk, 2008b: 145). İşletmelerin doğru, güvenilir, zamanlı ve güncel veri gereksinimini karşılamak amacıyla bir veri tabanı oluşturma, işletme kaynaklarını bütünleşik olarak yönetebilme ve işletme dışı kişi ve kuruluşlar ile olan ilişkileri tek çatı altında toplama gereksinimi işletmeleri kurumsal kaynak planlaması uygulamalarına yönlendirmektedir (Sevim, 2009: 155).

Kurumsal kaynak planlaması yönetsel açıdan, kaynakların daha etkin yönetimi, geliştirilmiş planlama ve karar alma, performans iyileşmesi; stratejik açıdan, işbirliklerinin desteklenmesi, dış bağlantıların güçlendirilmesi; bilgi teknolojileri açısından, işletme esnekliğinin sağlanması ve bilgi teknolojilerinin kapasitesinin artması; örgütsel açıdan da örgütsel değişimin desteklenmesi ve ortak vizyonların geliştirilmesi gibi faydalar sunmaktadır (Karagül, 2005: 73-74).

1.2.5. Elektronik veri işleme

Elektronik veri işleme; verilerin derlenmesi, sınıflandırılması, sıralanması, hesaplanması, karşılaştırılması, özetlenmesi, saklanması ve raporlar biçiminde kullanıcı ve karar vericilere iletilmesini gerçekleştiren teknolojilerdir (Erdoğan, 1998: 5).

Elektronik veri işleme, işletmelerin günlük işlemleri sonucu elde edilen kayıtların toplanması ve bu kayıtların işlenmesi görevini yerine getirir. İşlem hatalarının azaltılması, verinin/bilginin güvenliğinin sağlanması, terminaller aracılığıyla veri ve bilgiye ulaşılması, doğruluk ve güvenilirlik oranının artırılması, işlemlerin gerçekleştiği anda kayda geçirilmesi ve analizlerin gerçekleştirilmesi elektronik veri işleme teknolojisinin işletmelere sağladığı kolaylıklardır. Elektronik veri işleme sonucu elde edilen çıktılar belirli zaman aralıklarına göre belirlenmiştir, fakat bu teknolojilerin karar alma işlemleri üzerinde etkisi azdır (Anameriç, 2005: 141).

1.3. Bilgi Teknolojisi Kontrolleri

Bilgi teknolojisi kontrolleri, birbirine bağlı bir koruma sürecinin bütününü oluştururlar, fakat bir zayıf halkadan dolayı tavizler söz konusu olabilir. Bu kontroller, hatalara açık olabilir ve yönetimin umursamazlığına konu olabilirler; basit kontroller

olabilecekleri gibi son derece teknik de olabilirler ve dinamik bir ortamda varlıklarını sürdürürler. İç denetçinin bilgi teknolojisi kontrollerindeki rolü, sağlam bir kavramsal anlayışla başlar, risk ve kontrol değerlendirmelerinin sonuçlarıyla en üst noktaya ulaşır. İç denetim birimi kontroller ile ilgili sorumlulukları bulunan kişilerle önemli bir etkileşim içindedir ve yeni teknolojiler ortaya çıktıkça ve kurumun fırsatları, kullanım amaçları, bağımlılıkları, stratejileri, riskleri ve gereksinimleri değiştikçe sürekli ve kesintisiz öğrenmesi ve yeniden değerlendirme yapması gerekir (İDKK, 2007).

Bilgi teknolojisi kontrolleri genel olarak ikiye ayrılmaktadır. Bunlar genel kontroller ve uygulama kontrolleridir.

1.3.1. Genel kontroller

Genel kontroller, elektronik veri işleme teknolojileri ve faaliyetleri ile ilgili olup, bunların etkinliğine büyük ölçüde aracı olurlar (Uzay, 1999: 142). Bilgisayar kullanılan bir işletmenin iç kontrol sistemindeki kontroller genel kontrollerdir. Denetçiler, işletmenin elektronik bilgi ortamı ile ilgili iç kontrol yapısını incelemeye genel kontrolleri değerleyerek başlarlar (Selvi, Türel ve Şenyiğit, 2006: 308).

Genel kontroller şunlardır (Uzay, 1999: 142-148; Erdoğan, 2006: 160):

1. Örgütsel kontroller: Örgütsel kontroller bireysel hilelerin önlenmesi konusunda etkilidir. Ancak işletmede çalışan bütün elemanlar arasında hile yapma ve gizleme konusunda gizli bir anlaşma varsa yönetim hilesi adı verilen bu yolsuzluğu bulmak ve önlemek güçtür.
2. Sistem geliştirme ve belgelendirme kontrolleri: Sistem geliştirme kontrolleri inceleme, test etme ve yeni sistemlerin onaylanması, program değişikliklerinin kontrolü ve belgelendirme yordamları ile ilgilidir. Sistem geliştirme, sistemin veya sistemlerin amaçlarına uygun olarak işlemlerini sağlar. Sistem geliştirmede, bir sistem önceden belirlenmiş amaçlarıyla karşılaştırılır ve daha sonra istenmeyen yönde sapmaların nedenleri göz önüne alınarak sistemin istenen sonuçları nasıl elde edilebileceği araştırılır. Belgelendirme kontrolleri ise bilgisayar işlem faaliyetlerini açıklamak için işletme tarafından korunan kayıtlar ve belgelerle ilgilidir. Belgelendirme denetçi için muhasebe kontrolleriyle ilgili ve sistem boyunca işlemlerin akışına ilişkin bilgi sağlar. Belgelendirme program mantığını anlamada ve

programlar içerisinde yazılı kontrolleri düzenleyerek program değişiklikleri üzerindeki kontrolleri incelemede yardımcı olur. Belgelendirme; sistem, program ve kullanıcı belgelendirmesi olarak üçe ayrılır. Sistem belgelendirmesi; girdi, işlem ve çıktının tanımlanmasını ve sistem akış şemalarını kapsayan bir işlem sisteminin açıklanmasını sağlar. Program belgelendirmesi, her hangi bir uygulama programının tanımlanmasıdır. Kullanıcı belgelendirmesi, programları kullanmada kullanıcılara yardımcı olan açıklamalardır.

3. Donanım ve yazılım kontrolleri: Modern bilgisayar teknolojisi kendi alanında güvenilirliği sağlamıştır. Bunu donanım özellikleri ve teçhizattaki herhangi bir aksaklığı bulmak için oluşturulmuş yazılım kontrol sistemleri sayesinde başarır.
4. Giriş kontrolleri: Veri dosyalarının ve bilgisayar programlarının izinsiz kullanımını önleyen kontrollerdir. Bilgisayar donanımına giriş, bilgisayar operatörleri ile sınırlandırılmalıdır.
5. Veri ve yordama kontrolleri: Bu kontroller günlük bilgisayar faaliyetlerini kontrol ederek işlem hataları olasılığını minimize etmekte ve bilgisayarın bozulması veya fiziksel bir aksaklık durumunda faaliyetlerin devamlılığını sağlamaya yönelik bir çerçeve hazırlamaktadır.
6. Elektronik veri değişimi kontrolleri: Elektronik veri değişimi kontrolleri, işlemlerin yetkilendirilmesi ve geçerli kılınması, erişim kontrolleri ve elektronik veri değişimi denetim kütüklerinin oluşturulmasını kapsar.

1.3.2. Uygulama (işlem) kontrolleri

Uygulama kontrolleri; girdinin kaynağından, çıktının son kullanıcıya ulaşma anına kadar elektronik veri işleme sürecinin her yönden kontrolünü kapsar. Bu kontroller verilerin kaydedilmesinin, işlenmesinin ve raporlanmasının uygun şekilde yapıldığına ilişkin güveni sağlamak için tasarlanmış olup, bunlar hata ve hileleri önleyici, ortaya çıkarıcı veya düzeltici kontrollerdir. Önleyici kontroller genellikle, girdi ve işlem kontrolleriyle ilgilidir. Ortaya çıkarıcı ve düzeltici kontroller ise girdi, işleme ve çıktı olmak üzere her üç işlem aşamasıyla da ilgilidir (Uzay, 1999: 148-149).

Uygulama kontrolleri üç grup kontrolden oluşmaktadır (Yılancı, 2006: 73-74; Özoğlu, Ceyhan ve Çakıroğlu, 2010 193):

1. Girdi kontrolleri: Bu kontrollerin amacı, verinin yetkilendirilmiş durumlarda ve bilgisayarın okuyabileceği doğru formda, bilgisayara giriş için hazırlanmasıdır. Girdi üzerinde verinin tam ve doğru işlenmesini garantiye almak üzere nihai çıktı ile doğruluğu sağlanabilecek bir kontrol kurulmalıdır.
2. İşleme kontrolleri: Bu kontroller işlem safhasında verinin uygun standartta olup olmadığının ve geçerliliğinin test edilmesini sağlar. İşleme kontrolleri, görevler ayrılığı prensibine uyulmasını ve yapılan işlerin doğrulanmasını temin eder.
3. Çıktı kontrolleri: Bilgisayar çıktısının güvenilirliğini garantilemek ve çıktının yalnızca yetkili personele dağıtımını sağlamak için düzenlenir. Çıktıların doğrulanması, çıktı kontrol toplamalarının, bilgi işlem ve girdi kontrol toplamalarıyla uyuşmasını sağlamaktır.

Bilgisayar sistemindeki genel ve uygulama kontrollerini tanıyan denetçi bu kontrolleri test etmek amacıyla Bilgisayar Destekli Denetim Tekniklerinden (BDDT) faydalanacaktır. BDDT, denetçilerin sistemsal bilgilere bilgisayar yardımı ile ulaşarak, denetim kanıtları ve destekleyici bilgileri temin ettikleri bir yoldur (Çatıkkaş ve Yurtsever, 2009: 180). Bilgisayar destekli denetim teknikleri, denetim fonksiyonunun etkinliğini ve verimliliğini arttıran bilgisayara dayalı araç ve yöntemleri kapsar (Coderre, 2009: 1). Bu tekniklerden bazıları bilgisayar sistemlerindeki kontrolleri test etmek için kullanılırken, bazıları da elektronik bilgi ortamlarındaki maddi doğruluk testlerini uygulamak için kullanılırlar (Selvi vd., 2006: 308). Bilgisayar destekli denetim teknikleri sonucunda, çalışma kağıtları elimine edilmekte ve böylece testlerin yapılmasındaki zaman kaybı yok edilmektedir (Akgül, 2002: 24). Bilgisayar destekli denetim teknikleri sayesinde denetim açısından yapılması gerekli ve bilgisayar tarafından yapılması mümkün olan matematiksel yığın işlemler, sıralamalar, sorgulamalar ve benzeri işlemler denetçi tarafından değil, bilgisayar tarafından yapılacaktır. Ayrıca BDDT'ler, insan unsurundan kaynaklanan hataları en aza indirmeye; en kısa sürede mümkün olduğunca fazla veriyi işleme tabi tutarak denetimin etkinliği artırmaya yardımcı olur (Ay, 2007: 277-278).

Bilgisayar destekli denetim teknikleri içerisinde en yaygın olarak kullanılanlar Veri Testi Tekniği⁵, Bütünleşik Test Tekniği⁶ ve Paralel Simülasyon Tekniği⁷dir. Bilgisayar destekli denetimde kullanılan en yaygın yazılımlar ise ACL⁸, IDEA⁹ ve CobiT¹⁰'tir.

1.4. Bilgi Teknolojileri ve Bilgi Teknolojisi Kontrollerinin İşletmeler Üzerine Etkileri

Bilgi teknolojisi alanında yaşanan hızlı gelişmeler ve değişimler işletme ve işletme çevrelerini değiştirmiş ve değiştirmeye devam etmektedir. Bilgi teknolojilerinin işletmelerde kullanımı, işletme yapılarında, çalışanların rollerinde ve iş süreçlerinde beklenmedik ölçekte değişimler meydana getirmiştir. Bilgi teknolojilerinin işletmelere sağladığı katkılar özellikle bilgi akışı ve bilgi yönetimi konularındadır (Öğüt, 2003: 141-143).

Günümüz rekabet ortamında hız, maliyet, kalite ve teknolojik yenilik gibi faktörlerin önem kazanmasından dolayı işletmeler bunlara ulaşmayı kolaylaştırıcı yeni organizasyon modelleri uygulamaya başlamışlardır. Bilgisayar teknolojisindeki hızlı gelişimin bir sonucu olarak ortaya çıkan bilgi teknolojileri, elektronik işletme¹¹ kavramını gündeme getirmiş ve bu kavramın da tüm işletmecilik fonksiyonlarını

⁵ Veri testi tekniği, veri dosyalarını değil bilgisayardaki kontrollerini test eder (Alptürk, 2008b: 154)..

⁶ Bütünleşik test tekniği, veri testlerinin kullanımını ve ayrıca bilgisayar sisteminde ana kütükte hayali varlıklar oluşturmayı gerektiren eş zamanlı bir denetim tekniğidir (Alptürk, 2008b: 154).

⁷ Paralel simülasyon tekniği, bir muhasebe uygulamasında verilerin, denetçinin ve işletmenin programlarına paralel olarak işlenmesi sürecidir (Alptürk, 2008b: 154).

⁸ ACL, veri sorgulama, analiz ve raporlama, bilgisayar destekli denetim konularında pazar lideri bir üründür. ACL, veri araştırma, analiz ve raporlama konusunda uzmanlaşmış, ana iş kolu mali denetim ve mali suistimal ve dolandırıcılık araştırma olan, analiz gerektiren alanlarda kullanılan bir analiz programıdır (Kurnaz ve Çetinoğlu, 2010: 280-281). ACL ile çok uzun zaman alan denetim süreçleri dakikalara sığdırılarak, insan gücünden tasarruf edilmesi, zamanın ve paranın korunmasını sağlamak mümkündür (Alptürk, 2008b: 155).

⁹ IDEA, denetçilere işletmelerin yüz binlerce kaydın yer aldığı veri dosyaları üzerinde tarama, araştırma, özet, seçme veya örnekleme yapma imkanı sunar ve ayrıca çeşitli yazılım paketlerine ve bu paketlerden veri tanınmasına yardımcı olur (Kurnaz ve Çetinoğlu, 2010: 287).

¹⁰ CobiT, süreç tesisi ve süreç denetimi üzerine odaklanır. CobiT daha çok bir kontrol çerçevesi olarak kendini tanımlamaktadır. Bu çerçeve iş gereklilikleri ve iş birimleri ile BT bölümünün hedeflerinin ilişkilendirilmesi üzerine oturtulmuştur. CobiT yapısı ve diğer bileşenleri, yöneticilerin kendi departmanlarının kontrollerden ve güvenlik konularından nasıl yararlandığının anlamasına yardımcı olmuştur (Alptürk, 2008b: 156-157).

¹¹ Elektronik işletme; işletmenin faaliyetleriyle ilgili olarak kullanılan tüm bilgisayarların birbirine bağlanmasından oluşan özel bilgi ağından oluşan bir sistemdir. Elektronik işletmede işletme faaliyetleri, işletme içi ve işletme dışı tüm uygulamalar ile elektronik olarak dijital platformda bütünleşmiştir. Bu bütünleşme sürecinde; internet, intranet, extranet ve elektronik veri değişimi gibi teknolojiler kullanılmaktadır (Sevim, 2009: 21).

etkilediği görülmüştür (Uyar, 2006a). İşletmenin fonksiyonları olarak sayılan yönetim, pazarlama, üretim, finans, muhasebe, insan kaynakları, ar-ge, ve bu fonksiyonların alt fonksiyonları açısından doğru bilginin elde edilmesi ve kullanılması, faaliyetlerde etkinliğin ve verimliliğin sağlanabilmesi açısından önem taşımaktadır.

İşletmeler bilgi teknolojilerini kullanırken rekabetçi ve etkili olmalı ve aynı zamanda dijital işletmeciliğe (dijital girişimcilik) de olanak tanınmalıdır. Birçok işletme için dijital işletme¹² yaratmak ve avantajlarından yararlanmak güçtür. Dolayısıyla bilgi teknolojilerindeki gelişmelerden faydalanabilmek için işletmelerin birçoğu yeniden tasarlanmalıdır (Kağnıcıoğlu, 2008: 14).

Bilgi teknolojileri, kurumsal sorunları çözmeye yönelik donanımın, yazılımın, iletişim ağlarının kurulmasını ve işletilmesini sağlayacak insan kaynakları ve üretilen bilgileri işe dönüştüren kullanıcıların oluşturduğu bir sistem içinde algılanmalıdır (Öğüt, 2003: 227).

İşletmelerde bilgi teknolojilerinin kullanımının, kurumsal etkinliğin öğelerinden olan verimlilik düzeyini arttırdığı belirlenmiştir. Bilgi teknolojilerinin çok hızlı bir şekilde yayılması ve ucuzlaması, bir yandan kurumsal maliyetleri düşürürken, diğer yandan işletmenin verimliliğini arttırmaktadır. Dolayısıyla, bilgi teknolojileri verimlilik artışı ve maliyet tasarrufu yoluyla kurumsal etkinliğin artırılmasını sağlamaktadır (Öğüt, 2003: 227-228).

2. Bilgi Teknolojilerinin Yarattığı Uygulamaların Muhasebe Bilgi Sistemi İle

İlişkisi

Muhasebe bilgi sistemi, işletme içi ve işletme dışı finansal bilgi kullanıcılarına, işletme faaliyetlerinin sağlıklı bir şekilde devam ettirilmesi, planlanması ve denetlenmesi için gerekli olan bilgileri finansal tablolar aracılığıyla sunan bir bilgi sistemidir (Dinç ve Varıcı, 2008: 70). Muhasebe bilgi sistemi, faaliyetler ve işlemler hakkında veri toplamak ve kayıt etmek, planlama, uygulama ve kontrol faaliyetleri için karar vermede kullanılmak üzere veriyi işleyerek bilgiye dönüştürmek ve işletme

¹² *Dijital işletmenin* bütün müşterileri, satıcıları ve çalışanları ile olan önemli ilişkilerini baştan aşağı dijital ortamda sağlayan, şirket varlıklarını dijital yöntem ve araçlar aracılığıyla yöneten bir örgüttür. Temel iş süreci, işletmenin birçok işletmeyle dijital ağlar bağlantısını başarılı bir şekilde sağlar. Yeni ürünlerin geliştirilmesi, üretilmesi ve siparişlerin alınması ya da çalışanlara verilmesi iş sürecine verilebilecek örnekleri oluşturmaktadır (Sevim, 2005: 96). Dijital şirkette, temel işletme kararlarını destekleyebilecek her yerden ve her zaman ulaşılacak bilgiye gereksinim duyulur (Sevim, 2008: 61).

varlıklarını korumak için gerekli kontrolleri sağlamak gibi önemli işlevlere sahiptir (Daştan, 2008: 75).

Yaşanan değişimler işletmede bilgi teknolojilerinin en çok kullanıldığı bölümlerden birisi olan muhasebeyi önemli ölçüde etkilemiş ve farklı bir bakış açısı kazanılmasını sağlamıştır. Bilgi teknolojisindeki gelişmeler muhasebede elle işlem yapma sürecini neredeyse bitirmiştir. Üstelik muhasebe bilgi sistemleri daha hızlı, daha doğru, daha güvenilir hale gelmiş ve çok daha fazla sayıda muhasebe işlemi çok daha kısa sürede yapılabilmektedir (Toraman, 2008: 93). Çünkü bilgi teknolojileri sayesinde artık muhasebe bilgilerinin kaydedilmesi, sınıflandırılması, özetlenmesi ve raporlanması gibi süreçler daha basit bir şekilde ve kısa sürede gerçekleştirilmektedir. Dolayısıyla işletmeler bilgi teknolojisine dayalı bilgi sistemlerini kurarak daha hızlı, daha güvenilir ve daha az maliyetli bilgiler üretmeye başlamışlardır.

Günümüzde işletmeler tarafından gerçekleştirilen ekonomik olay ve işlemlerin artan bir biçimde elektronik ortamda gerçekleşmesi, bu olay ve işlemlerin tanımlanması, muhafaza edilmesi ve sunulmasıyla ilgilenen muhasebe bilgi sisteminin faaliyet ortamı kağıda dayalı ortamdan elektronik ortama taşınmıştır. İşlemlerin eş zamanlı gerçekleştiği bir ortamda muhasebe bilgi sisteminin fonksiyonlarının da eş zamanlı olarak gerçekleşmesi kaçınılmaz olmuştur (Ağca, 2007: 45). Bilgi teknolojilerindeki ilerleme, verilerin eş zamanlı olarak yevmiye defterine, defter-i kebire ve cari hesaba kayıtlanmasını sağlar ve bu nedenle bu veriler muhasebe fişlerine girilir girilmez finansal tabloları ve diğer raporları hazırlamak mümkün olmaktadır. Bilgi teknolojilerinin kullanımı; zaman, veri yoğunluğu ve veri çeşitliliği açısından sınırlamaları ortadan kaldırmaktadır. Bilgi teknolojilerindeki gelişmeler, farklı verilerin elde edilmesini, bunların tek bir veri tabanında saklanmasını ve bu verilerin farklı amaçlar için uygun şekillerde gerekli olduğu zaman raporlamasını mümkün kılmıştır (Sürmen ve Daştan, 2007: 225). İşletmelerin muhasebe bölümlerinde bilgi teknolojilerinin kullanımı, muhasebe bilgi sistemindeki zaman, bilgi yoğunluğu ve çeşitlilik sınırlamalarını ortadan kaldırmış, bilgilerin etkin bir biçimde düzenlenip yönetime sunulması olanağını sağlamıştır. Bilgi teknolojilerinin muhasebe bilgi sistemi içinde yer alması, insan hatası ve yetersizliği ile ilgili sorunların giderilmesi yanında verimlilik, kalite ve etkinlik gibi konularda olumlu etkiler sağlamaktadır (Daştan, 2008: 79-80). Önceleri sadece geçmiş olayları kaydeden bir "defter tutma sistemi" olan

muhasebe, bilgi teknolojileri yardımı ile planlama, değerlendirme ve analiz aracı haline gelmiştir. Bu bağlamda muhasebe, "kayıt" işlevinden "danışmanlık ve denetim" işlevine doğru yönelmiştir (Uyar ve Ünlüsoy, 2007).

Muhasebe bilgi sisteminde; gerek hesaplar üzerinde işlemlerin yapılmasında, gerekse para ve bilgi aktarımı ve finansal analiz gibi faaliyetlerde üst düzeyde bilgi teknolojisi kullanılmaktadır (Yereli, 2007: 16). Veri sağlayıcılardan elde edilen veriler, muhasebe bilgi sistemi vasıtasıyla işlenerek faydalı bilgiler elde edilmekte ve bu bilgiler üst yönetime, işletme içi ve dışı bilgi kullanıcılarına iletilmektedir. Bu süreç içerisinde bilgi üreticileri (örneğin, muhasebeciler) bilgilerin oluşumu ve toplanması açısından sisteme katkı sağlarken, bilgi muhafızları (örneğin, bilgi teknolojisi yöneticileri) bilgi teknolojilerinin tasarımı ve gelişimi konusunda katkı sağlamaktadırlar. Bilgi yöneticileri ise bilgi yönetimi, yani işletme bilgisinin üretilmesi, toplanması, saklanması, korunması ve dağıtılması için işletme içerisinde birtakım yöntemlerin geliştirilmesiyle muhasebe bilgi sistemine katkı sağlamaktadır. İç denetçiler ise muhasebe bilgi sisteminin gözlemlenmesi ile meşguldür ve işletmenin muhasebe bilgi sisteminin düzenli ve güncel bilgiyi doğru bir şekilde üreten bir bilgi sistemi olup olmadığını kontrol ederler.

İşletmelerde muhasebe bilgi sisteminin bilgisayar imkanlarının kullanılarak denetlenmesinde bilgisayar destekli denetim tekniklerinden yararlanılır. Bilgisayar destekli denetim tekniklerinin hedefi, denetçinin bir hesabı doğrulamada gerek duyduğu güvenceyi elde etmesinde denetçiye yardımcı olur (Çatıkkaş ve Yurtsever, 2009: 183). Bilgisayar destekli denetim araçlarının muhasebe bilgi sisteminin denetiminde kullanılmasının en önemli sebeplerinden biri işlenecek veri topluluklarının son derece büyük olmasıdır. Denetçinin uygulaması gereken maddilik testleri¹³ ve diğer denetim testlerinin sayısı ve bu testlerde incelenecek kayıt miktarı kaliteli, amaçlara uygun bir denetim faaliyetinin ve güvenilir bir denetim görüşünün hedeflendiği durumlarda son derece büyük miktarlara ulaşacaktır. Bu durumun da denetim çalışmasının süresi ve maliyetleri üzerinde çok büyük boyutlarda olumsuz bir etkisinin olacağı kesindir (Saygılı, 2005). Muhasebe bilgi sisteminde denetim gerçekleştirilirken ilk iş olarak sistemin doğru olarak kurulup kurulmadığının denetlenmesi gerekir. Bilgisayar kullanan işletmelerde bunun için iki ayrı kontrol mevcuttur. Bunlardan biri örgütsel kontroller, ikincisi ise donanım ve yazılım kontrolleridir (Türedi ve Dinç, 1997). İşlemlerin yetki

¹³ Maddilik testleri, finansal tablolarda yer alan parasal hataları ve yanlışlıkları ortaya çıkarmak için yapılan testlerdir (Erdoğan, 2006:102).

alanları içinde ve onay görerek yapılması ile işlemlerin kaydında girdi verilerinin tamlığı ve kesinliği konusunda muhasebe bölümünün sorumluluğu giriş kontrolleri ile desteklenmelidir (Erdoğan, 2006: 153).

İşletmelerin bilgi teknolojilerini kurarken başarılı bir muhasebe bilgi sistemini amaç edinmeleri, kullanılan bilgi teknolojilerinden en fazla faydayı elde etmelerini sağlamaktadır (Demir ve Bahadır, 2006: 58). Kullanılan bilgi teknolojilerine ve muhasebe bilgi sistemine işletmenin uyum gösterebilmesi çok önemlidir. Bazı işletmelerin yeni sistemlere uyum sağlayabilmesi için eski sistemlerini tamamen değiştirmeleri gerekebilir. Burada önemli olan işletmenin yapısına uygun ve işletmenin ihtiyaçlarına cevap verebilen teknolojilerin ve sistemlerin kullanımıdır.

Aşağıda bilgi teknolojilerinin yarattığı uygulamalar olan elektronik ticaret, internet, elektronik veri değişimi, kurumsal kaynak planlaması ve elektronik veri işleme teknolojilerinin muhasebe bilgi sistemi ile ilişkileri ele alınacaktır.

2.1. Elektronik Ticaret ve Muhasebe Bilgi Sistemi İlişkisi

Elektronik ticaretin kullanımı, işletmelerin geleneksel işlem biçimlerini ve süreçlerini tamamen değiştirmiştir. İşletmelerin bilgi/veri transferini en kısa sürede yapabilmeleri için, kritik muhasebe bilgisi gerekecektir.

Elektronik ticaret, işletme varlıklarını ve kaynaklarını etkiler, gelirlere veya giderlere neden olur ve finansal tablolarda açıklanması gereken olaylara götürür. Bu nedenle elektronik ticaret, muhasebe bilgi sistemiyle ilgili bir faaliyettir (Parlakkaya, 2005: 172).

Yasal zorunluluklar nedeniyle elektronik ticaret işlemlerinin de geleneksel ticarete olduğu gibi defter ve belgelerde izlenmesi gerektiğinden elektronik ortamda tutulacak defter ve kullanılacak belgeler konusundaki sorunların çözümü gerekmektedir. Bu sorunun çözümü, kullanılan bilgisayar programlarının belli standartları taşımasıyla mümkün olabilecektir (Parlakkaya, 2005: 172).

Elektronik ticaretteki gelişmeler, muhasebe sürecinde yer alan döngülerde, iş akışı ve süreçlerinde değişiklikler yaratmış ve mevcut yazılımlara yeni kabiliyetler kazandırılmıştır (Sevim, 2009: 46). Bu nedenle elektronik ticaretin beraberinde getirdiği değişime ayak uydurabilmesi için işletmelerin muhasebe bilgi sistemlerini değiştirmeleri gerekmektedir.

İşletmede kullanılan muhasebe yazılımları elektronik ticaretle entegrasyona sahipse, satış ve ödeme şekli ile ilgili bilgiler otomatik olarak satış, üretim, dağıtım ve muhasebe bölümlerine gönderilmekte ve muhasebeleştirme işlemleri anında gerçekleşmektedir. Kullanılan muhasebe yazılımı muhasebe bilgi sisteminin ihtiyaç duyduğu verileri otomatik olarak oluşturmaktadır. Bu durum, muhasebe bölümlerinde çalışan ve belge sayısında ve buna bağlı olarak maliyetlerde önemli ölçüde azalmaya neden olmaktadır. Ayrıca, muhasebe işlemlerinin güvenilirliği de artmaktadır. Ancak kullanılan muhasebe yazılımı, elektronik ticaret ile entegrasyona sahip değilse, elektronik posta ile gelen siparişlerin muhasebe bilgi sistemine manuel olarak girilmesi gerekecektir. Bu durum, çalışan ve belge sayısının ve buna bağlı olarak maliyetlerin artmasına ve muhasebe işlemlerinde güvenilirliğin azalmasına neden olacaktır (Parlakkaya, 2005: 173).

2.2. İnternet ve Muhasebe Bilgi Sistemi İlişkisi

İnternet, işletmelerin işlerini yürütme yöntemlerinde temel değişikliklere neden olmuştur. Bilginin üretilmesi, iletilmesi ve depolanması ile ilgili maliyetleri düşüren internet, çok yüksek oranda bilginin doğrudan, eş zamanlı ve ücretsiz olarak ilgili taraflara iletilmesini de sağlamaktadır.

Günümüzde işletmelerin elektronik ortamda gerçekleşen finansal nitelikli olay ve işlemlerine ait veriler, işlemlerin gerçekleşmesi ile eş zamanlı veya işlemlerin gerçekleşmesinden kısa bir süre sonra işletmelerin muhasebe bilgi sistemleri tarafından, yine aynı şekilde elektronik ortamda tanımlanabilmekte ve kayıt edilebilmektedir. Bu verilerden oluşturulan ve iç kontrol mekanizmasının süzgecinden geçen bilgiler, internet üzerinden işletmeyle ilgili taraflara sunulabilmektedir. Ayrıca internet; verileri toplama, işleme, sınıflandırma, saklama ve iletilme açısından da muhasebe bilgi sistemi üzerinde doğrudan etkili olmaktadır. Bilgi teknolojisindeki gelişmeler sayesinde çok kısa sürede ve çeşitli bilgi üretebilecek düzeye gelen muhasebe bilgi sisteminin ürettiği bilgilerin güvenilirliğinin işletme dışından üçüncü taraflarca yine aynı hızla onaylanarak bilgi kullanıcılarına zamanında sunulması mümkündür (Ağca, 2006: 66-67).

İnternet teknolojisinin yarattığı uygulamalardan birisi olan intranetler de işletme içi bilgi sistemlerine (muhasebe, finans, insan kaynakları, pazarlama, vb.) ve dokümanlara tek bir noktadan erişim sağlar. İtranetler işletmelerin tüm temel işlevleri

ile ilgili alanlara hızla yayılmış ve işletmelerin süreçlerini elektronik ortamda yönetebilmelerine yardımcı olmuştur. Geleneksel finansal raporlama sistemleri, karar alma ve performans ölçümü için gerekli olan bilgileri bütünleştirmekte güçlüklerle karşılaşabilir. İtranetler, muhasebe bilgi sistemindeki bilgilerin kullanışlı bir formatta ve zamanında ilgili taraflara sunulması ve çevrimiçi eş zamanlı bir bakış açısı sağlanması bakımından önemlidir (Sevim, 2009: 24). İşletmeler, işletme içi süreçleri koordine etmek için intranetleri kullanırken, müşterileri, işletme ortakları ve diğer işletmeler ile paylaşılan süreçleri koordine etmek için bir başka internet teknolojisi uygulaması olan extranetleri kullanmaktadırlar.

2.3. Elektronik Veri Değişimi ve Muhasebe Bilgi Sistemi İlişkisi

Elektronik veri değişimi sistemleri, muhasebecilere mevcut bilgiyi anında sağlamak suretiyle, işlemlerin neredeyse anında kaydedilmesini, işlenmesini, raporlanmasını ve iletilmesini sağlamaktadır (Ömürbek, 2003: 165).

Bilgi teknolojisindeki ilerlemeler, elektronik veri değişimi gibi elektronik çevrelerde, finansal işlemlerin farklı şekillerde ortaya çıkmasına neden olmuştur. Elektronik veri değişiminin kağıt yerine elektronik işlemleri getirmesi, iş akışının yapısını ve bilgi üretme sürecini değiştirmiştir (Sevim, 2009: 58). Bunun sonucunda finansal işlemler, geleneksel olarak kağıda dayalı faaliyetlerden oluşan çevreler yerine muhasebe bilgi sistemindeki elektronik çevreye doğru kaymıştır ve sonuç olarak kayıtlama, sınıflandırma, raporlama ve analiz etme gibi tüm süreçlerde de değişim meydana gelmiştir. Aynı zamanda bu değişim defter tutma, finansal tablo hazırlama, vergi beyannamelerinin düzenlemesi ve denetim uygulamalarında da değişim yaratmıştır. Bilgi teknolojilerindeki gelişmeler, insan hataları, verimlilik, kalite, maliyet ve etkinlik ile ilgili problemlerin azaltılması açısından muhasebe bilgi sistemini etkilemiştir (Sürmen ve Daştan, 2007: 218-219).

Muhasebe yazılımları, elektronik veri değişimi zincirine çevirici yazılımlar aracılığıyla bağlanmaktadır. Çevirici yazılımlar ile muhasebe bilgi sistemi yazılımları arasındaki bütünleşmenin artması, çeşitli elektronik veri değişimi yapılandırmalarının gelişmesine neden olmuştur. İlk düzey, çevirici¹⁴ ve muhasebe bilgi sistemi arasında herhangi bir bütünleşmenin olmadığı düzeydir. İkinci düzeyde çevirici, muhasebe bilgi

¹⁴ Çevirici, genellikle fax makinesidir.

sistemiyle bütünleşmiş durumdadır. Bu durumda çevirici özel bir yazılım ile ağa bağlanır. Çevirici aynı zamanda daha önce elektronik veri değişimi mesajları için hazırlanmış olan bir yazılım sayesinde muhasebe bilgi sistemi yazılımıyla bütünleşmektedir. Ana bilgisayar çevresindeki çevirici, ön uçtaki işlemciye bağlanmakta ve böylece gelen elektronik veri değişimi mesajlarını alarak uygulamalarla iletişim kurmaktadır. Gönderilen mesajlar, muhasebe bilgi sisteminin oluşturduğu dokümanların şifrelenmiş haliyle çeviriciden geçmektedir. Günümüzde yüksek teknolojiye sahip muhasebe bilgi sistemi yazılımları, elektronik veri değişimi kabiliyetlerini de birlikte sunmaktadır (Sevim, 2009: 72).

2.4. Kurumsal Kaynak Planlaması ve Muhasebe Bilgi Sistemi İlişkisi

Gelişen bilgi teknolojileri ve yönetim bilgi sistemleri muhasebe bilgi sisteminde de değişiklikler meydana getirmiştir. İşletmeler yaşanan değişimler nedeniyle işletme genelinde tam entegrasyonu hedef almışlardır. Bu yaklaşım kurumsal kaynak planlaması sistemlerinin geliştirilmesine yol açmıştır.

İşletmelerde bütünleşik sistemlerin¹⁵ kullanılmaya başlanması (bütünleşik bilgi sistemi yaklaşımı) her hangi bir amaçla bilgisayara girilen bir bilginin muhasebe kaydının otomatik olarak yapılmasını sağlamıştır. İşletmenin iç ve dış çevresinde bilgi kullanıcılarının bilgi ihtiyacını karşılama fonksiyonunu yerine getiren muhasebe bilgi sistemi, bu bütünleşik sistemin odağında yer almaktadır. Kurumsal kaynak planlaması yazılımlarının en önemli etkisi muhasebe süreçleri üzerinde gerçekleşmektedir. Kurumsal kaynak planlaması sayesinde muhasebe, kayıt giren bir fonksiyon olmaktan kurtulmakta ve analiz ve yorumlama fonksiyonuna daha fazla zaman ayırabilmektedir. Artık geleneksel muhasebe yazılımı yoktur, kurumsal kaynak planlaması yazılımları vardır (Sevim, 2009: 139).

Kurumsal kaynak planlaması, gerçek zamanlı ve çevrimiçi bilgi sağlamaktadır. Çünkü kurumsal kaynak planlaması ile birlikte bilgi, kaynağından direkt olarak alınmakta, böylece büyük miktarlarda ve kağıt üzerindeki bilgiyi işlemeye gerek kalmamaktadır. Veriler ve bilgiler gerçek zamanlı ve çevrimiçi olduklarından dolayı,

¹⁵ Bütünleşik (entegre) sistem, işletmede satın almadan satışa, muhasebeden insan kaynaklarına kadar tüm işletmecilik fonksiyonlarını aralarında bilgi alışverişine imkan sağlayacak şekilde birbirleri ile ilişkilendiren bir sistemdir (Aktaş, 2009: 22).

bütün işletme çalışanları planlama ve kontrol amacıyla aynı bilgiye erişebilmektedir (İlter, 2007: 17).

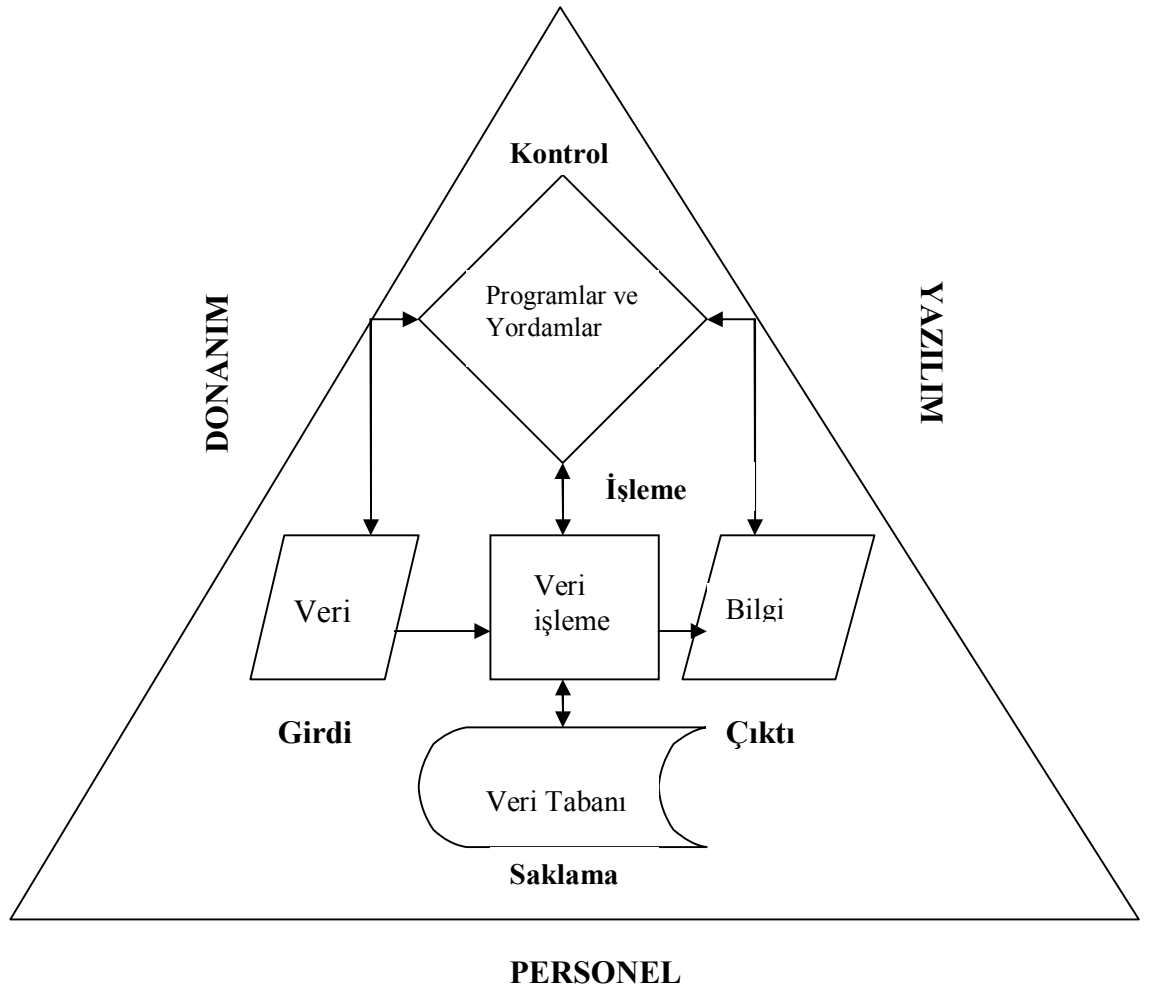
2.5. Elektronik Veri İşleme ve Muhasebe Bilgi Sistemi İlişkisi

Elektronik veri işleme, işletmede gerçekleşen olayların kayıt altına alınmasında ve güncellenmesinde destek sağlayan sistemlerdir. Muhasebe bilgi sistemi, işletmenin hedeflerine yöntemli ve sistematik bir biçimde ulaşmasını sağlamaya yönelik olup, bu süreçte elektronik veri işleme muhasebe bilgi sisteminin bel kemiğini oluşturmaktadır. Elektronik veri işleme, muhasebe bilgi sisteminin ayrıntılı tasarımını oluşturmada ve sistemi uygulamaya geçirmede rol oynamaktadırlar (Dinç ve Abdioğlu, 2009: 164).

Veri işleme süreci, ulaşılmak istenen ortak amaca uygun olarak girdileri kabul ederek çıktılar üretmektedir ve bu süreç birbiriyle ilişkili bileşenlerden oluşmaktadır. Temel bileşenler girdi, işleme ve çıktıdır. Bunlara ek bileşenler ise kontrol ve saklamadır. Elektronik veri işlemenin temelinde donanım, yazılım ve personel unsurları yer almaktadır. Donanım sisteme ilişkin fiziksel öğeleri, yazılım ise çeşitli donanım bileşenlerinin işlevini sağlayan ve denetleyen programları kapsar. Donanım ve yazılım öğelerini tamamlayan üçüncü unsur da bilgisayar personeldir (Erdoğan, 2006: 132).

Muhasebe bilgi sistemlerinin bilgi teknolojisi ile bütünleşmesi sonucu muhasebe verilerinin toplanması, işlenmesi, saklanması ve iletilmesinde önemli değişiklikler olmuştur. Buna paralel olarak, bir denetim çalışmasında denetçi tarafından izlenen denetim prosedürleri ve muhasebe bilgi sisteminin değerlendirilmesi ile ilgili iç kontroller elektronik veri işleme ortamından etkilenmiştir (Ömürbek, 2003: 175).

Aşağıda yer alan Şekil-1’de elektronik veri işleme sistemi gösterilmektedir.



Şekil-1. Elektronik Veri İşleme

Kaynak: Erdoğan, 2006: 133.

Elektronik veri işleme temel olarak şu şekilde sınıflandırılmaktadır:

1. Yığın işleme sistemleri
2. Çevrimiçi işlem sistemleri
3. Dağıtılmış sistemler
4. İletişim sistemleri
5. Zaman bölüşümlü sistemler
6. Veri tabanı sistemleri

Yığın işlem sistemleri, işlemlerin meydana geldikçe belgelere aktarılmasını, bu belgelerin belirli zaman aralıklarında biriktirilmesini, biriktirilmiş ve gruplanmış belgelerdeki verilerin bilgisayar ortamına aktarılmasını ve bu veriler üzerinde gerekli işlemlerin yürütülmesini sağlar (Kurnaz ve Çetinoğlu, 2010: 223). Yığın işlem daha

çok, geniş ölçüdeki rutin işlemlerin işlenmesinde kullanılan bir yaklaşımdır. Yığın işleme tipik örnekler olarak; satışlar, faturalama işlemleri, kasa tahsil ve kasa ödeme işlemleri, envanter kayıtlarını tutma uygulamaları, ücret ödemeleri, maliyet muhasebesi uygulamaları ve büyük defter işlemleri verilebilir (Erdoğan, 1998: 36).

Çevrimiçi işlem sistemleri, işlemlerin beklemeksizin ve biriktirilmeksizin yapılmasını öngörürler. Çevrimiçi işlem sistemi, girdi verilerinin olduğu yerden ve anında girildiği, çıktı bilgilerinin ise gereksinim duyulan ve gereksinim duyulduğu anda alınabildiği bir kullanım biçimidir. Çevrim içi işlem sistemleri, çevrimiçi yığın işlem sistemleri ve çevrimiçi gerçek zamanlı işlem sistemleri olmak üzere iki şekilde incelenir. Çevrimiçi yığın işlem sistemlerinde veri bilgisayara doğrudan verilir ve farklı bir zamanda işlenmek üzere saklanır. Çevrimiçi gerçek zamanlı işlem sistemlerinde ise veriyi uzaklık ve belirli bir zaman aralığı belirlenmeksizin anında işleyerek çıktı alınabilir (Kurnaz ve Çetinoğlu, 2010: 224).

Dağıtımli Sistemler; bir işletmede bilgisayar hizmetine gereksinim duyan çeşitli birimlerin ayrı ayrı bilgisayar kullanarak işleme çalışmalarını kendi sistemlerinde yürütmeleridir. İletişim Sistemleri; birden fazla bilgisayar arasında iletişim ağı kurularak bilgi alış verişini sağlayan bir sistemdir. Bu iletişim ağı, ülkelerarası düzeyde de oluşturulabilir. Zaman Bölüşümlü Sistemler; çok sayıda kullanıcının işlerini aynı anda yürütebilen bir işletim düzenidir (Erdoğan, 1998: 43). Veri tabanı sistemleri, birbiriyle ilişkili kütüklerin birleştirilmesiyle birbirinden bağımsız alanlarda ortaklaşa kullanıma imkan veren bir yapılandırma. Bu sistem sayesinde işletmeye ait tüm bilgiler ortak kullanıma açık hale gelir (Erdoğan, 2006: 140).

3. Bilgi Teknolojilerinin Yarattığı Uygulamaların İç Denetim İle İlişkisi

Bilgi teknolojilerindeki gelişmeler iç denetim mesleğini büyük ölçüde etkilemiştir. Bilgi teknolojilerinin işletmelerin günlük faaliyetlerinin yürütülmesinden finansal tabloların üretilmesine kadar birçok alanda kullanılmaya başlanması, bilgilerin elektronik ortamda işlenip saklanması ile birlikte bu elektronik ortamların denetimlerinin yapılması kaçınılmaz olmuştur. Manuel yöntemlerle yapılan denetim çalışmaları sırasında hem işletmedeki teknolojiye dayalı muhasebe sistemlerinin denetlenmesi hem de denetim sürecinin etkinliğinin artırılması konusunda yetersiz kalınmaktaydı (Ertaş ve Güven, 2008: 50). Denetim süreçlerinde bilgi teknolojisi

araçlarının kullanılmaya başlaması ile birlikte denetçilerin daha fazla dikkatli davranması ve bilgi teknolojilerinin anlamı, karmaşıklığı ve denetim sırasında kullanılacak verinin geçerliliği hakkında fikir sahibi olmaları gerekmiştir (Abu-Musa, 2008: 440).

İç denetim, işletme faaliyetlerinin kuruluş amaçları doğrultusunda, verimlilik ve rekabet gücünü arttıracak biçimde yönlendirilmesini, işletme varlıklarının rasyonel olarak yönetilmesini, yatırım ve yönetim danışmanlığını, işletmede hata ve hilelerin önlenmesini sağlamaya yönelik ve yönetime bağlı; ancak, yürüttüğü faaliyet yönünden bağımsız denetçiler tarafından yürütülen bir denetimdir (Kurnaz ve Çetinoğlu, 2010: 31). İç denetim, işletmelerdeki işlevleri kapsamında sağlanan kalite güvencesiyle, işletmenin bünyesinde bulunan finansal giriş ve çıkışlara yönelik bilgi teknolojilerine ilişkin iç kontrol sistemlerini değerlendirme hususunda yönetim ve denetim komitesine destek sağlamalıdır (Zhang, Zhau ve Zhau, 2007: 301). İç denetim finansal hesapların kontrolü, iç kontrol sisteminin oluşturulması ve izlenmesinin yanı sıra bilgi teknolojilerinin ileri düzeyde kullanımı nedeniyle risk yönetimi üzerinde de yoğunlaşmakta ve üst yönetime stratejik yönetim kararlarına rehber olacak nitelikte bilgiler aktarmaktadır.

İç denetim bölümünün örgütlenme sürecinde, düzenli ve güncel bilgiyi hızlı üreten ve ulaşabilen bir muhasebe bilgi sisteminin kurulmuş olmasına ihtiyaç vardır. Bu kapsamda ilgili işletmede; yetki ve sorumluluk alanına göre düzenlenmiş uygun bir hesap planı, muhasebe politika ve prosedürlerini ayrıntılı olarak düzenleyen bir muhasebe yönetmeliği, etkin bir bütçe, standart kontrol sistemi, iyi düzenlenmiş muhasebe belge ve formları bulunmalıdır (Uyar, 2009: 87). Muhasebe bilgi sisteminden sağlanan bilgiler yöneticiler tarafından işletmenin stratejik kararlarında, gelecekle ilgili yapılacak tahminlerde veri olarak kullanılmaktadır. Ekonomik faaliyetlerle ilgili belirli kriterlere uyularak toplanan bilgiler ve kanıtlar sistematik bir değerlendirme sürecinden geçmektedir. Burada iç denetim bölümüne önemli görevler düşmektedir (Karacaer ve İbrahimoglu, 2003: 226). İç denetim, muhasebe bilgi sistemleri ile ilgili olarak kullanılan kaynakların etkinliği ve verimliliği üzerinde görüş bildirir. Bu konudaki değerlendirmeler iç denetçiler tarafından raporlar halinde üst yönetime sunulur.

İç denetim işlevini, uygun bilgi teknolojilerini kendi etkinliği ve verimliliği için kullanmalıdır. Dolayısıyla iç denetçiler bilgi teknolojisi riskleri, kontroller ve bilgisayar

destekli denetim teknikleri kadar bilgi teknolojilerinin nasıl kullanıldığı ve işletmelerdeki kullanım şekilleri hakkında bilgi sahibi olmalıdır (Weidenmier ve Ramamoorti, 2006: 206). Aksi halde, bilgi teknolojilerindeki gelişmeler, bu konuda yeterli bilgi sahibi olmayan iç denetçiler için mesleğin icrasını oldukça güçleştirecektir.

Bilgi teknolojilerinin yarattığı elektronik bilgi ortamı, iç denetimin genel alanını ve kapsamını değiştirmiş; bu süreçte kullanılan tekniklerde ve anlayışta değişimler meydana gelmiştir. Dolayısıyla, iç denetçiler bu duruma uyum sağlamak amacıyla yeni denetim yöntemleri geliştirmişler ve bilgi teknolojilerini denetimde vazgeçilmez bir unsur olarak kullanmışlardır. (Selvi vd., 2006: 301-302).

Bilgi teknolojilerindeki gelişmeler iç denetimi güvence ve danışmanlık eylemi haline getirmiş ve iç denetim türleri arasına bilgi teknolojileri denetimi ve sistem denetimi gibi yeni denetim türlerinin katılmasına neden olmuştur (Uyar, 2009: 66). Ayrıca sadece iç denetim türleri açısından değil, iç denetim sürecindeki yaklaşımlar açısından değişimler yaşanmıştır. Bilgi teknolojileri alanında yaşanan gelişmelere bağlı olarak değişen beklentilere anlamlı ve hızlı bir şekilde karşılık verebilmek için bilgi teknolojilerinden faydalanılması işletmelerin risk özelliklerini, iç kontrol sistemlerinin değerlendirilmesini, finansal tabloların hazırlanması ve raporlanması süreçlerini önemli ölçüde değiştirmiştir. Bu değişimler sonucu sürekli denetim, risk odaklı iç denetim ve kontrol öz değerlendirme yaklaşımları gibi yaklaşımlar ortaya çıkmıştır¹⁶.

Bilgi teknolojilerinin işlem hızını arttırması ve denetim yazılımlarının kolaylığı etkili bir iç denetim yürütme fırsatı sağlamaktadır. İç denetim birimlerinin risklerini izlemek, gereksiz işlemleri tespit etmek, sapmaları ortaya çıkarmak için veri analizleri yapmak ve iç denetim biriminin verimliliğini arttırmak amacıyla bilgi teknolojilerinden yararlanılmaktadır (Demirbaş, 2005: 184).

Aşağıda bilgi teknolojilerinin yarattığı uygulamalar olan elektronik ticaret, internet, elektronik veri değişimi, kurumsal kaynak planlaması ve elektronik veri işleminin iç denetim açısından önemi ayrı başlıklarda ele alınacaktır.

3.1. Elektronik Ticaret ve İç Denetim İlişkisi

Elektronik ortamda gerçekleştirilen ticari işlemlerin artması, yalnızca iç denetim mesleğinin gereksinimleri arasında yer alan muhasebeye ilişkin becerilerin değil, aynı

¹⁶ İç denetim türleri ve yaklaşımlar ikinci bölümde detaylı olarak ele alınacaktır.

zamanda elektronik ticaret ve bilgi sistemlerindeki gelişmeye ilişkin gelişmiş bilgi ve becerilerin de edinilmesini gerektirmektedir (Pathak ve Lind 2006: 3).

Elektronik ticaretin iş ortamı üzerindeki etkisi göz önüne alındığında, bu gelişmeler risk faktörlerini tanımlamanın önemini ortaya çıkarmıştır. İç kontrolün etkili olmadığı bir ortamda gerçekleştirilen elektronik ticarete, sahte finansal raporlar veya yanlış mali tablo hazırlanması gibi durumlar ortaya çıkabilmektedir (Mock ve Turner, 2005:60). Etkin bir iç kontrol sistemi kurmak isteyen yönetimlerin temel hedefi, etkin bir bilgi sistemi, güvenilir bilgi ve verimlilik artışları hedeflerine ulaşmak olmalıdır. Etkin bir iç kontrol sistemi kurulurken öncelikle finansal verilerin kayıtlanması, işlenmesi, özetlenmesi ve raporlanması için özel politika ve prosedürler oluşturulmalıdır. Aynı zamanda işletmenin belirli işlem gruplarını yürütmek için gerekli kontrol usul ve yöntemlerine sahip olup olmadığının göz önünde bulundurulması gerekmektedir. Etkin bir iç kontrol sistemi için görevlerin ayrımı, yetki ve onay, geçerlilik, eksiksizlik, kayıtların uygulugu, koruma ve karşılaştırma ilkeleri dikkate alınmalıdır (Yılancı, 2001: 41).

Elektronik ticaret işlemlerinin örgütlenmesinde iç denetçiler bazı katkılar sağlamaktadırlar. İşlem değerlerinin tespiti, işlem sürecinin gözden geçirilmesi, onay sürecinin incelenmesi, dijital imza prosedürlerinin gözden geçirilmesi, elektronik ticaret işlemlerine dair bilgilerin gizliliği bu katkılar arasında yer almaktadır (TİDE, 2008: 247-248).

3.1.1. Elektronik ticaret görevinin anlaşılması ve planlanması

Elektronik ticaretin hızlı bir şekilde büyümesinin ve teknoloji değişikliklerinin, denetim planlarının hazırlanması ve uygulanmasında iç denetçilerin dikkate alması gereken önemli kontrol ve yönetim sorunları yarattığı açıktır. Bilgi teknolojisindeki devamlı ve kesintisiz değişiklikler, iç denetim mesleği için hem büyük fırsatlar hem de büyük riskler yaratmaktadır. Sistemler ve süreçler hakkında bir güvence vermeden önce bir iç denetçi, işteki ve bilgi sistemlerindeki değişiklikleri, bunlarla ilgili ve bağlantıları riskleri ve ayrıca stratejilerin kurumun tasarımına ve pazar koşullarına uygun olup olmadığını anlamalıdır (TİDE, 2008: 242)

İç denetim yöneticisinin bir elektronik ticaret işinin yürütülmesinde ilgilenmesi gereken konular, iç denetimin etkinliğini ve kapasitesini kapsar. Elektronik ticaret

projesi ve programı, elektronik ticaret sisteminin planlama, tasarım ve uygulamasının kurum stratejileriyle bütünleşmesi, sistemin performansı, güvenliği, güvenilirliği ve kullanıma hazırlığı, sistemin işlevselliği, idari ve hukuki koşullar, donanım ve yazılımın güvenilirliği, işlem süreçlerinin güncelliği, doğruluğu ve tamlığı, kontrol ortamı, risk değerlendirmesi, internetle ilgili riskler ve bilgi gizliliği iç denetçinin ilgilenmesi ve dikkate alınması gereken konulardır (TİDE, 2008: 243-244).

3.1.2. Elektronik ticaret riskleri ve kontrol sorunları

Bilgi teknolojisindeki devamlı ve kesintisiz değişiklikler, iç denetim alanında hem büyük fırsatlar hem de riskler yaratmaktadır. Elektronik ticaret genel olarak ticari faaliyet ve işlemlerin internet üzerinde yürütülmesidir. Elektronik ticaret risk ve kontrol ortamı oldukça karmaşıktır. Riski yönetme çabasında, öncelikle, risk unsurlarının anlaşılması ve kavranması şarttır. Bilgi güvenliği konusunda yeni zayıf ve savunmasız noktalar açan teknoloji değişikliklerinin ve yeni tehditlerin bilinmesi ve anlaşılması da önemlidir (TİDE, 2008: 245).

İç denetçinin ele alması gereken risk ve kontrol sorunlarının bazıları şunlardır (TİDE, 2008: 246):

1. Genel proje yönetim riskleri,
2. Hizmetin reddi, fiziksel saldırılar, virüsler, kimlik hırsızlığı, verilere yetkisiz erişim ve verilerin ifşası gibi özel güvenlik tehditleri,
3. Web sitesi incelemesi ve onayı,
4. Hızlı teknoloji değişiklikleri,
5. Bilgi güvenliği,
6. Vergi ve muhasebe sorunları gibi hukuki konu ve sorunlar,
7. Çevresel iş süreçlerinde ve işletme yapılarındaki değişiklikler.

3.1.3. Elektronik ticaret faaliyetlerinin denetlenmesi

Elektronik ticaret faaliyetlerinin denetiminin temel unsurları şunlardır (TİDE, 2008: 242-243):

1. Üst yönetimin belirlediği tarz da dahil iç kontrol yapısını değerlendirmek,
2. Hedef ve amaçlara ulaşabileceği konusunda makul güvence sağlamak,
3. Risklerin kabul edilebilir olup olmadığını tespit etmek,

4. Bilgi akışını anlamak,
5. Arayüz sorunlarını incelemek,
6. İş devamlılığı ve felaket sonrası toparlama planlarını değerlendirmek.

Denetimin hedefi, bütün elektronik ticaret süreçlerinde etkili iç kontrollerin bulunmasını sağlamak olmalıdır. Elektronik ticaretin yönetimi, çok geliştirilmiş ve onaylanmış bir stratejik planla belgelendirilmelidir. Bir elektronik ticaret görevinde denetim hedefleri şunları içerebilir (TİDE, 2008: 246-247):

1. Elektronik ticaret işlemlerinin delilleri,
2. Güvenlik sisteminin kullanılmaya hazırlık durumu ve güvenilirliği,
3. Elektronik ticaret ve finans sistemleri arasında etkin arayüz,
4. Parasal işlemlerin güvenliği,
5. Kimlik doğrulama sürecinin etkinliği,
6. İş devamlılığı süreçlerinin yeterliliği,
7. Genel ortak güvenlik standartlarına uyum,
8. Dijital imzaların etkin kullanımı ve kontrolü,
9. Şifreleme teknikleri,
10. İşletme verileri ve bilgilerinin yeterliliği ve zamanında elde edilmesi,
11. Etkin bir iç kontrol sistemini gösteren deliller.

İç denetçi suiistimallere karşı uyanık olmalıdır. Bunun için dikkat etmesi gereken hususlar şunlardır (TİDE, 2008: 248):

1. Yetkisiz para hareketleri,
2. Ödemelerin tekrarlanması,
3. Verilen veya alınan siparişlerin, teslim alınan malların ya da yapılan ödemelerin reddedilmesi,
4. İstisna raporları ve prosedürleri ve takip etkinliği,
5. Dijital imzalar,
6. Virüs ve korsanlık faaliyetlerine karşı korunma,
7. Erişim hakları,
8. İşlemlerin yetkisiz kişiler tarafından engellenmesi ve durdurulmasıyla ilgili geçmiş kayıtlar.

İç denetçi, yapılan işlemlerde kimlik doğrulamasıyla ve uygulanan kontrollerin değerlendirilmesiyle ilgili politikaları gözden geçirmelidir. Ayrıca iç denetçi veri

bütünlüğü üzerindeki kontrolleri ve yönetimin e-ticaret sürecini iyi yönetip yönetmediğini de değerlendirmelidir (TİDE, 2008: 248-249).

3.2. İnternet ve İç Denetim İlişkisi

Bilgi teknolojilerdeki değişiklikler ve internet uygulamalarının yaygınlaşması yararlanılabilen ve uygulanması gereken özel kontrol faaliyetlerini değiştirmektedir de kontrole duyulan temel gereksinimler önemini korumaktadır (Demirbaş, 2005: 171).

İnternetin kullanımı denetim sürecinde kullanılan teknolojilerde yenileşmeyi zorunlu kılmıştır. Bu konuda önde gelen başlıklar, kontrol öz değerlendirme yaklaşımı, otomatik çalışma kağıtları, bütünleştirilmiş denetim ve sürekli denetim olmuştur.

Kontrol özdeğerlendirme yaklaşımı, işletme amaçlarının, bu amaçların gerçekleştirilmesinde karşı karşıya kalınan risklerin ve bu risklerin belgelerinin ele alınması için iç denetimin gözden geçirilmesidir. Kontrol öz değerlendirmesi iç denetçilerin denetledikleri birim, faaliyet ve sistem içinde mevcut risklerin ve kontrollerin tespit edilmesi amacıyla uygulanır. Bu süreçte iç denetçiler eğitmen gibi görev yaparlar, ancak sürece karışmazlar. Yani, risk ve iç kontroller denetim konusu alanın yönetimi ve çalışanları tarafından pek çok farklı yöntem kullanılarak takım çalışması ile belirlenir (Alptürk, 2008a: 35). Kurucu veya lider kim olursa olsun, kontrol öz değerlendirmesi, paydaşların işletmenin amaçlarından daha fazla haberdar olmasını ve işletme amaçlarının başarılmasında iç kontrolün rolünün göz önüne alınmasını sağlayarak, işletmenin kontrol çevresini geliştirmiş olacaktır. Hatta kontrol süreçlerinin tasarımı, uygulanması ve sürekli geliştirilmesi için çalışanları teşvik edecektir. Eğer iç kontrol sistemi, faaliyetleri tüm yönleriyle kapsayan büyük bir ERP sistemini izliyorsa, kontrol öz değerlemesi daha da etkin olacaktır (Moeller, 2004: 156)

Otomatik çalışma kağıtları, özellikle denetçinin kişisel olarak takip etmesi gereken anormallikler veya hataların tanımlanması süreçlerinde kullanılmaktadır ve dolayısıyla etkin elektronik iletişim sistemlerini gerektirmektedir (Nastase ve Nastase, 2007: 45).

Bütünleştirilmiş denetim, risk odaklıdır. İç denetim işlevi açısından işletmedeki riskler ele alınmaktadır. İşletme içinde ve çevresindeki riskler tanımlanır ve belirlenen risklere karşı iç denetim mekanizmaları oluşturulur. İşte bu safhada bilgi teknolojileri,

internet teknolojisinin yapılanması, yönetimi ve kontrolü gibi alanlarda tanımlanmalıdır (Nastase ve Nastase, 2007: 46).

Sürekli denetim, teknolojik imkanlardan yararlanarak otomatik metotlarla belirli bir aralıkta düzenli ve sürekli olarak bilgi teknolojisi sistemlerinin, mali verilerin oluşumunu sağlayan en detaylı işlemlerin ve süreçlerin izlenmesi, kontrol ve risk değerlendirmelerinin yapılmasıdır (Sevimli, 2009: 30). Sürekli denetimde internete bağlı olarak oluşmuş süreçlerin denetiminde sorgu araçları, istatistik ve veri analizi, veri tabanı yönetim sistemleri, veri bankaları, yapay zeka, iliştilmiş denetim modülleri, çeşitli bilgileri bir arada tutan network teknolojisi ve XBRL kullanılmalıdır (Nastase ve Nastase, 2007: 48).

Artık günümüzde işletmeler finansal tablolarını ve raporlarını internet erişim sayfalarından yayınlamaktadır. İnternet ortamında finansal raporlama sürecinde İşletmelerde Genişletilebilir İşletme Raporlama Dili (XBRL) kullanılmaktadır. XBRL, finansal bilginin hazırlanmasını, yayınlanmasını ve denetlenmesini kolaylaştıran, ticari işlemlerin raporlanması için standart hale getirilmiş elektronik bir dildir (Aktaş ve Başcı, 2007: 44). XBRL, kabul edilmiş muhasebe standartlarını kullanarak internet dahil çeşitli teknolojiler arasında eş zamanlı finansal bilgi alış verişi sağlayabilir. XBRL formatı altında kullanılan gerçek zamanlı muhasebe sistemleri, sektör şartnamelerine ve sınıflandırmalarına uygun elektronik finansal raporlamaların en uygun şekilde kullanılmasını belirlemek için iç denetçileri cesaretlendirmektedir (Kurnaz ve Çetinoğlu, 2010: 195). Denetçiler, XBRL sayesinde bilgiye daha hızlı, konsolide bir biçimde erişme ve analizlerin otomatik hale gelmesi gibi avantajlardan faydalanır. Ayrıca denetçiler elektronik formatta aldıkları bilgiyi, başka bir formata dönüştürerek yeniden kullanabilirler. Ayrıca XBRL, veri transferinin eş zamanlı gerçekleşmesini sağlayarak, eş zamanlı raporlamanın ve sürekli denetimin gerçekleştirilmesine imkan sağlamaktadır. İşletmeye ilişkin finansal bilgilerin analiz edilmesinde ve kullanılmasında etkili ve hızlı bir ortam yaratan XBRL, şeffaflık sağlamakta, işlem maliyetlerini azaltmakta ve işlem etkinliğini arttırmaktadır. Bu sayede sürekli gözden geçirme, sürekli denetim ve işletme içi ve işletme dışı finansal analiz faaliyetlerinin geliştirilmesi mümkün olmaktadır (Aktaş ve Başcı, 2007: 54-57).

3.3. Elektronik Veri Değişimi ve İç Denetim İlişkisi

Elektronik mesajlar, belirli kaynak dokümanlarla yer değiştirebilir. Örneğin, satın alma emirleri, hesap pusulaları, gönderilen faturalar, çekler gibi belgeler içerdikleri elektronik veri değişimleri yoluyla elektronik mesajlara dönüşebilmektedir. Elektronik veri değişimi yardımıyla, firmanın kendisi, müşterileri, tedarikçileri, haberleşme hatları yardımıyla iş ilişkilerini elektronik ortamda devam ettirebilmektedirler. Ancak, bazı elektronik kanıtlar kısa dönemde ortaya çıkabildiği için, belirli bir dönem içerisinde değiştirilmez veya yedeklenmezse kullanılamaz hale gelebilirler. Bu nedenle, denetçilerin elektronik bilginin ortaya çıktığı tarihe dikkat etmeleri veya elektronik bilginin oluştuğu zamanı, biçimini ortaya koyan doğrulayıcı testlerin kontrol amaçlı olarak uygulanması gerekmektedir. Elektronik veri değişimi, kağıt içermeyen muhasebe sistemlerinin denetiminde, denetçinin birkaç denetim ve kontrol uygulaması yapabilmesine olanak sağlar. Elektronik veri değişimi vasıtasıyla müşteri firmanın işlerini nasıl devam ettirdiğini anladıktan sonra, denetçiler denetim plan ve süreçlerini, bu bilgilere göre yeniden oluşturmalıdırlar (Toraman, 2002).

Elektronik veri değişimi, firmadan çevreye veya çevreden firmaya gerçekleşen tüm işlemlerde tek yetkilidir, süreç devam ederken, kopya edilemez, kaybolmaz veya değiştirilemezler ve sadece yetkili olan personel verilere girebilir. Bunlar elektronik veri değişimi sistemlerinin iç kontrol üzerinde önemli etkiye sahip olduğunu göstermektedir. Elektronik veri değişimi, denetçilerin müşterinin iç kontrol sistemlerinin etkinliğini ve yeterliliğini belirlemeye uygun denetim süreçlerini uygulamasını gerektirir. Ayrıca firmada alım-satım gibi faaliyetler devamlı meydana geldiği için, elektronik veri değişimi sistemlerinin, süreç içerisinde meydana gelen hataları bulması ve düzeltmesi gerekmektedir. Dolayısıyla her zaman uygun koruma yöntemlerinin (firewalls, şifreleme, vs.) uygulanması gerekmektedir (Toraman, 2002).

3.4. Kurumsal Kaynak Planlaması ve İç Denetim İlişkisi

Kurumsal kaynak planlaması sistemlerini kuran birçok işletme ortak veri tabanı sayesinde fonksiyonlar arası bilgi tutarsızlığını azaltmayı amaçlamaktadır.

Kurumsal kaynak planlaması sistemlerinin kurulması süreçlerin otomatikleştirilmesini ve çalışan sorumluluklarının elektronik ortama taşınmasını sağlayarak profesyonelleri izleme maliyetlerinin azalmasına neden olacaktır. Kurumsal

kaynak planlaması tek bir veri tabanına ulaşımı kolaylaştırmasıyla, yöneticiler çalışanların hareketlerini etkin biçimde eş zamanlı olarak izleme imkanına ulaşacaklardır. Genellikle kurumsal kaynak planlaması sistemleri izleme faaliyetlerinin verimliliğini artırmakta ve çalışanların hatalarını azaltmaktadır. (Demir ve Bahadır, 2006: 64).

Kurumsal kaynak planlaması gibi çok karmaşık ve çok yaygın bir şekilde tüm işletme türlerinde uygulama alanı bulan sistemlerin denetiminde en önemli nokta iç kontrol yapısının iyi bir şekilde ele alınması, anlaşılmaya çalışılması ve söz konusu risklerin belirlenmesidir. Böylece sürekli denetimden de verim alınabilir. Diğer bir ifadeyle sürekli denetimde iç kontrol sistemi üzerine yoğunlaşmak ve sistemin etkinliğini ve verimliliğini ölçmek temel amaç gibi algılanmaktadır. Kurumsal kaynak planlaması sistemlerine sahip işletmelerde genelde iç kontrol sisteminin güvenliğini sağlamak için riskleri azaltmak amacıyla SysTrust, WebTrust gibi güvenlik sistemleri kullanılmaktadır. Denetçi kurumsal kaynak planlaması sistemleri kullanılan işletmelerde, işletmenin iç kontrol sisteminin değerlerken “Bütünleşik Test Tekniği¹⁷” olarak adlandırılan kontrol testlerini yapmak zorundadır. Çünkü bu tür sistemlerin gerçek zamanlı olarak, elektronik veri değişimi şeklinde ve genişletilebilir işletme raporlama diline (XBRL) sahip olması nedeniyle bütünleşik test tekniği ile iç kontrol sisteminin etkinliğinin ölçülmesi gerekir (Selimoğlu, 2006a: 286-288).

3.5. Elektronik Veri İşleme ve İç Denetim İlişkisi

Elektronik veri işleme sürecinde yer alan kontroller, işlemlerin doğru, eksiksiz ve yetkiye dayalı olarak kayıtlara geçmesini sağlarlar. Veri girişlerinin doğruluğu, belirlenmiş bir düzenlemeye veya kontrol dosyalarına uygunluğu karşılaştırılarak sağlanır. Günümüzde bilgisayarlı sistemler bu karşılaştırmaları yapmakta ve mutabakatlara yazılım düzeyinde sahip olunmaktadır. İç kontrol sistemi artık elektronik veri işleme teknolojilerinin gelişimi ile birlikte bilgisayarlarda yazılım düzeyinde yapılandırılmış durumundadır (Yılancı, 2006: 68). Denetçi, iç kontrol faaliyetlerinin yeterliliği ve etkinliği üzerinde gerçek zamanlı muhasebe sisteminin kontrol risk merkezli denetim planını kullanmalıdır Ayrıca denetçi, gerçek zamanlı muhasebe

¹⁷ Bütünleşik test tekniği ile denetçi işletme uygulamalarının mantığını ve kontrollerini tüm muhasebe bilgi sistemini içerecek şekilde test edebilir. Denetçi, hayali kayıtlar yaratarak bu kayıtları kukla verilerle çalıştırabilir ve böylece testin etkinliği önemli ölçüde artmış olur (Erdoğan, 2006: 171).

sisteminde bilginin geçerliliğini ve güvenilirliğini sağlayacak şekilde ticari işlemlerin akışını ve ilişkili kontrol faaliyetlerini anlamalıdır. (Kurnaz ve Çetinoğlu, 2010: 191).

Güvenilir elektronik veri işleme teknolojileri geliştirildikçe, defter ve belgelerin olmadığı bir dünyada yaşamamız mümkün olacaktır. Bu gelişmeler sayesinde, gerçekleştirilen işlem türleri ile her işletmede ortaya çıkabilecek gereksinimler karşılanabilecek şekilde bir yapılandırma oluşturulacaktır (Pekdemir ve Önal, 1999: 10). Modern işletmelerde, kağıt dokümanlardan elektronik veri işlemeye ve çevrimiçi gerçek zamanlı işlemlere geçiş, denetim alanındaki uygulayıcılar ve meslek örgütleri açısından iç denetim mesleğine ilişkin ciddi kaygıları gündeme getirmiştir (Liang, Lin ve Wu, 2001:130). Gelişen bilgi teknolojilerinin yarattığı kaygılar, bu teknolojilerin bazı riskleri beraberlerinde getirmeleriyle ilgilidir. Örneğin, elektronik veri işleme teknolojilerinin kullanımı hatalı işlemleri azaltmış olsa da hileli işlemlerin sayısını arttırmıştır. Ortaya çıkan güvenlik açıkları aracılığı ile kimlik gizleme, kimlik taklidi, yetkisiz girişler gibi pek çok bilgi güvenliği tehdidinin gerçekleşmesi mümkün olmaktadır.

İkinci Bölüm

İç Denetim ve İç Denetimin Değişen Faaliyet Alanları

1. İç Denetim İle İlgili Genel Bilgiler

İç Denetçiler Enstitüsü (IIA) sayesinde profesyonel anlamda bir meslek olarak kabul gören iç denetim, değişen koşullara ayak uydurarak gelişimini sürdürmüş ve iç denetimin üstlendiği sorumluluklar ve güvence ve danışmanlık hizmetlerini yürüttüğü alanlar zamanla işletmelerin ihtiyaçlarına uygun olarak değişmiştir. Yaşanan bu değişimler iç denetim tanımlarının güncellenmesine neden olmuştur. 1940'lı yıllarda iç denetim sadece muhasebe faaliyetleri ile ilgilenmekteyken günümüzde artık bir bütün olarak işletme faaliyetleri ile ilgilenmektedir.

Aşağıda iç denetim ile ilgili genel bilgiler kapsamında iç denetimin tanımı ve tarihsel gelişimi, amaçları, önemi, faydaları, işlevleri, ilkeleri, uygulama süreci ve iç denetçiler ve uluslar arası iç denetim standartları ayrı başlıklar altında ele alınacaktır.

1.1. İç Denetim Kavramı

Değişen ticari şartlar işletmeleri dinamik bir yapıya kavuşturmuş ve hızlı bir rekabet ortamı içine almıştır. Bu şartları ve rekabet ortamını dikkate alan işletmeler gelecekle ilgili belirsizlikleri ortadan kaldırma adına çeşitli çabalar göstermeye başlamışlardır. Bu açıdan işletmeler daha kaliteli mal ve hizmet üreterek, rekabet ortamında varlıklarını sürdürebilmek için organizasyon yapılarını gözden geçirerek çeşitli yeniliklere uyum sağlamaya çalışmışlardır.

İç denetim faaliyeti işletmelerin bu değişim süreci içinde organizasyonlarının yenilenmesinde öncelikli olarak örgütsel yapı içinde yer almaktadır. İşletmelerin her türlü faaliyetlerini geliştirmek ve katma değer sağlamak için bağımsız, tarafsız ve objektif bir güvence ve danışmanlık hizmeti sağlayan iç denetime ihtiyaç duyulmaktadır. İç denetim değişen koşullar dikkate alınarak geliştirildiğinde gelecekle ilgili beklentileri ve hedefleri garantilemeyi sağlamaktadır. İç denetim bu gelişim ve değişim sürecinde kendine düşen görev ve sorumlulukları yerine getirirken, işletme,

işletme yöneticileri, işletme çalışanları ve işletme içindeki diğer tüm bölümlerle kendi işlevlerini bütünleştirmekte ve işletme içindeki her kişiye ve bölüme yardımcı olmaktadır.

1.1.1. İç denetimin tarihsel gelişim ve tanımı

İç denetim kavramını iyi açıklayabilmek için öncelikli olarak kısaca denetim ve kontrol kavramlarından bahsetmek yerinde olacaktır. Literatürü incelediğimizde çoğu yerde denetim ve kontrol kavramlarının bir arada ve yakın anlamlarda kullanıldığını görebiliriz. İşletme yönetimi ile ilgili kitaplarda yönetimin bir fonksiyonu olarak bazen kontrolün bazen denetimin ele alındığını görmekteyiz.

Pek çok yazar denetim kavramını kontrol kavramı ile açıklamıştır. Bunun sebebi kontrol kavramının denetim kavramını da içine alan çok geniş bir kavram olmasıdır. Kontrol; bir kişinin, bir örgütün veya bir konunun üzerinde egemenlik kurmayı ve onu istenilen yöne yöneltmeyi sağlayan yöntem ve davranıştır (Yılancı, 2006: 3). Kontrol, önceden belirlenmiş politikalar ve kararlar vasıtasıyla işletmeyi belirlenen bir amaca ulaştırma gücünün işletmede var olması olarak da tanımlanabilir (Kepekçi, 1982: 9). Kontrol, bir sistem içerisine yerleştirilmiş olan faaliyetleri ifade eder; işlemlerin ve kayıtların yapıldığı süreçte uygulanır ve süreklilik gösterir. Kontrol, işletmenin uyum ve reaksiyon gösterme yeteneğinin artmasını ve koordinasyon özelliğinin geliştirilmesini amaçlamaktadır (Yılancı, 2006: 3).

Denetim ise ekonomik faaliyet ve olaylarla ilgili beyan edilen bilgilerin önceden oluşturulmuş kriterlere uygunluk derecesini belirlemek için bu ekonomik faaliyet ve olaylara ilişkin bilgilerle ilgili delillerin objektif olarak elde edilmesi, değerlendirilmesi ve sonuçların bu bilgilerle ilgilenen taraflara iletilmesini sağlayan sistematik bir süreçtir (Bozkurt, 2010: 24). Denetim, uygulamaların etkinliğini ölçen ve bu uygulamaları önceden belirlenmiş bir amaca yönlendiren bir süreçtir. Denetim, iş sürecinden bağımsızdır ve işletme dışından kurmay görevi üstlenmiş kişiler tarafından yürütülür. Buraya kadar yapılan tanımlamalardan da anlaşılacağı üzere denetim, işletmede kontrolü sağlamak için kullanılan bir araçtır. Kontrol ise içerisinde denetimi de barındıran daha geniş bir kavramdır (Yılancı, 2006: 4-6).

İç denetim, ilk olarak fiziki eşya ve işletme varlıklarının korunması amacıyla gözlem ve sayım yapmıştır. Zamanla işletmelerin büyümesi, belge ve kayıtların

artmasına ve denetimde kayıtların incelenmesi yerine örnekleme yönteminin kullanılmasına neden olmuştur. Böylelikle iç kontrolün önemi de artmış ve 1940'lı yıllarda iç denetim iç kontrol odaklı denetime dönüşmüştür (Kishalı ve Pehlivanlı, 2006: 81-82).

İşletme yapılarındaki değişimlerle birlikte iç denetim uygulamalarında da köklü değişimler yaşanmaya devam edilmiştir. 1950'li yıllarda iç denetim faaliyetleri finansal denetimlere odaklanmış ve finansal işlemlerin doğruluğunun değerlendirilmesi rolünü üstlenmiştir (Memiş, 2008: 77). 1960'lı yıllarda iç denetim işletme verilerinin güvenilirliğinin denetlenmesi iken 1970'li yıllarda uygunluk denetiminin yapılması ve 1980'li yıllarda işletme etkinliğinin denetlenmesi olarak gerçekleşmiştir (Memiş, 2006: 83). 1990'lı yıllara geldiğimizde ise iç denetim, riskleri yönetmek için gerekli alt yapıya sahip olacak şekilde yeniden yapılandırılmıştır. Böylece iç denetim, geçmişin incelenmesi değil, bugünün ve geleceğin dikkate alınmasıyla birlikte işletme yönetimine yol gösteren ve işletmenin amaçlarına ulaşmasına yardımcı olan fonksiyon olmuştur. 2000'li yıllarda Enron gibi işletme skandallarının ortaya çıkmasıyla iç denetim işletmenin en üstüne rapor veren ve kurum içinde vazgeçilmez niteliğe sahip olan bir yapı haline gelmiştir. Sonrasında yeni iç denetim standartları ve iç denetime ilişkin çeşitli düzenlemeleri içeren Sarbanes-Oxley Yasası (2002) yayınlanmıştır (Uyar, 2009: 55).

Büyük işletmelerdeki hissedarlar ve yönetim kurulu üyeleri, şirket çalışanlarının faaliyetlerinin etkinliği hakkında bilgi sahibi olmak isterler. Hissedarların bu istekleri doğrultusunda, vekalet teorisi kapsamında yetkilendirilmiş müdür ve diğer çalışanların faaliyetleri, denetim komitesinin bir bölümü şeklinde hizmet veren iç denetim bölümü tarafından izlenmektedir. İç denetim bölümü bir güvence sistemi olarak, kayıtların doğrulundan ziyade, organizasyonun eğilimlerini dikkate alan ve organizasyondaki işlemlerin etkinliği ve verimliliği üzerine katma değer yaratan bir faaliyet olarak görülmektedir (Tuan ve Memiş, 2007: 89).

İç Denetçiler Enstitüsü tarafından 2003 yılında yapılan en son tanım ise şöyledir: İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. Ayrıca iç denetim, kurumun risk yönetimi, kontrol ve kurumsal yönetim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım

geliştirilmesine yardımcı olur (Hass, Abdolmohammadi ve Burnaby, 2006: 836). Bu tanıma göre iç denetim, bir güvence hizmeti olarak, kayıtların doğruluğundan ziyade, işletmenin eğilimlerini dikkate alan ve işletmedeki işlemlerin etkinliği ve verimliliği üzerine katma değer yaratan bir faaliyet olarak görülmektedir. Böylece iç denetim, işletme içerisinde daha fazla önem kazanmış ve bunun yanında daha fazla sorumluluk alan bir birim haline gelmiştir. İşletme çalışanları, iç denetim biriminin önderliğini daha iyi anlamış ve gerek organizasyon gerekse üst düzey yöneticiler bu birimden daha yüksek düzeyde fayda sağlar hale gelmişlerdir (Memiş, 2007: 461-462). Fakat unutulmaması gereken bir gerçek vardır ki, iç denetim, üst yönetim danışmanlığı ile bağımsızlık arasındaki ince çizgide yer almaktadır (Abu-Musa, 2008: 441). İşletmenin faaliyetlerini incelemek ve değerlendirmek suretiyle işletmeye hizmet sunan ve işletme içerisinde oluşturulmuş olan iç denetim, bağımsız bir değerlendirme fonksiyonudur (Moeller ve Witt, 1999: 11).

Bu tanımlamadan faydalanarak iç denetimi aşağıdaki şekilde unsurlarına ayırabiliriz (Korkmaz, 2007: 5):

1. Objektif olması,
2. Güvence ve danışmanlık hizmeti vermesi,
3. Kurumun faaliyetlerini geliştirmesi ve değer kazandırması,
4. Kurumun hedeflerinin geliştirilmesine yardımcı olması,
5. Risk yönetimi, iç kontrol süreçleri ve kurumsal yönetim süreçlerinin denetimi,
6. Sistematiik ve disiplinli çalışma.

İç denetim ile ilgili önemli çalışmalar yapan Sawyer'e (2005) göre iç denetim; bir örgütte a) finansal ve finansal olmayan bilgilerin doğruluğu ve güvenilirliği, b) işletmenin karşı karşıya olduğu risklerin tanımlanması ve en aza indirilmesi, c) dış düzenlemelere, iç politika ve yordamlara uyulması, d) standartlara uyulması, e) kaynakların etkin ve verimli kullanılması ve f) örgütsel amaçlara etkin bir şekilde ulaşılması konularında tüm faaliyetlerin ve kontrollerin iç denetçiler tarafından sistematiik ve objektif olarak değerlendirilmesidir (Sawyer, Dittenhofer ve Scheiner 2005: 10).

INTOSAI (Uluslararası Yüksek Denetleme Kuruluşları Örgütü-International Organization of Supreme Audit Institutions) Denetim Standartlarında ise iç denetim,

yöneticilerin hesabını vermekle yükümlü oldukları yönetim süreçlerinin yolsuzluk, hata, verimsiz ve israfçı uygulamaları en aza indirecek şekilde işlediği konusunda güvence sağlayan fonksiyonel araçlar olarak ifade edilmiştir (Uyar, 2009: 53).

İç denetim, işletme faaliyetlerinin ve uygulayıcıların yaptıkları işlerin, uygunluk ve etkinliğinin, üretilmiş her türlü bilginin güvenilirliğinin, finans, muhasebe ve diğer tüm alanlardaki kontrollerin işlerliğinin araştırılıp üst yönetime rapor edilmesidir (Tuan ve Sağlar, 2004: 2) İç denetim faaliyeti, işletmenin yönetimini, faaliyetlerini ve bilgi sistemlerini kapsayacak kontrollerin yeterliliğini ve etkinliğini değerlendirmelidir. Bu değerlendirme, finansal ve operasyonel bilgilerin güvenilirliğini ve bütünlüğünü, operasyonların etkinliğini ve verimliliğini, aktiflerin korunmasını, yasa, düzenleme ve sözleşmelere uyumu içermelidir (Alptürk, 2008a: 21).

İç denetim, artık işletmedeki iş akışlarından birisi olarak kabul edilmektedir. İşletmedeki tüm bölümlerin yaptığı gibi iç denetim de organizasyona katma değer sağlayan bir birim olmalıdır (Memiş, 2006: 87). Değer yaratabilmek üzere iç denetçi, daha iyi yönetim uygulamalarına yol açacak gelişmeler için önerilerde bulunmalı ve işletmenin bütün faaliyetlerini incelemelidir. İç denetim işlevinin kapsamını, işletmenin iç kontrol sistemlerinin verimliliği ve etkinliği ile performans kalitesinin incelenmesi ve değerlendirilmesi faaliyetleri oluşturur (Özeren, 2000: 1).

İç denetimin kapsamına giren faaliyetleri şu şekilde sıralayabiliriz (Uyar, 2009: 59-60):

1. İç kontrolün yeterliliğini sağlamak, etkin kontrol sistemleri geliştirmek ve uygulamak,
2. Hata ve hileleri ortaya çıkarmak ve önlemek,
3. Faaliyet ve işlemlerin belirlenmiş politikalar, planlara ve yönergelere uygunluğunu araştırmak,
4. İşletme varlıklarını her türlü zarara karşı korumak,
5. Yönetimin düzenlediği her türlü bilginin doğruluk ve güvenilirliğini araştırmak,
6. Üstlenilen sorumlulukların yerine getirilmesi ile ilgili faaliyetlerin kalitesini araştırmak,
7. Faaliyetlerle ilgili iyileştirme önlemlerini yönetime tavsiye etmek,
8. Üst yönetime bağlı olarak görev almak,

9. Raporlama prosedürlerini yerine getirmek.

Görüldüğü üzere iç denetimin kapsamına hem finansal nitelikte, hem de finansal olmayan nitelikte işlemler girmektedir. Bu kapsam içerisinde iç denetimin tavsiye etme, uygulama, raporlama ve danışmanlık olmak üzere dört önemli rolü vardır.

Günümüzün iş ortamında iç denetim bölümü, sağladıkları katkıların dışarıdan nasıl görüldüğünü dikkate almalıdır. Denetimde değer katma faaliyetleri ortaya çıktıkça, denetimin iç şekli değişmeye başlamıştır. İç denetimi işletme için bir maliyet olarak gören yönetimler, artık iç denetim bölümünü bir kar merkezi olarak görmeye başlamışlardır (Majdalawieh ve Zaghloul, 2009: 358).

1.1.2. İç denetimin amaçları

İç denetim, işletme faaliyetlerinin amaç ve politikalara, kalkınma planına, programlara, stratejik planlara, performans programlarına ve mevzuata uygun olarak planlanmasını ve yürütülmesini, kaynakların etkili, ekonomik ve verimli kullanılmasını, bilgilerin güvenilirliğini, bütünlüğünü ve zamanında elde edilebilirliğini amaçlar. İç denetim, güvence sağlamanın yanında, özellikle risk yönetimi, kontrol ve kurumsal yönetim süreçlerini geliştirmede yönetime yardımcı olmak üzere bağımsız ve tarafsız bir danışmanlık sağlar (Sezal, 2006: 43).

İç denetimin bazı belirgin amaçlarını şu şekilde sıralayabiliriz (Uyar, 2009: 61):

1. Bir işletmede finansal olmayan kontroller de dahil olmak üzere faaliyetlerin etkinliği, verimliliği ve yeterliliğinin sağlanması, işletme faaliyetlerinin sağlıklı ve verimli bir şekilde yürütülmesi,
2. İşlemlerin önceden saptanmış işletme politikasına uygunluğu ve doğruluğunun kontrol altında tutulması, işlemlerin amaçlara, programlara, stratejik planlara, performans programlarına ve mevzuata uygun olarak planlanması ve yürütülmesi,
3. İşletme varlıklarının etkin ve verimli bir şekilde kullanılmasının sağlanması, varlıkların güvence altına alınması,
4. Bilgilerin güvenilirliğinin, bütünlüğünün ve zamanında elde edilebilirliğinin sağlanması,
5. Muhasebe ve iç kontrol sisteminin yeterlilik ve etkinliğinin incelenmesi, değerlendirilmesi, risklerin asgariye indirilmesi ve yönetilmesi,

6. Muhasebe sürecinin Genel Kabul Görmüş Muhasebe İlkeleri doğrultusunda devamının sağlanması,
7. İşletmede meydana gelen veya gelebilecek olan hata ve hilelerin ortaya çıkartılması ve önlenmesi,
8. Varlıkların fiziki durumları ile defter kayıtları arasındaki ilişkinin kontrol altında tutulması,
9. Yönetime yardımcı olunması ve üst yönetime danışmalık yapılması,
10. Belirli alanlarda özel araştırmaların yapılması,
11. Denetim sonucunda maddi açıdan tasarruf sağlanması.

Yukarıda sıralanan amaçlar iç denetimin, işletmenin verimliliği konusunda fikir verdiğini ve bu verimliliği artırma yönünde öncülük ettiğini göstermektedir. İç denetim işletmenin amaçlarına ulaşmasında yönetime yardımcı olmaktadır.

1.1.3. İç denetimin önemi

Son yıllarda yaşanan skandallarla ortaya çıkan muhasebe hileleri, finansal raporların güvenliğini sağlama konusunda iç kontrol sürecinin ve iç denetimin yeniden yapılmasına neden olmuştur. Gelecekte karşılaşılabilecek risklerin tahmin edilebilmesi ve buna uygun yeni kararların alınabilmesi iç denetimi zorunlu kılmaktadır. İç denetimin kurulmasını zorunlu kılan yasal düzenlemeler olsa da işletmelerin pek çoğu sağladığı faydalar açısından iç denetim uygulamalarını gönüllü olarak kabul etmişlerdir.

İç denetim, işletme faaliyetlerinin etkinliğinin ve verimliliğinin sağlanmasında, örgütlerin yönetim anlayışında ve kültüründeki değişimlere bağlı olarak her geçen gün önem kazanmaktadır. İşletmeler büyüyüp karmaşık bir hale geldikçe faaliyetlerle ilgili çeşitli sorunlar ortaya çıkmakta ve bunların çözümü için iç denetim birimlerine başvurulmaktadır. Güçlü bir iç denetim, işletmedeki denetim mekanizmalarının sağlıklı çalışmasına katkıda bulunur, verimliliği ve rekabet gücünü artırır, faaliyetlerle ilgili riskleri, dolandırıcılığı ve gelir kayıplarını engeller (Uyar, 2009: 56).

İç denetim faaliyeti, işletme ve işletme ile ilişkili taraflara karşı güvence sağlamak ve yönetime danışmanlık yapmak suretiyle, işletmenin amaçlarını gerçekleştirme fırsatlarını geliştirerek, faaliyetleri geliştirme imkanlarını belirleyerek ve ortaya çıkabilecek riskleri azaltarak işletmeye değer katmaktadır. Bu nedenle iç

denetim, işletme içinde hata, yolsuzluk ve düzensizliklerin önlenmesi bakımından işletme yönetiminin elinde çok etkin bir araç olarak karşımıza çıkmaktadır (Aslan, 2010: 73). Bunların yanı sıra işletmelerde iç denetim; risk ve kontrol değerlendirme faaliyetlerine destek sağlamakta, işletme faaliyetlerini izlemekte, faaliyetlere ilişkin risk ve kontrol faaliyetleri ile ilgili önerilerde bulunmakta, ilgili kontrollerin uygunluğunu ve etkinliğini test etmektedir. İç denetim; işletmelerde finansal raporlama sisteminin güvenilirliği, yasa ve düzenlemelere uygunluk, faaliyetlerin ekonomikliğı, etkinliğı ve verimliliğı, bilgi sistemlerinin güvenilirliğı açısından olmazsa olmaz faaliyetlerden biri olarak kabul edilmelidir.

Büyük işletmelerde hissedarlar ve yönetim kurulu üyeleri, çalışanların faaliyetlerinin etkinliğinden haberdar olmak ve onları gözlemlemek istemektedirler. Bu istekler, iç denetimi gerekli kılan sebepleri oluşturmakta ve bu isteklerin gerçekleşmesi için iç denetim bölümü tarafından çalışanların ve yöneticilerin izlemesi gerekmektedir. İç denetimi gerekli kılan bu sebepleri şöyle sıralayabiliriz (Biçer, 2006: 66-70):

1. *Sorumluluk ve Hesap verebilme*: Yöneticilerin, çalışanların görevlerini etkin ve verimli bir biçimde yerine getirip getirmediğini ve bireysel hedeflere ulaşp ulaşamadıklarını bilmeleri gereklidir. Bu doğrultuda, iç denetçiler bilgi toplama, koşulları irdeleme ve sorunları tanımlama konularındaki mesleki yeterlilikleri nedeniyle, sistemlerin, usullerin, kontrollerin değerlendirilmesini ve verimliliğı ile ilgili hedeflere ulaşılıp ulaşamadığını belirlemeyi yöneticiler adına vekaleten yaparlar. İç denetçiler temel olarak üst düzey yöneticilerde dahil olmak üzere her kademedeki yöneticilerin görevlerini yerine getirmek konusundaki performanslarını yönetim kurulu adına incelerler.
2. *Vekalet Teorisi*: İşletme sahipleri, istihdam ettikleri çalışanların görevlerindeki performanslarını ve faaliyetlerin verimliliğini değerlendirebilecek yeterli bilgiye sahip değildir. Bu nedenle bu görevi yöneticilere bırakırlar. İşletme sahipleri ve yöneticiler arasındaki bu ilişki vekalet teorisi olarak adlandırılmaktadır. Bir vekil olarak görev yapan yöneticinin yükümlülüklerini yerine getirip getirmediği ile ilgili olarak işletme sahibinin endişelerini giderecek en önemli kontrollerden biri; iç denetimdir.

3. *Yönetime Danışmanlık ve Yardım:* İç denetçiler sadece işletmedeki hata ve hileleri tespit etmekle kalmaz, ayrıca ileride benzer sorunların yaşanmaması için yöneticilere danışmanlık hizmetinde de bulunurlar. Günümüzde iç denetçiler, birçok organizasyonda, hedeflerin başarılmasında, denetim, danışmanlık ve eğitmenlik yaparak yönetime yardımcı olan yönetim takımının üyeleri olarak görülmektedir. İç denetçiler çalışmalarında denetlenen işletmelere katma değer sağlarken, kontrol sisteminden kaynaklanan eksiklikleri ve suistimallerden kaynaklanan riskleri de göz önünde bulundururlar. İç denetçiler bir yanda bölüm yöneticilerinin güvenini sürekli kılmaya çalışırken diğer yanda eksik bulgularını üst yönetime raporlamaktadır.
4. *Tasarruf İhtiyacı:* Kapsamlı denetim çalışmaları sonucunda işletme bölümlerinde ve faaliyetlerinde tespit edilen aksaklıkların giderilmesi sayesinde işletmelerde büyük tasarruflar sağlanmaktadır. Zaman zaman ortaya çıkarılan eksikliklerden kaynaklanan fayda iç denetim biriminin bir yıllık maliyetini karşılayacak düzeyde dahi olabilmektedir.
5. *Hileli İşlemlere Karşı Korunma İhtiyacı:* Hata ve hileler, genel itibariyle, işletme varlıklarında azalmaya yol açan ve işletmeyi hedeflerinden uzaklaştıran düzensizlikler olarak ifade edilebilir. Günümüzde pek çok işletme, özellikle muhasebe çalışanlarından kaynaklanabilecek aksaklık, hata ve hile olasılıklarına karşılık kontrole gereksinim duymaktadır. Çalışanlarca gerçekleştirilen hileli işlemlerde, çalışanın iç kontrol sisteminin yetersiz olduğunu görmesi onları hileli işlem yapmaya sürüklemektedir. İç kontrol hata ve hilelerin oluşumunu en aza indirerek aynı zamanda yapılan sisteminin kalitesi, yapılan denetimlerde bunların ortaya çıkarılmasını kolaylaştıracaktır. Etkin bir iç kontrol sistemi ile her durumda çalışma alanlarının birbirinden ayrılması ve birimlerin birbirini kontrol etmesi sağlanmalıdır. Etkin bir iç kontrol sisteminin yanı sıra; şirketin iç denetçilerinin etkinliklerinin artırılması ve denetim komitelerinin oluşturulması da hata ve hilelerin önlenmesini sağlayan etkenlerdir.

İç denetimi gerekli kılan bu sebepler iç denetimin sadece iç kontrolün etkinliğinin ve verimliliğinin ölçülmesi olmadığını, aynı zamanda işletme faaliyetlerinin tarafsız bir şekilde sürdürülmesini sağlamaya çalışan bir fonksiyon olduğunu göstermektedir.

1.1.4. İç denetimin faydaları

İç denetimin etkin ve verimli bir şekilde yürütülmesi işletmedeki iç kontrol sisteminin sağlıklı çalışmasını sağlar. Risklerin önceden belirlenmesi, hile ve kayıpların engellenmesi verimlilik açısından işletmeye katkı sağlar. İç denetim işletme faaliyetlerine ilişkin sağladığı analizler, değerlemeler, tavsiyeler ve görüşler ile işletme çalışanlarına yardımcı olur. Etkin bir iç denetim işletmeye değer katar.

Etkin bir iç denetimin sağladığı faydalar şöyle sıralanabilir (Biçer, 2006: 54-55):

1. Etkin bir iç denetim ile daha az maliyetli, zamanında ve güvenilir bilgi sağlanır ve böylece sağlıklı yönetsel kararların alınmasına yardımcı olur,
2. Uygun kontroller ile işletme varlıklarının ve kayıtlarının korunmasını sağlar,
3. Faaliyetlerin etkinliğini ve verimliliğin artırır,
4. Çalışanların belirlenmiş politikalara ve kurallara uygun davranmalarını sağlar,
5. İşletmelerde denetim kültürünün gelişmesini sağlar,
6. İlgili yasal düzenlemelere uygunluğu sağlar,
7. Bulgu ve önerileriyle yönetim etkinliğinin artmasını sağlar,
8. Otokontrolü sağlayarak iç kontrol sistemini değerlendirir ve geliştirilmesi için öneriler sunar.

İç denetimin sağladığı faydalar, işletme çalışanlarının sorumluluklarını etkili bir şekilde yerine getirmelerine yardımcı olmakta ve işletme faaliyetlerinin yerine getirilmesi sırasında üst yönetimin, yönetim kurulunun ve çalışanların işbirliği halinde olmasını sağlamaktadır.

1.2. İç Denetimin İşlevleri

İç denetim, yönetsel bir kontroldür; diğer kontrollerin etkinliğini ölçer ve değerlendirir. İç denetim, yönetim hedeflerinin gerçekleşme yolunda olduğu konusunda

yeterli güvence sağlamada yararlanılan bir yönetim aracıdır. Bu nedenle iç denetimin yapısının yeterliliğinden ve etkinliğinden yönetim sorumludur (Uzun, 1999: 1).

Günümüzde işletme yönetiminde iç denetim pro-aktif bir rol üstlenmektedir. Önceleri sadece geçmiş uygulamaların kontrolünden ibaret olması yönüyle reaktif bir süreç olan iç denetim faaliyeti, danışmanlık ve değer katma gibi işlevler ile birlikte aynı zamanda pro-aktif bir süreç haline gelmiştir. Modern organizasyonlarda iç denetim faaliyetleri, güvence sağlama ve danışmanlık etme şeklinde iki önemli işlevi yerine getirmek suretiyle kuruma ilave değer katmaktadır. Güvence sağlama hizmeti iç denetçinin; organizasyondaki süreçler, sistemler ve diğer konularla ilgili objektif değerlendirmeler yapmak suretiyle görüşlerini yönetime bağımsız bir şekilde sunmasını kapsamaktadır. İç denetçinin değerlendirmeleri ve görüşleri, organizasyondaki süreçlerin nasıl işlediği hakkında yöneticilere güvenli bilgiler sunmaktadır. Yöneticiler, organizasyondaki süreçlerde meydana gelen problemlere çözüm bulunması, süreçlerin yeniden yapılandırılması ve sistemlerin geliştirilmesi gibi konularda iç denetçilerden öneriler almakta ve bu önerileri dikkate almak suretiyle ileride ortaya çıkması muhtemel sorunların da önüne geçme imkanı bulmaktadırlar (Memiş, 2007: 462-463).

İç denetim, özellikle, organizasyonun risk yönetimini, kontrolünü ve kurumsal yönetimi geliştirmede bölüm yönetimine yardımcı olmak üzere bağımsız ve tarafsız bir danışmanlık hizmeti sağlar. İç denetimin danışmanlık hizmeti, yönetimin organizasyonun hedeflerini gerçekleştirmesini sağlamak üzere uygulamaya koyduğu politikaların, prosedürlerin ve faaliyetlerin sistemli ve düzenli bir biçimde değerlendirilmesi ve geliştirmeye yönelik tavsiyelerde bulunulması yoluyla iç denetim becerilerinden yararlanılmasıdır. Bu tür danışmanlık çalışması iç denetimin risk yönetimi, kontrol ve kurumsal yönetim hakkında sunduğu görüşe katkıda bulunur (Korkmaz, 2007: 4-5).

Aşağıda güvence ve danışmanlık hizmetleri daha detaylı olarak ele alınacaktır.

1.2.1. Güvence hizmetleri

Güvence ihtiyacı yeni değildir. Yatırımcıların ve karar alıcıların finansal nitelikli bilgiler ve işletme başarısının ölçümlenmesi ile ilgili olarak güvence hizmetine ihtiyaçları vardır. Güvence hizmetleri, ölçme, analiz etme, test etme ve raporlama gibi geleneksel hizmetlerin getirdiği becerilere dayanmaktadır. Geleceğe yönelik bilgilere

talep arttıkça ve bilgi teknolojilerinin kullanımı söz konusu oldukça güvence hizmetlerine ilişkin talep artacaktır.

1.2.1.1. Güvence hizmetlerinin tanımı

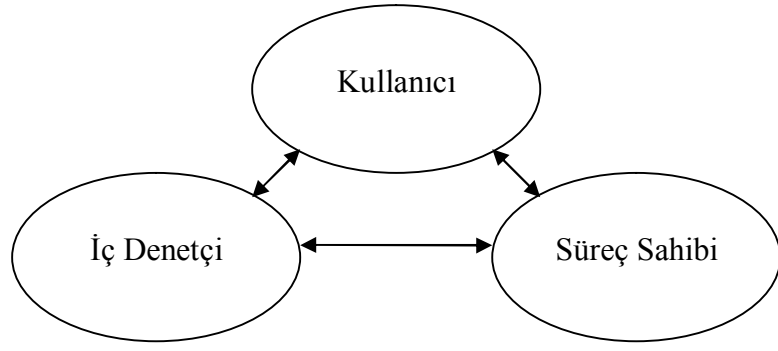
Güvence hizmetleri, iç denetçinin, bir süreç, sistem veya bir başka konu hakkında bağımsız görüş veya kanaat sunabilmek için, eldeki bulguları objektif bir şekilde değerlendirmesini içerir. Güvence görevlerinin nitelik ve kapsamı iç denetçi tarafından belirlenir (TİDE, 2008: 15).

Güvence hizmetleri, işletmenin risk yönetimi, iç kontrol ve kurumsal yönetim süreçlerine dair bağımsız bir değerlendirme sağlamak için bulguların tarafsız olarak incelenmesidir. Gerçekleştirilen faaliyetlerin işletmenin finansal yapısına, mevzuat ve düzenlemelere uyumunu incelemek, bilgi sistemlerinin güvenliğini araştırmak, ayrıntılı durum analizleri (ihtimam denetimi) yapmak güvence hizmeti kapsamındaki işlere örnek olarak verilebilir (Özoğlu, vd. 2010. 113).

Güvence hizmetleri denetim fonksiyonunu bir uzantısı olarak geliştirilmiştir. Güvence hizmetleri, ilgili taraflar açısından bilgi riskini azaltmaktadır. Bilgi kullanıcılarının beklentilerini önemli ölçüde değiştiren bilgi teknolojilerindeki ilerlemeler, güvence hizmetlerine olan talebi arttırmıştır (Whittington ve Pany, 2004: 699).

Güvence hizmetleri, işletmedeki karar alıcılar için bilgi kalitesini arttıran bağımsız mesleki uzmanlık hizmetlerdir. İşletmedeki karar mercileri, kararlarına temel oluşturan bilginin güvenilirliğini ve ilgililiğini arttırmaya çalışan güvence hizmetlerine ihtiyaç duyarlar. Güvence hizmetleri, güvence sağlayıcısını bağımsız olması ve incelenen bilgi açısından tarafsız olması nedeniyle değerli kabul edilir (Arens, vd., 2003: 4).

Aşağıda Şekil-2’de güvence hizmetlerinde ilişki içinde olan taraflar gösterilmektedir.



Şekil-2. Güvence Hizmetlerinde Taraflar ve İlişkiler

Kaynak: Anderson, 2003: 108.

Güvence hizmetlerinin üç tarafı vardır (Özoğlu, vd., 2010: 112):

1. Süreç, sistem veya ele alınan diğer bir konunun doğrudan içinde olan kişi veya grup (süreç sahibi),
2. Değerlendirmeyi yapan kişi veya grup (iç denetçi),
3. Değerlendirmeyi kullanan kişi veya grup (kullanıcı).

Güvence hizmetleri, geleneksel onaylama sözleşmelerinin sağladığından fazla rapor türü içerebilir veya açık sonuçları olmayan veya sadece ne zaman ortaya çıktığı bilinen problemlere ilişkin raporlar gibi daha az yapılandırılmış iletişim sağlayabilirler. Güvence hizmetleri, genellikle belirli durumlarda karar alıcıların ihtiyacı olan bilgiyi hazırlamak için uğraşır. Bağımsızlık, profesyonellik, bilgi ve karar alıcılar güvence hizmetlerinin unsurlarını oluşturmaktadır. Güvence hizmetlerinde sunulan bilgiler iç ve dış karar alıcılar açısından finansal veya finansal olmayan, tarihsel veya geleceğe yönelik, araştırma verisi veya sistemler hakkında bilgi olabilir. Bilginin kapsamı, nasıl sunulduğu ile ilgilidir. Güvence hizmetleri bilginin güvenilirliği, ilgililiği ve kullanımının veya anlaşılabilirliğinin kolaylığı ile ilgili güvence sağlayarak, bilginin değerini artırır. Güvence hizmetinin bilginin değerini artırma amacı, karar alıcıların daha bilinçli ve daha iyi kararlar almasını sağlayacaktır. Karar alıcıların bilgi ihtiyaçları değişmektedir. Uzun zamandır bilgi ihtiyaçları, periyodik olarak yayınlanan maliyet tabanlı finansal tablolar tarafından karşılanmıştır. Ancak bilgi teknolojilerindeki gelişmeler ve değişen ihtiyaçlar karşısında güvence hizmetleri de gelişmektedir.

1.2.1.2. Güvence hizmetlerinin türleri

Güvence hizmetlerini üç gruba ayırarak inceleyebiliriz. Bu gruplar ve alt grupları aşağıda sıralanmıştır (Güredin, 2007: 5-8; Arens, vd., 2003: 4-7):

1. *Onaylama Hizmetleri*: Onaylama, denetim biriminin başka bir tarafın sorumluluğu olan bir iddianın güvenilirliği hakkında rapor hazırladığı bir çeşit güvence hizmetidir. Dört tür onaylama hizmeti vardır:
 - a. *Tarihsel Finansal Tabloların Denetimi*: Bu denetim türü, denetçilerin finansal tabloların genel kabul görmüş muhasebe ilkeleri ile uyumlu olup olmadığı hakkındaki görüşlerini belirten yazılı bir rapor hazırladıkları bir tür onaylama hizmetidir. Güvence hizmetlerinin en yaygın olanıdır.
 - b. *İç Kontrolün Etkinliğinin Onaylanması*: İşletmeler yıllık faaliyet raporlarında işletmenin iç kontrol sisteminin etkinliği ile ilgili olarak bir rapor hazırlamak zorundadırlar. İç kontrol sisteminin etkinliğinin incelenmesi aslında finansal tabloların denetimi sırasında yürütülür ve amacı temelde geleceğe yönelik bilgi üretmektir. Çünkü etkin bir iç kontrolün varlığı gelecekte finansal tablolarda hata ve yanlışlık olma olasılığını azaltır.
 - c. *Tarihsel Finansal Tabloların Gözden Geçirilmesi*: Denetim hizmeti yüksek seviyede güvence verirken, gözden geçirme orta seviyede güvence sağlar. Bu seviyedeki güvenceyi desteklemek için daha az kanıtı ihtiyacı vardır.
 - d. *Diğer Onaylama Hizmetleri*: Denetçilerin verdiği diğer onaylama hizmetlerinin çoğu finansal tabloların denetiminin doğal bir uzantısıdır.

Onaylama hizmetlerinde risk, uygulamadaki kişilerin raporun düzenlemesi sırasında bilmeden hata yapmasıdır. Bu duruma onaylama riski de denilebilir ve denetim riskinde olduğu gibi asıl risk, kontrol riski ve bulgu riski olmak üzere üç çeşittir. Bir onaylama sözleşmesinde uygulayıcılar asıl ve kontrol risklerini değerlendirir ve bulgu risklerini makul seviyede tutmak için prosedürleri tasarlar (Whittington ve Pany, 2004: 703).

2. *Diğer Güvence Hizmetleri*: Bu güvence hizmetleri de başka bir tarafça iddia edilmiş veya edilmemiş bilginin güvenilirliği ile ilgilidir. Bu hizmetler denetçinin bağımsız olmasını gerektirdiği ve karar alıcılar tarafından kullanılan bilgi hakkında güvence verdikleri için onaylama hizmetlerine benzerler. Ancak denetçi yazılı bir rapor hazırlamak zorunda değildir ve güvence başka bir tarafın belirlenmiş ölçüt ile uyum hakkındaki yazılı iddiasının güvenilirliği hakkında olmak zorunda olmadığından güvence hizmetlerinden farklılık gösterir.

Denetimleri ve onaylamayı içeren tüm güvence hizmetlerinin ortak özelliği karar alıcılar tarafından kullanılan bilginin kalitesinin artırılmasına odaklanmasıdır.

3. *Bilgi Teknolojisi İle İlgili Güvence Hizmetleri*: İnternette var olan eş zamanlı bilgilerin miktarı, güvence ihtiyacını finansal tablolar gibi belirli bir tarihteki bilgilerden, eş zamanlı bilgi üreten süreçlerin güvenilirliğine ilişkin güvenceye kaydırmıştır. Bilgi teknolojileri ile ilgili güvence hizmetleri iki türdür:

- a. *WebTrust Hizmetleri*: İnternet üzerinden yapılan işlemlerdeki ani artış sonucu güvence hizmetlerine ilişkin ihtiyacın artması, WebTrust güvence hizmetlerinin ortaya çıkışını sağlamıştır. WebTrust, bir onaylama hizmetidir.
- b. *SysTrust Hizmetleri*: Bilgi sistemlerinin güvenilirliğine ilişkin güvence hizmetleridir. SysTrust, güvenlik ve bilgilerin dürüstlüğü gibi konularda sistem güvenilirliğini değerlendirmeye ve test etmeye yönelik onaylama türüdür.

WebTrust esas olarak bir web sitesini kullanan üçüncü şahıslara güvence vermeyi amaçlarken, SysTrust işletme yönetimine, yönetim kuruluna ve üçüncü kişilere eş zamanlı bilgi üretmede kullanılan bilgi sistemlerinin güvenilirliğine dair güvence vermeyi amaçlar.

Aşağıda WebTrust ve SysTrust hizmetlerine ilişkin ilkeler bir tablo yardımıyla gösterilmektedir:

Tablo-1. WebTrust ve SysTrust Hizmetlerine İlişkin İlkeler

Güven İlkeleri	Güvencenin Tanımı
Çevrimiçi Gizliliği	Kişisel bilgilerin gizliliğinin korunduğuna dair güvence sağlar.
Güvenlik	Bir web sitesinin sistemine erişimin ve bilgilerin yetkili kişiler ile sınırlı olduğuna dair güvence sağlar.
İşletmecilik uygulamaları ve işlemlerin dürüstlüğü	Elektronik ticaret işlemlerinin eksiksiz ve doğru olarak yapıldığına ilişkin güvence verir.
Kullanılabilirlik	Elektronik ticaret sistemlerinin ve bilgilerin kullanıcıların ihtiyaç duydukları zaman onlar tarafından kullanılabilir olmalarına dair güvence verir.
Gizlilik	Gizli olması istenen bilgilerin gizliliğinin korunduğuna dair güvence sağlar.
Onama Makamları (sadece SysTrust)	Elektronik işlemleri onaylama sorumluluğu olan yetkili makam veya bilirkişilerce kullanılan kontrollerin uygunluğuna ve etkinliğine dair güvence sağlar.

Kaynak: Güredin, 2007: 7.

1.2.2. Danışmanlık hizmetleri

Danışmanlık hizmetleri, tavsiye niteliğinde olup genellikle görevlendirmeyi talep eden müşterilerin talebiyle gerçekleştirilir. Danışmanlık hizmetlerinin niteliği ve kapsamı, değerlendirmeyi talep eden müşteri ve iç denetçi arasındaki sözleşmeyle belirlenir. İç denetçi danışmanlık hizmeti verirken, tarafsızlığını korumalı ve yönetimle ilgili sorumluluk almamalıdır.

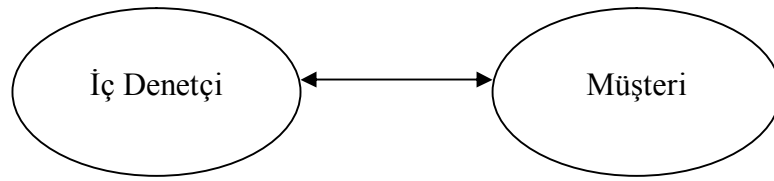
1.2.2.1. Danışmanlık hizmetlerinin tanımı

Her hangi bir yönetsel sorumluluk üstlenmeden, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden, niteliği ve kapsamı müşteri/denetlenen ile birlikte kararlaştırılan tavsiyeye dayalı faaliyetler ve bunlarla bağlantılı hizmetlerdir (TİDE, 2008: 35). İç kontrol eğitimleri, yeni kurulan sistemlerdeki kontrollerle ilgili şüpheleri ortadan kaldırmak amacıyla yönetime sunulan

tavsiyeler, politika ve prosedürlerin planlanması, kalite takımlarına katılım danışmanlık hizmetlerine örnek olarak verilebilir (Anderson, 2003: 106).

İç denetçiler danışmanlık faaliyetleri sırasında sadece üst yönetime ve denetim komitesi karşı sorumlu davranmakla kalmaz, aynı zamanda yakın iş ilişkilerinde bulundukları işletmelerin bölüm yöneticilerine karşı da sorumluluk taşırlar. Danışmanlık hizmetleri sırasında iç denetçi hem tavsiye veren hem de gözlem (denetim) yapan olduğu için bölüm yöneticileri ile iç denetçi arasında çatışma yaşanması mümkün olabilmektedir. Bu ikili rol iç denetçinin tarafsızlığını olumsuz etkilemekte ve zaman zaman iç denetçinin tarafsızlığı ve bağımsızlığı konularında bazı şüpheler ortaya çıkmasına neden olmaktadır (Brody ve Lowe, 2000: 171).

Aşağıda Şekil-3’de danışmanlık hizmetlerinde ilişki içerisinde olan taraflar gösterilmektedir.



Şekil-3. Danışmanlık Hizmetinde Taraflar ve İlişkiler

Kaynak: Anderson, 2003: 108.

Danışmanlık hizmetlerinin genellikle iki tarafı vardır (TİDE, 2008: 15):

1. Tavsiye veren kişi veya grup (iç denetçi),
2. Tavsiye talep eden ve alan kişi veya grup (müşteri).

Danışmanlık hizmetlerinin niteliği, iç denetim yönetmeliğinde tanımlanmalıdır. İç denetçilerin, ilgili görevin başlangıcında belirlenen kapsam ve amaçta yeri olmayan bir yönetim sorumluluğunu, uygunsuz veya kasıtsız olarak üstlenmelerini engellemek amacıyla, özellikle, niteliği gereği devamlı veya kesintisiz olan danışmanlık görevlerinde çok dikkat edilmelidir. İç denetçiler, bir danışmanlık hizmeti yaparken, özellikle aşağıdakileri anlamalı ve azami mesleki özen ve dikkati göstermelidir (TİDE, 2008: 52-53):

1. Görev sonuçlarının niteliğine, zamanlamasına ve raporlanmasına yönelik yöneticilerin talep ve öncelikleri,

2. Hizmeti talep edenlerin, taleplerinin ardındaki sebepler,
3. Amaca ulaşmak için gereken işlerin kapsam ve niteliği,
4. Görev için gereken beceri ve kaynaklar,
5. Denetim komitesinin daha önce onayladığı denetim planının kapsamına etkisi,
6. Gelecekteki denetim görevleri ve taahhütleri üzerindeki muhtemel etkileri,
7. Kurumun bu görevden elde edebileceği yararlar.

İç denetçiler tarafından yürütülen danışmanlık hizmetleri iç denetim standartlarında sınırlandırılmıştır. Bu durum, iç denetçi tarafından yapılan tüm gözlemlerin ve elde edilen sonuçların sağlam kanıtlara dayanması yönünden fayda sağlamaktadır.

İç denetçiler, danışmanlık hizmetleri sırasında uygulanan risk yönetimi ve kontrol süreçlerinin verimliliğini izlemeli ve bu konuda dikkatli olmalıdır. Tespit edilen büyük risk ve risk maruziyetleri veya önemli kontrol zayıflıkları, yönetimin dikkatine sunulmalı ve rapor edilmelidir. Bazı durumlarda, denetçinin kaygılarının da üst yönetime, denetim komitesine ve/veya yönetim kuruluna bildirilmesi gerekir. İç denetçiler risklerin, zayıflıkların önem düzeyini ve bunları azaltmak veya düzeltmek için alınan veya alınması öngörülen tedbirleri tespit etmek için ve bu risklerin veya zayıflıkların rapor edilmesi konusunda, üst yönetim, denetim komitesi ve yönetim kurulunun beklentilerini araştırıp bulmak için mesleki karar verme yetilerini kullanmalıdır (TİDE, 2008: 55).

İç denetçi, danışmanlık hizmetini sunduğunda veya sunduktan sonra bağımsızlık ve objektifliğini riske edecek eylemlerden uzak durmalıdır. Standartlara göre bir iç denetçinin danışmanlık görevinde bulunduktan sonra en az bir yıl süre ile danışmanlık hizmeti verdiği görevle ilgili güvence hizmeti vermemesi gerektiğini yoksa güvence hizmetinin bağımsızlığı ve tarafsızlığı olumsuz etkileyeceğini belirtmektedir (Özoğlu, vd., 2010: 114).

1.2.2.2. Danışmanlık hizmetlerinin alanları

İç denetim yöneticileri, işletme içindeki görev alanlarına ilişkin yapacakları faaliyet sınıflandırmalarında, hangi görevin danışmanlık hizmetleri, hangisinin güvence

hizmetleri kapsamında olduğunu belirleyerek, bunları ayrı ayrı fonksiyonlarda uygulayabileceği gibi birleştirip karma bir görevlendirmede de bulunabilir (Özoğlu, vd., 2010: 113).

İç denetçi, danışmanlık görevinin iç denetim faaliyetiyle ilgili temel görev planına uygunluğunu göz önünde bulundurmalıdır. İç denetçiler risk odaklı bir görev planı uyguladıklarından işletmenin ihtiyaç duyduğu denetim kapsamını belirleyerek, bu planın izin verdiği ölçüde danışmanlık hizmetini yerine getirmelidirler (Özoğlu, vd., 2010: 114). Danışmanlık hizmetleri, iç denetçiler tarafından sunulan ve denetlenenin işletme amaçlarına ulaşmasını sağlayacak tavsiyeleri içerir (Anderson, 2003: 100).

Danışmanlık hizmet alanları dört ana bölüme ayrılabiliriz:

1. *Risk yönetimi*: Risk yönetimi, kurum yönetiminin temel sorumluluklarından biridir. İş hedeflerine ulaşabilmek için, yönetimin, kurum içinde sağlam risk yönetimi süreçlerinin bulunmasını ve kullanılmasını sağlaması gerekir. Denetim komitesi ve yönetim kurulu, uygun risk yönetimi süreçlerinin bulunup bulunmadığını ve bu süreçlerin yeterli ve etkin olup olmadığını tespit etmek konusunda denetleyici bir rol oynar. İç denetçiler, yönetimin uyguladığını risk süreçlerinin yeterliliği ve etkinliğini inceleyerek, değerlendirerek, rapor ederek ve bu konuda iyileştirici önlemler önererek hem yönetime hem de denetim komitesine yardımcı olmalıdır. Kurumun risk yönetimi ve kontrol süreçlerinden işletme yönetimi, denetim komitesi ve yönetim kurulu sorumludur. Ancak, danışmanlık hizmetini üstlenen iç denetçiler de, bu risklerin tanımlanması, değerlendirilmesi, risk yönetimi yöntemlerinin uygulanması ve bu risklerle ilgili kontrol önlemlerinin alınması ve uygulanması konularında yardımcı olabilir (TİDE, 2008: 224).
2. Performans ölçümü: İşletmelerde, sürekli ve dönemsel performans değerlendirmeleri yapmalı ve sistemin engellenmesinde bilgisayar teknolojisi kullanımının etkisini değerlendirmelidir. İç denetçinin sunduğu raporlar, potansiyel iyileşmeler hakkında tavsiyeleri, tatmin edici performans başarılarını ve düzeltici tedbirleri de içermelidir. Bu tavsiyeler, iç denetçinin kendi tespit ve kanaatlerine dayanır. Tavsiyelerde, mevcut durumun düzeltilmesi veya faaliyetlerin

iyileştirilmesine yönelik eylem çağrısı yapılır. Ayrıca yönetime, istenen sonuçlara ulaşması konusunda yol göstermek için, performansın düzeltilmesi veya iyileştirilmesine yönelik yaklaşımlar da önerilebilir (TİDE, 2008: 409).

3. Sistem güvenliği: Elektronik veri değişimi güvenliği alanında en çok karşılaşılan risk faktörlerinin başında sistem güvenliği kontrolleri ve sonrasında da güncel olmayan sistemler ve yönetim stili gelmektedir (Bedard, Graham ve Jackson, 2005: 148). Bilgi teknolojilerindeki hızlı değişimler sonucu sistem güvenliği iç denetçilerin sağladıkları danışmanlık hizmetleri arasında yerini almıştır. Sistem güvenliğinin amacı, kontrollerin yetkisiz girişlere engel olup olmadığını veya işletim sistemindeki kontrollerin yeterli olup olmadığını belirlemektir. Sistem güvenliği incelemelerinin sonuçlarından yola çıkarak iç denetçinin vereceği tavsiyelerle uygun kontrol amaçları belirlenebilir (Senft ve Frederick, 2009: 733).
4. Elektronik ticaret: Elektronik ticaretin hızlı büyümesinin ve bu teknoloji değişikliklerinin, denetim planlarının hazırlanması ve uygulanmasında iç denetçilerin dikkate alması gereken önemli kontrol ve yönetim sorunları yarattığı açıktır (TİDE, 2008: 242). İşletmelerde elektronik ticaret kullanımı denetim izlerinin izlenmesi konusunda zorluklar yaşanmasına neden olmuştur. Ayrıca elektronik ticaret kullanımı iç denetçilerin işletmenin elektronik ticaret stratejisine, bilgi teknolojilerinin kullanımının yarattığı asıl risklere ve elektronik ticaret konusundaki bilgi ve becerilerine dikkat etmesine neden olmuştur. İç denetçi finansal tabloların denetiminin planlandığı ve uygulandığı süreçte elektronik ticaretin yaratmış olduğu risklere dikkat etmelidir. Bu durumda denetçi elektronik ticaretin denetim aşamasına etkilerini değerlendirmek için işletmenin elektronik ticaret faaliyetlerinin yapısını bilmelidir. İç denetçi işletmenin elektronik ticaret stratejisi, kontrollerin yönetimi, iç kontrol sisteminin yeterliliği gibi konularda yönetime danışmanlık hizmeti sunabilecektir. Buna göre yönetim elektronik ticaretin sebep olduğu fırsat ve riskleri bilebilecek ve uygun kontrolleri oluşturabilecektir.

1.3. İç Denetim İlkeleri

Tüm dünyada kabul gören ve etkin bir iç denetimin oluşturulmasında dikkate alınması gereken temel iç denetim ilkeleri şunlardır (Uyar, 2009: 65-66):

1. *Görevlerin ayrımı*: Muhasebe kontrolü ile ilgili konuları içeren bir ilkedir. Görevlerin ayrımı ilkesi bir kıymet hareketinin başlangıcından sonuna ve muhasebe kayıtlarına alınmasına kadar olan sorumluluğun birkaç görevli arasında paylaştırılmasını öngörmektedir. Bunun için bir kıymetin alınması, kıymet hareketinin kayıtlara aktarılması ve bu kıymet hareketi sonucu oluşan değer koruma altına alınması görevleri farklı kişiler tarafından yerine getirilmelidir.
2. *Kıymet hareketlerinin yetkilendirilmiş olması*: Her işlem mutlaka yetkili kişilerin bilgisi çerçevesinde yürütülmelidir.
3. *Belgeleme ve muhasebe kayıt düzeni*: Etkin bir kontrol için belgeleme ve muhasebe kayıt düzeninin varlığı şarttır. Kıymet hareketine neden olan olayın muhasebe kayıtlarına geçirilmesi belge ile gerçekleştirilir ve sorumluluk belge ile gösterilir.
4. *Fiziki koruma*: Varlıkların ve muhasebe kayıtlarının fiziki olarak korunması için her türlü fiziksel önlem alınmalıdır.
5. *Bağımsız mutabakat*: İç denetimin uygun çalışıp çalışmadığını kontrol etmek için bağımsız iç mutabakatların yapılması zorunludur. Bu mutabakatlar, sorumlu kişilerin dışındaki kişiler tarafından, belirli aralıklarla ve önceden haber verilmeden yapılmalıdır.

Bu ilkeler tüm dünyada kabul gören ve iç denetimin oluşturulması sırasında dikkate alınması gereken ilkelere aittir. İç denetim faaliyetinden beklenen faydaların sağlanabilmesi için bu ilkelere uyulması gerekmektedir.

1.4. İç Denetimin Türleri

Uygulamada iç denetimin temel olarak beş türden oluştuğu görülmektedir. Bunlar; finansal denetim, uygunluk denetimi, faaliyet denetimi, bilgi teknolojileri denetimi ve sistem denetimidir.

1.4.1. Finansal denetim

Finansal denetim; gelir, gider, varlık ve yükümlülüklerle ilişkin hesap ve işlemlerin doğruluğunun, finansal sistem ve tablolarının güvenilirliğinin değerlendirilmesidir. Finansal denetim sonucu çok sayıda işlemsel kusur tespit edilirse kayıtların doğruluğu, yasalara uygunluğu ve düzenliliği üzerine daha fazla hesap denetiminin yapılması gerekir (Alptürk, 2008a: 22).

Finansal denetimin amacına göre denetçi finansal tabloların eksiksiz ve özenle analizini yaparak, finansal tabloların kabul edilebilir muhasebe standartlarına uygun olarak hazırlanıp hazırlanmadığını, denetlenen kurumun şartlarını dikkate alarak hazırlanıp hazırlanmadığını, finansal tabloların çeşitli öğeleri hakkında yeterli açıklamanın mevcut olup olmadığını, çeşitli öğelerin uygun biçimde değerlendirilip değerlendirilmediğini, ölçülüp ölçülmediğini ve gösterilip gösterilmediğini araştırır (Özoğlu, vd., 2010: 177-178).

1.4.2. Uygunluk denetimi

Uygunluk denetimi, işletmenin finansal ve finansal olmayan işlemlerinin üst yönetimce belirlenmiş kontrol önlem ve yöntemlerine (yordamlarına) uygunluğunu araştırmaktır. Bütün işlemler denetimin konusunu, bütün kontrol önlem ve yöntemleri (yordamları) da denetimin ölçütünü oluşturur. Uygunluk denetimi, iç denetimin iç kontrol sisteminin etkinliğinin ölçülmesi ve değerlendirilmesi ile ilgili yönüdür. (Elitaş, 2004: 222). Uygunluk denetimleri işletmelerin dış ve iç düzenlemelere uygunluk derecesi konusunda yönetime bilgi veren denetimlerdir (Yılancı, 2006: 116-117).

Uygunluk denetiminde amaç, belli bir otorite tarafından konulan kurallara, uygulayıcıların uyma derecelerinin belirlenmesidir. Uygunluk denetiminde önceden saptanmış ölçütler olarak kabul edilen kurallar uygulamada iki farklı grup tarafından oluşturulmaktadır. Bunlar işletme üst yönetimleri ve devlettir. İşletmeler kendi iç yapılarındaki çalışma düzenini sağlayabilmek için, çalışmalarına uymaları gereken kuralları oluşturmaktadır. Bunlara uyulup uyulmadığını öğrenmek içinde denetime başvurulur. İşletmelerde bu denetimler iç denetçiler tarafından yapılmaktadır (Bozkurt, 2010: 28).

1.4.3. Faaliyet denetimi

Faaliyet denetimi, işletmenin bölümlerinin etkinlik ve verimliliklerinin değerlendirilmesi amacıyla o bölümlerin faaliyetlerine ilişkin yöntem ve yordamların gözden geçirilerek incelenmesi faaliyetidir. İşletmelerin finansal tablolarının denetlenmiş olması önemlidir, ancak bu işletmelerin faaliyetlerinin de denetlendiği anlamına gelmemektedir. Faaliyet denetimi işletmenin belirli bir faaliyeti veya faaliyetleri ile sınırlı olabileceği gibi daha kapsamlı da olabilir. Kapsamlı bir faaliyet denetiminin amacı, işletmenin güçlü ve zayıf yönlerini tarafsız bir gözle değerlendirerek, yöneticilere ve işletme sahiplerine işletme hakkında güvenilir bilgi vermektir. İşletmenin amaçlarına ulaşabilmesi için kaynakların yüksek etkinlikte kullanılması ve bu sürecin işleyişinin garanti altına alınması gerekir (Can ve Uyar, 2010: 11-12).

Faaliyet denetiminde fiili durumun karşılaştırılacağı olması gereken durumlarla ilgili ölçütlerin saptanması büyük ölçüde öznelidir. Bu açıdan faaliyet denetiminde denetçi mevcut başarının doğrudan doğruya ölçülüp raporlanması eylemini değil, bu başarının iyileştirilmesi ile ilgili tavsiyelerini belirtme ve bu konuda kılavuzluk yapma yolunu seçer. Bu nedenle faaliyet denetimi, diğer denetim türlerinden farklı olarak yönetsel danışmanlık şeklinde nitelendirilmektedir (Güredin, 2007: 19).

1.4.4. Bilgi teknolojileri denetimi

Bilgi teknolojileri denetimi, işletmelerin sahip oldukları bilgi teknolojisi kaynaklarının değerlendirilmesi sürecidir. Bu noktada bilgi teknolojileri ile ilgili unsurların güvenlik altında olduğu, bilgisayar verilerinin bütünlüğünün ve doğruluğunun sağlanmış olduğu ve işletmenin amaçlarına ulaşmış olduğu dikkatlice incelenmelidir. Bilgi teknolojisi denetiminin temel amacı, bilgisayar sistemleri için mevcut kontrol standartlarını, politikalarını ve süreçlerini incelemek ve bu süreçlerle ilgili geliştirilebilecek ek kontrolleri tanımlamaktır. Böylece olumsuzluklar karşısında olası kayıpların en aza indirilmesi amaçlanmaktadır (Kurnaz ve Çetinoğlu, 2010: 244).

Bilgi teknolojileri denetimi sürecinde bilgi teknolojisi kontrolleri birbirine bağlı bir koruma sürecinin bütünü oluşturur. Ancak zayıf halkadan kaynaklanan bir tavizle karşılaşmak mümkündür. Bilgi güvenilirliği ve bilgi hizmetleri konusunda güvence sağlayan bilgi teknolojileri kontrolleri, bir kurumun teknoloji kullanımının

doğurabileceği risklerin azaltılmasına yardımcı olur. Bilgi teknolojisi kontrolleri, kurumsal politikaların şifrelenmiş talimatlarla fiziksel olarak korunmasına, eylem ve işlemleri izleme kabiliyeti yoluyla bu kontrollere fiziksel olarak erişimden sorumlu olan kişilere yardımcı olmasına, büyük veri grupları için otomatik giriş yapılmasına, bilgilerde düzeltme ve düzenleme yapılmasına ve yapılan analizlerin makul olup olmadığının araştırılmasına olanak sağlar. Bilgi teknolojisi kontrollerine duyulan ihtiyacın altında, kurumsal masrafların kontrol altına alınması ve rekabet gücünü koruma gereği, iç ve dış kurumsal yönetim ilkelerine uyma koşulu gibi faktörler bulunmaktadır. Bu yönüyle, bilgi teknolojisi kontrolleri, bilginin güvenilirliği ve etkinliğini arttırmakta ve kurumun değişen risk ortamlarına uyum sağlamasına imkan tanımaktadır (Özoğlu, vd., 2010: 189-190).

Bilgi teknolojisi denetiminin yapısını aşağıda bir tablo yardımıyla gösterebiliriz:

Tablo-2. Bilgi Teknolojisi Denetiminin Yapısı

BT Kontrollerinin Değerlendirmesi	BT Kontrollerini Anlamak	Yönetişim, Yönetim, Teknik
		Genel / Uygulama
		Önleyici, Savunma, Düzeltici
		Bilgi Güvenliği
	BT Kontrollerinin Önemi	Güvenilirlik ve Etkinlik
		Rekabet Avantajı
		Mevzuat ve Düzenlemeler
	Görevler ve Sorumluluklar	Yönetişim
		Yönetim
		Denetim
	Risk Bazlı Değerlendirme	Risk Analizi
		Risk Cevabı
		Ana Hat Kontrolleri
	İzleme ve Teknikler	Kontrol Çerçevesi
		Sıklık
	Değerlendirme	Metodolojiler
		Denetim Komitesiyle Etkileşim

Kaynak: Özoğlu, vd., 2010: 191.

1.4.5. Sistem denetimi

Sistem denetimi, denetlenen birimin finansal yönetim usullerinin eksikliklerini tespit etme ve giderme konusunda etkili olup olmadığının değerlendirilmesidir. Sistem denetimi finansal işlemlerin ekonomiklik, etkinlik ve verimliliklerinin yanı sıra genel

bağlayıcı hukuki düzenlemeler ve iç yönergelerle uyumunu inceler (Alptürk, 2008a: 23).

Sistem denetimi sayesinde denetlenen birimin faaliyetlerinin ve iç kontrol sisteminin işletme yapısına katkı sağlayıcı bir yaklaşımla analiz edilmesi, kalite ve uygunluğunun araştırılması, kaynakların ve uygulanan yöntemlerin yeterliliğinin ölçülmesi mümkündür. Sistem denetiminde amaç, yürütülen kontrol faaliyetlerinin etkinliğini ölçmek amacıyla iç kontrol sisteminin detaylı olarak değerlendirilmesidir (Özkan, 2008: 95).

1.5. İç Denetim Planı, Uygulama Süreci ve Raporlama

İç denetim faaliyeti, denetim stratejisi dahilinde denetimin planlanmasından, denetim görevinin gerçekleştirilmesinden ve ulaşılan sonuçların raporlanmasından oluşur.

İç denetim yöneticisi, kurumun hedeflerine uygun olarak, iç denetim faaliyetinin önceliklerini belirleyen risk esaslı planlar yapmalıdır (TİDE, 2008: 25). İç denetim yöneticisi, kaynakların etkin şekilde kullanılmasını sağlamak amacı ile faaliyetleri planlamalı, kaynak ve görev dağılımını yapmalıdır. Bu plan, iç denetim faaliyetinin performansının değerlendirilmesi için temel oluşturur. İç denetim planı, iç denetim kaynaklarının ve projelerinin kurumun ihtiyaçlarına göre belirlenmesi açısından da önemlidir. Denetim faaliyetlerinin hedeflenen şekilde sonuçlanabilmesi için denetim planının uzun dönemli olarak planlanması gerekir. İç denetim planı iç denetçiler ile yönetim kurulu, denetim komitesi, üst yönetim ve dış denetçiler arasındaki ilişkilerde önemli bir iletişim aracıdır. İç denetim planı, kurumun faaliyetlerinin ve karşı karşıya olduğu risklerin kapsamlı olarak incelenmesi ve analizinden sonra hazırlanır (Uyar, 2009: 68-69). İç denetimin planlanması uygulamada şu faaliyetleri içerir (Pehlivanlı, 2010: 119):

1. Planlama öncesi hazırlık aşağıdaki aşamalardan oluşur:

- a. *Denetim stratejisi*: İç denetimde planlama faaliyetine işletmenin denetim stratejisi yön verir. Denetim stratejisi genel anlamada gerçekleştirilecek faaliyetlerin çerçevesini çizer.
- b. *Risk kayıtlaması*: Risk kayıtlaması, kurumsal risk yönetimi sürecinde risklerin tanımlanması, risklerin değerlendirilmesi ve

risk tutumunun belirlenmesi aşamalarının sonuçlarından oluşur. Kurumsal risk yönetimi sürecinin bir çıktısı olan risk kayıtlaması, iç denetçi tarafından önemli riskleri kapsayıp kapsamadığı ve alınan önlemlerin yeterliliği konularında değerlendirilir.

- c. *Denetim evreninin hazırlanması:* Risk kayıtlaması oluşturulduktan sonra denetim evreni hazırlanır. Denetim evreni; kurumsal risk yönetimi sonucunda tanımlanmış ve ölçülmüş riskleri, risk altında bulunan kurum süreçlerini ve hedeflerini, risk sorumluluklarını, bir önceki denetime ve gelecek denetime ait detayları ve risklerin kontrolüne ilişkin detayları içerir. Denetim evreni, işletmenin stratejik planından unsurlar içerebilir. Bu durumda denetim evreni işletmenin genel iş hedeflerini de hesaba katmakta ve yansıtmaktadır. Denetim evreni normal şartlarda risk yönetim sürecinin sonuçlarından etkilenir.
- d. *Gerekli güvence seviyesinin belirlenmesi:* Güvence seviyesi işletmenin veya faaliyette bulunan sektörün doğal özelliklerinden veya kurumun risk alma istekliliğinden etkilenebilir. Güvence seviyesine bağlı olarak denetimin kapsamı ve gerekecek test miktarı değişir.

2. Denetim planının tasarlanması aşağıdaki aşamalardan oluşur:

- a. *Maksimum denetim kapsamının belirlenmesi:* Denetim kapsamı, denetim faaliyetine dahil edilecek veya edilmeyecek faaliyetlerin çerçevesini çizer. Denetim kapsamı ile denetimin amaçları ve öncelikleri arasında yüksek düzeyde ilişki vardır. Denetim kapsamı; denetimin nedeni, hedefler, riskler ve ilgili aşamalar ve anahtar kontroller, çalışma programı, denetim süreçlerinin sınırları, yönetim istekleri gibi özel durumlar, denetim faaliyetini gerçekleştirecek personel ve özel sorumluluk alanları, denetim zamanlaması gibi faktörler dikkate alınarak belirlenir.
- b. *Denetim planının hazırlanması ve denetim komitesine raporlama:* İç denetim yöneticisinin gözetiminde hazırlanan denetim planı,

üst yönetime, yönetim kuruluna ve denetim komitesine gözden geçirmeler ve onaylamalar için sunulur.

- c. *Plana son şeklinin verilmesi:* İlgili tarafların denetim planını gözden geçirmesi sonucunda eğer planda değişiklik olacaksa, iç denetim yöneticisi tarafından gereken düzeltmeler yapılır ve daha sonra plan tekrar tarafların onayına sunulur.

İç denetim planı hazırlandıktan sonra iç denetim faaliyetinin uygulama sürecine geçilir. Uygulama sürecinde denetçi görüşüne ulaşabilmek için denetimin yürütülmesi açısından denetim planına paralel bireysel denetim planları oluşturulur. İç denetim faaliyetinin uygulanması şu aşamalardan geçilmesi ile gerçekleşir (Pehlivanlı, 2010: 128):

1. Görev planının hazırlanması: Her denetim görevi için kapsam, amaç, zamanlama ve harcama bütçesini ele alan, yıllık iç denetim planı çerçevesini gözeten ve denetimin başlama ve sona erme tarihini gösteren bir görev planı hazırlanır. Görev planının hazırlanması aşağıdaki aşamaları içerir:
 - a. *Denetim personelinin tahsisi:* Denetim personelinin tahsisi görevin niteliği, karmaşıklığı, zaman kısıtlamaları ve mevcut kaynaklar dikkate alınarak belirlenir. Denetim personelinin tahsisini ve bütçeyi ilgilendiren temel konu denetim için görevlendirilecek personel sayısıdır.
 - b. *Denetim konusunun araştırılması:* Görev planının hazırlanması için alan hakkında yeterli bilgiye sahip olunması gerekir. İlgili alan hakkında gerekli verilere; anahtar bilgilerin, istatistiklerin ve trendlerin gözden geçirilmesi, analitik inceleme prosedürleri yardımıyla ve diğer güvence sağlayıcıların raporları aracılığıyla ulaşılabilir.
 - c. *Çalışma kağıtlarının tasarlanması:* Verilerin kayıtlanması, saklanması ve ulaşılan denetim sonucunun açıklanması açısından çalışma kağıtları çok önemlidir. Çalışma kağıtları; göreve ilişkin raporların temel desteğini oluşturur, görevlerin planlanması, uygulanması ve gözden geçirilmesine yardımcı olur, görev

amaçlarına ulaşıp ulaşılmadığını gösterir, iç denetim personelinin mesleki gelişimine yardımcı olur, iç denetim faaliyetinin standartlara uygun gerçekleşip gerçekleşmediğini gösterir.

- d. *Kapsam ve hedefin belirlenmesi*: Gerçekleştirilecek her denetim görevi için kapsam ve hedeflerin belirlenmesi gerekir. Kapsamın belirlenmesi aşamasında; denetlenecek veya denetlenmeyecek alanlar, iletişim kurulacak personel, denetim süresi, zaman ve denetimi gerçekleştirecek personel belirlenir. Kapsamla birlikte göreve ilişkin denetim hedefleri belirlenir. Denetim hedefleri yönetimin isteklerine göre şekillenirken aynı zamanda denetim elemanının yeterliliğinden, görev konusunun özelliklerinden, kaynaklardan ve zamanda da etkilenir.
2. Test seviyesi ve testlerin belirlenmesi ve uygulanması: Denetim planlama aşamasında denetim evreni sonuçlarına uygun olarak test seviyelerinin belirlenmesinin ardından her görev alanı için kullanılacak testler ve yöntemler belirlenir. Uygulanacak başlıca testler; analitik inceleme, görüşme, gözlem, izleme testi, anakütle denetimi, doğrulama, işlem testi ve uygunluk testidir.
3. Denetim programları: Denetim programları, benzer denetim türleri için denetim süreçlerinin tutarlı ve etkili bir şekilde yürütülmesinde kullanılır. Bunlar denetim süreçlerinin içerdiği aşamalarını tamamlayan ve denetçi tarafından gerçekleştirilecek testleri içeren belgelerdir.
4. Denetim araçları: Denetimde etkinliği arttırmak amacıyla tasarlanmış çeşitli denetim yazılımları bulunmaktadır. Söz konusu yazılımlar dosya karşılaştırmalarına, trend analizlerine ve diğer spesifik denetim testlerinin yürütülmesine uygundur.

İç denetim yöneticisi, iç denetim faaliyetinin amacı, yetkileri, görev ve sorumlulukları ve plana kıyasla performansı konularında, denetim komitesi ve yönetim kuruluna ve üst yönetime dönemsel raporlar sunmalıdır. Bu raporlar, önemli riskleri, kontrol sorunlarını, kurumsal yönetim sorunlarını ve denetim komitesinin, yönetim

kurulunun ve üst yönetimin ihtiyaç duyabileceği veya talep edebileceği başka konuları da içermelidir (TİDE, 2008: 26).

1.6. İç Denetçiler ve Uluslararası İç Denetim Standartları

Tüm mesleklerde olduğu iç denetim mesleği ve iç denetçilere yönelik olarak da standart belirleme çalışmaları yapılmakta ve bu standartlar uygulanmaktadır. İç denetim mesleği ile ilgili tüm düzenlemelerde olduğu gibi, standartların belirlenmesinde de İç Denetçiler Enstitüsü (Institution of Internal Auditors-IIA) öncülük etmektedir. İç Denetçiler Enstitüsü, 2002 yılına kadar geçerli olan standartları revize etmiş ve yeniden yayınlamıştır. Çalışmamızda standartlar bu yeni haliyle ele alınacaktır.

Aşağıda iç denetim mesleğinin kapsamı ve örgütlenmesinden, iç denetçilerin görevleri ve niteliklerinden bahsedildikten sonra uluslararası iç denetim standartlarından bahsedilecektir.

1.6.1. İç denetim mesleğinin kapsamı ve örgütlenmesi

İç denetim, faaliyet gösterdiği çevrede değişimi öngören ve işletmenin yapısında, süreçlerinde ve kullanılan bilgi teknolojilerinde meydana gelen değişime uyum sağlayan dinamik ve gelişen bir meslektir (Sawyer, vd., 2005: 9).

İç denetim mesleği, ilk başlarda hırsızlık, hata bulma ve bunlara engel olmaya yönelik iken, zamanla bu kapsam faaliyetler etkinliğine doğru genişlemiştir. 1960’larda işletmelerin halka açılmaya başlaması ile birlikte finansal raporlama alanı iç denetim mesleğinin kapsamına girmiştir. 1970’lerde ise iç kontrol sistemi odak noktası haline gelmiştir. İç denetim mesleğinin gelişiminde veri işlemedeki gelişmelerin, işletmelerin uluslararası nitelik taşımalarının ve yasal düzenlemelerin de etkisi olmuştur. İç denetçiler finansal, faaliyet ve uygunluk denetimi yanı sıra son yıllarda bilgi teknolojileri denetimi de yapmaktadırlar. Bu durum iç denetim mesleğinin işletme içinde oldukça etkin bir konuma geldiğini göstermektedir (Uyar, 2009: 85).

İç denetim mesleğinin örgütlenmesinde ve gelişmesinde İç Denetçiler Enstitüsünün katkısı büyüktür. ABD’de yaşanan yoğun işletme iflasları, iç denetim mesleğinin işletmelerde yerine getiriliyor olmasının önemini ortaya çıkarmış ve iç denetim mesleğinin tüm dünyada olduğu gibi ülkemizde de gelişmesine katkı sağlamıştır. Ülkemizde 1995 yılında dernek statüsünde örgütlenen Türkiye İç Denetçiler

Enstitüsü, diğer Avrupa ülkelerinin oluşturduğu Avrupa İç Denetçiler Enstitüleri Konfederasyonuna (ECIIA) üye ülkeler arasındadır. Türkiye’de 1995 yılında bu mesleğe ilişkin yapılanma başlamış olsa da 1996 yılında ECIIA ve IIA üyeliğimiz kabul edilmiştir (Özoğlu, vd., 2010: 373).

1.6.2. İç denetçilerin görevleri

İşletmenin sürekli çalışanı olarak işletme bünyesinde denetim faaliyeti yürüten kişilere iç denetçi denilmektedir. İç denetçilerin temel amacı, işletme tepe yönetiminin istekleri doğrultusunda denetim hizmeti vermektir. İç denetçilerin başlıca görevleri şöyledir (Bozkurt, 2010: 33):

1. İşletme varlıklarının yeterince korunup korunmadığını araştırmak,
2. Muhasebe belge ve bilgilerinin güvenilir olup olmadığını belirleme,
3. İşletme tepe yönetimi tarafından belirlenmiş olan politika ve prosedürlere uyulma derecesini izleme,
4. İşletme faaliyetlerinin etken ve etkin olup olmadığı konusunda görüş oluşturma,
5. İşletme yönetiminin istediği özel araştırmaları yapma,
6. Bağımsız denetçilerle işbirliği yapma.

Yukarıda sayılan görevlere göre iç denetçiler, işletmede uygunluk ve faaliyet denetimi yaparlar. İç denetçiler yaptıkları çalışmalar sonucunda bulgularını ve önerilerini rapor halinde üst yönetime sunarlar.

İç denetçi, denetim faaliyetlerini yürüten, mesleki bilgi ve deneyime sahip, bağımsız davranabilen ve yüksek ahlaki nitelikleri taşıyan kariyer sahibi uzman kişidir. İç denetçi, mali yönetim ve kontrol süreçlerinin denetimini yapmakta ve bu konularda tavsiyelerde bulunmakla yükümlüdür. Denetim sonuçları çerçevesinde iyileştirmelere yönelik önerilerde bulunmak ve denetim sırasında veya denetim sonuçlarına göre soruşturma açılmasını gerektirecek durumlarda, ilgili yönetimin en üst amirine bildirimde bulunmak iç denetçilerin görevlerindendir (Alptürk, 2008a: 33-34).

İç denetçiler çalıştıkları işletmede iç denetim hizmeti yapan kurmay bölümün üyeleridir. Yapılan denetimler sonucu ulaşılan bulgular doğrudan üst yöneticiler tarafından kullanılır. Bunun yanı sıra iç denetçiler tarafından hazırlanan iç kontrol

sistemi ile ilgili rapor bağımsız denetçinin çalışmalarına da yardımcı olur (Güredin, 2007: 20-21).

İç denetçilerin görev ve sorumlulukları işletmenin örgüt yapısına ve faaliyet alanına göre değişiklik gösterir. Bazı işletmelerde iç denetçi finansal verilerden çok personel politikası, pazarlama yaklaşımı ürün kalitesi gibi işletme ile ilgili çeşitli faaliyetlere odaklanmaktadır (Tuan ve Sağlar, 2004: 2).

Günümüzde bilgi teknolojilerinin işletme faaliyetlerinde önemli bir yer tutması nedeniyle iç denetçilerin bilgi teknolojileri denetimi konusunda da çeşitli önemli görevleri bulunmaktadır. Bunlar (Uyar, 2009: 89-90):

1. Denetim komitesine ve üst yönetime, bilgi teknolojileri konularında danışmanlık yapmak,
2. Bilgi teknolojilerinin denetim ortamına ve denetim yıllık planına dahil edilmesini sağlamak,
3. Denetim faaliyetlerine kaynak tahsisinde ve denetimle ilgili önceliklerin belirlenmesinde bilgi teknolojileri risklerinin de dikkate alınmasını sağlamak,
4. Bilgi teknolojileri risk değerlendirmeleri yapmak,
5. Bütün bilgi teknolojileri risklerini asgari düzeye indiren faaliyetlerin yürütülmesini sağlamak ve buna ilişkin izleme ve kontrollere yardımcı olmak.
6. Denetim personelinin uzmanlık eğitimi de dahil, iç denetim bölümünün ihtiyaç duyduğu bilgi teknolojileri kaynaklarını tanımlamak,
7. Denetimin planlamasında bilgi teknolojileri sorunlarının dikkate alınmasını sağlamak,
8. Bilgi teknolojileri ile ilgili kurum seviyesinde kontrol amaçlı denetimler yapmak,
9. Bilgi teknolojileri genel kontrol denetimleri, uygulama kontrolü denetimleri ve uzman teknik kontrol denetimleri yapmak,
10. Sistem geliştirme veya analiz faaliyetleri sırasında, ilgili kontrollerin nasıl uygulanabileceğini değerlendirmek,
11. Denetim süreçlerine yardımcı olmak amacıyla bilgi teknolojilerinden etkin ve verimli bir şekilde yararlanmaktır.

Günümüzde iç denetimin faaliyet alanının genişlemesiyle birlikte iç denetçilerin sorumluluk alanlarının ve üzerlerine düşen görevlerin arttığını görmekteyiz. İç denetçinin görevleri tüm işletme içi görevleri ifade etmektedir. İç denetçinin görevleri dikkate alındığında, bu görevlerinin yerine getirilmesinin en çok üst yönetim açısından önemli olduğu görülmektedir. Çünkü iç denetim hata ve hile gibi işletmeye zarar verebilecek nitelikteki fiillerin önlenmesi konusunda yönetime bağlı olarak denetim yapar. Dolayısıyla, yönetim karar alırken veya ilgili kişilere bilgi sunarken iç denetim faaliyetinin sonuçlarına güvenecektir.

1.6.3. İç denetçilerin nitelikleri

İç denetçiler görev ve sorumluluklarını etkin bir şekilde yerine getirmek için bazı niteliklere sahip olmalıdır.

Bugünün iş yaşamının hızlı değişimi, iç denetçiyi bu değişime ayak uyduracak yapıda olmaya zorlamaktadır. Bu kapsamda iç denetim mesleğinin alanı, önemi ve fonksiyonu da hızla gelişmektedir. Yaşanan gelişmeler sonucu ve özellikle kurumsal yönetim anlayışı ile beraber, iç denetçilerden beklentiler de artmaktadır. Artan beklentiler kapsamında iç denetçiler şu niteliklere sahip olmalıdır (Abdioğlu, 2007: 124-125):

1. Saydamlık ve hesap verilebilirlik ihtiyacını karşılayabilmek için geçmişi analiz edip geleceğe dönük kestirimler öngörebilme,
2. Mevcut sorunları olduğu kadar potansiyel fırsatları da görebilme,
3. Süreç odaklı değerlendirme yapabilme,
4. Yönetimin taleplerini karşılayabilecek şekilde risk odaklı bakış açısına ve gelişen teknolojiyi etkin kullanabilecek beceriye sahip olma,
5. Kurum içi danışmanlık görevini yerine getirebilme,
6. Yönetim süreçlerini denetleyebilme,
7. Bilgi teknolojileri denetimi (IT Audit) yapabilme,
8. Kurumun geliştirme ve yenilik projelerine katkı sağlayabilme,
9. Performans ölçümü ve verimlilik analizi yapabilme.

Bu nitelikler dışında iç denetime ilişkin tüm düzenlemeler değerlendirildiğinde, iç denetçiler çalışmalarında etkin ve başarılı olabilmek için şu niteliklere sahip olmalıdır (Ak: 2004: 355, Uyar, 2009: 91):

1. Çalışmalarında bağımsız olmalıdır. İç denetçi çalışmalarını bağımsız yürütebilmesi için üst yönetime karşı sorumlu olmalıdır; yönetim görevinden uzak durmalıdır; görüşünü çekinmeden açıklamalıdır,
2. Gerekli mesleki bilgi ve tecrübeye sahip olmalıdır,
3. Bazı kişisel ve ahlaki nitelikleri taşımalıdır,
4. Çalışmalarında gerekli özen ve dikkati göstermelidir,
5. Problem çözme yeteneklerine sahip olmalı ve yeniliklere açık olmalıdır.

İç denetimin değişen rolü gereği iç denetçiler için önemi artan yetkinlik, iletişim, eğitim, vb konuların yanı sıra performans ölçümlemesi de iç denetimin kalite güvencesinin sağlanmasını destekleyecektir. İç denetçilerin performans değerlendirmesindeki performans faktörleri; gerçekleştirilen işin miktarı ve kalitesi, denetim bilgisi ve yeteneği, problem analiz ve karar verme yetisi, planlama, talimatları uygulama, yazılı ve sözlü iletişim olarak sıralanabilir. İç denetçi profilinde profesyonel yetenek kadar yaratıcılık, girişimcilik, ekip çalışmasına yatkınlık, uyum, ikna kabiliyeti, liderlik, özgüven, tutum gibi kişisel karakteristik özellikler ve karakter kalitesi de büyük önem taşımaktadır. Ayrıca iç denetçiler görevlerini yerine getirirken geleneksel denetim anlayışı yerine katılımcı yaklaşımı benimsemelidirler. İç denetçilerin uygulamalarında doğruluk, dürüstlük, tarafsızlık, güvenilirlik ve yetkinlik gibi mesleki etik kurallarına uymaları, teknik yetenek ve işletmede her düzeyde çalışanlar ile ilişki kurabilmek gibi yüksek standartlara sahip olmaları gerekir (Tektüfekçi, 2008: 102).

İç denetçinin sorumlulukları ve taşıması gereken nitelikleri göstermektedir ki, iç denetim faaliyetinin sonucu en çok yönetim için önem taşımaktadır. Çünkü iç denetim işletme içerisinde kötü niyetli olsun olmasın hata ve hile gibi işletmeye zarar verecek nitelikteki fiillerin önlenmesi konusunda işletme bünyesinde yönetime bağlı olarak yürütülen denetimdir. Böylece, yönetim karar alırken veya ilgili kişilere bilgi sunarken iç denetim sonuçlarına güvenecektir (Tuan ve Sağlar. 2004: 4).

1.6.4. Uluslararası iç denetim standartları

İç denetim faaliyetinin etkin bir şekilde yürütülebilmesi ve kalitesinin ölçülebilmesi iç denetim standartları ile mümkündür. İç denetim faaliyetinin iç denetim standartlarına uygun bir şekilde yerine getirilmesi ve bu faaliyeti gerçekleştiren denetçilerin de mesleki ahlak kuralları çerçevesinde hareket etmiş olmaları durumunda

iç denetimin makul bir güvence verdiği kabul edilmektedir. Genel olarak iç denetim standartları, yapılacak denetim çalışmalarına ve bu denetimi yapacak kişilere ilişkin belirlenmiş asgari kriterlerden oluşmaktadır. (Aslan, 2010: 74-75).

Uluslararası iç denetim standartların amaçları şunlardır (Gönülaçar, 2007: 9):

1. İç denetim uygulamasını olması gerektiği gibi temsil eden temel ilkeleri tanımlamak;
2. Katma değer yaratan iç denetim faaliyetlerini teşvik etmeye ve hayata geçirmeye yönelik bir çerçeve oluşturmak,
3. İç denetim performansının değerlendirilmesine uygun bir zemin oluşturmak,
4. Gelişmiş kurumsal süreç ve faaliyetleri canlandırmak.

Uluslararası iç denetim standartları, nitelik (attribute-1000 serisi), performans (başarım) (performance-2000 serisi) ve uygulama (implementation) standartlarından oluşur.

Nitelik standartları, iç denetim faaliyetlerini yürüten taraf ve kurumların özelliklerine yönelik standartlardır. Performans standartları, iç denetim faaliyetlerinin tabiatını açıklayan ve bu hizmetlerin performansını değerlendirmekte kullanılan kalite kıstaslarını sağlayan standartlardır. Nitelik ve performans standartları tüm iç denetim hizmetlerine uygulanırken, uygulama standartları belirli bir görev türüne uygulanır. Uygulama standartları, iç denetçiler tarafından sunulan geniş bir alandaki güvence ve danışmanlık hizmetleri içerisindeki özel bazı görevlere uygulanabilen standartları düzenlemek içindir. Uygulama standartları sayesinde nitelik ve performans standartları daha iyi anlaşılabilir (TİDE, 2008: 16).

2. İç Denetim Sürecindeki Yaklaşımlar

İç denetim, durağan bir alan değildir. Karşılaşılan durumların çeşitliliği ve değişen işletme koşulları değişik denetim araçları ve metotları kullanılmasına neden olmaktadır. Son yıllarda yaşanan finansal skandallar, hileli finansal raporlama ve iflaslar, iç denetimin etkinliğini attırma çabalarını yoğunlaştırmıştır. Bu çabalar sayesinde zamanla yeni yaklaşımlar ortaya çıkmıştır. Bu yaklaşımlar; geleneksel iç denetim yaklaşımı, sürekli denetim yaklaşımı, risk odaklı iç denetim yaklaşımı ve kontrol özdeğerlendirme yaklaşımıdır.

2.1. Geleneksel İç Denetim Yaklaşımı

Geleneksel iç denetim yaklaşımının yöntemi Minnahen Committee tarafından belirlenmiş ve kapsamı çizilmiştir (Uyar, 2009: 73). Geleneksel iç denetim yaklaşımı, iç kontrol üzerine odaklanmıştır. Bu yaklaşımda iç denetçi yönetim adına iç kontrol sistemini izler ve üst yönetime rapor verir.

Geleneksel iç denetim yaklaşımının özellikleri şunlardır (Kurnaz ve Çetinoğlu, 2010: 84):

1. Önceden belirlenmiş denetim programları kullanılır,
2. Denetimler rutinleşmiştir,
3. Kullanılmakta olan denetim sistemi kolaydır,
4. Raporlar, çözüm önerilmeksizin sadece sorunları gösterir.

Geleneksel iç denetim yaklaşımında riskler doğal (asıl) risk, kontrol riski ve bulgu (detaksiyon) riski olarak sınıflandırılmaktadır. Doğal risk, iç kontrol prosedürlerinin olmadığı varsayıldığında, bir hesap bakiyesinde veya işlemler grubunda önemli hata veya düzensizliklerin oluşma olasılığıdır. Kontrol riski ise, bir hesap bakiyesi veya işlemler grubunda oluşacak önemli hata veya yolsuzlukların, olduğu anda iç kontrol sistemi tarafından meydana çıkarılamama olasılığıdır. Bulgu riski ise, denetçinin finansal tablolardaki önemli hata ve düzensizlikleri bulup çıkarmada başarılı olamayacağı olasılığıdır (Erdoğan, 2006: 52-53).

Geleneksel iç denetim yaklaşımının aşamaları şunlardır (Yılancı, 2006: 121-123):

1. *Genel ve özel kontrol amaçlarının belirlenmesi:* İç denetçiler belirledikleri alandaki denetim çalışmalarına bu alanla ilgili genel ve özel kontrol amaçlarını belirleyerek başlarlar. Genel ve özel kontrol amaçları iç denetçi için işletmenin iç kontrol sistemi ile ilgili değerlendirme standardı olacaktır. Genel kontrol amaçları, işletmenin kontrol usul ve yönteminin değerlendirilmesinde genel bir çerçeve sağlayacaktır. Özel kontrol amaçları ise denetimi yapılan süreç ve işlem grubunun ayrı ayrı değerlendirilmesini sağlar.
2. *Kontrol tekniklerinin belirlenmesi ve uygunluğunun değerlendirilmesi:* Kontrol teknikleri, özel kontrol amacına ulaşılması için gerekli bir eylem, politika ve prosedürdür. Denetçi, her bir kontrol amacına ulaşılması için özel kontrol politika ve prosedürleri belirlemelidir. Kontrol tekniklerinin

eksikliği veya zayıflığı, özel kontrol amaçlarının başarılabilmesi ile sonuçlanacaktır. Bu durum kontrol zayıflıklarının ortaya çıkmasına neden olur.

3. *Anahtar kontrollerin belirlenmesi:* Denetçi kontrol tekniklerini belirledikten sonra bunlarla ilgili testleri yapacaktır. Mevcut kontrol tekniğinin uygun bir iç kontrol sistemi sağlayacağı düşünülürse, kontrollerin planlandığı gibi işleyip işlemediğini araştırmak için yapılacak testlerin büyüklüğü belirlenmelidir.
4. *Seçilmiş kontrol tekniklerinin test edilmesi:* Denetçi tarafından seçilen kontrol tekniklerine testler uygulanır.
5. *Bireysel kontrollerin etkinliğinin değerlendirilmesi:* Test sonuçlarına göre bireysel kontrollerin başlangıçta planlandığı gibi işleyip işlemediğinin konusu değerlendirilir. Böylece tüm iç kontrol sistemi hakkında bir değerlendirme yapılmış olur.
6. *Kontrol amaçlarını elde etmede iç kontrol sisteminin uygunluğuna bağlı olarak düşünce ve tavsiyeleri raporlama:* Denetçi test sonuçlarına göre iç kontrol sistemi ile ilgili ciddi zayıflıklar olduğunu düşündüğü noktaları, tavsiyelerini ve iç kontrol sisteminin tanımlanmış kontrol amaçlarını elde etmedeki uygunluğunu raporlamalıdır.

Buraya kadar bahsedilenlerden anlaşılacağı üzere geleneksel iç denetim yaklaşımı, geçmişe dönük faaliyetler üzerine odaklanmış ve yapılan testler ile geçmişteki hatalar ortaya çıkartılmaya çalışılmaktadır. Geleneksel iç denetim yaklaşımı, iç kontrol sistemine ilişkin öneriler getirmektedir. Ayrıca bu yaklaşımda daha çok muhasebe denetimi riskleri dikkate alınmaktadır.

2.2. Sürekli Denetim Yaklaşımı

Gelişmiş bilgi teknolojilerine bağımlılığın artması, büyük hacimli verilerin bu bilgi teknolojileri tarafından işlenmesi, yönetimin iç kontrolün yeterliliği için üstlendiği sorumlulukların çoğalması ve denetim alanında bilgi teknolojilerinin kullanımı sürekli bir süreç denetimini gerektirmiştir. Bu yaklaşımla birlikte işletmeler daha güvenilir, sürekli, eş zamanlı ve kaliteli finansal bilgiler üretmeye yönelmişlerdir. Bu noktada

sürekli denetim, sürekli gözlem, sürekli kontrol ve sürekli raporlamayı içeren sistemler oluşturulması gerekmiştir.

2.2.1. Sürekli denetimin tanımı ve unsurları

Sürekli denetim, fiziki belge olmaksızın gerçek zamanlı muhasebe bilgi sisteminde üretilmiş olan finansal tablolarda yer alan finansal karakterli bilgilerin doğruluğuna ve güvenilirliğine ilişkin bir görüş oluşturmak amacıyla bilgisayar destekli denetim tekniklerini ve analitik prosedürleri kullanarak elektronik denetim kanıtlarını toplamaya ve toplanan kanıtlardan ulaşılan görüşü bir denetim raporu ile bilgi kullanıcılarına sunmaya yönelik sistematik bir süreçtir (Selimoğlu, 2006b: 150).

Sürekli denetim, bilginin açıklanması ile birlikte veya çok kısa bir süre içinde denetçilerin sürekli bilgi üzerinde bir dizi güvence vermesini sağlayan kapsamlı bir elektronik denetim sürecidir. Sağlanan güvence yüksek düzeyde ve sürekli bilgi de finansal raporlar hakkında ise sürekli denetim bir denetim işi olarak yapılır. Sağlanan güvence orta düzeyde ve sürekli bilgi de finansal bilgiler olduğunda sürekli denetim işi bir onaylama hizmeti olarak kabul edilir. Fakat sağlanan güvencenin her türlü finansal veya finansal olmayan sürekli bilgiyi kapsadığı durumlarda sürekli denetim işi bir güvence hizmeti olarak kabul edilir. Sürekli denetim, yönetim ve üçüncü kişiler tarafından sunulan bilgiye güvenilirlik kazandırmaktadır (Kurnaz ve Çetinoğlu, 2010: 154).

Geleneksel denetim ve sürekli denetim arasında bazı farklılıklar vardır. Bu farklılıklardan ilki zaman konusundadır. Sürekli denetim ile işletme hakkında karar alma durumunda olan tarafların işletmenin tamamı veya bir kısmı denetlenmiş bilgileri sık aralıklarla düzenlenebilecek raporlar ile ulaşabilirken, geleneksel iç denetim yaklaşımında zamana ilişkin herhangi bir belirli zaman olmamakla birlikte denetim genelde dönem sonunda gerçekleştirilmektedir. Sürekli denetim, geleneksel iç denetim yaklaşımının aksine, karar vermede ihtiyaç duyulan herhangi bir bilginin üzerine odaklanmanın ve denetçinin sadece finansal olan bilgiler üzerinde değil, finansal olmayan bilgiler üzerinde de denetim uygulayıp rapor oluşturması mümkündür. Örnek verilecek olursa, elektronik ticaret ile ilgili işlemlerin varlığı, doğruluğu, güvenilirliği, herkese açık veritabanı kontrollerinin etkinliği gibi sayılabilir. Geleneksel yaklaşımda insan faktörü ön plandayken, sürekli denetimde çeşitli yazılımlar ve donanımlar

kullanılır. Çünkü sürekli denetim, elektronik ortamda ortaya çıkan verilere ve denetim kanıtlarına odaklanır. Sürekli denetimde denetim sürecinde bilgi teknolojilerinin yoğun bir şekilde kullanılması maliyet avantajı sağlamaktadır. Sürekli denetimde, denetime konu olan işlemlerin gerçekleştiği anda izlenebilmesine imkan veren donanım ve yazılımlar sayesinde insan faktöründen kaynaklanan hatalar ve zaman kayıpları engelleneceği ve denetçinin ayrıntılarla uğraşması yerine sadece denetim riskini ve denetim stratejisini etkileyebilecek olaylar üzerine odaklanmasını sağlayarak denetimin etkinliği ve verimliliği artırılabilir (Ağca, 2006: 69-70).

2.2.2. Sürekli denetimin uygulama süreci

Sürekli denetim, pek çok şekilde geleneksel denetim sürecini etkilemektedir. Elektronik dokümanlar, kayıtlar ve verilerin doğruluğunu ve güvenilirliğini sağlamak için denetçinin, müşterinin işi ve sektörü hakkında sürekli daha çok bilgi edinmesinin gerekliliği denetim sürecini etkilemektedir. Gelişen bilgi teknolojileri, elektronik finansal raporlamaların en uygun şekilde kullanılmasını belirlemek için denetçileri yönlendirmekte ve müşterilerinin iş süreçlerine denetimin planlanması aşamasında daha fazla önem vermelerine neden olmaktadır. Denetçiler gerçek zamanlı muhasebe sistemleri içinde bilginin güvenilirliğini ve doğruluğunu sağlayan işlem akışını ve ilgili kontrol faaliyetlerini daha iyi anlamalıdır. Gerçek zamanlı muhasebe sistemlerinde faaliyetler elektronik ortamda iletilmekte, işlemler elektronik ortamda gerçekleşmekte ve erişimi elektronik ortamda olmaktadır. Elektronik verilerin doğruluğu ve güvenilirliği iç kontrol sistemine bağlıdır. Sürekli denetimde denetçiler gerçek zamanlı muhasebe sistemleri üzerine odaklanmakta ve elektronik işlem ve dokümanların test edilmesini ikinci plana itmekte, kontrol ve risk yönelimli bir denetim planı gerçekleştirmektedir (Kurnaz ve Çetinoğlu, 2010: 195-196).

Sürekli denetimde tüm denetim işleri yeterli ve doğru kanıtları bir araya getirerek yönetimin açıklamalarını test etmeyi kapsamaktadır. Kanıtların elektronik biçimde olacakları göz önünde bulundurulmalı ve bunun sonucunda gerekecek test ve kontrollerin boyutunu ve maddilik testlerinin içeriği, zamanlaması ve boyutunu belirlemeleri gerekecektir. Sürekli gelişen bilgi teknolojileri ve elektronik ticaretin kullanımı, denetçilerin kanıtlarını elektronik olarak elde etmelerini gerektirmektedir (Kurnaz ve Çetinoğlu, 2010: 200).

Sürekli denetim yaklaşımında iç denetçilerin uyguladığı denetim programı şöyledir (Coderre, 2009: 79-80):

1. Güvenli veri girişi ve veri kalitesinin sağlanması:
 - a. Anahtar uygulama sistemlerine giriş geliştirilmesi ve korunması
 - b. Uygulamaları anlama
 - c. Veri bütünlüğünü ve güvenilirliğini değerlendirme
2. Analiz becerilerini ve araçlarını geliştirme
 - a. Analiz araçları satın alma (yazılım ve donanım)
 - b. Analiz tekniklerini geliştirme
 - c. Becerileri denetim yapılacak işletmede paylaşma.
3. Tüm istisnaları önceden tahmin edin:
 - a. Alanın seçilmesi ile birlikte uygulamaya geçmek için en kritik raporların belirlenmesi
 - b. Süreç akışının ve geçmiş denetimlerin incelenmesi
 - c. Sektördeki en iyi uygulamalar üzerinde çalışma ve dış denetçiden faydalı bilgiler edinme
 - d. Aşağıda bahsedilenleri gerçekleştirmek için faaliyet yönetiminin desteğini almak:
 - i. Programın ve işletmenin amaçları
 - ii. Risklerin etkilerinin belirlenmesi ve hangi faktörler riski arttırır
 - iii. Riskleri gözlemlemek için kullanılacak araçlar
 - iv. Planlanana karşılık tüm personelin gerçek ilgililiği
 - v. Bir gözlem raporunun hazırlanması
4. Öncelikler ve denetim planı:
 - a. Yüksek öncelikli alanları seçmek için risk analizi yapma
 - b. Hangi durumların araştırılacağının belirlenmesi ve zamanlılığa karşı etkinlik konusunun dikkate alınması
 - c. Denetimin ve sürekli denetimin yapılacağı zaman ve risk aralığının planlanması
5. Planın uygulanması:
 - a. Sürekli denetim için uygun bir hedefin belirlenmesi

- b. Değerlendirme yapmak için işletmeyi ve kategorileri tanımlamak
- c. Analizleri yapmak ve göstergeleri hesaplamak
- d. Sonuçları geçmiş dönemlerle karşılaştırmak

6. Sonuçları iletmek:

- a. Sonuçları ilgili yönetime bildirmek
- b. Sürekli denetim sürecinin etkinliğini gözlemlemek ve değerlendirmek

Sürekli denetim, risk yönetimi, kontrol değerlendirme, denetim planlama, dijital analizler ve diğer denetim araç ve tekniklerini bir arada tutan birleştirici bir yapı ve çerçevedir. Sürekli denetim, yıllık denetim planının hazırlanması sırasında değerlendirilen riskler gibi makro denetim konularını ve bireysel denetim amaçlarını ve ölçütlerini geliştirmek gibi mikro denetim konularını kapsar. Makro ve mikro denetim konuları arasındaki temel fark, ele alınan detayın miktarıdır (Coderre, 2009: 71-72).

2.3. Risk Odaklı İç Denetim Yaklaşımı

Bilgi teknolojileri alanlarında yaşanan gelişmeler işletmelerde geleneksel risklerin yanı sıra yeni ve daha karmaşık riskler oluşmasına neden olmuştur. İşletmelerin hızlı değişim gösteren risk profillerinin tanınmasında yeterli olmayan geleneksel denetimin eksikliklerini gidermek amacıyla risk odaklı iç denetim yaklaşımı benimsenmiştir.

2.3.1. Risk odaklı iç denetimin tanımı ve unsurları

Risk odaklı iç denetim, denetim faaliyetinin odak noktasını geçmiş faaliyetlerden geleceğin yönetilmesine çevrilmesini sağlamıştır. Risk odaklı iç denetim yaklaşımı, işletmelerin risk profillerinin belirlenmesi, denetim sürecinin işletmenin risk profiline göre şekillendirilmesi ve denetim kaynaklarının buna göre dağıtılması esasına dayanan ve denetimin etkinliğini arttırmayı amaçlayan bir denetim yaklaşımıdır (Kurnaz ve Çetinoğlu, 2010: 84). Risk odaklı iç denetime dayalı denetim yaklaşımı, denetim kaynaklarının sınırsız olmadığı, denetlenecek birim faaliyetlerinin farklı risklerle karşı karşıya olduğu ve denetlenecek birim faaliyetlerinin göreceli olarak farklı önem derecesine sahip olduğu varsayımlarına dayanır (Başpınar, 2006: 27).

Risk odaklı iç denetimi geleneksel iç denetim yaklaşımından farklı kılan bazı özellikler vardır. Risk odaklı iç denetim, işletme süreçlerinin tanınması, işletme riskleri ve bunların yönetimi üzerine odaklanmaktadır. Risk odaklı iç denetim, risk yönetimi alanına doğru kaymıştır. Risk odaklı iç denetimde içsel risk yönetim süreçlerinin yeterli olduğunun belirlenmesi veya risklerin minimum düzeyde olduğunun tespit edilmesi durumunda işlem testleri¹⁸ (uygunluk testleri) azaltılır. Bunun aksi söz konusu ise, ilave işlem testlerine başvurulması gerekmektedir. Uygulanan testler, belirli bir faaliyet ve fonksiyonun etkilendiği riskin derecesini tam olarak değerlendirmelidir (Ergin, Çetinoğlu ve Kurnaz, 2008: 21).

Risk odaklı iç denetim yaklaşımı, etkin bir risk yönetimi, iç denetim ve iç kontrol sistemlerinin kurulmasını yönetim bilgi sistemlerinin güçlendirilmesini ve uygunluk değerlendirme birimlerinin oluşturulmasını gerektirir (Ergin, vd. 2008: 22). Risk odaklı iç denetim yaklaşımı risk yönetimi süreçlerinin çıktılarından yararlandığından denetimin etkinliği, zaman ve maliyet tasarrufu açısından fayda sağlar ve iç denetçilerin işletmelerin yüksek riskli alanlarına odaklanmasına yardımcı olur (Özer, 2008: 1).

2.3.2. Risk odaklı iç denetimin uygulama süreci

Etkin bir iç denetim sisteminin en önemli görevlerinden biri tüm risklerin tespit edilmesi ve minimize edilmesi için uygun öneriler geliştirmektir. Geleneksel iç denetim yaklaşımında denetim faaliyeti sadece geçmiş döneme ait hataların incelenmesi ve belirli bir faaliyete veya kişiye yönelik yürütülen çalışmaları ifade etmektedir. Günümüzde denetimin risk odaklı yapılması ise, işletmelerin geçmiş faaliyetlerin değerlendirilmesinden çok, gelecekte daha iyi yönetilmesine odaklanmaktadır (Anıl, 2006: 24).

Risk odaklı iç denetimi yönetmek için aşağıdaki süreçleri izlemek gerekir (Ergin, vd., 2008: 24-27):

¹⁸ Uygunluk testleri; *işlem testleri*, gözlem ve soruşturmadan oluşur. Uygunluk testleri, muhasebe kontrollerine ilişkin yönetim tarafından hazırlanan ve iç kontrolün işleyişi için uyulması zorunlu olan kontrol yordamlarıdır. (Erdoğan, 2006: 99). İşlem testleri, yoklama ve yinleme testlerinden oluşur. Yoklama testlerinde gözden geçirilmiş ve incelenmiş işlemlere ilişkin uygunluk testleri yapılır. Yinleme testlerinde ise kontrol yordamlarının işlevselliği açısından ek kanıtlar sağlanmaya çalışılır ve yoklama testleri ile bulunamayan iç kontrol aksaklıklarını bulmaya çalışır. Uygunluk testlerinin yapılması ve sonucu maddilik testlerinin yapısını ve büyüklüğünü belirleyecektir (Erdoğan, 2006: 113-114).

1. İşletme Faaliyetleri Hakkında Bilgi Toplamak: İç denetçi işletme içindeki olası risk alanlarını araştırmak durumundadır. İşletmedeki muhtemel riskli işlemlerin varlığına ilişkin bilgilerin varlığının araştırılması ve yönetimin bu davranışlara ilişkin tutumunun araştırılması gerekir. Buna göre iç denetçi denetim planını ve programını etkileyecek risk faktörlerini içeren bilgiler edinecektir.
2. Risk Tanımlama: Bir iç denetim görevi planlanırken, iç denetçiler incelemekte oldukları eylemle ilgili riskleri belirlemeli ve değerlemelidirler (Yılancı, 2006: 126). Risk tanımlamasında işletme bünyesinde bulunan riskler her risk seviyesine göre (düşük, orta, yüksek) değerlendirilir ve risk alanları tablosunda gösterilir.
3. Risk Ölçümü: Risk değerlendirmesini tanımlamak için denetçi bu alanların her birinde ve geçmişe yönelik herhangi bir risk alanında riski öncelikli hale getirme ve ölçme yollarına ihtiyaç duyar. Risk faktörleri tespit edildikten sonra bu faktörlerin toplam risk içindeki nispi önemini belirlemek gerekir. Nicel tekniklerle, hile riskinin oluşma ihtimali ve sonuç üzerindeki etkisi sayısal olarak ifade edilir ve risk büyüklüğü sayısal bir değer olarak hesaplanır (Risk niceleme/Risk sayısallaştırma). Nitel tekniklerle ise riskin derecesi belirlenir (Risk derecelendirme).
4. Risk Önceliklendirme (Risk Değerlendirmesi): Belirlenen riskler derecelerine bağlı olarak sıraya konulur. Risk önceliklendirme süreci sonunda işletme için en kritik risk belirlenmiş olur. En yüksek dereceye sahip risk en kritik risktir ve bu risklere öncelikli olarak kaynak ayrılarak, kısıtlı denetim kaynakları etkin kullanılmış olur. Bu süreçte kullanılan risk matrisleri, risklerin oluşma olasılığı, sonuca etkisi, büyüklüğü ve oluşabileceği zaman aralığı gibi bilgileri kapsar.
5. Sonuçların raporlanması: Risklerle ilgili sonuçlar yönetim kuruluna, denetim komitesine ve diğer ilgililere iletilir.

Risk odaklı iç denetim sürecinde işletmenin içinde bulunduğu olası tüm riskler tanımlanır. Bu riskler ağırlık derecesine göre sıraya konur ve risk seviyesi belirlenir. Risklerin azaltılması için gereken önlemler alınır ve uygulanır. Risk denetimine ilişkin raporlama yapılır (Uyar, 2006b).

2.4. Kontrol Özdeğerlendirme Yaklaşımı

İç denetimde son yıllarda kabul gören denetim yaklaşımlarından birisi de kontrol özdeğerlendirme yaklaşımıdır. Kontrol özdeğerlendirme yaklaşımı (Control Self-Assessment-CSA) kendi kendine kontrol yaklaşımı olarak da literatürde karşımıza çıkmaktadır. Kontrol özdeğerlendirme yaklaşımı, işletmenin risk yönetimi ve kontrol süreçlerinin uygunluğunu değerlendirmek için yöneticiler ve iç denetçiler tarafından kullanılabilir (Uyar, 2009: 75).

Kontrol özdeğerlendirme yaklaşımı, kontrol kalitesinin değerlendirilmesinde iç denetçilere ve yönetime gerekli olan iç kontrol bilgisinin ortaya çıkarıldığı bir süreçtir. Ayrıca bu yaklaşım, doğru faaliyetlerin belirlenmesi, ortaya çıkan risklerin tanımlanması, iç kontrolün tasarımı ve yürütülmesi faaliyetleri ile iç denetim mesleğine değer katacaktır (Kurnaz ve Çetinoğlu, 2010: 113).

2.4.1. Kontrol özdeğerlendirmenin tanımı ve unsurları

Kontrol özdeğerlendirme yaklaşımı, işletmelere, hedeflerini gerçekleştirme ve yeteneklerini güçlendirme konusunda yardımcı olan, daha çok iç kontrol sisteminin etkinliğini artırmaya yönelik bir dizi etkinliği kapsayan yöntemdir. Kontrol özdeğerlendirmenin amacı; işletme amaçlarını başarma olasılığını, bu amaçları gerçekleştirme sorumluluğu olan çalışanların bilgisinden faydalanarak saptama ve değerlendirme yapmayı sağlamaktır. Kontrol özdeğerlendirme, ortak bir amaç veya hedef için bir grup çalışandan oluşan, çalışma takımlarını hem değerlendirme yapan ve hem de işletme amaçlarını karşılama konusundaki değişiklikleri ve yeni düzenlemelerle hedef yükseltmeyi gerçekleştiren ve bunlarla ilgili ilerlemeler hakkında yorum yapmaya teşvik eden; inisiyatifi elinde bulunduran bir süreçtir (Anıl, 2006: 31).

Kontrol özdeğerlendirme yönteminin çıktıları yardımıyla iç denetçi, işletme içindeki kontrol süreçleri hakkında daha fazla bilgi edinir ve bu bilgileri, kıt olan denetim kaynaklarını, önemli kontrol zayıflıkları olan ve yüksek risklerle karşı karşıya olan iş birimlerinin ve fonksiyonlarının araştırılmasına ve bu konuda gereken testlerin yapılmasında kullanabilir (TİDE, 2008: 329).

Kontrol özdeğerlendirme yaklaşımını geleneksel yaklaşımdan ayıran bazı özellikler vardır. Geleneksel iç denetim yaklaşımında mevzuata uygunluk ve mali

kayıpların olup olmadığı denetlenirken kontrol özdeğerlendirme yaklaşımında tüm süreç denetlenmektedir. Geleneksel denetim yaklaşımı muhasebeye dönük kontrollere ağırlık verirken kontrol özdeğerlendirme risk ve kontrol süreçlerinin değerlendirilmesi ile ilgilenmektedir. Kontrol özdeğerlendirme yaklaşımında iç denetçilerin rolü, risk ve kontrol konularında eğitim ve danışmanlık vermektir. Kontrol özdeğerlendirme yaklaşımında iç kontrol sisteminin değerlendirilmesinde bölüm çalışanları ve yönetim de yer almaktadır. Geleneksel iç denetim yaklaşımının aksine raporlar çalışma grupları tarafından yayınlanmaktadır. Kontrol özdeğerlendirme yaklaşımı yönetim tarzı, liderlik, takım çalışması, davranış kuralları ve personelin dürüstlüğü gibi geleneksel iç denetim yaklaşımı için yumuşak sayılan kontrolleri değerlendirmede de kullanılabilecek en iyi yaklaşımdır. Son olarak kontrol özdeğerlendirme yaklaşımında geleneksel yaklaşıma oranla bilgi teknolojilerinde daha fazla yararlanılmaktadır (Kurnaz ve Çetinoğlu, 2010: 114-115).

Kontrol özdeğerlendirme yaklaşımı, maliyet etkinliği, iç kontrol sisteminin yıllık değerlendirmesi, problemlerin çözümüne yardımcı olma, yönetici ve çalışanların işletme hedeflerine ulaşmada kontrolün önemi konusunda eğitilmesine katkı sağlar. Ayrıca işletmenin iç kontrol sisteminin üst düzeyde incelenmesini sağlar (Yılancı, 2006: 135).

2.4.2. Kontrol özdeğerlendirmenin uygulama süreci

İç Denetçiler Enstitüsü'nün uygulama tavsiyelerinde 2120 A1-2 de "Kontrol Süreçlerinin Yeterliliğinin Değerlendirmede Kontrol Özdeğerlendirmenin Kullanımı" başlığında bu yöntemin kullanılmasını önermektedir.

Bir işletmede kontrol özdeğerlendirme yaklaşımının uygulama sürecinde dikkat edilmesi gereken bazı kurallar vardır. Öncelikle işletmenin hangi kısımlarında kontrol özdeğerlendirme yaklaşımının uygulanacağına karar verilmelidir. Ayrıca çalışmalar sırasında ortaya çıkan risk değerlendirme ve diğer sonuçların iç denetim eylemleri sırasında kullanılıp kullanılmayacağının belirlenmesi gerekir. Kontrol özdeğerlendirme süreçlerinin başarısı için bu programları yürüteceklerin hangi araçları, teknikleri, dokümanı ve raporları kullanacakları belirlenmelidir (Ergin, vd. 2008: 22).

Kontrol özdeğerlendirme yaklaşımının ortaya çıkışında, işletmelerde bilgi teknolojilerinin kullanımındaki artış gerekli desteği sağlamıştır. Özdeğerlendirme ve

bilgisayar yazılımları denetçilere yardımcı olmaktadır. Yazılımlar, hangi kontrollerin önemli olduğunun veya hangi kontrollerin daha iyi işlediğinin belirlenmesi açısından yapılan denetimler sırasında, faaliyet alanlarındaki çalışanların bu çalışmalara katılımını teşvik etmek için denetçilere yardımcı olabilir. Kontrol özdeğerlendirme, işletmenin temel amaçlarının belirlenmesi ve bu amaçların desteklenmesi ile başlar. Kontrol özdeğerlendirme sürecini yöneten denetçi, bilgisayar yardımıyla çalışanların tartışma sonuçlarını izler. Kullanılan yazılımlar, tartışmalara katılarak katkı sağlamaya izin vermektedir. Çalışanlar, süreç açısından önemli ve uygun olan giriş ve çıkışlarını bilgisayar ekranında görebilirler. Ayrıca yazılımlar, kontrollerin etkin bir şekilde çalışıp çalışmadığı konusunda katılımı ölçmek için çalışanların oy kullanarak fikrini beyan etmesine izin verir. Sonuçlar gerçek zamanlı olarak grafiklerde gösterilir ve bu durumda kontrollerin güçlü veya zayıf olduğu ortaya konulur (Coderre, 2009: 49).

Kontrol özdeğerlendirme yaklaşımı, yöneticilerin ve iç denetçilerin kontrol prosedürlerini değerlendirmek ve incelemek konusunda işbirliği yapmaları için faydalı ve etkin bir yaklaşım ve araçtır. Özü itibarıyla, kontrol özdeğerlendirme, iş hedefleri ve risklerini kontrol süreçleriyle bütünleştirir ve birleştirir. Kontrol özdeğerlendirme yaklaşımını kullananlar genellikle farklı yöntemler kullanmasına rağmen, uygulanan programların çoğunluğu bazı temel özellikleri ve hedefleri paylaşmaktadır (TİDE, 2008: 328).

Kontrol özdeğerlendirme yaklaşımında kullanılan yöntemler şunlardır:

1. *Basitleştirilmiş kontrol grupları (Workshop)*: İşletme içindeki değişik kademeleri temsil edebilen çalışma takımlarından iç kontrol bilgisinin toplanmasını sağlar (Yılancı, 2006: 132).

Basitleştirilmiş kontrol grupları kontrole, sürece, riske ve hedefe dayalı olarak gerçekleştirilir. Kontrole dayalı biçimde, işletme faaliyetleri içerisinde yerleştirilmiş kontrollerin iyi çalışıp çalışmadığı üzerine odaklanılır. Anahtar riskler ve kontroller çalışma grubu başlamadan önce belirlenmiştir. Sürece dayalı biçimde, seçilmiş süreçler içindeki faaliyetlerin incelenmesi söz konusudur. Bu çalışma grubu türü, tüm sürecin amaçlarının belirlenmesini ve bazı ara adımları kapsar. Bu grubun amacı, tüm süreci ve faaliyetlerin bileşenlerini değerlendirmek, güncellemek ve geliştirmektir. Riske dayalı biçimde, iç kontrol amaçlarının başarılması için risklerin belirlenmesi ve

yönetilmesi üzerine odaklanılır. Öncelikle tüm olası engeller, kısıtlar, tehlikeler belirlenir ve ondan sonra belirlenen riskleri yönetmeye yeterli olup olmadığını belirlemek için iç kontrol prosedürleri incelenir. Hedefe dayalı biçimde, bir amaca ulaşmadaki en iyi yol üzerine odaklanılır. Öncelikle sistem amaçlarını desteklemek için gereken kontroller belirlenir ve daha sonra kontrollerin çalışıp çalışmadığını anlamak için kalan artık riskler belirlenir (Moeller, 2004: 158).

2. *Soru kağıtları (Anket Yöntemi)*: Kişilerin kendi süreçlerindeki kontrol mekanizmalarını kontrol etmeleri için imkan sağlar. Evet/Hayır veya Var/Yok şeklindeki araştırma aracı olarak kullandığımız soru kağıtlarını kişiler kendileri de doldurarak, kontrol yapılarını değerlendirebilir (Yılancı, 2006: 134).

3. *Yönetimin ürettiği analizler*: Bu yaklaşımda yönetim, işletme sürecinin bir portresini üretir. İç denetçi bu çalışmaları birleştirir ve çalışma sonuçlarını kombine eder (Yılancı, 2006: 134).

3. İç Denetimin Değişen Faaliyet Alanları

Güvence ve danışmanlık hizmetleri denetim faaliyetinin özünde yer almaktadır. İç denetim, işletmenin her türlü etkinliğini geliştirmek, iyileştirmek ve işletmeye değer katmak amacıyla bağımsız ve tarafsız bir güvence ve danışmanlık hizmeti vermektedir. İç denetçiler, risk yönetimi, iç kontrol ve kurumsal yönetim süreçlerinin etkinliği ve verimliliğinin değerlendirilmesi ve geliştirilmesi için sistematik yaklaşımlar vasıtasıyla işletmenin hedeflerini başarmasına katkıda bulunur.

İç denetimin faaliyet alanlarını üç ana başlıkta ele alabiliriz:

1. Risk yönetimi
2. İç kontrol
3. Kurumsal yönetim

3.1. Risk Yönetimi

Risk yönetimi, işletmelerin işlevleri sırasında ortaya çıkabilecek risklerin önceden değerlendirilmesi ve bu riskleri azaltacak veya ortadan kaldıracak önlemlerin alınmasıdır. Risk yönetimi süreçleri sırasında iç denetçiler bütün denetlenebilir faaliyetleri ve ilgili risk faktörlerini belirler ve tanımlar, bu risklerin önem düzeylerini değerlendirir (Alptürk, 2008a:235-236).

3.1.1. Risk yönetiminin tanımı ve bileşenleri

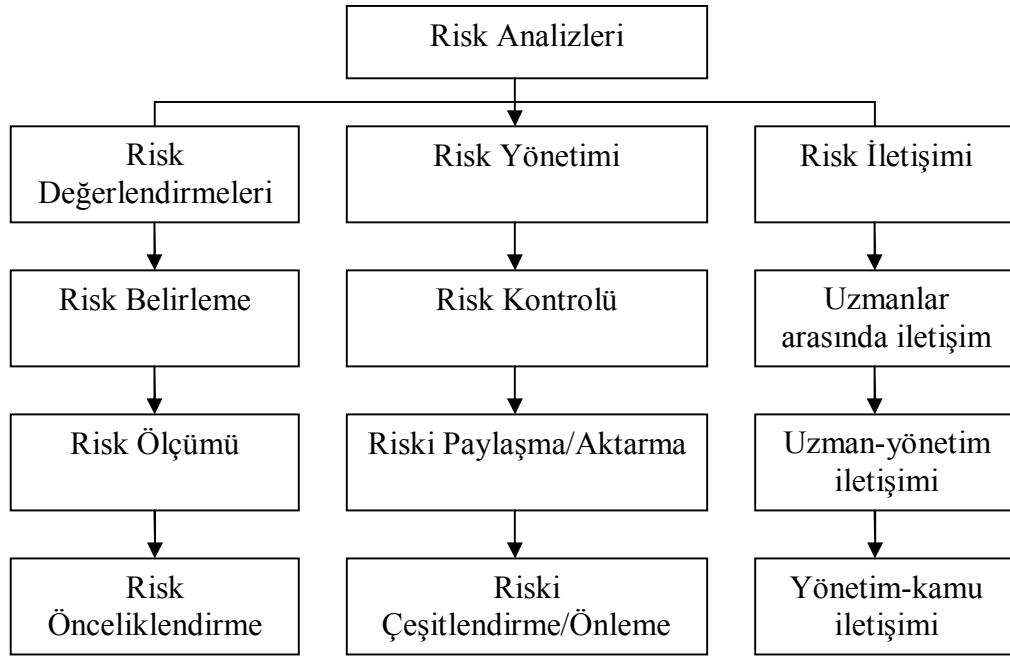
Risk yönetimi, risklerin belirlendiği, değerlendirildiği ve kontrol altına alındığı bir süreçtir. Risk yönetiminin amacı, risk alınan faaliyetlerin farkındalığını arttırmak, işletmeye zarar verebilecek olayların sıklığını azaltmak ve zarar verici bir olay gerçekleşmişse, bu durumun sonuçlarının şiddetini azaltmaktır (Griffiths, 2005: 20-21).

Risk yönetimi, Treadway Komisyonu Sponsor Organizasyonlar Komitesi (COSO-Committee of Sponsoring Organisations of the Treadway Commission) ve İç Denetçiler Enstitüsü tarafından da tanımlanmıştır. COSO'ya göre risk yönetimi, işletmenin amaçlarına ulaşmasını etkileyebilecek potansiyel durumları tanımlayan, bunları risk alma istekliliği sınırları içinde yöneten ve işletme amaçlarını başarılması konusunda makul bir güvence sağlayan tüm işletme çapında yapılandırılmış ve yönetim kurulu, yönetim ve diğer çalışanlar tarafından etkilenebilen bir süreçtir. IIA'ya göre risk yönetimi, işletmenin amaçlarına ulaşmasını etkileyen fırsat ve tehlikelerin belirlenmesi, değerlendirilmesi ve bu fırsat ve tehlikelere karşı çözüm yollarının üretilmesi konusunda raporlama yapan, tüm işletme çapında aktif bir rol oynayan tutarlı, sürekli ve yapılandırılmış bir süreçtir (Fraser ve Henry, 2007: 393).

Risk yönetimi, işletmenin karşı karşıya olduğu risklerin belirlenmesi ve değerlendirilmesiyle başlar. Riskin tespiti ile yapılan değerlendirmeden sonra işletme yönetimi tespit edilen risklerin kabul edilebilir düzeyde olup olmadığına karar verir. Eğer risk kabul edilemeyecek düzeyde bir risk olarak değerlendirilirse yönetim buna karşı alınacak önlemleri belirleyecektir. Riske karşı en önemli kilit nokta iç kontrol sisteminin oluşturulmasıdır. Yönetim iç kontrol sistemindeki kontrollerin etkinliğinden ve yeterliliğinden emin olmalıdır (Özoğlu, vd., 2010: 152).

Risk yönetimi için altyapı oluşturulup gerekli dönüşüm faaliyetleri yerine getirildikten sonra artık sistemin işleyişine geçilir. Risklerin kurumsal olarak yürütülmesine

risklerin tanımlanması ile başlanır. İşletmenin muhtemelen karşılaşacağı riskler böylece tespit edilir. Tanımlanan riskler analiz edilir ve ölçülür. Bu ölçüm sayesinde risklerin şiddetleri ve işletmenin bu risklere ne kadar maruz kalacağı belirlenmiş olur. Risklerin ölçüm değerleri ve işletmenin maruz kalma seviyesi göz önünde bulundurularak riskler önceliklendirilir. Bu sayede kurum için en önemli risklerin hangileri olduğu ortaya çıkar. Öncelikli riskler belirlendikten sonra bunlar karşısında takınılacak tavrın ne olması gerektiğine karar verilerek kararlaştırılan karşılıklar uygulamaya konur. Tüm bu süreç bir yandan izlenir, bir yandan ortaya çıkan aksaklıklar aktif olarak ortadan kaldırılır, diğer yandan da değişen koşullara göre sistem iyileştirilir (Arslan, 2008: 55-56).



Şekil-4. Risk Yönetimi Çerçevesi

Kaynak: Selim ve McNamee, 1999: 148.

Risk değerlendirme, risklerin tanımlandığı, ölçüldüğü ve önceliklendirildiği bir yöntemdir. Risk değerlendirme, makul risk düzeyinin belirlendiği ve risklerden kaçınma, riski paylaşma ve kontrol altına alma eylemlerini yerine getiren bir süreç olan risk yönetiminin önkoşuludur (Allegrini ve D’Onza, 2003: 195).

Risk yönetimi çerçevesi işletme hedeflerinin başarılmasına odaklanmıştır ve bu hedefleri dört kategoriye ayırabiliriz (Arslan, 2008: 28):

1. Strateji: İşletmenin misyonuyla alakalı üst seviye amaçlardır.

2. Faaliyetler: Kaynakların etkili ve verimli kullanılmasıdır.
3. Raporlama: Raporların güvenilirliğinin sağlanmasıdır.
4. Uygunluk: Yürürlükteki yasa ve yönetmeliklerle uyum sağlanmasıdır.

Kurumsal risk yönetimi bu dört hedefin elde edilmesi sürecinde risklerin yönetilmesi için kurumlara yardımcı olurken, faaliyetler kurumun her düzeyinde yürütülmektedir. Bu düzeyler işletme seviyesi, bölüm, şube ve iş birimleri olarak belirlenmiştir (Arslan, 2008: 28).

Kurumların yukarıda belirtilen hedeflerine her kurum düzeyinde ulaşılabilmesi için COSO birbiriyle alakalı sekiz unsur tanımlamıştır (Arslan, 2008: 29-39):

1. *Kontrol ortamı*: Kontrol ortamı, risklerin kurumda çalışan kişiler tarafından nasıl görüntülenmesi ve yönlendirilmesi gerektiğine dair bir temel oluşturur. Kontrol ortamı kurum ile ilgili risk yönetimi felsefesi, risk kapasitesi, dürüstlük etik değerler ve faaliyet gösterilen çevre gibi kavramları içerir. Yetki dağılımı, yönetim biçimi, tanımlanmış rol ve sorumluluklar gibi yönetimle ilgili unsurlar da yine kontrol ortamı içinde yer alır. COSO strateji, faaliyet, raporlama ve uyumla ilgili hedefleri içeren bir planlama süreci anlatır. Kurumsal risk yönetimi programının nasıl tasarlanacağı ve ne kadar etkili yerleştirilebileceği bu kontrol ortama bağlıdır.
2. Hedef belirleme: Yönetim faaliyette bulunurken, ulaşmak istediklerini elde etmesini etkileyecek riskleri tanımlamadan önce, etkilenecek hedefler var olmalıdır. Hedef belirleme sürecinde misyona ve vizyona uyumlu olma ile hedeflerin onlara ulaşmak için karşılaşılabilecek risklerin risk kapasitesi içinde kalmasını sağlayacak seviyede koyulması dikkate alınarak yürütülmesi gerekir. Sonuç olarak hedef belirleme süreci, yönetimin risk stratejisini de göz önünde bulundurarak hedefleri belirlemesidir. Risk yönetimi için hedef belirlemenin iki önemli işlevi vardır:
 - a. İşletmenin risk kapasitesini biçimlendirir: Risk kapasitesi, gerçekleşirse kabul edilebilir ve mazur görülebilir olarak düşünülen riske maruz kalma seviyesini kapsar. Bu bakımdan kapasite, riski sınırlamanın maliyetini (finansal veya başka türlü)

riske maruz kalma gerçekleşirse, maruz kalmanın maliyetiyle kıyaslamakla ve kabul edilebilir bir denge bulmakla ilgilidir.

b. Risk toleransı risk kapasitesi ile uyumlaştırılır: Hedefler etrafındaki değişimlere göre kurumun ne kadar risk üstlenmeyi kabullenebileceği ile ilgilidir.

3. Risk (Olay) tanımlama: Riski etkili bir biçimde yönetebilmek için önce varlığının fark edilmesi gerekmektedir. Risk tanımlama belirsizliklerin risk mi fırsat mı olduğu konusunda ayırım yapmaya imkan verir. Risk tanımlama süreci, kurumun hangi risklerle karşılaşabileceğine odaklanmak için, kurum içindeki farklı perspektife, deneyime ve göreve sahip temsilcileri bir araya getiren işbirlikçi bir yapıya sahip olmalıdır. Risk tanımlama sırasında en çok kullanılan yöntemler; grup çalışması (çalıştay), görüşme, anket ve beyin fırtınasıdır. Risk tanımlama süreci sonunda riskler sınıflandırılmış olur. Uygulamadaki en yaygın sınıflandırmaya göre riskler, stratejik riskler, operasyonel riskler, finansal riskler, itibar riski, bilgi teknolojileri riski, düzenleme riski ve birey temelli riskler olarak sınıflandırılmaktadır (Pehlivanlı, 2010: 76-78).
4. Risk değerlendirme: Riskler tanımlandıktan sonra bunların kurum üzerindeki olası etkilerinin ve meydana gelme olasılıklarının değerlendirilmesi gerekir. Risk değerlemesinin üç önemli ilkesi vardır; her risk için hem etki hem de olma olasılığının açıkça düşünülmesi ki risklerin değerlendirilmesi bu iki perspektiften yapılabilir, risk değerlendirmesinin tesislerin izlenerek ve risk öncelikleri tanımlanarak kaydedilmesi ve risklerin yapısal risk ve artık risk tabanında değerlendirilmesidir. Risk değerlemesi, kurumun potansiyel olayların hedefleri etkileme büyüklüğünü anlamasını sağlar. Risklerin değerlendirilmesi ayrıca alakalı hedeflerin ölçülmesinde kullanılır. Faaliyetin gerçekleşme zamanı ile hedef ufkunu ilişkilendirir.
5. Risk tutumu: Riskler tanımlanıp değerlendirildikten sonra sıra, bu risk yığınının kurumun risk kapasitesi ve risk toleransı içinde olup olmadığının belirlenmesine gelir. Riske verilecek karşılık riskin kurumun üstlenmeye hazır olduğu seviye sınırı içinde olup olmamasına göre

değişir. Riskin yapısına göre verilecek karşılıklar kabul etme, kaçınma, azaltma veya paylaşma, şeklinde sınıflandırılabilir. İşletmeler risklere ne tip karşılık vereceklerine karar verirken karşılık faaliyetinin tahmini fayda-maliyet ilişkisini göz önünde bulundururlar. En uygun karşılığı seçerek riskleri risk kapasitesi sınırları içinde tutmak, yönetimin risk yönetimi uygulama sürecinde alacağı önemli kararlardan biridir.

6. Kontrol faaliyetleri: Risklere verilecek karşılıklar belirlendikten sonra, riskleri minimize etmek için yöntemler geliştirme safhasına geçilir. Kontrol faaliyetleri, riske verilecek karşılıkların etkili bir biçimde yerine getirilmesi, devam eden risklerin risk kapasitesi sınırları içinde yönetilmesi ve kurumun yürürlükteki yasa ve yönetmeliklerle uyumunun sürekli sağlanmasına yardımcı olmak için yerleştirilen politika ve prosedürlerdir. Bunun yanında politika ve prosedürler, diğer kurum talimatlarının da yerine getirilmesini sağlamaya yöneliktir. Tüm kurumda, her seviyede ve tüm fonksiyonlarda geçerlidir.
7. Bilgi ve iletişim: Kişilerin sorumluluklarını yerine getirmesi için ilgili bilgi belli bir biçimde ve belli zaman aralıkları ile tanımlanır, ele geçirilir ve iletilir.
8. İzleme: Gelişimini ölçmek için risk yönetiminin uygulaması izlenir ve etkinliği arttırmak için gerektiğinde ayarlamalar yapılır. İzleme devam eden yönetim faaliyetleri bazında, tek tek olaylar bazında veya her ikisinin karışımı şeklinde yapılabilir.

İşletmenin ulaşmaya çalıştığı hedefler ile onlara ulaşmak için gerekli olanları temsil eden bileşenler arasında doğrudan ilişki vardır. Bir kurumda risk yönetiminin etkin işleyip işlemediğine karar vermek, bu sekiz bileşenin bulunup bulunmadığı, bulunuyor ise etkin işleyip işlemediğinin değerlendirilmesi sonucu ulaşılabilecek bir yargıdır. Dahası bu unsurlar etkili bir risk yönetiminin kriterleridir (Arslan, 2008: 39).

Risk yönetiminin başlıca faydaları şunlardır (Pehlivanlı, 2010: 69):

1. Risk alma istekliliğine bağlı olarak risk stratejilerini oluşturur ve riskli alanlara kaynak tahsisini kolaylaştırır,
2. Risk ve getiri arasındaki ilişkiyi kuvvetlendirir,

3. İşletme yönetiminin risk tutumlarına ilişkin uygun kararlar alması için uygun metotlar ve teknikler sağlar,
4. İşletme amaçlarına ulaşma olasılığını arttırır ve böylece maliyet ve zararları azaltır,
5. Risklerin izlenmesini ve işletmeye etkisinin ölçeklendirilmesini sağlar,
6. İşletme amaçlarına ulaşılabilmesi açısından risk yönetim sisteminin sağlamlığı hakkında güvence sağlar,
7. İç denetçinin risk algılamasını değiştirerek işletmenin amaçlarına ulaşmasını engelleyerek risklere odaklanmasını sağlamaktadır.

Risk yönetimin yukarıda sayılan faydaları sağlayabilmesi sistemin etkin çalışıp çalışmadığı ile ilgilidir. Eğer iç denetim birimi risk yönetimi sürecinde güvence rolü üstlenmişse risk yönetiminin etkinliğinin değerlendirilmesi, alınması gereken düzeltme önlemlerinin önlenmesi ve bundan sonraki sürecin izlenmesinde iç denetim önemli bir rol oynar (Pehlivanlı, 2010: 70).

3.1.2. Risk yönetimi ve iç denetim ilişkisi

İç denetim faaliyetinin bir kurumun risk yönetim sürecinde oynadığı rol, zamanla değişebilir ve hiç rolü olmamaktan, iç denetim planının bir parçası olarak risk yönetimi sürecini denetlemeye, izleme komitelerine, izleme faaliyetlerine ve durum raporlama çalışmalarına katılmak gibi risk yönetim sürecinde faal ve kesintisiz destek ve katılıma, risk yönetim sürecinin yönetimi ve eşgüdümüne kadar uzanan bir aralıkta olabilir (TİDE, 2008: 225).

İç denetim, risklerin değerlendirilmesinde ve yönetim tarafından belirlenen risklere ilişkin kontrollerin ve yöntemlerin geliştirilmesinde önemli bir rol oynamaktadır. İç denetçi, risk süreçlerini ve kontrollerin etkinliğini yeniden değerlendirmek için risk tolerans seviyelerinin belirlenmesi ve izleme faaliyetlerinin devam ettirilmesi konusunda yönetime yardımcı olmalıdır. İç denetim, yönetim sürecine risklerin belirlenmesi, değerlendirilmesi ve yönetimi konularında güvence vermelidir. İç denetçi, risk yönetim süreçlerinin işletmeden işletmeye farklılık göstereceğini bilmelidir. Bu nedenle işletmenin büyüklüğü, iç ve dış çevresi kadar örgüt kültürü, işletme amaçları ve yönetim stili konularında da bilgi sahibi olmalıdır (Coderre, 2009: 99). Ayrıca iç denetim faaliyeti, işletme çapında düzgün risk yönetim süreçlerinin

kurulmasına ve uygulanmasına katkıda bulunan danışmanlık faaliyetlerinde de bulunmaktadır (Özoğlu, vd., 2010: 154).

İç denetçilerin işlerinin olağan akışı içinde önemli risk ve risk maruziyetlerini tespit etmeleri ve değerlendirmeleri beklenir. İç denetim risk yönetimi sürecinde üstlenmemesi gereken görevler de vardır. Bunlar (Pehlivanlı, 2010: 61-62):

1. Risk alma istekliliğinin sınırlarının belirlenmesi,
2. Risk yönetimi süreçlerinin kuruma dayatılması,
3. Riskler hakkında yönetim adına güvence verilmesi,
4. Risk tutumu kararının alınması,
5. Yönetim adına risk tutumlarını uygulama,
6. Risk yönetimi konusunda hesap verme.

İşletmenin risk yönetimi sürecinde rol oynayan bütün kişi ve gruplar arasında faaliyetlerin ve sorumlulukların eşgüdümü gerekir. Bu sorumluluk ve faaliyetler, kurumun stratejik planlarında, denetim komitesi ve yönetim kurulunun politikalarında, yönetmeliklerde, genelgelerde, faaliyet prosedürlerinde ve başka idarî belgelerde de açıkça ifade edilmelidir. Kayıtlara geçirilmesi gereken faaliyet ve sorumluluklara örnek olarak şunları gösterebiliriz (TİDE, 2008: 224-225):

1. Stratejik yönün tayini görevi denetim komitesine, yönetim kuruluna veya bir başka komiteye verilebilir,
2. Risklerin sorumluluğu üst yönetim kademelerine verilebilir,
3. Ek risklerin kabulü sorumluluğu icra kurulu düzeyinde olabilir,
4. Kesintisiz risk tespit, tanımlama, değerlendirme, azaltma ve izleme faaliyetleri, faaliyetler düzeyinde yürütülebilir,
5. Dönemsel değerlendirme ve güvence sağlama görevleri, iç denetim faaliyetine verilmelidir.

İç denetimin risk yönetimi sürecindeki rolünü tespit etmek, üst yönetimin ve denetim komitesinin görevidir. Yönetimin iç denetimin rolü konusundaki görüşü de, muhtemelen, kurumsal kültür, iç denetim personelinin kabiliyeti, ülkenin mahallî koşulları ve gelenekleri gibi etkenler dikkate alınarak belirlenir (TİDE, 2008: 225).

3.2. İç Kontrol Sistemi

İç kontrol sistemi, işletmelerin amaçlarına ulaşmalarını sağlamak için geliştirip uyguladıkları, işletme planları, iş politikaları ve yöntemlerinin bütünüdür. İç kontrol sistemi dinamik bir yapıya sahiptir. Zamanla işletmelerde ortaya çıkan değişiklik ve farklılaşmalar iç kontrol sisteminin etkinliğinin yeniden değerlendirilmesini gündeme getirmiştir. İç kontrol, finansal bilgilerin güvenilirliği, işlemlerin etkinliği, yasa ve yönetmeliklere uygunluk alanlarında sınırlı bir güvence sağlar. Yani, iç kontrol sistemi finansal tablolarda yer alan bilgilerin ve bunlara dayanak oluşturan muhasebe kayıtlarının mutlak surette doğru olduğu anlamına gelmeyeceği gibi, işlemlerin yasa ve yönetmeliklere uygunluğu konusunda eksikliklerin olabileceği olasılığı söz konusudur (Akışık, 2005: 91).

İç kontrol sistemlerinin etkinliğinin sağlanması, işletmelerin amaçlarına ulaşmasında önemli bir rol oynamaktadır. İşletmeler gelişen ekonomik ilişkilerin etkisiyle fiziki olarak büyüdükçe, faaliyetlerin ve meydana gelen değer hareketlerinin sayısı ve karmaşıklığı arttıkça, işletme yönetiminin işletme faaliyetlerini doğrudan doğruya kontrol etme olanağı ortadan kalkmaktadır. İşletme yönetimi açısından bu durum ancak etkin bir iç kontrol sisteminin kurulması ve yürütülmesi ile ortadan kaldırılabilir (Aksoy, 2007: 215).

3.2.1. İç kontrol sisteminin tanımı ve amaçları

Günümüzde dünyada en çok kabul gören iç kontrol modeli COSO tarafından oluşturulmuş olan COSO İç Kontrol Çerçevesidir. COSO İç kontrol Çerçevesine göre iç kontrol sistemi, bir işletmenin yönetim kurulu, üst yönetimi ve çalışanlarından etkilenen ve faaliyetlerin etkinliği ve verimliliğine, finansal raporlamanın güvenilirliğine ve yürürlükteki kanun ve düzenlemelere uyuma ilişkin makul düzeyde güvence sağlayan bir süreçtir. İç kontrol sisteminin özellikleri arasında bir süreç olması, çalışanlar tarafından yürütülmesi, makul bir güvence sağlaması ve amaçların başarılmasına yönelik olması yer alır (Pehlivanlı, 2010: 32).

İç kontrol sisteminin temel amaçları şunlardır (Pehlivanlı, 2010: 31-32):

1. Faaliyetlerin etkinliğini ve verimliliğini sağlamak,
2. İşletme varlıklarının korunmasını sağlamak,
3. Finansal raporlamanın güvenilirliğini sağlamak,

4. İşletme içi ve yasal düzenlemelere uygunluğu sağlamak,
5. İşletme faaliyetlerini kayıt altına almak.

İç kontrolün amaçları doğrultusunda sağlanmak istenen ise çalışanların hesap verebilirliğini sağlamak ve kurumsal iletişimin tüm yollarını açık tutmaktır. İç kontrolün amaçlarına ulaşması için ileri bilgi teknolojilerinden destek alması gerekmektedir (Chorafas, 2009: 4).

İç kontrol sistemi genellikle muhasebe ve yönetim kontrollerinden meydana gelmektedir. Yönetim kontrolleri, yönetim politikasına uyumu özendiren ve faaliyetlerin verimliliğini iyileştirmeyi amaçlayan kontrollerdir. Bu kontroller; güvenilir bilgi sağlanması, işletme varlıkların ve kayıtlarının korunması, verimliliğinin artırılması, belirlenmiş yönetim politikalarına bağlılığı özendirme olarak sıralanabilir. Muhasebe kontrolleri ise varlıkların korunmasını ve finansal kayıtların güvenilirliğini sağlamaya yönelik kontrollerdir. Muhasebe kontrolleri; hilelere karşı varlıkların korunması, finansal kayıtların güvenilirliği ve kıymet hareketleridir (Güredin, 2007: 318-320). Muhasebe kontrolünün temel olarak dört unsuru bulunmaktadır. Bunlar iç kontrol sisteminin ve iç kontrol risklerinin değerlendirilmesi konusunda ön plana çıkmaktadır. (Arens, Elder ve Beasley, 2003: 270, Güredin, 2007: 322):

1. Yönetim sorumluluğu: İç kontrol sistemini kurmak ve devamlılığını sağlamak yönetimin sorumluluğudur. Yönetim, sistemi sürekli gözetim altında bulundurmalıdır.
2. Makul güvence: İç kontrol sistemi kuruluşu sırasında sistemden amaçlara ulaşma konusunda makul seviyede güvence sağlaması beklenir. İç kontrol sistemi, maliyet ve fayda açısından değerlendirmesi yapıldıktan sonra yönetim tarafından oluşturulur.
3. Sistem kısıtları: İç kontrol sisteminin hiçbir zaman tamamen etkili olduğu kabul edilmez, bazı sınırlayıcı faktörlerin etkisi altında kalabilir. Eğer sistem uzmanları tarafından ideal bir sistem kurulmuşsa, bu durumda iç kontrol sistemin etkinliği, bu sistemleri kullanan personelin yeterliliğine ve güvenilirliğine kalmıştır.
4. Bilgi işleme yöntemleri: İşletmedeki bilgi işleme yöntemleri, manuel veya elektronik olabilir. Bilgi işlem yöntemleri ne olursa olsun muhasebe kontrolleri ile gerçekleştirilmesi beklenen amaçlar, tüm bilgi işleme

sistemleri için geçerlidir. Bu sistemler muhasebe kontrolünün kurulmasına ve uygulanacak kontrol yordamlarına etki yapar.

3.2.2. İç kontrol sisteminde yönetimin ve iç denetçinin sorumluluğu

İç kontrol sisteminin kurulup çalıştırılmasına ilişkin sorumluluk işletmenin üst yönetimine aittir. Yönetimin iç kontrol üzerindeki sorumluluğunu şu şekilde sıralayarak özetleyebiliriz (Pehlivanlı, 2010: 40):

1. Kontrol noktası oluşturulması gereken alanları üst yönetim belirler,
2. Kontrol ihtiyacı belirlendikten sonra yönetim tarafından en uygun kontroller belirlenir,
3. Yönetim oluşturulan kontrollerin çalışıp çalışmadığından emin olmalıdır,
4. Kontrollerin oluşturulması kadar bu kontrollerin değişen koşullara uygun hale getirilmesini sağlar.

İç denetçi ise iç kontrol sisteminin uygunluğunu, işleyişini ve etkinliğini araştırmakla sorumludur. İç denetçilerin iç kontrol sistemini gözden geçirmelerindeki amaç, üst yönetim tarafından belirlenmiş yönerge ve kurallara uygun davranıldığının; yönetim kararlarına esas olan çeşitli raporların doğru, zamanlı ve eksiksiz hazırlanarak yönetime sunulduğunun belirlenmesidir (Güredin, 2007:315).

İç denetçiler öncelikle iç kontrol sistemi hakkında bir anlayış geliştirir, daha sonra sisteminin bileşenlerinin birbiriyle ilişkisini ve yönetimin oluşturduğu ve sisteminin yönetimine izin veren kontrollerin yönetimini değerlendirir. İç denetçi süreci incelemeli ve bu sürecin nasıl işlediğini anlamaya çalışmalıdır. Bunun için denetim işinin planlanması ve denetim amaçlarının ortaya konulması gerekir (Moeller ve Witt, 1999: 22-24). İç kontrol sisteminin denetimi işinin planlaması iç denetçi açısından oldukça önemlidir. İç kontrol sisteminin incelenmesi sonucu denetçinin belirleyeceği kontrol riski, çalışmalarının kapsamını, zamanlamasını ve niteliğini etkileyecektir. Denetçi planlama aşamasında finansal tablolara yansıyabilecek önemli hata türleri, bu hataların kontrol riskini etkileme durumu ve maddilik testleri ile ilgili denetim programlarının oluşturulması konularında bazı sonuçlara ulaşmak ister (Bozkurt, 2010: 129-130).

İç denetçiler, iç kontrol sisteminin incelenmesi ve geliştirilmesi konusunda danışmanlık sağlamakla yükümlüdürler. Bu konu Uluslararası iç denetim

standartlarında da belirlenmiştir. Standarda göre iç denetçiler finansal ve faaliyetlerel bilgilerin doğruluğu ve güvenilirliğinin incelenmesi, varlıkların korunmasıyla ilgili kontrollerin incelenmesi ve yasa ve yönetmeliklere uygunlukla ilgili kontrollerin incelenmesinden sorumludurlar (Yılancı, 2006: 37).

3.2.3. İç kontrol sisteminin bileşenleri ve iç denetim ilişkisi

COSO Risk Yönetimi Çerçevesi kapsamında oluşturulmuş bileşenler COSO İç Kontrol Çerçevesi kapsamında belirlenmiş iç kontrol sistemi bileşenleri ile benzerlik göstermektedir. Aradaki farklılık, COSO Risk Yönetimi Çerçevesi risk yönetimi bileşenleri risklerin anlaşılması ve yönetimi için tasarlanmışken, COSO İç kontrol Çerçevesi iç kontrol bileşenleri ise işletme içi kontrollerin anlaşılması ve yönetimi için tasarlanmıştır (Pehlivanlı, 2010: 70). COSO İç Kontrol Çerçevesi kapsamında belirlenmiş iç kontrol sistemi bileşenleri şunlardır (Gönen, 2009: 195-201):

1. *Kontrol Ortamı (Kontrol Çevresi)*: İç kontrolün diğer tüm unsurlarının temelini oluşturan kontrol ortamı; örgütsel davranışlar bütünüün örgütteki insanların kontrol bilineine yansıyışını ifade etmekte olup, söz konusu bu unsur örgütsel disiplini ve örgütsel yapıyı oluşturmaktadır. Kontrol ortamını etkileyen faktörler şunlardır:
 - a. Dürüstlük ve Ahlaki Değerler
 - b. Uzmanlığın Değerlendirilmesi
 - c. Yönetim Kurulu ve Denetim Komitesi
 - d. Yönetim Felsefesi ve Çalışma Tarzı
 - e. Örgütsel Yapı
 - f. Yetki ve Sorumluluk Verme Yöntemleri
 - g. İnsan Kaynakları Politikaları ve Uygulamaları
2. *Risk Değerlemesi*: İşletme üst yönetimi, işletmeyi yakında ve ileride etkileyecek riskleri belirlemek ve bunlara karşı önlemler almak zorundadır. Burada iki tür riskten söz edilmektedir. Bunlardan birincisi işletme riskleridir. Söz konusu riskler, işletmenin yaşamını ve hedeflerini etkilemekte ve dış çevresinden kaynaklanmaktadır. İkinci tür riskler ise, işletme içi risklerdir. Özellikle personelin kasıtlı ve kasıtsız hareketleri ile bilgi ve eğitim düzeyinin eksikliğinden kaynaklanmaktadır.

3. *Kontrol Faaliyetleri*: Kontrol faaliyetleri, yönetimin talimatlarının gerçekleştirilmesini sağlayan politika ve prosedürlerden oluşmaktadır.

Kontrol faaliyetleri aşağıdakilerden oluşur:

- a. Üst Düzey İncelemeler
 - b. Doğrudan Fonksiyonel ve Eylemsel Yönetim
 - c. Bilgi İşleme
 - d. Fiziksel Kontroller
 - e. Performans Göstergeleri
 - f. Görevlerin Ayırımı
4. *Bilgi ve İletişim*: Bilgi sistemleri, bir işletmenin faaliyetlerinin devamını ve kontrolünü sağlayan, faaliyetssel, finansal ve uygunlukla ilgili bilgileri kapsayan raporları üretmekle görevlidir. İç kontrolün etkinliği açısından sadece uygun bilginin üretilmesi yeterli değildir. Bilgi, çalışanların faaliyetlere, finansal raporlamaya yönelik uyum ve sorumluluklarını yerine getirebilmesi açısından uygun personele sağlanmalıdır. Bu bağlamda iletişimin, kişi ve grupların sorumluluklarını ve diğer önemli konuları yerine getirmeyi olanaklı kılacak şekilde geniş bir perspektifte gerçekleşmesi gereklidir.
5. *İzleme*: İşletmenin amaçlarına ulaşmasında çok önemli bir mekanizmasını oluşturan iç kontrol yapısının etkin bir şekilde çalışıp çalışmadığını belirlemeye ilişkin yöntemlerin kullanılması izleme unsurunu ifade etmektedir. İzleme iç kontrolün zaman içindeki performansının kalitesini değerlendirme sürecidir.

Aşağıda iç kontrol sisteminin bileşenlerinin iç denetim ile ilişkisi ele alınacaktır.

3.2.3.1. Kontrol çevresi ve iç denetim ilişkisi

İç denetçi öncelikle yönetimin iç kontrol sisteminin yapısına bakış açısını ve yaklaşımını incelemeye çalışmalıdır. Kontrol çevresi ile iç denetim arasında iki yönlü bir ilişki vardır (Özoğlu, vd., 2010: 250):

1. İç denetçiler farklı alanlarda yaptıkları incelemelerde kontrol çevresini göz önünde bulundurma gerekliliğini dikkate almalıdır. İç denetçiler inceleme yaparken farklı alanlarda yaptıkları incelemelerdeki farklılığı

göz önünde bulundurarak buna uygun test tekniği seçmeli ve uygulamalıdır. İç denetçiler böyle bir yaklaşımda işletme aleyhine gerçekleştirilen hatalı, hileli ve suistimale konu işlemleri algılaması ve bulması halinde en uygun yolu izlemiş olduğu görülecektir.

2. Gerekli nitelikleri taşıyan iç denetim işlevi bir işletmenin kontrol çevresinin güçlü bir tarafı olarak hizmet verir. İç denetim mekanizmasının zayıflaması veya gereken nitelikleri taşınamaması durumunda iç kontrol mekanizmasının kontrolünde veya değerlendirilmesinde yöneticilere yardımcı olamayacaktır.

İç denetçiler işletmede yönetim adına çeşitli faaliyetlerde bulunurlar. Bu çalışmaların arasında en önemli olanı iç kontrol ortamının bir unsuru olarak görev yapmalarıdır. İç denetçiler, yönetim adına işletmede mevcut iç kontrol yapısını sürekli olarak izler ve rapor verirler. İç denetim kontrol ortamının bir parçası olduğundan bağımsız denetçiler iç kontrol yapısını incelerken, işletmedeki iç denetim işlevini de yakın incelemiş olurlar (Bozkurt, 2010: 134).

3.2.3.2. Risk değerlemesi ve iç denetim ilişkisi

İşletmelerde risk değerlendirme, denetçinin finansal tablolarda hata olabileceği ihtimaline yönelik olarak yaptığı doğal ve kontrol risklerini değerlemesinden farklı olarak, işletmenin amaçlarını etkileyen risklerin tanımlanması, analiz edilmesi ve yönetiminden oluşan bir süreçtir. Risklerin değerlemesinde öncelikli olarak bu risklerin hangileriyle karşı karşıya olduğu tespit edilmelidir. Riskler belirlendikten sonra risk analizi sürecinde; riskin öneminin tahmin edilmesi, riskin meydana gelme olasılığının değerlendirilmesi, riskin nasıl yönetileceğinin dikkate alınması ve gerekli düzeltici önlemlerin uygulanması yapılır. Riskler her zaman ortaya çıkabileceğinden değişim yönetimi ile sürekli bir risk değerlendirme modeli oluşturulmalıdır. Bu bağlamda risk değerlendirme süreci adımları; amaçların belirlenmesi, risk tolerans seviyelerinin belirlenmesi, risklerin belirlenmesi, kontrollerin belirlenmesi, kontrollerin değerlendirilmesi, kontrollerin geliştirilmesi ve sürekli gözlem olarak sayılabilir (Uyar, 2009: 36-37).

Risk değerlendirilmesi, yönetimin geleceği yönlendirebilmesi için göz önünde bulundurulması gereken bileşenlerdendir. Bu yönüyle yönetim ileride meydana gelecek

değişiklikleri tahmin etmek suretiyle değerlendirecek ve işletme için uygun değişiklikleri planlayacaktır. İç denetçilerin işletmenin potansiyel riskleri ve önemli gördükleri faaliyet alanlarındaki risklere yoğunlaşmaları risk yönetiminin güçlenmesine etki eder (Özoğlu, vd. , 2010: 525).

3.2.3.3. Kontrol eylemleri ve iç denetim ilişkisi

Kontrol eylemleri, işletme amaçlarına ulaşabilmek için yürütülen faaliyetlerde, veri güvenilirliği için yönetim tarafından oluşturulan çeşitli politika ve prosedürlerdir. Kontrol eylemleri genel kontrollerin, uygulama kontrollerinin, aktifler üzerindeki kontrollerin ve veri güvenliğinin iç denetçilerce gerçekleştirilmesini sağlar. Genel kontroller kontrol eylemlerinin başlangıcıdır ve bunlar etkili çalışmaz ise kontrol eylemlerinde başarılı olunması zorlaşır. Genel kontrollerin oluşturulması uygulama kontrolleri için ortam hazırlamaktadır. Uygulama kontrolleri sayesinde muhasebe birimi tarafından üretilen bilgiler doğrudan iç denetçi tarafından kontrol edilebilecektir. İşletmenin aktiflerini fiziki olarak koruyabilmek amacıyla ise aktifler üzerinde oluşturulmuş kontrollerden faydalanılır. Böylece varlıklara erişim konusunda kısıtlama getirilerek gerekli personeli yetkilendirmek mümkün olmaktadır. Yaratılmış, işlenmiş ve kaydedilmiş verilerin güvenliğini sağlayabilme amacıyla veri güvenliğini sağlayacak kontroller oluşturulmalıdır. Bu kontroller sayesinde sürekli dosyalarda saklanan ve bu verilerin yetkisiz kişilerce değiştirilmesi ve silinmesi engellenir (Bozkurt, 2010: 127-129).

Kontrol eylemleri iç kontrol sürecinin bir parçasıdır. Uygun kontrol eylemleri, belirlenmiş risklere yöneltmek için düzenlenmiş olmalıdır. Eğer riskler belirlenmemiş ise bu alanda kontrol eylemleri de düzenlenmemiş olacaktır. Eğer riskler belirlenmiş ve eylemler bunlara göre planlanmış ise kontrol eylemleri yönetim süreci içerisinde doğrudan yer almış olacaktır (Yılcı, 2006: 70). Kontrol faaliyetleri sayesinde işletmenin amaçlarına ulaşmasını engelleyecek risklere karşı gerekli önlemler alınmış olacaktır.

3.2.3.4. Bilgi-iletişim ve iç denetim ilişkisi

İşletme çalışanlarının sorumluluklarını yerine getirebilmesi için gerekli bilgiler, belirli bir formatta ve zamanında iletişime hazır olmalıdırlar. Bilgi sistemleri sayesinde

üretilen raporlar aracılığıyla işletmelerin faaliyetlerini sürdürmesi ve bu faaliyetlerin kontrolü mümkün olabilmektedir. Fakat bilgi ve iletişim sadece işletme içi olarak düşünülmemelidir. Düzenleyici otoriteler, ortaklar, işletme dışı ilgili taraflar da bu süreçte ihmal edilmemelidir. İşletme dışı taraflarla iletişimde en etkili araç yıllık faaliyet raporları ve kurumsal yönetim raporlarıdır (Pehlivanlı, 2010: 37).

İç denetçiler bilgi, bilgi sistemleri ve iletişimle ilgili işletmenin ihtiyaçlarını mevcut durumla karşılaştırmak suretiyle fiili durumun ihtiyaçları karşılayıp karşılamadığını değerlendirip görüşlerini raporda belirtmelidir (Özoğlu, vd., 2010: 255). İç denetçi bilgi ve iletişim bileşeni açısından gerekli raporların yönetime sağlanması, işletmede çalışan kişilerin sorumluluklarını etkin ve verimli olarak yerine getirebilmeleri için yeterli detayda, zamanında ve doğru kişi için bilgi sağlanması, gerekli bilgi sistemlerinin geliştirilmesi için yönetim desteğinin sağlanması, çalışanların görevleri ve sorumlulukları konusunda bilgilendirilmesi, yanlışlıkları raporlamada uygun iletişim kanallarının oluşturulması gibi konularda iç kontrolü değerlendirmelidir (Yılancı, 2006: 81).

3.2.3.5. İzleme-gözlem ve iç denetim ilişkisi

İzleme temelde iki nedene yöneliktir. Birincisi, iç kontrol sisteminin etkinliğinin izlenmesi ve değerlendirilmesi amacıyla yapılan izlemelerdir. Bu izlemenin yapılma nedeni iç kontrol sisteminin zaman içerisinde değişebilmesidir. İkincisi, yeni gelişmeler değişen koşullar neticesinde işletmede uygulanabilecek yeni kontrol yöntemlerinin tespitine yönelik izlemedir. Bu durumda yönetim yeni risk alanlarını tespit ve buna uygun kontrol sistemindeki prosedürler ve eylemlerde yapabileceği değişiklikleri belirleme ve uygulama ihtiyacı duyar (Yılancı, 2006: 82).

İç denetçiler, mevcut iç kontrol prosedürlerinin uygulanması ve bu prosedürlerin uygunluğunun belirlenmesi için incelemeyi yapacak kişilerdir. İç denetçiler genellikle iç kontrol sisteminin tasarımındaki eksiklikler üzerine odaklanmıştır. Potansiyel zayıflıkları belirleyerek yönetime bildirirler. İç denetçilerin hazırladıkları raporlar kontrol zayıflıklarının belirlenmesinde ve düzeltme eylemlerinin başarılmasında önemli bir rol oynarlar (Özoğlu, vd., 2010: 257).

İzleme eylemleri, iç kontrol sisteminin etkinliği konusunda değerlendirme yapılmasını sağladığından iç denetçilere önemli bilgiler vermektedir. İç kontrol

sisteminin değerlendirilmesi bir süreçtir. Bu değerlendirme süreci iç denetçiler açısından da oldukça önemlidir. COSO iç denetçilere değerlendirme sürecinde “benchmarking” (kıyaslama) yöntemini önermiştir. Benchmarking yöntemini kullanmak işletmenin süreçlerini, kontrol prosedürlerini ve diğer eylemlerini bir diğer eş işletme ile karşılaştırmasıdır. Bu yöntem henüz çok yaygın olarak kullanılmamakla birlikte bunun yerine akış şemaları, soru kağıtları gibi teknikler kullanılmaktadır. Bu konuda geliştirilmiş kantitatif tekniklerde vardır (Yılancı, 2006: 85).

3.3. Kurumsal Yönetim

Kurumsal yönetim işletmenin ilgili tüm hak sahiplerinin çıkarlarının adil bir şekilde gözetilmesini amaçlar. Bu nedenle iç denetim birimi, kurumsal yönetim süreçlerinin işleyişi açısından etkin bir çalışma göstererek iyi bir bu sürecin desteklenmesinde önemli rol oynar (Pehlivanlı, 2010: 101).

3.3.1. Kurumsal yönetimin tanımı ve ilkeleri

Kurumsal yönetim; bir işletmenin tepe yönetiminden tüm çıkar gruplarına uzanan ilişkiler bütününde, tarafların hak ve sorumluluklarını ortaya koyan, karar alma ve uygulama süreçlerinde ilkeleri toplumsal değerlere ve etik kodlara duyarlı biçimde belirleyen, sonuçları tam, zamanında, sorumluluk bilinci içinde, hesap verebilir bir yapıda tüm taraflara şeffaf bir şekilde sunan yapı olarak tanımlanabilir (Daştan, 2010: 5).

Kurumsal yönetim, işletme yönetimi, yönetim kurulu, hissedarlar ve diğer çıkar grupları arasındaki ilişkiler dizisini içerir. Kurumsal yönetim, kurumsal disiplin, şeffaflık, sorumluluk, hesap verebilme, tarafsızlık ve sosyal sorumluluk ile yasa ve düzenlemelere uyumun sağlanması, işletmenin finansal durumu, performansı, sahiplik ve yönetim düzenlemelerine ilişkin zamanda ve doğru bilgilerin açıklanmasını kapsar (Kurnaz ve Çetinoğlu, 2010: 91).

Kurumsal Yönetimin temel olarak dört ilkesi vardır (Daştan, 2010: 9):

1. Eşitlik: İşletme ile ilgisi bulunan ve hak sahibi konumundaki kişi ve kurumların bilgi edinme, kar payı, oy kullanma, genel kurula katılma gibi haklarının adil muamele ile eşitlikçi yaklaşımla ele alınması gereğini ifade eder.

2. Şeffaflık: İşletmenin finansal durumu, performansı, mülkiyet yapısı ve yönetim biçimi gibi her konuda, tam, güvenilir, açık, anlaşılabilir ve yorumlanabilir bilgilere ulaşımın en kısa sürede, kolay ve en düşük maliyetle sağlanması ve bilgilere ilişkin doğru ve zamanında açıklama yapılması gereğini ifade eder.
3. Sorumluluk: İşletme yönetimince alınan kararların ve gerçekleştirilen eylemlerin hukuk kuralları ile toplumsal ve ahlaki değerlere uygunluğunu ve denetlenmesini ifade eder.
4. Hesap verebilirlik: İşletme yönetiminin, kendisine tahsis edilen kaynakların veya verilen yetkilerin kullanım biçimi ve etkinliği ile ilgili hesap verme sorumluluğunu ifade eder.

İyi bir kurumsal yönetimin dinamikleri ve temel unsurları şunlardır (Çetiner ve Erol, 2007: 18):

1. Kurumsal yönetim stratejileri,
2. Faaliyetlerin etkin ve verimli gerçekleştirilmesi,
3. Finansal raporlamada güvenilirlik,
4. Yönetim kurulu ve komiteler (denetim komitesi)
5. Yasal düzenlemeler,
6. Şeffaflık
7. Risk yönetimi ve risk değerlendirme
8. İzleme ve gözetim, iletişim,
9. Kontrol çevresi,
10. Mesleki davranış kuralları,
11. İnsan kaynakları politika ve uygulaması,
12. İç denetim,
13. İç kontrol ve işleyiş eksikliklerinin raporlanması.

İç denetim iyi bir kurumsal yönetimin desteklenmesinde önemli rol oynar. İç denetim risk yönetimi, iç kontrol ve kurumsal yönetim süreçlerinin etkinliğini değerlendirerek ve geliştirerek işletme faaliyetlerinin iyileştirilmesinde yardımcı olabilecek önemli bir konuma sahiptir (Pehlivanlı, 2010: 102). İç denetim biriminin çalışmaları ve sunacakları raporlar, denetim komitesinin ve üst yönetimin önemli bir

veri kaynağı olduğu kabul edilmekte ve bu konularla ilgili sorumlulukların paylaşıldığı görülmektedir (Demirbaş, 2008: 40).

3.3.2. Kurumsal yönetim ve iç denetim ilişkisi

Modern anlamda iç denetim, kurumsal yönetimin temel fonksiyonlarından birini teşkil etmektedir. Başlangıçta bağımsız denetim veya dış denetimden beklenen sosyal sorumluluğun yeterli düzeylerde karşılanamaması ve kurum faaliyetlerinin karmaşık bir yapıya bürünmesi gibi nedenlerden ötürü, hem kurum içerisinden hem de kurum dışındakilerce bir ihtiyaç olarak talep edilen iç denetim, günümüzde kurumsal yönetim süreçlerine katkı sağlaması açısından kuruma değer katan ve kurum faaliyetlerini geliştiren bir yönetsel kontrol aracı haline gelmiştir (Aslan, 2010: 83).

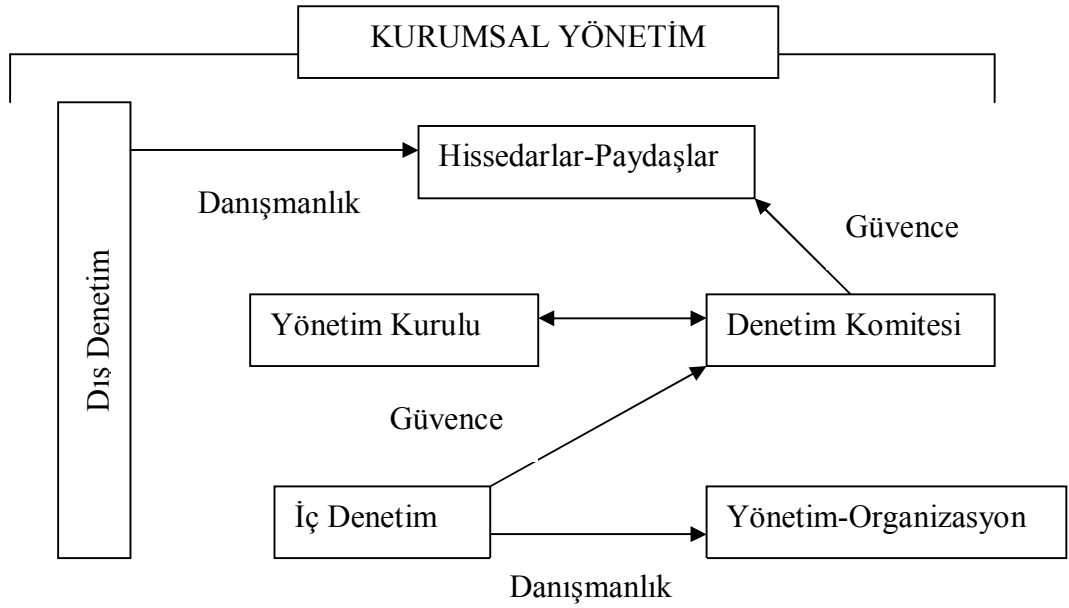
İşletmelerde kurumsal yönetim ilkelerinin yerleşmesi, denetim komitesini ön plana çıkarmıştır. İşletmelerde kurumsal yönetimin profesyonel olarak çalışması için en büyük görev denetim komitesine düşmektedir. Denetim komitesi yönetim kuruluna yardımcı bir organ ve pay sahiplerinin işletme ile ilgili öğrenmek istediği bilgiler konusunda onlara güvence veren kuruldur. Kurumsal yönetim ilkelerine göre halka açık işletmelerin denetim komitesi kurmaları zorunludur. İşletmelerde denetim komitesinin varlığı kurumsal yönetimin etkin şekilde işlemlerini ve iç kontrol ile iç denetim sistemlerinin güçlendirilmesini sağlar. Denetim komitesinin etkin çalışabilmesi ve bağımsız olabilmesi için komuta yerine kurmay hattında çalışması genel kabul görmüş bir yaklaşımdır. Komite bu konumuyla yönetim kurulunu izler, iç denetçilerin çalışmalarıyla birebir ilgilenir ve iç denetimin etkin çalışmasını sağlar. Denetim komitesinin işlevleri; finansal raporlama sürecini izlemek, olası hata ve hilelere, yönetim başarısızlıklarına engel olarak ortakların çıkarlarını korumak, bağımsız dış denetim ve iç denetim çalışmalarını gözlemlemektir (Ergin, Sevim ve Eliuz, 2008: 3).

Denetim komitesi, sorumluluk alanına giren herhangi bir konuyla ilgili incelemeler yapmak ve bu konuda yetki vermekle mükelleftir. Denetim komitesi bu çerçevede; yöneticiler, iç denetçiler, dış denetçiler, hissedarlar ve çalışanlar için büyük bir sorumluluk üstlenmektedir. Bu sorumluluklardan birkaçını şöyle sıralayabiliriz (Gerekan ve Pehlivanlı, 2009: 126):

1. Finansal tabloların, oluşabilecek her türlü hata ve hilelerden arındırılarak gerçeği yansıtacak bir biçimde karar vericilere sunulması,

2. İç kontrol sisteminin etkililiğinin sağlanması ve oluşabilecek her türlü aksaklığın önlenmesi,
3. İç denetim faaliyetlerinin etkili bir şekilde yerine getirilebilmesi amacıyla iç denetçilerle koordineli bir çalışma yürütülmesi,
4. Dış denetim faaliyetlerinin etkili bir şekilde yerine getirilebilmesi amacıyla dış denetçilerle koordineli bir çalışma yürütülmesidir.

İç denetim faaliyeti, işletmenin amaçlarına ulaşabilmesi için uygun kaynakların temin edilip edilmediği, kaynakların etkin, verimli, ekonomik kullanılıp kullanılmadığı, kurumsal faaliyetlerin yürürlükte bulunan kanunlara ve yönetmeliklere uygun yürütülüp yürütülmediği, kurumsal varlıkların korunup korunmadığı, iç kontrol süreçlerinin yeterli olup olmadığı, işletmenin bilgi teknolojileri kapsamında edinmiş olduğu bilgilerin güvenilirliğini ve korunmasının yeterli olup olmadığı, kurumsal yönetim ilkelerini gerçekleştirme konularında denetim komitesine ve yönetime danışmanlık hizmeti sağlar (Özoğlu, vd., 2010: 166). İç denetim, yönetim kurulu ve denetim komitesi arasındaki ilişkileri aşağıdaki şekil yardımıyla da görmek mümkündür.



Şekil-5. Kurumsal Yönetimde İç Denetimin Rolü

Kaynak: Kurnaz ve Çetinoğlu, 2010: 120.

İç denetimin, bağımsız kişilerden oluşan denetim komitesine bağlanması kurumsal yönetimin etkinliğini artıran bir unsurdur. İç denetim faaliyeti, aşağıdaki amaçların gerçekleştirilmesi için kurumsal yönetim anlayışına yönelik gerekli tavsiyelerde bulunur (Abdioğlu, 2008: 191-192):

1. Kurum içerisinde gerekli etik değerlerin oluşturulması ve geliştirilmesi,
2. Etkili bir kurumsal performans yönetimi ve hesap verebilirlik,
3. Risk ve kontrol bilgilerinin kurumun gerekli alanlarına etkili bir şekilde iletilmesi,
4. Yönetim kurulunun, denetim kurulunun, iç ve dış denetçilerin ve üst yönetimin faaliyetleri arasında eşgüdüm sağlamak ve bunlar arasında gerekli bilgilerin etkili bir şekilde iletimini gerçekleştirmek.

İç denetim her türlü düzensizlik ve yasadışı durumu tespit edip bunlarla ilgili yeni kurallar koyar. İç denetim elde ettiği sonuçları ve sonuçlar sonucunda yönetimin aldığı düzeltici eylemleri denetim komitesine raporlar. Böylece denetim komitesi tarafından da iç kontrol sistemi izlenmiş olur ve işletme risklerini engelleme konusunda yeterli bilgiye sahip olan denetim komitesi iç kontrolle ilgili emniyet sağlamış olur (Yılcı, 2003: 27).

İç denetimin finansal raporlama, kurumsal yönetim ve iç kontrolle ilgili sorumluluklarını etkin bir şekilde yerine getirebilmesi denetim komitesi ile bir raporlama ilişkisi gerektirir. Böyle bir ilişki sonucu iç denetim, yönetimin içinde bulunduğu hile, yolsuzluk, düzenlemelere uyumsuzluk gibi durumları bildirmek için denetim komitesine başvurabilir. Denetim komitesi, iç denetimin örgütsel yapısının incelenmesi ve onaylanması, iç denetim bölümü yöneticisinin işe alımı ve değiştirilmesi, iç denetim plan ve bütçelerinin incelenmesi, iç denetim sonuçlarının incelenmesi, iç denetim projeleri için talepte bulunma gibi konularda iç denetim üzerinde de aktif bir gözetim rolü üstlenmektedir (Yılcı, 2003: 29-30).

3.3.3. Kurumsal yönetim bağlamında yıllık faaliyet raporları ve iç denetim ilişkisi

İşletmedeki tüm hak sahiplerinin çıkarlarının adil bir şekilde gözetilmesi kurumsal yönetimin temel amaçları arasında yer almaktadır. Dolayısıyla işletme ortaklarının veya potansiyel yatırımcının işletme faaliyetlerinin performansı hakkında

bilgi edinme ihtiyacı faaliyet raporları ile karşılanmaktadır. Faaliyet raporlarının ve beraberinde kurumsal yönetim uyumluluk raporlarının hazırlanıp yayınlanma amacına hizmet edebilmesi için şu temel bilgileri içermesi gerekir (Pehlivanlı, 2010: 113):

1. İç denetim ve iç kontrol sistemi hakkında bilgi,
2. İç denetim biriminin fonksiyonel raporlama ve bağımsızlık yapısı,
3. Risk yönetimi uygulamaları hakkında bilgi,
4. Denetim Komiteleri, sorumluluk alanları ve toplantı sıklıkları hakkında bilgi.

Faaliyet raporlarında yer alan bilgilerin sorumluluğu üst yönetime aittir. Faaliyet raporlarında yer alan bilgilere ait sorumluluğun yanı sıra bir de bu raporların yayınlanmadan önce denetim süzgecinde geçirilmiş olması gerekir ki böylece, bu raporlarda yayınlanan bilgilere güven artar.

Üçüncü Bölüm

Bilgi Teknolojilerindeki Değişimlerin İç Denetimin İşlevlerindeki ve İç Denetim Sürecindeki Etkileri

1. Bilgi Teknolojilerindeki Değişimlerin İç Denetimin İşlevleri Üzerine Etkileri

İşletmelerde iç denetim; risk ve kontrol değerlendirme faaliyetlerine destek sağlar, işletme faaliyetlerini izler, faaliyetlere ilişkin risk ve kontrol faaliyetleri ile ilgili önerilerde bulunur, kontrollerin uygunluğunu ve etkinliğini test eder. İç Denetim faaliyetinin çok yönlü kapsamı; finansal denetim, uygunluk denetimi, faaliyet denetimi, bilgi teknolojileri denetimi gibi çeşitli denetim faaliyetlerini içerir. Bu işlev ve kapsam özellikleri ile iç denetim; işletmelerde finansal raporlama sisteminin güvenilirliği, yasa ve düzenlemelere uygunluk, faaliyetlerin ekonomikliği, etkinliği ve verimliliği, bilgi sistemlerinin güvenilirliği için vazgeçilmez, olmazsa olmaz faaliyetlerden biri olarak kabul edilmelidir.

Bilgi teknolojilerinde meydana gelen değişimlerin etkisiyle birlikte işletmelerin risk profillerinin değişmesi ve risklere karşı korunma ihtiyacının artması sonucu iç denetimin faaliyet alanları genişlemiştir. İşletmelerin finansal performansları ve risk durumları hakkında bir kanıya varabilmek için bütünleşik ve gerçek zamanlı bilgilere ihtiyaç vardır. Yapılacak raporlamaların sıklığı belirsizlikleri azaltacak ve denetim verilerinin doğruluğunu sağlayacaktır. İç denetim zaman içinde işletmelerdeki mevcut sistemlerin güvenilirliği, iş süreçlerinin iyileştirilmesi ve bu konularda risklerin neler olduğu konularında üst yönetime ve denetim komitesine güvence ve danışmanlık hizmetleri sunmaktadır. İç denetimin üstlenmiş olduğu bu işlevler hem yönetsel kontrol hem de muhasebe kontrolü kapsamındadır.

İç denetçiler teknolojinin hızla ilerlemesi, her örgütsel fonksiyonda bilgi teknolojilerinin kullanılması, yönetim tarafından kullanılan bilginin çeşitliliğinin artması, bilgi sistemleri tarafından işlenen verinin güvenilirliği konusunda şüpheciliğin artması, sistem yönetiminin profesyonel bilgisayar programcılarından son kullanıcıya kadar değişmesi, bilgi teknolojileri kullanımının toplumda geniş bir yer bulması gibi

nedenlerden ötürü bilgi teknolojileri ile ilgili risk ve fırsatları anlamalı ve değerlendirmelidirler (Sawyer, Dittenhofer ve Scheiner 2005: 539).

1.1. Güvence Hizmetlerindeki Değişimler

Bilgi teknolojilerindeki gelişmelerle birlikte artan iş yükünün karşılanabilmesi için yine bilgi teknolojilerinin sağlamış olduğu imkanlardan faydalanmak ve klasik yöntemleri bir kenara bırakmak gerekmektedir.

Günümüzde işletmelerin elektronik ortamda gerçekleşen finansal nitelikli olay ve işlemlerine ait veriler, işlemlerin gerçekleşmesi ile eş zamanlı veya işlemlerin gerçekleşmesinden kısa bir süre sonra işletmenin muhasebe sistemleri tarafından elektronik ortamda tanımlanabilmekte, kayıt edilebilmekte, saklanabilmekte ve bu verilerden oluşturulan ve iç kontrol sisteminin incelemesinden geçen bilgiler, bilginin üretilmesinin ardından internet üzerinden işletmeyle ilgili taraflara sunulabilmektedir. Bilgi teknolojilerindeki gelişmelerle birlikte kısa sürede ve çok çeşitli bilgiler üretebilecek hale gelen muhasebe bilgi sisteminin ürettiği bilgilerin bilgi kullanıcılarına fayda sağlayabilmesi için bu bilgilerin güvenilirliğinin onaylanarak bilgi kullanıcılarına zamanında sunulması gerekmektedir (Alptürk, 2008b: 81).

İç denetçiler, güvence hizmetlerinin kapsamının belirlenmesi ve hangi hizmetlerin kendilerince sağlanacağını belirlenmesi konusunda sorumludurlar. Güvence hizmetlerinin belirlenmesi ile birlikte elde edilen kanıtların kalitesi ve yeterliliği ayrıca düzenlenen raporların kapsamı ve şekli de iç denetçilerin sorumluluğundadır ¹⁹.

Güvence hizmetleri tüm işletme raporlama sistemi açısından bazı avantajlar sağlar. İşletmede alınan kararları etkileyen tüm taraflara bilgi akışının sağlanmasında güvence hizmetlerinin rolü vardır. Alınan kararlardan sorumlu olan yöneticiler bilgilerin güvenilirliği ve kesinliği konusunda güvence hizmetlerine başvururlar. Güvence hizmetini sağlayan biriminin bağımsızlığı ve tarafsızlığı işletmede alınan kararların değerlendirilmesi açısından oldukça önemlidir (Soltani, 2007: 15).

¹⁹ http://www.bic.ac/assets/3-1int_syllabus.pdf (01.09.2011).

1.1.1. Bilgi teknolojileri ile ilgili güvence hizmetleri

Bilgi teknolojileri, hayatımızı kısa sayılabilecek bir sürede yeniden şekillendirmiş olmasına rağmen, bu kaynağı üretim ve tüketimlerinde kullanan birey ve işletmeler için, son derece olağan ve vazgeçilmez bir araç haline gelmiştir. Bilgi teknolojilerinin kullanımı öyle bir düzeye ulaşmıştır ki, bilgi teknolojisi olmadan faaliyetlerini sürdürmek imkansız veya çok zor olan işletmeler ortaya çıkmış, bunlardan bazılarının varlığını sürdürmesi, bizzat teknoloji sayesinde mümkün olmuştur. İşte bu nedenle verimlilik artışında önemli katkı sağlayan bilgi teknolojileri araçları ve bu araçların beklenen düzeyde hizmet üretmesini sağlayan kaynaklar, bazı işletmeler için son derece kıymetli, iyi yönetilmesi ve korunması gereken varlıklar haline gelmiştir.

Güvence hizmetleri denetim işinden daha kapsamlıdır. Güvence hizmetleri, finansal tablolarda gösterilen finansal performans ve koşullara ilişkin bilgileri, etkinlik ve verimlilik hakkında bilgi sağlayan finansal olmayan bilgileri, etkinlik hakkında bilgi sağlayan sistem ve süreçlere ilişkin bilgileri kapsayabilir (Soltani, 2007:14).

Geleceğin güvence hizmetleri kapsamında, yeni mantıksal araçlar kapsamında ortaya çıkan gerçek zamanlı bilgiler finansal tablolardaki tarihi bilgilerden ziyade gerçek zamanlı sistemlerde üretilen bilgilere güvence sağlanması yönünde güvence ihtiyacını değiştirmiştir (Soltani, 2007: 16).

2003 yılından itibaren bilgi teknolojileri ortamında denetime ilişkin olarak Amerika Sertifikalı Mali Müşavirler Birliği (American Institute of Certified Public Accountants-AICPA) tarafından sunulan Webtrust ve Systrust hizmetleri ve bunlara ilişkin standartlar revize edilmiştir. Oluşturulan standartlar doğrultusunda yapılan denetim çalışmaları tamamlandığında olumlu görüşlü rapor ve denetimin çeşidine bağlı olarak Webtrust ve Systrust hizmetleri mührü verilebilmektedir (Kurnaz ve Çetinoğlu, 2010: 256).

Webtrust ve Systrust hizmetlerinin sağladığı güvence hizmetlerine ilişkin beş ilkesi vardır (Kurnaz ve Çetinoğlu, 2010: 256):

1. *Güvenlik*: Sistemin mantıksal ve fiziksel seviyede izinsiz girişimlerden korunmasını sağlar.
2. *Erişilebilirlik*: Sistemin önceden tanımlanmış erişim seviyelerine uygun olarak kullanılmasıdır.

3. *İşlem Bütünlüğü*: Sistemin tam, doğru, zamanında ve kullanıcının verdiği izinlerle uyumlu şekilde çalışmasıdır.
4. *Kişisel Gizlilik (Mahremiyet)*: Elektronik ticaret vasıtasıyla elde edilen kişisel bilgilerin toplanması, kullanılması, açıklanması veya sistem hafızasında tutulması için belirlenen hizmet seviyelerine uygun olarak işlemin gerçekleştirilmesidir.
5. *Gizlilik*: Gizli olarak nitelendirilen bilginin, belirlenen hizmet seviyelerine uygun olarak korunmasıdır.

Güvenlik ilkesini diğer ilkelere ayıran en önemli fark, sistem sahibi işletmenin izni alınmadan gerçekleştirilebilecek ihlallere karşı tüm sistemin üzerinde kontroller kurulmuş olmasıdır. Sisteme girişler kısıtlı tutularak, izinsiz sisteme girme, yanlış yazılım kullanımı, yetkisiz bilgiye erişim, bilgi değiştirme, silme gibi risklerin bir bölümü önlenmektedir. Özellikle elektronik ticaret yapan işletmelerde sistem kullanıcıları bilginin sadece işlemi gerçekleştirecek olanlara iletiğinden emin olmak isterler. Sistemde tutulan kişilere/işletmelere ilişkin bilginin korunmasında ise kişisel gizlilik ilkesi ile ilgili kontroller etkili olmaktadır. Örneğin, elektronik ticaret birçok kaynaktan kişisel/kurumsal bilginin toplanmasına sebep olmaktadır. Yaklaşım farklılıkları dikkate alındığında, kişilerin/işletmelerin ne tür bilgi topladığı, bu bilginin nasıl kullanıldığı veya nasıl kullanılacağı konularında bilgilendirilmesi gerekmektedir. İnternet sayesinde halka açık bilgi ağları vasıtasıyla iletilen bilgilerin kişisel gizliliklerinin ihlali son derece artmıştır. Uygun güvenlik duvarı veya benzeri güvenlik yöntemleri uygulanmazsa özel bilgiler işletme ile bir ilgisi bulunmayan tarafların eline geçebilir. Erişilebilirlik ilkesi ise sistem erişilebilirliğinin faaliyet alanları ve kullanılabilirliğiyle ilgilidir. Erişilebilirlik ilkesi, sistemlerin işlem gerçekleştirebilir olması, izlenebilir olması ve yenilenebilir olması ile ilgilidir. İşlem bütünlüğü ilkesinin varlığı ise, sistem içinde işlem bütünlüğü olmasından ve işlemlerin amaçlarına uygun olarak gerçekleştirilmesinden anlaşılır. Webtrust ve Systrust hizmetlerinin sağladığı güvence hizmetlerine ilişkin ilkeler dikkate alındığında kişisel gizlilik ve işlem bütünlüğü ilkesini içeren bir Webtrust denetimiyle Webtrust tüketici korunma (Consumer Protection Seal) mührü elde edilebilirken, güvenlik, işlem bütünlüğü ve erişilebilirlik ilkelerini içeren bir Systrust denetimine güvenilirlik (System reliability) mührü verilebilmektedir (Kurnaz ve Çetinoğlu, 2010: 257-260).

1.1.1.1. Webtrust hizmetleri

Webtrust denetimleri sistem kontrollerinin hem etkin hem de çalışır durumda olduklarını onaylamaktadır. Webtrust denetimleri internet ortamında sunulan parasal işlem içeren ve elektronik ticaret türü hizmetler sunan sistemlerde yapılmaktadır (Kurnaz ve Çetinoğlu, 2010: 261).

Webtrust, internet vasıtasıyla yapılan işlemler açısından güvence sağlanması amacıyla kullanılmakta ve geliştirilmektedir. Webtrust hizmetlerinin temel özellikleri şunlardır (Rao, Cerpa ve Jamieson, 2001: 523):

1. Daha iyi kontrol sağlama
2. Yasallık ve bütünlük arasında uyum sağlama
3. İşletmeye değer katma ve güvence hizmetleri sunma
4. Bilgi gizliliğini garantileme
5. Sürekli kılavuzluk (danışmanlık) ve iç denetçilere yardım sağlama
6. Daha doğru ve güvenilir değerlendirme yapma

1.1.1.2. Systrust hizmetleri

Systrust denetimleri sistem kontrollerinin sadece etkin olduklarını onaylamaktadır. Systrust denetimler herhangi bir sistemde yapılabilir (Kurnaz ve Çetinoğlu, 2010: 261).

Systrust güvenlik sistemi kurumsal kaynak planlaması sistemi kurulurken işletmeye sistemin bir parçası şeklinde entegre edilir. Denetçi denetim raporunda işletmenin iç kontrol sisteminin güvenilirliğini belirtirken kurumsal kaynak planlaması sistemiyle entegre edilmiş olarak kullanılan Systrust sisteminin ilkeleri ve kriterlerine uyulmak suretiyle bu güvenilirliğe ulaşıldığını görüşünde bildirir (Selimoğlu, 2006b: 287).

1.1.1.3. Diğer bilgi teknolojileri türlerine ilişkin güvence hizmetleri

İç denetçiler tarafından verilecek güvence hizmetlerinin biçimlerinin çoğaltılması mümkündür. Amerikan Yetki Belgeli Kamu Muhasebecileri Enstitüsü Güvence hizmetleri Özel Komitesi (AICPA Special Committee on Assurances Services)

tarafından yapılan çalışmada 200'den fazla güvence hizmeti belirlenmiştir (Arens, Elder ve Beasley, 2003: 7-8). Bunları bir tablo yardımıyla özetlemek mümkündür:

Tablo-3. Diğer Güvence Hizmetleri

Diğer güvence hizmetleri	Hizmet Faaliyetleri
Yatırımlara ilişkin kontroller ve riskler	Riskleri ve süreçlerin etkinliğini belirlemek için işletmenin yatırım uygulamaları ile ilgili süreçleri incelemek.
Dijital bilgilerin biriktirilmesi, dağıtılması ve saklanması	Güvenlik risklerinin ve ilgili kontrollerin değerlendirilmesi
Hile ve yolsuzluk ile ilgili risk değerlendirmesi	Hile riski profillerinin geliştirilmesi ve hile ve yolsuzluğu önleme ve belirleme açısından işletmenin sistemlerinin ve politikalarının yeterliliğinin değerlendirilmesi
Ticari politika ve prosedür arasındaki uyum	Ticaret yapılan taraflarla karşılıklı olarak yapılan anlaşmalara uygun davranılıp davranılmadığının ve bu anlaşmalardaki risklerin incelenmesi.
Kalite sertifikasyonları	Kalite kontrol standartlarına uygunluğun incelenmesi.
Çevre denetimi	İşletmenin politika ve prosedürlerinin çevre standartları ve düzenlemeleri ile uyumunu değerlendirmek.

Kaynak: Arens, Elder ve Beasley, 2003: 8.

1.1.2. Güvence hizmetlerinin yerine getirilmesindeki değişimler

Güvence hizmetlerinin sağlanmasında uygulayıcıların mücadele ettiği çok sayıda sorun ortaya çıkmaktadır. Özellikle son yıllarda bilgi teknolojilerinde ortaya çıkan hızlı gelişmeler sonucu işletmelerde iş uygulamalarının değişmesi ve işletmelerin bu uygulamalara uyum sağlamaya çaba göstermeleri sonucunda ortaya çıkan değişimler güvence hizmetlerinin sağlanmasında bazı sorunların yaşanmasına sebep olabilmektedir.

1.1.2.1. Güvence derecesi

İç denetim faaliyetinin yürütülmesinde güvence derecesinin önemi oldukça önemlidir. Güvence derecesi konusunda standartları da dikkate alarak raporlanan sonuçları desteklemek için toplanan kanıtların yeterli olması gerekmektedir. Finansal tablo denetimi diğer güvence hizmetleri içerisinde güvence düzeyi en düşük denetim

türüdür. Bu durum iç denetim güvence anlaşmalarında da aynıdır (Anderson, 2003: 113).

Kanıt türleri ve güvence derecesi arasında bir ilişki mevcuttur. Bu ilişkiye istinaden SAS 47’de finansal tabloların değerlendirilmesinde finansal tablolardaki verilerin güvenilirliğinin teyid edilmesi açısından güvence derecesi ve kanıtların yeterliliği konusunda temel bir çerçeve sağlanmaktadır. SAS 47 bir süre sonra SAS 68 ile biraz daha genişletilmiş ve son olarak SAS 68’in yerini SAS 74 almıştır (Anderson, 2003: 114).

1.1.2.2. Kanıt türleri ve güvence hizmetleri arasındaki ilişki

Önemli finansal tablo kalemleri için riskleri belirleyen denetçiler yeterli denetim kanıtı toplayabilmek için manuel denetim tekniklerini, bilgisayar destekli denetim tekniklerini veya her ikisini birden kullanabilir. Ancak belirli uygulamalar için bilgisayar kullanılan muhasebe sistemlerinde denetçinin bilgisayar yardımı olmadan denetim kanıtı toplaması söz konusu olamaz. Denetimin elektronik ortamda yapılması ile birlikte elektronik kanıt kavramı da ortaya çıkmıştır.

Denetim süreci içerisinde yer alan veriler elektronikleştikçe iç denetçilerin, bu verilerin geçerliliğini, güvenilirliğini ve eksiksizliğini test etmeleri gerekmektedir. İç denetçilerin, elektronik bilgi içeren gönderi, süreç ve girişleri elektronik kanıtların güvenilirliği ve doğruluğu açısından test etmek zorundadır. Böylece olumlu veya olumsuz denetçi görüşü ortaya çıkacaktır. Basılı belgelerin sayısının azaldığı, işletmelerin elektronik bilgi sistemlerine bağlılığının arttığı böyle bir ortamda denetçiler kaçınılmaz olarak elektronik bilgileri denetçi görüşünün oluşturulmasında daha fazla bir şekilde denetim kanıtı olarak kullanacaklardır.

Elektronik kanıt, elektronik araçlar yardımıyla bilginin iletimi, kullanılması, devam ettirilmesi, saklanması ve denetçinin yayımlanan finansal tabloların değerlendirilmesinde kullanılır. Elektronik kanıtın oluşturulma amacı geleneksel kanıtın oluşturulma amacı ile aynıdır. Ancak, elektronik kanıtta, kanıtın geçerliliği, eksiksizliği ve güvenilirliği ile ilgili soruların cevaplanmasında, geleneksel kanıt için gerekenden daha fazla kontrole gereksinim duyulur. Elektronik veri süreci sistemlerindeki elektronik kanıtların, mutlaka her sistemdeki geleneksel kanıtlarla yer değiştirmesi gerekmemektedir. Bilgi teknolojisi, elektronik kanıtın kaynağı veya basit bir ifadeyle

geleneksel kanıtların deposu olacaktır. İç denetçilerin, elektronik kanıtla ilgili olarak, firmanın yeterliliği, sunuşları ve belirli elektronik veri süreci denetim faktörlerini tanınması gerekmektedir. Elektronik kanıtın güvenilirliği, önemli oranda iç kontrol yapısının etkinliğine bağlıdır. Elektronik kanıt açık değildir ve denetçilerin, kullandıkları süreçlere göre, değerlendirmelerinin farklı olmasına neden olabilir (Toraman, 2002; Selvi, Türel ve Şenyiğit, 2006: 305).

Tablo-4. Elektronik Bilginin Denetim Kanıtı Olarak Güvenilirliğinin Belirlenmesi

Doğrulama	Bilgiyi üreten kurum ve kişinin kimliğinin tanımlanması
Bütünlük	Bilginin gerçekliği, cari niteliği, doğruluğu, tamlığı. Bütünlük geçerliliğinin sağlandığına; yani bilginin hazırlanma, işleme, iletilme, alınma süreçlerinde kasten veya tesadüfen değiştirilmediğine ilişkin güvenceyi ifade eder.
Yetki	Yetkili veya sorumlu kişilerce bilginin hazırlanması, işlenmesi, iletilmesi, düzeltilmesi, gönderilmesi, alınması.
Reddetmeme	Bilginin hazırlanması, iletilmesi, alınması süreçleri içerisinde ilgili tarafların bilgi içeriğini reddetmemesi, işlemin taraflarca kabulü .

Kaynak: Şirin, 2006: 33.

Finansal tablo kullanıcıları artık geçmişe dönük bilgi yerine gerçek zamanlı bilgiyi daha fazla talep etmektedirler. Mevcut durum itibari ile denetim talebindeki bu değişikliğin yavaş yavaş (sürekli denetim gibi) denetim uygulamalarında da yer almaya başladığını görmekteyiz. Bütün bunlar gelişen bilgi teknolojilerinin işletmelerin üretim ve ticari uygulamalarını değiştirmesinin bir sonucudur. Amerikan Yeminli Muhasebeciler Enstitüsü (AICPA) geleneksel denetim kanıtları ile elektronik denetim kanıtları arasındaki farklılıktan doğan sorun alanlarını şöyle özetlemiştir (Şirin, 2006: 29-30):

1. Elektronik bilgilerin yeterli denetim kanıtı olarak kabulü,
2. Elektronik kanıtların sunumunun farklı formatlarda mümkün olması,
3. Elektronik denetim kanıtlarına ulaşabilmek için yeterli denetim araçlarının varlığı,

4. Elektronik denetim kanıtlarına ulaşımın zorluğu,
5. Bilgi sistemleri kontrol performansının değerlendirilmesinin zorluğu,
6. Hataların tanımlanması (Denetçinin hataları tespit edememe riskinin artması).

Bazı işletmelerde muhasebe kayıtları ve destekleyici bilgiler sadece elektronik formda olabilmektedir. Satın alma emirleri, konşimentolar, faturalar ve çekler gibi kaynak belgeler, elektronik biçimlere dönüşmektedir. Günümüzde artık işletmeler müşteri ve satıcılar ile işlerini iletişim hatlarını kullanarak elektronik ortamda gerçekleştirmekte ve birçok işletme elektronik veri değişim teknolojilerini kullanmaktadır. Ayrıca görüntü işleme sistemleriyle kaynak belgeler taranarak, saklamak ve gereğinde başvurmak üzere elektronik görüntülere dönüştürülmektedir. Bazı elektronik kanıtlar belli bir süre için mevcut olabilmekte ve eğer kütükler değiştirilmişse ve yedek kütükler yoksa geri alınmaları güçleşmektedir. Bu nedenle denetçi, bilginin elde edilebilir olduğu zamanı, maddi doğrulama testlerinin yapısı, zamanlaması ve kapsamının belirlenmesi bakımından uygunluğunu dikkate almalıdır (Erdoğan, 2004: 44).

Elektronik kanıtlar belli bir süre korunabilir fakat belirli bir süre geçtikten sonra bu kanıtlar değiştirilebiliyorsa veya yedekleme dosyaları yoksa bu kanıtlara erişim güçleşebilir. Bu açıdan maddi doğruluk testlerinin yapısını, zamanlamasını ve kapsamını belirlemek için kanıtların ne zaman erişilebilir olduğunu dikkate almak gerekir (Alptürk, 2008b: 229).

1.1.2.3. Hile araştırmalarında güvencenin yapısı

Denetçi, finansal tablolarda hilenin veya hatanın neden olduğu yanıltıcı beyanların bulunup bulunmadığı hakkında güvence elde etmek için denetimi planlamak ve yerine getirmekten sorumludur. Denetim kanıtlarının yapısı ve hilenin özellikleri itibariyle denetçi önemli yanlışlıkları belirlemenin mutlak bir güvencesinin olmadığını bilir (Kurnaz ve Çetinoğlu, 2010: 70).

Hilelere karşı yetkili bir iç denetim işlevi oluşturmak ve sürdürmek, İç Denetçiler Enstitüsü'nün tavsiyeleri arasında yer almaktadır. İşletmeler kurumsal yapılarını korumak ve kendilerine yapılan yatırımları geliştirmek istiyorlarsa, olası riskleri belirlemeli ve oluşturulan kontrolleri izlemelidirler. Böyle bir sorumluluğun

yerine getirilmesinde etkili bir iç denetim işlevi önemli bir rol oynamaktadır (Kurnaz ve Çetinoğlu, 2010: 70).

Hile araştırmaları uzun bir zamandır iç denetim işlevi tarafından sağlanan hizmetin bir parçası olmuştur.

1.2. Danışmanlık Hizmetlerindeki Değişimler

Bilgi teknolojilerinin yaratmış olduğu değişimler işletmelerde hemen hemen her süreçte kendini göstermiş olmakla birlikte risk yönetimi, sistem güvenliği, elektronik ticaret ve performans ölçümü konularında iç denetçilerin verdiği danışmanlık hizmetleri dikkat çekmektedir.

1.2.1. Bilgi teknolojilerinin danışmanlık hizmet alanlarına etkisi

Bilgi teknolojilerindeki gelişmeler işletmelerin risk profillerini değiştirmiştir ve işletmelerde riskin anlamını ve önemini anlamak ve açıklamak, farklı türlerdeki riskleri açıklamak, bu riskleri analiz etme yollarını göstermek gibi konularda iç denetçilerin ve iç denetim birimi çalışanlarının kılavuzluğuna ihtiyaç duyulmuştur.

Günümüzde risk yönetimi iç denetim biriminin danışmanlık verdiği alanların başında gelmektedir. Risk yönetimi sürecinin işleyişi ile ilgili sorumluluklar üst yönetimde olmakla birlikte yönetimin risklere karşı oluşturduğu çözüm yollarını değerlendirmek, risk değerlendirme yöntemlerinin niteliksel ve niceliksel avantaj ve dezavantajlarını bildirmek, yönetimin risk değerlendirmesi ile denetçilerin risk değerlendirmesini karşılaştırmak iç denetim birimince sunulan danışmanlık hizmetleri kapsamındadır²⁰.

İşletmelerde performans ölçümü üzerinde güvence sağlamanın faydalarının belirlenmesi de iç denetim biriminin sağladığı danışmanlık hizmetleri arasında yerini almıştır. Bilgi sistemlerinin performans güvenilirliğinin nasıl değerlendirileceğinin belirleme konusunda da iç denetim biriminin çalışma sonuçları yönetime kılavuzluk sağlamaktadır. Bilgi teknolojilerinin gelişimi ve işletmelerde her süreçte yer almaları nedeniyle bu teknolojilerin performanslarının değerlendirilmesi son derece önemli bir çalışmadır. Ayrıca bilgi güvenliği ve kontroller açısından ihtiyacın belirlenmesi,

²⁰ http://www.bic.ac/assets/3-1int_syllabus.pdf (01.09.2011).

güvenilir ve tam zamanlı raporlama ihtiyacının belirlenmesi ve yönetime sağlanacak güvencenin faydasının belirlenmesi, iç kontrolün etkinliğinin değerlendirilmesindeki prosedürlerin yönetime anlatılması da sistem güvenliği konusunda iç denetim biriminin sağladığı danışmanlık hizmetinin kapsamı içinde yer almaktadır²¹. Yalnız yönetim iç kontrollerin kendi sorumlulukları altında olduğunu ve iç kontrolleri oluşturmaları gerektiğini bilmelidir (Rao, vd. 2001: 527).

E-ticaret konusunda da bilgi teknolojilerinin yaygın kullanımı iç denetime bu alanda da danışmanlık rolü yüklemiştir. E-ticaret sırasında çeşitli bilgi teknolojilerini kullanan işletmelere yol göstermek, e-ticaretin işletme risklerini nasıl etkilediğini üst yönetime bildirmek, işlem ve iletişim açısından bilginin gizliliğini ve güvenilirliğini sağlamak ve bu konularda üst yönetime bildirimde bulunmak ve web güvencesi ile ilgili ilkeleri ve kriterleri açıklamak gibi konularda iç denetim birimlerinde danışmanlık hizmeti alınabilmektedir²².

Elektronik ortamda işlemlerini yürüten işletmeler, bu işlemlerin geliştirilmesi için iletilen verinin bütünlüğü ve güvenliği hakkında endişelere sahip olabilirler. Danışmanlık hizmetleri risklerin belirlenmesi ve elektronik işlemleri ve elektronik dokümanları destekleyen sistemlerin bütünlüğünün ve güvenliğinin sağlanmasına yardımcı olur. Bu hizmetler sırasında WebTrust gibi hizmetler de işletme politikaları ve internet aracılığıyla gerçekleşen diğer işlemleri açısından güvence sağlanmasında yardımcı olur.

1.2.2. Danışmanlık hizmetlerinin yerine getirilmesindeki değişimler

Danışmanlık hizmeti, bir durum hakkında mesleki yargıda bulunabilmek için mesleki yeterliliğe sahip olmayı gerektirir. Danışmanlık hizmetleri, iç denetim işlevinin son zamanlarda gösterdiği gelişmelerden ötürü dikkate alınması ve önemli araştırmaların gerçekleştirilmesini gerektiren bir işlevi haline gelmiştir.

1.2.2.1. Güvence ve danışmanlık hizmetlerinin dengelenmesi

Son 20 yılda iç denetim, risk değerlendirme ve riskleri en aza indirme konularında denetim kaynaklarının tahsis yeteneği konusunda önemli gelişmeler

²¹ http://www.bic.ac/assets/3-1int_syllabus.pdf (01.09.2011).

²² http://www.bic.ac/assets/3-1int_syllabus.pdf (01.09.2011).

kaydetmiştir. Ancak risk değerlendirme mekanizmaları sadece güvence hizmetlerine ayrılmış kaynaklar üzerinde sistematik tahsisi sağlamaktadır; bu mekanizmalar denetim fonksiyonunun işletmeye kattığı değeri arttırmak için güvence ve danışmanlık hizmetleri arasında kaynakların nasıl dağıtılacağına yönelik değildir. Bu konuda sistematik bir mekanizma oluşturulmazsa iç denetim birimi yöneticileri kaynak dağıtım problemleri ile karşı karşıya kalacaktır (Anderson, 2003: 120).

1.2.2.2. Danışmanlık hizmetlerinin beraberinde getirdiği riskler ve ödülleri

Danışmanlık hizmetinin beraberinde getirdiği riskler arasında iç denetçinin tarafsızlığını kaybetmesi, danışmanlık projesinin başarısızlığa uğraması sonucu danışmanlık işlevinin itibarına zarar gelmesi, güvence sorumluluğunun yerine getirilmemesi, maliyet ve zaman aşımı (süre kısıtları) sayılabilir. Danışmanlık hizmetlerinin sağladığı ödüller arasında işletmeye değer katma, üretim yönetimleriyle iç denetim birimi ilişkilerinin ilerlemesi, personelin gelişimini ve kariyer fırsatlarını değerlendirmesini sağlama sayılabilir (Anderson, 2003: 122).

2. Bilgi Teknolojilerindeki Değişimlerin İç Denetim Sürecindeki Etkileri

Bilgi teknolojilerindeki gelişmeler ve web tabanlı denetim programları sayesinde iç denetçiler işletmeleri ile ilgili iş ve sektör bilgilerini ilişkilendirerek potansiyel risklerin nerede olduğunu ve bu riskleri yönetmek için hangi kontrol yöntemlerinin gerektiğini belirlemektedirler. Artık iç denetçiler eskiden olduğu gibi finansal tabloları geçmişe dönük olarak incelemek yerine, muhasebe bilgi sistemlerinin güvenilirliğini ve doğruluğunu, iç kontrollerin uygunluğunu ve etkinliğini sürekli olarak denetleyebilmektedirler.

Bilgi teknolojileri ortamında tüm iç kontroller manuel olarak değil, elektronik ortamda gerçekleştirilmektedir. Bu durumda denetçinin muhasebe, üretim, finans, satın alma gibi fonksiyonları bütünleşik olarak ele alan kurumsal kaynak planlaması sistemleri, bir bilgisayar sisteminden diğerine elektronik olarak sipariş veren veya ödeme emri gerçekleştiren elektronik veri değişimi gibi teknolojiler üzerinde kontrol testi yapması gerekmektedir (Selimoğlu, 2006b: 152).

2.1. Sürekli Denetim Sürecindeki Etkiler

Bilgi teknolojilerindeki gelişmeler, işletmelerin denetimlerindeki anlayışını değiştirmiştir. Böyle bir değişim sonucu ortaya çıkan sürekli denetim kavramının yeni bir Enron vakasını engelleyip engellemeyeceği önemli bir tartışma konusu olmuştur. Belirli zamanlarda geçmişe dönük gerçekleştirilen denetim, sürekli denetime olanak sağlayan bilgi teknolojileri ile süreklilik temeline oturtulmuştur. Günümüz bilgi teknolojileri, kurumsal veri tabanlarına dışarıdan girişe izin verebilmekte ve kurumsal bilgiler ve muhasebe bilgi sistemi gerçek zamanlı olarak analiz edilebilmektedir. Ancak böyle bir durum bilginin güvenliği konusunda soru işaretleri oluşmuştur. Yakın bir gelecekte işletmelerden daha da hızlı raporlama yapmaları istenecektir. Hızlı bir şekilde sağlanacak olan bu bilginin denetimden geçmiş olması, bilginin güvenilirliği konusundaki soru işaretlerinin ortadan kalkmasına ve bilgi güvenliğinin artmasına yardımcı olacaktır (Kurnaz ve Çetinoğlu, 2010: 183). Dolayısıyla finansal tablolarda yer alan bilgilerin doğruluğu garanti altına alınmış olacak ve işletme ile ilgili taraflar doğru bilgiye ulaşabileceklerdir.

Sürekli denetim, tam otomatik bir süreçte ve olayların sonuçlarına anında erişim sağlandığında iyi sonuçlar verir. Bu sonuçların elde edilmesi için sürekli denetimi çevrim içi bir bilgisayar sisteminde uygulamak gerekir. Sürekli denetim, elektronik ortamlarda güvence hizmetlerinin yerine getirilmesinde önemli bir rol oynamaktadır. Bilgi talep edenler, sunulan bilginin doğruluğu, güvenilirliği ve zamanlılığı konusundaki beklentilerini sürekli denetim ve güvence hizmetleri ile temin etmeye çalışmaktadır.

Sürekli denetim, ilgili bilginin ortaya çıkarılmasını hızlı bir şekilde gerçekleştirir. Denetçi raporları, kısa aralıklarla veya anında yayınlanır. Sürekli denetim geleneksel denetimin aksine, karar almaya uygun bilginin herhangi bir niteliğine odaklanabilir. Bu bilginin niteliği; güvenilirlik, doğruluk, ulaşılabilirlik ve kontrollerin etkiliği kapsamında olabilir (Kurnaz ve Çetinoğlu, 2010: 158).

Geleneksel denetimde bilgisayar yazılımları ve donanımları kullanılsa da insan faktörü ön plandadır. Sürekli denetimde ise bilgi teknolojileri ön plana çıkarak, insan faktörünü geri planda bırakmıştır. Çünkü sürekli denetimin odak noktasını elektronik ortamlarda ortaya çıkan veriler ve denetim kanıtları oluşturmaktadır. Sürekli denetimde

denetim verilerinin ve kanıtlarının elde edilmesi, muhasebe bilgi sistemi ve iç kontrol sisteminin değerlendirilmesi, denetim risklerinin belirlenmesi gibi işlemler bilgi teknolojileri tarafından gerçekleştirilmektedir. Sürekli denetim sürecinde, denetimin esas konusu olan olay gerçekleştiği anda veya bu olayın kısa bir süre sonrasında güvence hizmetini gerçekleştirmek bilgi teknolojileri sayesinde mümkün olmaktadır (Selimoğlu, 2006b: 285; Kurnaz ve Çetinoğlu, 2010: 159).

Sürekli denetimde denetçi kontrol testlerini, analitik prosedürleri ve işlem testlerini aynı anda gerçekleştirebilmekte ve işletmenin bilgi teknolojilerinin güvenilir ve doğru finansal bilgiler üretip üretmediği konusunda kanıtlara ulaşabilmektedir. Sürekli denetim araç ve teknikleri, işlemler ile ilgili testlerin yıl içinde sürekli bir şekilde gerçekleştirilmesine imkan sağlamaktadır (Kurnaz ve Çetinoğlu, 2010: 161).

Bilgi teknolojileri geliştikçe ileri bilgi sistemleri daha az maliyetli hale gelmiştir. Bu durum zamanla bilgi sağlayabilmek için bilgi teknolojilerine bağımlı hale gelmeyi kolaylaştırmıştır. Üst yönetimin gerçek zamanlı, eksiksiz ve doğru bilgi ihtiyacı, bilgi teknolojilerinin tasarımına ve güvenilirliğine odaklanılmasını önemli hale getirmiştir. Bilginin ilgili ve güvenilir olduğu konusundaki güvence hizmetine talebin artması sonucunda iç denetçiler açısından sürekli denetim yaklaşımının benimsenmesi gerekli olmuştur. Sürekli denetim, iç denetimin güvence hizmetlerinin tüm yönlerini desteklemektedir (Kurnaz ve Çetinoğlu, 2010: 162).

2.1.1. Sürekli denetimin uygulama sürecindeki etkiler

Sürekli denetim, denetçiler tarafından denetimle ilişkili faaliyetleri sürekli olarak gerçekleştirmek için kullanılan bir metoddur. Faaliyetler sürekli kontrol değerlendirmeden sürekli risk değerlendirmeye kadar geniş bir yelpazeyi kapsamaktadır. Bilgi teknolojileri ise otomasyon vasıtasıyla sürekli denetimi makul bir seçenek haline getirmede önemli bir rol oynamaktadır (The Institute of Internal Auditors, 2005: 2).

Sürekli denetim, işletmelerin finansal bilgilerinin güvenilirliğini ve bütünlüğünü korumak ve yatırımcıların finansal piyasalara olan güvenini arttırmak için işletmelerin raporlama ihtiyaçlarının karşılanmasında en iyi alternatif olarak gözükmektedir. Sürekli denetimin amaçlandığı gibi gerçekleştirilebilmesi için işletmelerde denetim ihtiyacının belirlenmesi, yönetimin desteğinin alınması, sürekli denetimde ele alınacak alanların ve

denetimin kapsamının belirlenmesi, temel iş süreçlerinin ve uygulama sistemlerinin belgelerden elde edilme şeklinin belirlenmesi ve önemli kontrol ve risklerin belirlenmesi gerekmektedir (Kurnaz ve Çetinoğlu, 2010: 288).

İşletmelerin daha güvenilir, gerçek zamanlı ve kaliteli finansal bilgileri üretmeye yönelmeleri sürekli denetimin uygulanmasıyla birlikte **sürekli raporlama, sürekli izleme** ve **sürekli güvence** gibi uygulamaları da ortaya çıkarmıştır.

Sürekli raporlama, denetim olmaksızın veya düzenli bir denetim ortamında bilginin internette yayınlanmasını ve bu bilgiye ulaşmanın kolaylaşmasını sağlamaktadır (Kurnaz ve Çetinoğlu, 2010: 168). Sürekli raporlama ve sürekli denetim, işletme içi kontroller ve yönetim konusunda işletmenin iç ihtiyaçlarına cevap verecek şekilde kurulmalı ve iç denetimde ihtiyaç duyulan geri bildirimler anında ve kapsamlı bir şekilde ulaşmalıdır. Sürekli raporlama ve sürekli denetim sistemi kurulurken yasal düzenlemeler, muhasebe ve denetim standartları dikkate alınmalı, doğru, güvenilir ve kaliteli bilgiler üreten bir sistem kurulmalıdır. İşletmelerin küreselleşmeden etkilenerek kurumsal kaynak planlaması (ERP), bilgisayar destekli denetim teknikleri (BDDT) ve genişletilebilir işletme raporlama dili (XBRL) gibi teknolojileri ve bu teknolojileri içinde barındıran sistemleri kullanmaya başlamasıyla birlikte sürekli denetim ve sürekli raporlama sistemi de bu uygulamalar içinde yer almıştır (Selimoğlu, 2006b: 149-150). Bilgi teknolojilerinin bilgi üretiminde çok hızlı olması, istenilen her bilgiyi üretmesi ve gerçek zamanlı bilgi akışı sağlaması sürekli denetim ve raporlama sisteminin de bu duruma uygun yapılanmasına neden olmuştur (Murthy ve Groomer, 2004: 140).

Sürekli güvence, iç denetim tarafından iç kontrolleri ve risk yönetimi sürecini bağımsız olarak değerlendirmek ve işletme yönetiminin kontrolleri gözlemleme faaliyetlerini değerlendirmek için uygulanan faaliyetlerin kombinasyonudur (The Institute of Internal Auditors, 2005: 2).

Sürekli izleme, işletmedeki veri türlerinin, bilgi sistemlerinin, işlem süreçlerinin tümünün veya bunlardan herhangi birinin performansını ölçülmesi ve bu aşamalarda iç denetçi ve üst yönetim kademesinin birlikte çalışmasıdır (Kurnaz ve Çetinoğlu, 2010: 173). Kontrollerin sürekli izlenmesi, yönetimin uygulamaya koyduğu politika ve prosedürlerin uygunluğunu ve işletme süreçlerinin etkin bir şekilde gerçekleştiğini garantilemeye yönelik bir süreçtir. Sürekli izleme genellikle tüm işlemlerin otomatik olarak sürekli test edilmesini içerir (The Institute of Internal Auditors, 2005: 2).

Sürekli denetim, bir denetim çalışmasıdır ve sürekli güvence sürecinin bir parçasını oluşturur. Sürekli izleme ise, bir yönetim çalışmasıdır (Kurnaz ve Çetinoğlu, 2010: 176). Sürekli denetim, kontrol ve sürekli izleme çalışmalarından bağımsız olmalıdır. Sürekli izleme ve sürekli denetim bir arada yapıldığında sürekli güvence sağlanabilir (Nastase ve Nastase, 2007: 47).

Sürekli denetim alanına geçişte ve sürekli izleme sürecinde teknolojinin rolü büyüktür. Teknolojiyi içeren geleneksel yöntemler sürekli denetim ve izleme teknolojileri tarafından değiştirilecek ve tanımlanacaktır. Sürekli izleme sistemleri yönetim bilgi sistemlerine benzer. Sürekli izleme, kontrollerin etkili ve yeterli bir şekilde ortaya çıkarılması yoluyla yönetimin sorumluluklarını yerine getirmesini sağlar. Sürekli izleme, bir iş süreci içerisindeki kontrol noktalarının belirlenmesini, her bir kontrol noktası için güvenlik durumlarının ve kontrol amaçlarının belirlenmesini, otomatikleşmiş bir seri test sisteminin kurulmasını, doğru işlemin belirlenmesini ve kontrol zayıflıklarının belirlenmesini kapsar. Sürekli izlemenin en önemli noktası, etkili kontrol sistemlerinin çalıştırılması ve uygulanmasıdır. Bu noktalar yönetimin sorumluluğunda olan ve yönetim tarafından gerçekleştirilmesi gereken süreçlerdir (Kurnaz ve Çetinoğlu, 2010: 173-174).

Sürekli denetim ve sürekli izleme, işletmenin üst yönetiminin sorumluluğunda olmalıdır. Risk yönetimi uygulamaları, sürekli denetim ya da sürekli izleme uygulamalarında üst yönetimin yer aldığını göstermektedir. Ayrıca iç denetçiler de üst yönetimin aktif olarak sürekli denetim ve sürekli izleme uygulamalarında yer aldığını garantilemektedir (Kurnaz ve Çetinoğlu, 2010: 175).

2.1.1.1. Sürekli denetim yeteneğinin oluşturulması

Sürekli denetim içindeki otomasyon düzeyi, denetim sistemi tasarımı ve uygulamasına göre değişiklik göstermektedir. Yüksek düzeyde otomasyona sahip süreçler nedeniyle sürekli olarak izleme ve raporlama sağlayan sistemler içinde denetim programları da yer alabilmektedir. Düşük seviyedeki otomasyona sahip süreçlerde ise veri otomatik olarak yakalanır, değiştirilir ve yüklenir. Burada iç denetçiye düşen görev, olağan dışı durumların algılanması ve gereken sorgulamanın yapılmasıdır (Kurnaz ve Çetinoğlu, 2010: 197-198).

Sürekli denetim, denetim konusuna giren işlemlere ilişkin anında veya işlemler gerçekleştikten hemen sonra yazılı bir güvence verilmesini sağlar. Sürekli denetim, bilginin ortaya çıkmasıyla denetçi tarafından bu sürekli bilgiye ilişkin güvence verilmesini sağlar (Erkuş, 2008: 130).

Bazı şirketlerin sebep olduğu finansal krizler kurumsal yönetim ve kurumsal raporlama üzerine odaklanılmasını sağlamıştır. Bu durumda sadece finansal tabloların doğruluğu sorgulanmamakta, aynı zamanda bilgi teknolojisi sistemlerinin gizliliği ve güvenilirliği ile ilgili kaygılar da söz konusu olmaktadır (Kurnaz ve Çetinoğlu, 2010: 179).

2.1.1.2. Sürekli denetim uygulamasının planlanması

Sürekli denetimde diğer denetim çeşitlerine oranla etkili bir denetim planı oluşturmak oldukça önemlidir. Denetim planının oluşturulması sırasında veri ve mevcut bilginin geçerliliğinin mutlaka dikkate alınması gerekmektedir. Denetimin planlanmasından sonra sürekli denetim teknikleri uygulanmaya başlandığında iç denetçinin karşılaştığı en önemli sorun denetim yazılımlarının nasıl uygulanacağı konusunda verilecek kararlardır. Yanlış başlangıçları, gereksiz teknoloji ve yazılım maliyetlerini azaltmak için bir teknoloji kullanım planına da ihtiyaç duyulacaktır. Günümüzde iç denetçilerin ACL ve IDEA ya da herhangi bir denetim bağlantılı veri analiz araçlarına ve bu araçların kullanımı ile ilgili bilgiye sahip olmaları gerekmektedir. Denetim planlamasında kullanılacak bilgi teknolojisi araçlarının seçilmesi seçeneği için belirli amaçları geliştirme geçerli bir ihtiyacın fayda-maliyet analizine dayanır. Sürekli denetim planı, risk tahmini gibi periyodik olarak gözden geçirilen ve güncellenen denetim amaçları üzerine kurulur (Kurnaz ve Çetinoğlu, 2010: 208).

İç denetçiler sürekli denetimi geliştirmek için veri analizi kullanımını geliştirmelidirler. Bilgi teknolojisi denetiminde iç denetçiler veriyi çıkarmak ve analiz etmek için yaygın olarak denetim yazılımlarını kullanmaktadırlar ve denetim yazılımlarının kullanımı sayesinde sürekli denetim genişletilmiştir (Kurnaz ve Çetinoğlu, 2010: 231). Artık işletmeler ve diğer finansal bilgi kullanıcıları XBRL kullanarak veri toplama işlemini otomatik olarak gerçekleştirmektedir. Finansal bilgiler ve işletmenin performans bilgileri XBRL ile sunulduğunda finansal ve finansal olmayan

işletme verileri hızlı bir şekilde bir araya getirilip değerlendirilebilir. XBRL veri analizinde, verilerin seçilmesinde ve işlenmesinde de yardımcı olmaktadır. Bilgiye hızlı ulaşılması veri analizine veri yönetiminden daha fazla zaman ayrılmasına imkan vermektedir (Erkuş, 2008: 141).

2.1.1.3. Sürekli denetim–gerçek zamanlı muhasebe ilişkisi

Muhasebe bilgi sistemi tarafından kısa sürede üretilen bilginin karar alıcıların kullanımına da hızlı sunulabilmesi, bu bilgilerin doğruluğunun ve güvenilirliğinin de aynı hızla onaylanmasına bağlıdır. Geleneksel denetim mekanizmasının muhasebe bilgi sistemlerinin çok gerisinde kalmıştır (Alptürk, 2008b: 80). Bilgi teknolojilerindeki gelişmeler muhasebe bilgi sistemlerine otomatik veri yakalama, veriye anında ulaşma ve işleme, çok yönlü analiz ve raporlama, ek veri tipleri için yeterli kapasite, işletme dışı veri tabanlarına ulaşma gibi pek çok katkı sağlamıştır (Daştan, 2008: 79).

Sürekli denetim yaklaşımında gerçek zamanlı muhasebe sisteminin denetlenmesi şu aşamalardan meydana gelir (Kurnaz ve Çetinoğlu, 2010: 209):

1. Analitik prosedürleri içeren denetim planlaması,
2. Gerçek zamanlı muhasebe sistemine ilişkin iç kontrol yapısının dikkate alınması,
3. İşlemlere ilişkin aralıklı ve sürekli testlerin uygulanması,
4. Hesap bakiyelerinin ve analitik prosedürleri içeren sonuçların dönem sonu testlerinin yapılması,
5. Denetimin tamamlanarak denetim raporunun düzenlenmesi.

Bilgi teknolojileri sayesinde işletmeler ticari faaliyetlerini her geçen gün daha arttıran bir oranda elektronik olarak gerçekleştirmekte ve finansal tablolarını çevrim içi ve gerçek zamanlı olarak hazırlamaktadır. Dolayısıyla gerçek zamanlı muhasebe sistemlerinde, çoğu mali bilgi ve denetim kanıtı sadece elektronik ortamda bulunmaktadır. Bilgi teknolojileri ortamının işletmelerin iş yapma ve mali tablo bilgilerini yayınlama biçimlerini değiştirmesi üzerine işletmelerin büyük bir çoğunluğu bu tip mali tablo bilgilerini internet aracılığıyla HTML (HyperText Markup Language-

Hareketli-Metin İşaretleme Dili)²³ formatında sunmaktadır. HTML, bilgileri herhangi bir hesap tablosuna veya benzer bir yazılıma indirmeden işlem ve analiz yapmaya izin vermemektedir. İnternet üzerinde raporlanan mali bilgiler, kağıt dokümanların hypertext²⁴ formatında sunulan kopyalarıdır. XML (Extensible Markup Language-Genişletilebilir İşaretleme Dili)²⁵ ve bunun mali sürümü olan XBRL (Extensible Business Reporting Language- Genişletilebilir İşletme Raporlama Dili) kabul edilen muhasebe standartlarını kullanarak bilgi teknolojileri arasında mali bilgilerin paylaşımını sağlamaktadır. XBRL formatında, mali veri bir kez sisteme girilir ve daha sonra istenilen her türlü forma dönüştürülür. İşletmeler, iş ortaklarına işletmenin mali bilgilerine gerçek zamanlı erişim hakkını sunmaktadırlar. İşletmeler, kurumlar, denetçiler ve finansal tabloları kullananlar arasında böyle ortak bir dilin yaratılması sonucu finansal tabloların ulaşılabilirliği, güvenilirliği ve uyumluluğu gelişecektir (Kurnaz ve Çetinoğlu, 2010: 209-210). XBRL muhasebe verilerinin değişimini standart hale getirerek, iç denetçiler tarafından işletmenin muhasebe verilerinin kendi özel yazılımlarına transfer edilmesini sağlar. XBRL, verileri muhasebe sürecinin ilk aşamalarında elde ettiği için sürekli denetimin yapılmasına imkan verecektir (Erkuş, 2008: 129-130).

Gerçek zamanlı olarak hazırlanmış raporlarda yer alan tüm bilgi ve gerçek zamanlı hazırlanan güvence raporları önemli ölçüde sürekli güvence ihtiyacını karşılamaktadır. Günümüzdeki bilgi teknolojileri, finansal bilginin gerçek zamanlı raporlanmasına imkan sağlamaktadır. Sürekli denetimin uygulanabilirliği, iç denetçiler tarafından gerçek zamanlı ve önemli olan finansal bilginin bilgi teknolojileri vasıtasıyla sağlanabilmesine bağlıdır (Kurnaz ve Çetinoğlu, 2010: 211).

²³ HTML, internetin ilk programlama dilidir; internet üzerinden veri paylaşımı için yaygın olarak kullanılır. HTML dokümanları veriye ilişkin şekillendirme bilgilerini içerir. HTML dokümanın nasıl gösterileceğini belirtir, dokümanın ne olduğundan hiç bahsetmez (Alptürk, 2008: 266).

²⁴ HyperText, dokümanları biçimlendirmek, resim eklemek, bağlantılar yaratmak için kullanılan metottur.

²⁵ XML, verinin tanımlanması ve tarif edilmesi için kullanılan programlama dilidir. XML dokümanları verinin tanım bilgilerini içerir ve verinin taşınmasını sağlar. HTML ile benzerlik gösterir. Aralarındaki en önemli fark, XML'nin verinin kendisiyle ilgilenmesi, HTML'nin ise verinin sunumuyla ilgilenmesidir. XML sayesinde veri, bir veri tabanında yapısal özellikleri korunarak saklanmakta, yığın olmaktan kurtulmakta ve gerektiğinde filtre edilerek, sorgulanabilen bilgi olarak saklanmaktadır (Alptürk, 2008: 266).

2.1.2. Denetim çevresinde meydana gelen değişiklikler

Günümüzde işletme uygulamaları bilgi teknolojilerindeki değişimlere bağlı olarak gelişmektedir. Belgelere dayalı sistemin yerini bilgi teknolojilerinin kullanıldığı süreçlerin almasıyla birlikte işlemler bu teknolojiler vasıtasıyla yürütülür hale gelmiştir. Tüm bunlarla birlikte geleneksel denetim yaklaşımı da önemini yitirmiş ve bilgi teknolojileri konusunda bilgisi olmayan denetçilerin denetim işini yerine getirmesi güçleşmiştir. Tüm bilgi teknolojisi süreçleri, bilgi güvenliği, donanım, yazılım gibi konular ve bunların nasıl kontrol altında tutulacağı önem kazanmıştır. Bilgi teknolojilerinin doğrudan yönetsel karar alma sürecinde kullanılmaya başlanması, bilgi teknolojileri ortamında elde edilen ve üretilen bilginin doğruluğunu ve güvenilirliğini dikkate almayı gerektirmiştir.

Bilgi teknolojileri risklerine karşı önlem almak, bilgi teknolojilerinin ihtiyaçları karşılama optimum çözüm sunup sunmadığını belirlemek işletme bilgilerinin güvenliğini sağlamak, yetkisiz girişleri ve değişiklikleri engellemek için bilgi teknolojileri denetimlerini yapmak gerekmektedir. Diğer denetim türlerinde olduğu gibi bilgi teknolojileri denetiminde de yönetimin iddialarını destekleyen yeterli sayıda ve uygun nitelikte kanıt toplanmalı ve her hangi bir aksaklığın tespit edilmesi durumunda bunun denetçi raporunda yer alması gerekmektedir. İç denetçi neyin yanlış olduğunu tanımlamalı, nedenini belirlemeli, sisteme olası etkileri hakkında görüş bildirmelidir. Sorun çözülmezse mevcut durumda ve gelecekte ortaya çıkabilecek etkiler bildirilmeli ve iyileştirme için önerilerde bulunulmalıdır. Bilgi teknolojilerine dayalı ortamlarda denetimin amacı diğer denetim türlerinden farklı değildir, ancak denetçiyi bu amaçlara ulaştıracak denetim teknik ve yöntemleri farklıdır.

2.1.2.1. Sürekli denetimde bilgi güvenliği

İşletmelerin internetle dış dünyaya açılmaları, on-line olarak faaliyetlerini sürdürmeleri sadece işletme içinden değil işletme dışından tehditlere de yol açmaktadır. Bilgisayarlı ortamlar işlemleri hızlandırma, kolaylaştırma ve güncelleme ile bilgi iletiminde kolaylık sağlama gibi birçok fayda sağlamanın yanında güvenlik sorunlarını da beraberinde getirmektedir. İşletmenin bütün bölümlerinin bilgisayar ağları ile birbirine bağlı olması ve internet ile dış ortamlara erişim sağlanması güvenlik sorunlarının önemini arttırmıştır.

Bilgi güvenliği, bir değer yüklenen ve önemi bilinen, gizli tutulması gereken verilerin kaynaklarına ulaşılma hakkının yetkisiz kişilerden uzak tutulması ve bu bilgilerin koruma altına alınmasıdır. Bilgi güvenliği bir süreçtir. Bu süreç yazılım ve donanım güvenlik çözümlerinin alınması ile başlamakta, kullanıcıların bu çözümler içindeki güvenlik politikalarını uygulamaları ile devam etmektedir (Demir, 2005: 148).

Bilgi güvenliği programlarını uygulamada başarısız olan işletmeler, yetkisiz açıklama, değişiklik, hileler ve suiistimaller gibi bazı yıkıcı durumlardan zarar görmüşlerdir. Bu olaylar çeşitli yasal sorumlulukları gündeme getirmekte ve finansal kayıplar da büyük olmaktadır. İşletmelerin internet ağlarına yetkisiz girişleri ve finansal bilgilere zarar verilmesini önlemek amacıyla internet ağlarının sürekli izlenmesi gerekir. Finansal bilgilerin depolandığı bilgi teknolojileri, sürekli raporlamayı ve bilgi güvenliğini test etmesi ve geliştirmesi açısından fayda sağlayacaktır (Kurnaz ve Çetinoğlu, 2010: 212-213).

İnternet teknolojisi içinde yer alan ve sıklıkla kullanılan intranetler işletmelerin veri, bilgi, işlem ve iletişim güvenliği sorunları nedeniyle daha çok tercih ettiğini uygulamalardır. İnternet sayesinde işletmelerdeki süreçler sadeleşir ve faaliyet etkinliği artırılır. İnternetin teknik altyapısının ve mantığının kullanıldığı ve yalnızca giriş izni olan kişilerin kullanabildiği extranetlerde ise zaman ve yer ölçütlerine hakim olmak mümkündür (Alptürk, 2008b: 62).

İnternet kullanımının ve internet üzerinden veri dolaşımının artması işletmelerin iş süreçlerini elektronik ortama taşımış, kurumsal kaynak planlaması ve elektronik ticaret uygulamalarını birleştirme çabalarını gündeme getirmiştir.

İşletme yönetimi, bilgi teknolojileri ve bunlarla ilgili dokümantasyondan, finansal bilgi üretim süreçlerine ait dokümantasyon ile her türlü kayıt, bilgi, belge, yapı ve uygulamadan, bilgi teknolojileri kapsamındaki her türlü genel ve uygulama kontrolleri ile iç kontrol sisteminin tesis edilmesinden, yeterliliğinden, verimli ve etkin çalışmasında sorumludur. Uygulama kontrolleri, işletme yönetimi tarafından, finansal veri üretim süreçlerini ve içerdikleri verileri oluşturan, destekleyen, kullanan ve saklayan tüm sistemler ve uygulamalar içinde belirlenir, değerlendirilir ve raporlanır. Bu kontrollerin değerlendirilmesinde, sistemlerin yazılı belgelere uyumu, yazılı kontrollerin yeterliliği ve uygulanması, içerdikleri verilerin güvenliği, bütünlüğü ve sürekliliği gözden geçirilir (Alptürk, 2008b: 164).

2.1.2.2. Sürekli denetimin teknolojik uygulanabilirliği

İşletme kendi faaliyetleri sonucunda ortaya çıkan işlem ve olaylara ilişkin verilerinin tamamını veya denetime konu olacak kısmını eş zamanlı olarak elektronik ortamda tanımlayıp, izleyip, kaydedip, saklayabilecek elektronik temelli bilgi teknolojilerine sahip olması gerekir. Ayrıca işletmenin elektronik ortamda yürütülen işlemlerine ilişkin veri ve bilgileri eş zamanlı izleyip, denetim prosedürleri ve denetim konusu hakkında görüş bildirmek için gerekli olan yeterli denetim kanıtlarını elde ederek denetim yapılmasına imkan verecek donanım ve yazılımlarla desteklenmiş elektronik temelli bir sisteme sahip olunmalıdır. Bunlarla birlikte iç denetçi de denetleyeceği teknolojiler hakkında bilgi sahibi olmalıdır (Ağca, 2006: 74).

Sürekli denetimin teknolojik uygulanabilirliği açısından işletmenin ürettiği bilgilerin doğruluğu, güvenilirliği ve kullanılan teknolojilerinin güvenilirliklerinin nasıl sağlanacağı çok önemlidir. Bir diğer önemli konu da sürekli denetimde olayların ve işlemlerin gerçekleşmesi ile bunların denetimleri, denetim kanıtlarının elde edilme süreci ve denetim raporunun düzenlenmesinin kısa zamanda gerçekleşmesidir. Geleneksel denetim de ise sürekli denetimin denetim kanıtlarının elde edilmesi ve bu kanıtlarla ilgili olayların incelenmesi bir hayli zaman geçtikten sonra gerçekleşmektedir (Kurnaz ve Çetinoğlu, 2010: 214-215).

2.1.3. Sürekli denetim ve bilgi teknolojileri denetimi

Elle yürütülen faaliyetler ile bilgi teknolojileri ortamında yürütülen faaliyetlerin kontrolünde ve denetiminde kullanılan araç ve teknikler farklıdır. Bilgi teknolojileri ortamında yürütülen işlemlerin güvenilirliğinin, uygunluğunun ve performansının devamlılığının sağlanması otomatikleşmiş kontrol mekanizmaları ile sağlanabilmektedir. Bilgi teknolojilerinin kullanıldığı süreçlerde veriler ve bilgiler elektronik olarak kodlanırlar. Bu süreçlerdeki kontrol risklerine müdahale edebilmek, risk yönetimi ve bilgi teknolojileri ortamlarında güvenliği sağlamak için bilgi teknolojisi risklerini bilmek ve denetim süreci ile bunları bütünleştirmek gerekmektedir. Bu nedenle artık bilgi teknolojileri denetimi, sürekli denetim sürecinin de bilgi teknolojilerini kullanmadan gerçekleşmeyeceğinden vazgeçilmez bir ihtiyaç haline gelmiştir. Bilgi teknolojileri denetimi, bilgi teknolojilerinin işletmelerde yaygın

şekillerde kullanımı sonucunda faaliyetlerin kontrol altına alınması ve denetlenmesi için kullanılmaktadır. Günümüzde bilgi teknolojilerinde yaşanan gelişmeler bilgi teknolojileri denetimini de zorunlu hale getirmiştir.

İç denetimin hizmet anlayışını geliştirerek sürekli denetim yaklaşımını benimseyebilmesi için, öncelikle kullandığı teknolojiyi ve denetim araç ve tekniklerini riskleri belirleyebilecek düzeye taşıması gerekmektedir. Sürekli denetim yaklaşımı önümüzdeki beş yıl içerisinde pek çok işletmenin uygulayacağı yaygın bir yöntem olacaktır (Kahyaoğlu, 2010: 14).

Sürekli denetim araç ve teknikleri, bilgi teknolojileri denetimi sırasında riskleri belirleyebilmekte, iç kontrol sistemini değerlendirebilmekte, elektronik olarak denetim prosedürlerini gerçekleştirebilmekte, maddi doğruluk ve kontrol testlerine ilişkin örnekleri seçebilmekte, anormal işlem ve farklılıkları tanımlayabilmektedir (Kurnaz ve Çetinoğlu, 2010: 196).

2.1.3.1. Bilgisayar destekli denetim teknikleri

Bilgisayar destekli denetim teknikleri, giderek artan bilgi teknolojileri ortamında gerçekleştirilen faaliyetlerin daha etkin ve verimli bir şekilde denetiminin yapılması için gerekli olan yöntemleri ortaya koymakta ve denetçileri veri yığınları ile uğraşmaktan kurtararak, belli kontrollerden geçirilmiş sonuçlar üzerinden denetim yapmalarına imkan sağlamaktadır.

2.1.3.1.1. Bilgisayar destekli denetim tekniklerin yapısı ve kullanımı

Bilgisayarların denetim alanına girmesi denetçilere etkili olmadıkları teknik bir alan olarak görülmektedir. Bilgisayar Destekli Denetim Teknikleri (BDDT) kavramının ilk olarak çıktığı zamanlar bütün yenilikler biraz endişe ve dirençle karşılanmıştır. Bugün bile bilgisayar endişe ile yaklaşılmakta ve “kara kutu” olarak bakılmakta, ancak denetimler bilgisayar çevresinden gerçekleştirilebilmektedir. Denetçilerin manuel yöntemlerden vazgeçip, yeni teknolojilere uyum sağlama konusunda başarısız olmaları BDDT’lere hak ettikleri önemin ve değerin verilmesini önemli ölçüde etkilemiş ve geciktirmiştir (Ay, 2007: 278).

Finansal denetim faaliyetlerinde denetçi tarafından yapılması zor olan bazı hesaplamaların yapılmasında, denetimin planlanması, iç kontrol sisteminin incelenmesi,

denetim işlerinin uygulanması sonucunda yeterli kanıtların toplanması gibi aşamalarda etkinliğin ve verimliliğin artırılmasında, zaman, personel ve maliyet tasarrufu sağlanmasında BDDT'lerin avantaj sağladığı bilinmektedir (Pekdemir ve Selvi, 2002: 199).

BDDT veri analizinde kullanılmak üzere bilgi elde etmek için kullanıldığı durumlarda iç denetçi, verilerin elde edildiği bilgi teknolojileri ortamını ve bütünlüğünü onaylamalıdır. BDDT'ler gizli tutulması gereken önemli program ve sistem bilgileri ile üretim verilerini elde etmek için de kullanılır. İç denetçi bu üretim verilerini ve program/sistem bilgilerini uygun bir gizlilik ve güvenlik düzeyinde tutmalı ve korumalıdır. İç denetçi BDDT'lerin güvenilirliği, faydalılığı ve güvenliğinden emin olmak için uygun prosedürler uygulamalı ve sonuçları kaydetmelidir. BDDT'lerde sadece izin verilmiş değişikliklerin yapıldığını garantilemek için sistemler içine gömülü denetim yazılımları üzerindeki program değişiklik kontrollerini incelemelidir. Eğer BDDT'ler iç denetçinin kontrolü altında olmayan bir ortamda yer alıyorsa, BDDT'lerdeki değişiklikleri bulmak için uygun kontroller yapılmalıdır. İç denetçi BDDT'lerde herhangi bir konuda değişiklik yapıldığında planlama, test etme, işlem yapma, belge inceleme gibi çalışmalar vasıtasıyla BDDT'lerin bütünlüğü, güvenilirliği, faydalılığı ve güvenliği hakkında güvence sağlamalıdır. BDDT'lere güvenmeden ve onları dayanak olarak kabul etmeden önce bu güvencenin elde edilmesi gerekmektedir (TİDE; 2008: 130).

2.1.3.1.2. Bilgisayar destekli denetim tekniklerinin çeşitleri

En yaygın olarak bilinen ve kullanılan BDDT'leri arasında genelleştirilmiş denetim yazılımları, paralel simülasyon, veri testi tekniği, bütünlük test teknikleri, elektronik çalışma kağıtları, uzman sistemler, analitik inceleme prosedürleri, kıyaslama (benchmarking), istatistiksel örnekleme, uygulama yazılımı izleme ve eşleme, süreç modelleme, akış şeması, dengeli ölçüm kartı (balance score card) yer almaktadır.

Denetçinin maddi doğruluk testlerinde kullanacağı teknik Genelleştirilmiş Denetim Yazılımıdır. Bu yazılım, denetçinin ihtiyaç duyduğu belirli bir bilgi işleme fonksiyonunu yerine getirmek için hazırlanmış paket programdır (Selimoğlu, 2006b: 289). Genelleştirilmiş denetim yazılımı, bilgisayar sistemindeki kontrolleri test etmektedir. Ayrıca hesap bakiyelerinin doğrulanması ve kayıtların tamliğinin ve

tutarlılığının incelenmesi, farklı dosyalardaki verilerin karşılaştırılması, denetimin örnekleminin seçilmesi gibi alanlarda da genelleştirilmiş denetim yazılımları kullanılır (Selvi, vd., 2006: 310). Genelleştirilmiş denetim yazılımları denetçi tarafından istenen denetim işlemlerinin alt programlar şeklinde bir araya getirilmesinden oluşurlar. Genelleştirilmiş denetim yazılımları verileri bilinçli veya tesadüfi olarak seçebilirler ve ihtiyaca göre yeniden düzenleyebilirler. Spesifik görevler ve amaçlar için hazırlanmış ve sistemdeki verileri işleyen, inceleyen ve sonuçları değerlendirerek denetçilere sunan özel denetim yazılımları da vardır. Bu yazılımlar denetçinin kendisi veya bilgi işlem danışmanlık firmaları tarafından belirli bir denetim işi için hazırlanabilir (Çatıkkaş ve Yurtsever, 2009: 182-183).

Paralel simülasyonda ise denetçi işletme yazılımları ile paralel işlem yapan bir yazılım kullanır. Bu yazılımdan elde edilen çıktılar ile işletmenin orijinal yazılımından elde edilen çıktılar karşılaştırılarak hem bilgisayar sistemindeki kontroller hem de bakiyelerle ilgili maddi doğruluk testleri yapılmasını sağlar. Denetçiler, paralel simülasyon tekniğini benimseyerek uyguladıklarında testlerde araç olarak çoğunlukla genelleştirilmiş denetim yazılımını kullanırlar (Selvi, vd., 2006: 310). Paralel simülasyon ile denetlenebilir herhangi bir uygulama yazılımı test edilebilir. Paralel simülasyon herhangi bir veri girişi gerektirmemektedir. Paralel simülasyon üretim sistemindeki veriyi aynen kullanmakta ve sonuçların elektronik olarak karşılaştırılması sonucu hatalar kolayca belirlenmektedir (Coderre, 2009: 51).

Veri testi tekniği, denetçi işletmede gerçekleşen finansal olaylarla ilgili iki farklı muhasebe işlem grubu seçer. Bu gruplardan biri doğru muhasebe işlemlerinden ikincisi hatalı muhasebe işlemlerinden oluşur. Daha sonra bu iki farklı muhasebe işlem grubunu bilgisayar sisteminde izler. Amaç, bilgisayar sisteminin meydana gelen finansal olaylardan geçerli olanları işleyip, geçerli olmayanları hata olarak listelediği konusunda bilgi sahibi olmaktır (Selvi, vd., 2006: 309-310).

Veri testi ve paralel simülasyon tekniklerine oranla sisteme entegre denetim modülleri daha avantajlı olabilir. Sisteme entegre denetim modülleri bir denetim fonksiyonu yürütmek için tasarlanmış bir uygulama programının içine yerleştirilmiş rutin iş programlarıdır (Ertaş ve Güven, 2008: 52).

BDDT'lerinde kullanılan yazılımlar sistemler içine gömülü olduklarında bu yazılımlar kullanıcı programlarına eklenir ve işleyişi kontrol ederek sonuçları

denetçilere aktaran devamlı denetim ve gözetim işlevi görürler. Programlara eklenen ve gerçek verinin denetçiler tarafından elde edilmesini sağlayan yazılımlar arasında bütünleşik test teknikleri yazılımları yer alır. Bütünleşik test teknikleri sayesinde denetçi uygulama programlarının mantığını ve kontrollerini tüm muhasebe bilgi sistemini ele alacak şekilde test edebilecektir. Veri testinin bir türü olan bu teknikte denetçi hayali kayıtlar oluşturarak, bu kayıtları kukla verilerle çalıştırabilir. Ayrıca simülasyon yazılımları sayesinde denetçinin veriler üzerinde karşılaştırmalı analizler yapması ve geleceğe ilişkin tahminler yürütmesi de mümkün olmaktadır (Çatıkkaş ve Yurtsever, 2009: 182-183).

Elektronik çalışma kağıtları, genel geçici mizanın, ön çizelgelerin ve denetim kanıtlarının kaydedildiği ve diğer çizelgelerin hazırlandığı tablolardır (Ertaş ve Güven, 2008: 52). Denetçiler elektronik çalışma kağıtlarını risk analizi, denetim programları, denetim sonuçları, kanıtlar ve raporlar gibi uygulamalar sırasında kullanabilirler (Nastase ve Nastase, 2007: 45). Elektronik çalışma kağıtları denetim sonucu hazırlanacak denetim raporunun kaynağıdır. Denetimin kapsamına ve konusuna uygun çalışma kağıtlarının hazırlanması ve düzenin sağlanması önemlidir (Alptürk, 2008b: 250).

Uzman sistemler, bir uzmanın önerdiği çözümleri üretebilen o alanın bilgileri ile donatılmış, gerçekleştirme metotları ile olayları süzebilen programlardır. Bu sistemler belli bir alanla ilgili bilgilerin yüklenmesiyle oluşmuş, o alandaki uzmanın getirdiği şekilde çözümler ortaya koyabilen bilgisayar tabanlı programlardır. Uzman sistemler insan bilgisini depolayıp işleminden geçirmeye yarayan bir araçtır (Alptürk, 2008b: 252).

Analitik inceleme prosedürleri (AİP), çeşitli finansal olan ve olmayan verileri ile işletmenin kayıtları arasındaki anlamlı ilişkilerin incelenmesiyle elde edilen bilgilerin, denetçi tarafından geliştirilen beklentilere uyup uymadığına bakılması işlemleridir (Ataman, Hacırüstemoğlu ve Bozkurt, 2001: 68). AİP denetim sürecinin planlama, test etme ve tamamlanma aşamalarında kullanılabileceğinden denetimin oldukça etkili yürütülmesine neden olmaktadır. AİP'lerinin hata, hile veya düzensizlik ortaya çıkma olasılığı olan riskli alanları işaret etme yeteneği bulunmaktadır. İç denetçiler AİP'lerini kullanırken inceleyecekleri veriler ile bu verilerin anlamlılığını karşılaştıracakları verileri belirleyecekler ve iki veri arasında önemli bir farklılık ortaya çıktığında araştırma faaliyetlerini derinleştireceklerdir (Bozkurt, 2000: 2-3).

Kıyaslama (benchmarking), sürekli gelişime inanmış kuruluşların müşteri doyumunu ve rekabet üstünlüğünü hedefleyerek, ürün, hizmet ve süreçlerde mükemmellik örneği olan lider kuruluşların gelişmiş ve etken uygulamalarını kendi kuruluşlarına uygulamak amacıyla kullanacakları sistematik bir karşılaştırmalı ölçme yöntemidir. Kıyaslama, süreçler ve uygulamalarla ilgilidir. Aynı zamanda büyük değişiklik gerektiren süreçleri tanımlama aracıdır. Kıyaslama çok çeşitli şekillerde yapılabilir. Organizasyonun kendi içindeki birimleri arasında kıyaslamalar yapılabileceği gibi, organizasyon dışındaki şirketler ile de kıyaslama yapılabilir. Kıyaslama çeşitleri içsel, rekabetçi, fonksiyonel, genel kıyaslama olarak sınıflandırılır. Bunlardan rekabetçi kıyaslamamanın potansiyel uygulama alanları, kaynak yönetimi, iç denetim, insan kaynağı yönetimi, ücret ve prim sistemleri, satın alma vb. dir. Bu çeşitler dışında odaklanılan noktaya göre süreç odaklı, performans odaklı, stratejik kıyaslama gibi sınıflandırmalar da yapılabilmektedir²⁶.

İstatistiksel örnekleme, bir denetim testinin ve denetim prosedürlerinin uygulanacağı alanın belirlenmesinde ve seçiminde denetçiler tarafından istatistiksel örnekleme yöntemlerinden yararlanılabilir. İstatistiksel örnekleme sayesinde denetçi duruma en uygun örnek büyüklüğünü belirleyebilmekte, arzu edilen güvenlik derecesi ve hata payını ortaya koyabilmekte, sonuçları bilimsel olarak savunabilmekte, örnekleme hatasını tahmin edebilmekte ve zaman ve maliyet tasarrufu sağlayabilmektedir (Bozkurt, 2010: 200-201). İstatistiksel örnekleme model türlerini nitelik örnekleme, nicelik örnekleme ve parasal birim örnekleme olarak sınıflandırmak mümkündür. Nitelik örnekleme, bir evren içinde belirli nitelikteki bir oluşumun yüzdesini tahmin etmede ve iç kontrolün ayrıntılı uygunluk testlerinde kullanılır. Nicelik örnekleme, işlemlerin veya hesapların parasal değerlerinin test edilmesinde kullanılır. Parasal birim örnekleme, nitelik örnekleminin içinde hem uygunluk testlerinin hem de maddi doğruluk testlerinin birlikte kullanıldığı bir biçimdir. Denetçinin bir evren içindeki hatanın toplam parasal tutarı hakkında sonuca varmasını sağlar (Erdoğan, 2006: 206-208).

Uygulama yazılımı izleme ve eşleme, uygulama yazılımının işleme mantığı aracılığıyla veri akışını analiz etmek ve izlenen mantık, yollar, kontrol koşulları ve işleme sıralarını kaydetmek için kullanılabilecek uzmanlaşmış araçlardır. Uygulama

²⁶ <http://www.yildiz.edu.tr/~palcan/word%20dokuman/BenchmarkingSON%20HAL.doc> (14.06.2011).

yazılımı izleme ve eşleme, sadece hatalı işlem potansiyeline işaret etmektedir ve gerçek verilerin bu araçlar ile değerlendirilmesi söz konusu değildir (TİDE, 2008: 132,134).

Süreç modelleme, BT hizmetlerinin izlenmesi ve gerçekten bu hizmetlerden beklenen faydanın sağlanıp sağlanmadığının ölçülmesi ve iyileştirilmesini sağlar. BT süreç modellemesinde CobIT, ITIL, PMI, ISO 27001 gibi standartlar temel alınmaktadır. Kurumlar bu doğrultuda BT ilişkin ana süreç modelini oluşturmaktadır (Şahinaslan, Kantürk ve Şahinaslan, 2010:)

Akış şeması analizleri sayesinde denetçi muhasebe işlem akışları işletme tarafından akış şemalarıyla gösterilmiş ve belgelendirilmişse, bu şemalardan faydalanarak muhasebe kontrollerini hem sistem hem de mantık akışı içinde saptayabilecek ve değerlendirebilecektir. Çünkü akış şeması analizleri hangi bölümler ve görev ayrımları arasında hangi belgelerin ve bilgilerin dolaştığını açıkça ortaya koyacaktır (Erdoğan, 2006: 108).

Dengeli ölçüm kartı, bir yandan finansal sonuçlar dikkate alınırken bir yandan da kapasite artırma ve gelecekte büyüme ve gelişme sağlamaya imkan verecek şekilde değer yaratma konularındaki gelişmeleri eş anlı ve devamlı takip etmeyi mümkün kılmaktadır (Saygılı, 2007). Denetçi, sürekli denetim sonuçlarının dengeli ölçüm kartı, kurumsal kaynak yönetimi, performans ölçümü ve izleme etkinlikleri gibi yönetim etkinliklerini içermesini sağlamalıdır (Yurdağül, 2010: 225).

Spesifik görevler ve amaçlar için hazırlanmış ve sistemdeki verileri işleyen, inceleyen ve sonuçları değerlendirerek denetçilere sunan özel denetim yazılımları da vardır. Bu yazılımlar denetçinin kendisi veya bilgi işlem danışmanlık firmaları tarafından belirli bir denetim işi için hazırlanabilir (Çatıkkaş ve Yurtsever, 2009: 182-183).

2.1.3.2. Sürekli denetimde kullanılan raporlama dilleri ve bilgi teknolojileri yazılımları

İşletmelerde finansal veriler yaygın olarak HTML, Excel (.xls), Word (.doc), Notepad, ya da adobe dosyası (.pdf) gibi biçimlerde saklanmaktadır. Üzerinde yazı yazabilmenin haricinde kağıt belgelerden pek farkı olmayan bu tip elektronik ortamlar farklı bilgisayar ortamlarında farklı uygulamalar arasında veri transferine izin vermemektedir. Bu durumda yeni uygulamaların kullanılması kaçınılmaz olmaktadır.

Bilgi teknolojileri denetimi kapsamında kelime işlemci programların [Notepad, Word (.doc), adobe (.pdf), vs.] sadece yapısal durumu ve ürettikleri dosyaların durumu denetime konu olabilir. İçerik olarak denetlenmeleri bir anlam ifade etmez. Programların yapısal durumu ürettikleri dosyaların yapısal olarak güvenli olup olmadığı, bu dosyaların güvenlik için şifreleme algoritmalarının yeterliliği gibi konularda olabilir (Alptürk, 2008b: 248).

İşletmelerin bilgi teknolojilerindeki gelişmelerle birlikte gerçek zamanlı finansal bilgiler üretmeleri işletmelerde ticari işlemlere ait bilgilerin kaydedilme, saklanma ve denetlenme şeklini de değiştirmiştir. Finansal raporlama ise kağıt üzerinde ve standart bilgileri içeren, periyodik olarak yayınlanan, geçmişe ilişkin ve işletme kontrolünde sunulan performans bilgilerinden, internet ortamında yayınlanabilen, standart yerine isteğe bağlı bilgilerden oluşan, süreklilik temelinde gerçekleştirilen, mevcut durum ve geleceğe ilişkin geniş bir performans raporlaması haline gelmiştir. Gerçek zamanlı olarak gerçekleştirilen raporlamada bilgilerin doğruluğunun ve güvenilirliğinin garanti edilmesi amacı ile sürekli denetim yaklaşımı benimsenmelidir.

Aşağıda literatürde ve uygulamada en sık karşılaşılan raporlama dilleri ve bilgi teknolojileri yazılımları ayrı başlıklar altında ele alınacaktır.

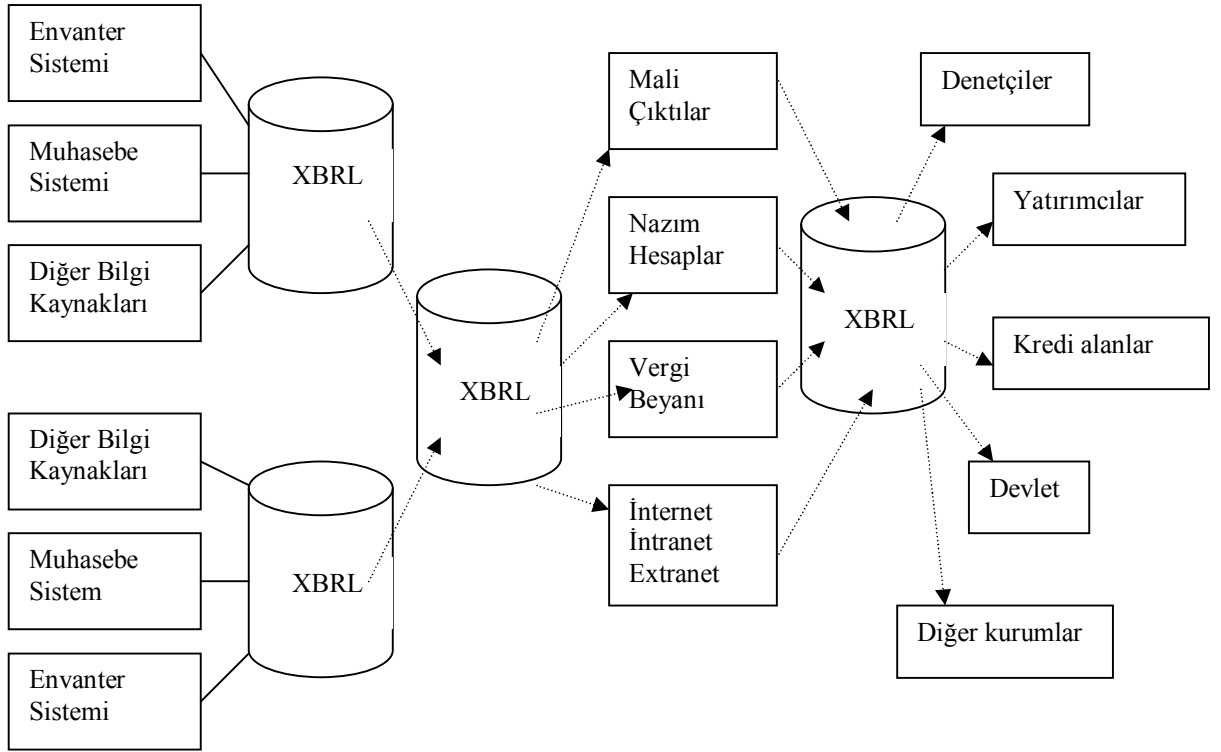
2.1.3.2.1. Raporlama dilleri

Sürekli denetimde kullanılan yazılımlar öncelikli olarak veri transferinin sağlanmasında iç denetçilere yardımcı olmaktadır. İç denetçiler, sürekli denetimi uygulama fırsatını arttırdığı için yaygın bir şekilde XBRL raporlama dilini kullanmaktadırlar. Sürekli denetim, işlemlerin oluşumundan kısa bir süre sonra veya anlık olarak işlemlerin değerlendirilmesini gerektirir. XBRL, finansal bilgilerin hazırlanmasını, yayınlanmasını ve denetlenmesini kolaylaştıran ve ticari işlemlerin raporlanması için standart hale getirilmiş XML tabanlı elektronik dildir. XBRL, çevrim içi finansal bilgi raporlaması için standart sunmakta ve bu sayede günümüzde kullanılmakta olan uygulamaların birbirinden farklılığını ortadan kaldırmaktadır (Aktaş ve Başçı, 2007: 42). XBRL son yıllarda tüm dünyada yaygın olarak kullanılan bir bilgi teknolojisi aracı haline gelmiştir.

XBRL, eş zamanlı raporlama ve denetimde yeni bir yaklaşım olarak karşımıza çıkan sürekli denetimin gerçekleştirilmesine olanak sağlamaktadır. XBRL sayesinde iç

denetçi veri transferini eş zamanlı olarak gerçekleştirmektedir. XBRL, hem işletme içi hem işletme dışı raporlamada, sürekli denetim, sürekli izleme ve finansal olmayan işletme ölçümlerinin yapılmasında kullanılabilir. XBRL ortamında finansal bilgi kullanıcıları otomatik olarak XBRL tabanlı raporlanan finansal tablolardan günlük satışlar, alacaklar ve hasılatındaki artış ile bunların karşılaştırmalı olarak analiz yapma imkanı elde edecektir. Ticari faaliyette bulunan veya üretim yapan işletmeler XBRL tabanlı finansal tabloları internette yayınladıklarında, kredi vermiş olan veya kredi verme aşamasında olan bankalar bu raporlara online olarak ulaşabilmektedir (Kurnaz ve Çetinoğlu: 2010: 271).

XBRL'nin bilgi giriş ve çıkış alanları aşağıdaki Şekil-6 yardımıyla da görülebilmektedir.



Şekil-6. XBRL Veri Akışı

Kaynak: Aktaş ve Başçı, 2007: 49.

XBRL uyumlu dosyalar, taksonomiler²⁷ yardımı ile gerçekleştirilmektedir. Veri olarak kabul edilen finansal bilgiler muhasebe bilgi sisteminden çekilmekte ve standart bir formata dönüştürülmektedir. XBRL taksonomilerini iki kısımda ele alabiliriz: XBRL FR (XBRL Financial Reporting) finansal raporlama taksonomisi ve XBRL GL (XBRL General Ledger) büyük defter taksonomisi. XBRL FR, finansal raporların üretilmesi, değiştirilmesi ve karşılaştırılması ile ilgili iken, XBRL GL, defter kayıtları ve büyük defter kayıtları ile ilgilidir (Garbellotto ve Hannon, 2005: 58).

XBRL FR taksonomileri işletme raporlarında açıklanan nakit, stok, borç, vergi giderleri, hisse başına kazanç, v.b.kavramların tanımlarını standartlaştırır. Böylece XBRL uyumlu herhangi bir sistem bu bilgileri okuyabilir, rapor içindeki diğer kalemlerle nasıl bir ilişkisi olduğunu anlayabilir ve miktarı tespit edebilir. XBRL FR taksonomisi içinde her bir kalem etiketlenebilir (Erkuş, 2008: 77). Geleneksel finansal

²⁷ XBRL’de taksonomi, işletme raporlarında yer alan bilgisayarlar tarafından okunabilen kavramların tanımlandığı sözcüklerdir. Taksonomiler, bir şema veya bir bağlantı tabanını içerebilir. Bir veya daha fazla sayıda taksonomi kullanımıyla veriler etiketlenmektedir. Taksonomiler, bilgilerin bilgisayarda nasıl tanımlanacağını ifade etmektedir (Erkuş, 2008: 57).

raporlamada finansal raporlar kağıt baskı, Excel, metin dosyası, adobe, veya HTML formatında olabilmekteyken, XBRL FR’de rapor örnek doküman olarak düzenlenerek bilgisayar ortamında istenilen şekil ve formata dönüştürülebilmektedir. XBRL FR taksonomisinin genişletilmesi ile bilanço düzenlenebilir ve denetim raporu gerekli taksonomilerin sağlanması ile finansal raporlara eklenebilir. Ayrıca örnek doküman olarak hazırlanan finansal raporlar internet üzerinden veya çevrimiçi olarak farklı yazılımlara aktarılabilir (Erkuş, 2008: 124-126).

XBRL GL ile finansal bilgi zincirine giren bir veri doğrudan XBRL GL taksonomileri etiketlenir ve XBRL FR’ye aktarılarak finansal raporlamaya elverişli hale getirilir. XBRL GL taksonomisi verilerin kurumsal kaynak planlaması sistemine akışı için genel bir model oluşturmaktadır. XBRL GL esnek bir yapıya sahiptir ve bu esnek yapı sayesinde elektronik veri değişimi gibi uygulamaları yetersiz kaldığı konuları çözebilmekte ve finans, muhasebe ve kredi verenlerin ihtiyaç duyduğu verilerin değişimini sağlamaktadır. XBRL GL, bütün muhasebe defteri fonksiyonlarını XBRL uyumlu hale getiren bir taksonomidir. XBRL GL, verileri organizasyonun farklı bölümlerine, finansal analiz araçlarına, arşive ve denetim işlerinde kullanılmak için denetçilere kolayca transfer edebilmektedir. XBRL GL finansal raporlamayı tamamlar ve finansal raporlar ve büyük defter arasında bağlantı kurulmasına ve denetçilerin ihtiyaç duyduğu özel bilgileri elde etmelerine imkan sağlar (Erkuş, 2008: 72-74). XBRL GL taksonomisi özellikle kurumsal kaynak planlaması sistemleri kullanan işletmelerde detaylı veriler tutulmasına ve daha sonra bunların özetlenerek finansal tablolara aktarılmasına yardımcı olmaktadır (Aktaş ve Başçı, 2007: 55).

Bu taksonomiler ülkelerin kanun ve muhasebe standartlarına uygun bir şekilde işletme veya çeşitli kuruluşların istekleri doğrultusunda, işletmenin amaçlarına ve çalışma alanına uygun raporlama yapmasına yardımcı olmaktadır.

Veri tabanı sistemlerinden kayıt alınması, değiştirilmesi veya yeni kayıtlar eklenmesi konularında ise SQL (Yapısal Sorgulama Dili-Structured Query Language) yardımcı olmaktadır. Ancak bu dilin kullanımında daha pek çok programlama dilleri (C++, Delphi, C, Basic, PHP, v.b.) kullanılabilmektedir. Veri tabanı yönetim sisteminde saklanan veriler SQL komutları ile yöneticilerin veya denetçilerin istekleri çerçevesinde işlenebilir veya değiştirilebilir (Kurnaz ve Çetinoğlu, 2010: 277).

2.1.3.2.2. Bilgi teknolojileri yazılımları

Sürekli denetimin başarılı olabilmesi için bilgi güvenilir ve kontrol edilmiş uygulama sistemleri tarafından üretilmiş olmak zorundadır. Sürekli denetim süreci otomatikleşmiş olmalıdır (Kurnaz ve Çetinoğlu, 2010: 186). Bunun içinde denetçilerin çoğunun denetim yazılımlarını kullanmaları gerekmektedir. Bu denetim yazılımlarında en yaygın kullanılanlar şunlardır: ACL, IDEA, SAS, Smart, SAP, AS 400, Excel, Access, Oracle, v.b. Bu yazılımlar içinde günümüzde en çok kullanılanlar ACL ve IDEA yazılımlarıdır ve bu yazılımların Türkiye’de de kullanımın yaygınlaştığı söylenebilir. Fakat bazı işletmelerin kendi ihtiyaçlarını karşılayacak şekilde özelleştirilmiş denetim yazılımlarını kullandıkları da bilinmektedir.

ACL, veri analizi, veri sorgulama, raporlama ve bilgisayar destekli denetim konusunda önde gelen bir yazılımdır. ACL, mali suistimal ve dolandırıcılıkların tespit edilmesinde işletmeye özel geliştirdiği tekniklerle ve basitleştirilmiş grup çalışmalarıyla (workshop) ile düzeyde finansal denetim yapılmasını sağlar. Ayrıca BDDT’lerin kullanımı öncesindeki örnekleme risklerini de ortadan kaldırır. ACL kullanılarak yapılan denetimler sayesinde büyük veriler ile çalışma ve verilerin tamamını denetleyebilme, mevcut programlar ile yapılamayan kontrolleri yapma, tekrarlayan işleri otomatik hale getirme mümkün olmaktadır (Alptürk, 2008b: 155).

IDEA ise veri elde etmeye ve veri analizine yardımcı olan bir yazılımdır. IDEA işletme verilerinin güvenliğinin analizinde çalışmalar yapılmasını sağlamaktadır. Veri güvenliğinin çok önemli olduğu günümüzde işletim sistemlerinin düzgün bir şekilde yapılandırılması dahi sistemlerin güvenlik seviyesini artırmaya yardımcı olur (Alptürk, 2008b: 156).

2.1.3.3. Bilgi teknolojileri denetimi

Bilgi teknolojileri denetimi, bilgi teknolojileri kaynaklarının değerlendirilmesi süreci olup, bilgi teknolojileri ile ilgili unsurların güvenlik altında olduğunun, bilgisayar verilerinin bütünlüğünün ve doğruluğunun sağlanmış olduğunun ve kurumsal amaçlara ulaşıp ulaşılmadığının özenle incelenmesidir.

BT denetimi, var olan BT varlıklarının, kaynakların, işletmenin düzenlemeler ile uygunluğunun ve risklerinin bir analizidir. BT denetimi bilgi güvenliği, risk yönetimi gibi konularda değerli bilgiler sağlar. BT denetimi, işletmenin BT varlıklarının ve

süreçlerinin nicel ve nitel anlamda BT yapısı, ağ, uygulama ve bilgi güvenliği, veri merkezleri, BT araçları ve yöntemleri, personel, ürünler ve iş süreçleri gibi konuları gözden geçirmeyi gerektirir.

İç denetçiler verilen görevleri yerine getirebilmek için bilgi teknolojileri ve kontrolleri ile ilgili kilit bilgilere ve mevcut teknoloji tabanlı denetim teknikleri hakkında bilgi ve tecrübeye sahip olmalıdırlar.

2.1.3.3.1. Bilgi teknolojileri kontrolleri

Bilgi teknolojileri denetiminde kontrolleri; yürütme kontrolleri, muhafaza kontrolleri, bilgisayar faaliyetlerinin kontrolleri, program güvenlik kontrolleri, bilgi dosyaları güvenlik kontrolleri, sistem program kontrolleri ve biçim değiştirme kontrolleri olarak sınıflandırabiliriz. Bunları kısaca aşağıdaki şekilde açıklayabiliriz (Kurnaz ve Çetinoğlu, 2010: 247-248):

1. Yürütme kontrolleri; yeni kurulan veya geliştirilen sistemler için programlanmış süreçlerin uygun olup olmadıklarını ve bu sistemlerin ihtiyaçları karşılayıp karşılamadığını test etmek amacıyla tasarlanan kontrollerdir.
2. Muhafaza kontrolleri; yapılan değişikliklerin test edildiğinden, yetkili makamlarca onaylandığından ve doğru bir şekilde yürütüldüğünden emin olmak için oluşturulan kontrollerdir.
3. Bilgisayar faaliyetlerinin kontroller; bilgi işlem faaliyetleri için yetkililerce onaylanmış, önceden programlanmış ve bilgi dosyalarının güncellenmiş en son biçimlerinin dikkate alınmasını sağlayan kontrollerdir.
4. Program güvenlik kontrolleri; programlar ve yazılımlar üzerinde yetkilendirilmemiş ve onaylanmamış değişikliklerin yapılması önlemek için geliştirilen kontrollerdir.
5. Bilgi dosyaları güvenlik kontrolleri; Bilgi dosyaları üzerinde yetkilendirilmemiş ve onaylanmamış değişikliklerin yapılması önlemek için geliştirilen kontrollerdir.

6. Sistem program kontrolleri; uygun sistem programının kullanımı ve yetkilendirilmemiş değişikliklere karşı koruma sağlanması konularında güvence yaratmak üzere oluşturulmuş kontrollerdir.
7. Biçim değiştirme kontrolleri; tüm bilgilerin eski sistemlerden yeni sistemlere dönüşüm sürecinin bütün ve doğru bir şekilde tamamlanmasına yardımcı olmak için kullanılan kontrollerdir.

Bilgi teknolojileri denetimi kapsam bakımından üçe ayrılır: Bunlar “uygulama kontrollerinin denetimi”, “genel kontrol alanlarının denetimi” ile “uygulama kontrolleri ile genel kontrol alanlarının birlikte gerçekleştirildiği geniş kapsamlı denetimler”dir (Alptürk, 2008b: 167).

Genel kontroller sistemin geliştirilmesi, sistem güvenliği, network ve veri merkezi, program değişikliği, bakım gibi konularda yapılan tüm bilgisayar aktivitelerini kapsarken, uygulama kontrolleri de bilgi teknolojileri tarafından yapılan veri girişi, raporlama gibi aktivitelerin kontrolü kapsar (Selimoğlu, 2006a: 152). Genel kontrolleri kullanıcı girişi, sistem geliştirme döngüsü, değişim ve yapılandırma yönetimi, fiziksel güvenlik kontrolleri, sistem ve veri yedekleme ve kurtarma konularındaki kontrolleri içerir. Uygulama kontrolleri girdi kontrolleri, süreç kontrolleri, çıktı kontrolleri, bütünlük kontrolleri ve denetim izlerini içerir (Coderre, 2009: 91). Bilgi teknolojileri denetimi sonunda yayınlanan raporda, bilgi teknolojileri ve finansal veri üretim süreçleri üzerinde değerlendirmelere yer verilir ve bilgi teknolojileri denetçisinin denetim görüşü açıklanır. Bilgi teknolojileri denetçisi, genel kontrol ve uygulama kontrolleri hakkında denetim kanıtlarını toplayıp inceler ve bu kanıtlar üzerinde bir sonuca ulaşır (Alptürk, 2008b: 171). Genel ve uygulama kontrolleri işletme kontrollerinin büyük bir kısmını oluşturmaktadır. Denetçiler, finansal tablo hatalarına neden olan zayıflık ve eksiklikleri bulmak amacıyla oluşturulmuş anahtar kontrolleri belirlemek için tüm işletme sürecini, BT uygulamalarını ve kontrollerini iyice anlamalıdır (Coderre, 2009: 91).

Tablo-5. Genel Kontroller ve Uygulama Kontrollerinin Sınıflandırılması

	Kontrol Türleri	Kontrol Örnekleri
Genel Kontroller	Bilgi işlemle ilgili yönetsel kontroller	Bilgi işlem müdürünün raporlamayı üst yönetime veya yönetim kuruluna yapması.
	Bilgi işlem görevlerinin birbirinden ayrılması	Bilgisayar programcısı ile bilgisayar operatörü görevlerinin ayrımı
	Sistem geliştirme	Kullanıcıların, sistem analistlerinin ve programcıların yazılımı geliştirmesi ve test etmesi.
	Fiziksel ve çevrimiçi güvenlik	Bilgisayar sisteminin çalışması, bilgilerin ve programların korunması için yetkili şifre gerekliliği.
	Yedekleme ve acil durum planlaması	Yazılı yedekleme planları hazırlanır ve yıl içinde düzenli olarak test edilir.
	Donanım kontrolleri	Monitörde hata mesajı çıkmasına neden olan bellek veya sürücü hataları.
Uygulama Kontrolleri	Girdi Kontrolleri	Veri işleme süreci öncesi
	Süreç (işleme) Kontrolleri	Satış işlemindeki birim satış fiyatının uygunluk testi
	Çıktı Kontrolleri	Satış departmanı tarafından satış işlemlerinin veri işleme süreci sonrası incelenmesi.

Kaynak: Selvi vd., 2006: 309.

Bilgi teknolojileri kontrolleri işletmenin teknoloji kullanımının ortaya çıkarabileceği risklerin azalması ve hafifletilmesinde yardımcı olur. İç kontrol sistemi içinde yer alan bilgi teknolojileri kontrolleri gerekli güvenceyi vermelidir. Bu güvence kesintisiz olmalı ve kanıtların güvenilir ve kesintisiz izlenmesine imkan vermelidir. İç denetçinin sağladığı güvence, verilen güvencenin bağımsızlığına ve objektifliğine bağlıdır. Sağlanan güvence yönetilen riskler için gerekli kontrolleri anlamaya, incelemeye ve değerlendirmeye dayanmaktadır. Kontrollerin uygun tasarlanmasını ve etkin ve kesintisiz çalışmasını sağlamak için yeterli testlerin yapılması gerekir (Alptürk, 2008b: 273).

Bilgi teknolojileri kontrollerinin risk değerlemesi açısından COSO modeli tüm işletme çapındaki riskleri ele alır. COSO modeli işletme ve bilgi teknolojisi risklerinin bütünleşmesini benimser ve iç denetçilerin riskin yüksek olduğu alanlarda veya fonksiyonlarda Bilgi teknolojisi kontrollerini belirlemesini teşvik eder (Coderre, 2009: 90).

2.1.3.3.2. Bilgi teknolojileri denetiminin uygulama süreci

Finansal işlemlerin ve faaliyetlerin teknik alt yapısının gittikçe karmaşıklaşması bilgi teknolojileri denetimini önemini ve bilgi teknolojileri denetçilerine olan ihtiyacı arttırmıştır. İşletmede yürütülen süreçler ile ilgili kontrollerin birçoğu artık kullanılan bilgi teknolojilerinin içine yerleştirilmiş durumdadır. Bilgi teknolojileri denetiminin sıklığı ve kapsamı denetim amaçlarına erimeyi sağlayacak şekilde belirlenmelidir. Bunun için uygulanacak bilgi teknolojileri denetimi faaliyetlerini kapsayan bir kılavuz (el kitabı) hazırlanabilir. Bu kılavuzda bilgi teknolojileri denetiminde izlenecek yollar ayrıntılı olarak ele alınmalıdır. Denetlenen alanlar ve faaliyetler, denetim sıklığı, denetim planı, otomatikleşmiş veri süreçleri içerisinde yer alan tüm önemli uygulamaların ve fonksiyonların denetimi için ayrıntılı hale getirilmiş yöntemler, denetim çalışma kağıtları, raporlama standartları, sistem geliştirme süreçlerinin kontrol yordamları açısından gözden geçirilmesi, denetim yazılımlarının niteliği ve kullanımı konularını içermesi gereken kılavuz çeşitli nedenlerle ortaya çıkabilecek değişiklikleri yansıtmak için belli aralıklarla gözden geçirilmeli ve yenilenmelidir (Kurnaz ve Çetinoğlu, 2010: 246).

Bilgi teknolojileri denetimi alanında CobIT (Control Objectives For Information And Related Technology-Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri) kriterleri denetim alanında çok sayıda uzmanın bilgisi dikkate alınarak hazırlanmış kabul görmüş bir metodolojidir. CobIT denetim çerçevesinin hedef kitlesi üst yönetimdir. CobIT olası bilgi teknolojileri risklerini üst yönetime görünür kılmayı amaçlamaktadır. CobIT, bilgi teknolojilerini etkin ve yaygın olarak kullanan risklerin yönetilmesi ve bilgi teknolojilerine dayanan kritik iş süreçlerini bilinçli ve sistematik yöntemlerle desteklemesinin yanı sıra, oluşturulacak kontroller ile ilgili yenilikleri ve zorunlulukları bildirmektedir. CobIT'in bilgi teknolojilerinin risk ve hedef odaklı yönetimini amaçladığı söylenebilir. CobIT bilgi teknolojilerini iş süreçlerinin destekçisi olarak görmektedir (Erhan, 2009: 100).

Uygulamada bilgi teknolojileri denetiminde yer alan konular şunlardır (Alptürk, 2008b: 247):

1. Verilerin güvenliği, yedekleme ve yedekten dönme, yedeklerin saklanması, bu kapsamda kullanılan yazılım ve donanımın yeterliliği,

2. Sistemin güvenliği, izinsiz erişimler ve engelleme, yazılım ve donanımın yeterliliği,
3. Sistemlerin sürekliliğinin sağlanması (yedekleme) ve test edilmesi,
4. Zararlı programlardan (virüs) korunma,
5. İşletim sistemleri uygunluk ve güncelleme kontrolü,
6. Kullanıcıların yetkilendirilmesi,
7. Bilgisayar ağı yapısı.

2.2. Risk Odaklı İç Denetim Sürecindeki Etkiler

Geleneksel yaklaşımda belirli aralıklarla ve rutin olarak gerçekleştirilen denetimler, modern yaklaşımlar geliştikçe sistematik bir risk değerlendirme yöntemi çerçevesinde objektif olarak gerçekleştirilen risk değerlendirme çalışmalarına yerini bırakmıştır. Buna göre ideal bir iç denetim modelinde, işletme süreçlerine ilişkin risk ve kontrollerin uygun risk ve kontrol metodolojileri çerçevesinin belirlendiği, analiz edildiği, sayısal hale getirildiği, elde edilen sonuçların değerlendirilerek yüksek ve düşük risk içeren süreçlerin denetim sıklığının farklı belirlendiği risk odaklı bir iç denetim planına dayanılarak gerçekleştirilmelidir (Gegin, 2010: 19).

Risk odaklı iç denetim hem işletme yönetiminin hem de iç denetçilerin iç denetimin işletme içindeki fonksiyonunun ve konumunun yeniden tanımlanmasındaki önemini kavramalarını sağlar. İç denetimin, risk yönetiminde odak noktası olup olmayacağına işletme yönetimi karar verir (Demirbaş, 2005: 184).

Günümüzde iç denetimin hedeflerini işletmenin hedefleri içinde gören bir anlayış oluşmuş ve iç denetimin amaçları arasına riskli durumları doğru tahmin edebilmek de katılmıştır. İşletme risklerini kontrol altına alabilmek işletme yönetiminin sorumluluğudur. Bu riskli durumları ve sonuçlarını öngörmek açısından iç denetim biriminin işletme içindeki önemi oldukça büyüktür.

İşletmelerde bilgi teknolojilerinin yoğun bir şekilde kullanımı, bilgi teknolojilerinin beraberinde getirdiği risklerin de değerlendirilmesini gerektirmektedir. İşletmelerdeki geleneksel risklerin yanı sıra bilgi teknolojilerindeki gelişmelerle birlikte yeni riskler oluşmuş ve bu riskler zamanla daha karmaşık hale gelmiştir. Bu durum işletmeleri risklere daha açık hale getirdiğinden, söz konusu risklerin ölçülmesi ve yönetilmesinde yeni yöntemler geliştirilmiştir. İşletmelerin hızlı değişim gösteren risk

profillerini kavramaları geleneksel yöntemlerle yapılamamaya başlandığı için dünyanın pek çok ülkesinde geleneksel denetimin eksikliklerini karşılamak amacıyla Risk odaklı iç denetim yaklaşımı benimsenmiştir (Selim ve McNamee, 1999: 149).

2.2.1. Risk odaklı iç denetimin uygulama sürecindeki etkiler

Risk odaklı iç denetim, işletme bünyesindeki iç kontrol sisteminin yeterliliğinin ve etkinliğinin incelenip değerlendirilmesi, risk yönetimi ve risk değerlendirme metotlarının uygulanmasının ve etkinliğinin incelenmesi gibi görevlerin yanı sıra bilgi teknolojileri dahil olmak üzere tüm yönetim ve finansal bilgi sistemlerinin gözden geçirilmesi, muhasebe kayıtları ile finansal tabloların doğruluğunun ve güvenilirliğinin incelenmesi, hem işlemlerin hem de iç kontrol sisteminin işleyişinin denetlenmesi gibi pek çok alanı kapsamaktadır. Risk odaklı iç denetimle birlikte denetimin yönü uygunluk denetiminden risk denetimine dönüşmüştür (BASEL Komite, 2000: 3).

İç denetçi risk değerlendirmelerine dayanan bir denetim planı oluşturmaktadır. Risk odaklı iç denetim planları denetim alan belirleme uygulamasından ve risk değerlendirme sürecinden kaynaklanan öncelikli risklerin finansal ve iç denetim hedeflerine hitap etmelidir. İç denetçinin hazırladığı planlar iç denetim anketlerini veya kişisel değerlendirmeleri ölçen araçları, muhasebe genel dengelere ilişkin testleri, parasal işlemleri test eden varlık testlerine ilişkin işlemleri, işletmenin faaliyet çevresindeki iç denetimin etkinliğini test etmek için kullanılan denetim testlerini ve analitik inceleme prosedürlerini kapsamalıdır (Kurnaz ve Çetinoğlu, 2010: 104).

2.2.2. Bilgi teknolojileri riskleri ve etkileri

Risk yönetim prensipleri geniş bir ilgi alanına sahip olmakla birlikte, pek az organizasyon bilgi sistemleri risk yönetim programlarını oluşturmuştur. Oysa son yıllarda artan sayıda organizasyon BT risk yönetimi adına CobIT, ITIL, ISO 27001 gibi uluslararası standart ve yaklaşımları bilgi sistemleri yönetimlerine adapte etmektedir.

BT risk alanları aşağıdaki gibi ifade edilebilir (Bağcı, 2009: 4-5):

1. *BT yönetim ve strateji riski*: BT stratejilerinin iş stratejileri ile uyumlu olmaması ve paylaşılmaması sonucu BT'nin iş ile ilişkili bir birim olarak çalışmaması riskidir.

2. *BT beceri ve teknolojik gelişme riski:* BT'nin iş birimlerini sektörün önde gelenleri arasında tutacak ve iş yeteneklerini geliştirecek yenilikleri gerçekleştirmek konusunda başarısız olması riskidir.
3. *BT mimari riski:* BT'nin iş birimlerinin ihtiyaçlarının verimli, maliyet-etkin ve iyi kontrol edilebilir şekilde olmasını destekleyecek etkin, standart ve sürdürülebilir alt yapısının olmaması riskidir.
4. *İş sürekliliği riski:* BT'nin kritik operasyon ve süreçleri devam ettirememesi riskidir.
5. *Uyumluluk riski:* BT'nin yasal düzenleyicilerin gerekliliklerini yerine getirecek desteği verememesi riskidir.
6. *BT kaynakları riski:* BT'nin insan ve finansal kaynaklarını uygun hazırlık ve planlama ile yönetememesi riskidir.
7. *Tedarikçi yönetim riski:* BT organizasyonlarının tedarik, dış kaynak alım ve servis sağlayıcılar ile uygun ilişki kuramaması riskidir.
8. *Üçüncü parti ilişkileri riski:* İş ortamının ve bilgilerin üçüncü parti kişi ve kuruluşlarca paylaşılması riskidir.
9. *Proje geliştirme riski:* BT'nin kötü proje planlaması ve yönetimi sonucu oluşan risklerdir.
10. *Değişiklik gerçekleştirme riski:* Teknoloji ortamının uygun bir şekilde değiştirilememesi riskidir.
11. *BT itibarı ve müşteri memnuniyeti riski:* BT'nin, iş isteklerini, hizmet seviyesi anlaşmalarını ve BT desteğini uygun şekilde karşılayamaması riskidir.
12. *Bilgi riski:* Hassas ve önemli iş bilgilerinin uygun şekilde yönetilememesi ve saklanamaması riskidir.
13. *BT güvenliği riski:* BT alt yapısı ve kaynaklarının tehditlere karşı zayıflıklara sahip olması riskidir.
14. *Online/Web riski:* BT'nin web varlığını devam ettirememesi riskidir.

Bilgi teknolojileri için risklerin belirlenmesi, sistem veri işleme ortamının iyi anlaşılmasını gerektirmektedir. Bu sebeple risk değerlendirmesi yapılmadan önce bilgi teknolojileri ile ilişkili donanım, yazılım, sistem ara yüzleri, veri ve bilgi, BT sistemine

destek veren ve sistemi kullanan kişiler, sistem görevleri (BT sistemi tarafından gerçekleştirilen süreçler), sistem ve veri kritikliği (sistemin organizasyon için değeri veya önemi vb.)ve sistem ve veri hassaslığı gibi bilgiler toplanmalıdır (Bağcı, 2009: 7).

Bilgi teknolojileri değerleri²⁸ne ilişkin riskler, nasıl kontrol edilecekleri ve yönetilecekleri belirlenmek üzere analiz edilir. Risk analizi, iş süreçlerinin etkilendiği bilgi sistemleri değerlerinin bütünüyle değerlendirildiği bir çalışmadır.

İşletmeler bilgi teknolojileri ile ilgili riskleri anlamalı, bunları analiz etmeli ve azaltma stratejilerini düzenlemelidirler. Bu amaçla işletmeye etkilerine göre risk sınıflandırması şu şekilde yapılmalıdır (Bağcı, 2009: 8):

1. *Güvenlik riski*: Bilgi değiştirilebilir, erişilebilir veya yetkisiz kişilerce kullanılabilir.
2. *Erişilebilirlik*: Bilgi veya uygulamalara bir sistem hatası veya doğal bir felaket sonucu erişilemeyebilir.
3. *Geri Kazanılabirlik*: Sistem kaybı veya çökmesi sonrasında BT sistemleri bilgiyi zamanında geri getiremeyebilir.
4. *Performans riski*: Sistemler, uygulamalar veya personelin veya tüm BT'nin beklenenin altında performans göstermesi sonucu iş üretkenliği veya değeri azalabilir .
5. *Ölçeklenebilirlik*: BT, organizasyonun değişen bilgi gereksinimlerini karşılama için geliştirilemeyebilir veya değiştirilemeyebilir.
6. *Uyumluluk riski*: Bilgi tutma ve işleme, düzenlemelere ve BT veya iş politika gereksinimlerine uygun gerçekleştirilemeyebilir.

Bilgi teknolojileri risk değerlendirmesi sadece risk yönetiminin değil aynı zamanda iş sürekliliği ve güvenlik planlamasının da önemli bir parçasıdır. Risk değerlendirmesi, iş süreçleri bağımlılıklarını ve risk oluşumunda etkilenen değerleri hesap etmektedir. Uygun risk değerlendirmesi için temel bazı varsayımlar yapılmaktadır. Bu varsayımlar aşağıdaki gibi ifade edilebilir (Bağcı, 2009: 9):

1. İş kolu tanımlanmış olmalıdır,
2. İş kolu bir otomasyona sahip olmalıdır,
3. Otomasyon, iş kolunun çalışma yapısı içinde kritik kabul edilmelidir,

²⁸ *Bilgi teknolojileri değerleri*, organizasyon için önemi olan, somut veya soyut bilgi sistemleri bileşenleridir. Bilgi teknolojileri değerleri, donanım, yazılım, veri, binalar, altyapı olabileceği gibi ürünler, bilgi kaynakları, müşteri ilişkileri veya itibar da değerler arasında sayılabilir.

4. İş sahibi tanımlanmış olmalıdır,
5. Risk değerlendirme sürecine yardımcı olacak personel belirlenmiş olmalıdır,
6. İş kolu BT dışındaki risklere açık olmalıdır,
7. Program servislerinin verilmesini kontrol eden yasal parametreler anlaşılır olmalıdır.

Risk yönetiminin izlenmesiyle ilgili çalışmalardan iç denetçiler sorumludur. Yapılan değerlendirmeler sonucu riskler belirlenmekte ve tespit edilen bulguların düzeltilmesi aktiviteleri ile reaktif bir yaklaşım izlenmektedir. Bununla birlikte, iş birimlerinin kendileri ile ilgili bilgi teknolojisi değerleri için öz değerlendirmeler yapmaları ve denetçiler tespit etmeden riskleri belirlemeleri ve önlemler almaları gerekmektedir.

2.2.3. Risk yönetimi ve kurumsal yönetim ile olan ilişkilere etkisi

Risk yönetimi ve kurumsal yönetimin etkinliğini zamanında ve sürekli olarak sağlama konusunda güvence ihtiyacı kritik öneme sahiptir. İşletmeler önemli finansal kayıplara neden olan ve riskleri arttıran hata, hile ve yolsuzluklara maruz kalabilmektedir. Hızla değişen işletme çevresi, işletmeleri iç kontrollerinin etkinliğini test etme ve riskleri azaltma konusuna önem vermeye yönlendirmiştir. Bu çabalar iç denetimden beklenenleri arttırmakla birlikte, risk yönetimi ve kurumsal yönetimin etkinliğini değerlendirme konusunda iç denetimin bağımsızlığını ve tarafsızlığını koruyabilme yeteneği açısından da şüpheleri arttırmıştır (The Institute of Internal Auditors, 2005: 1).

2.2.3.1. Risk yönetimi ile ilişkilere etkisi

Tüm riskler doğrudan insan veya süreçlerle ilgilidir. Risklere karşı başarı sağlamanın anahtarı ise projelerin etkinliğini sağlayamamak, bilgi teknolojilerinden kaynaklanan kayıplar, uzman personel yokluğu, sistem güvenliğinin ihlali, sistem gelişiminin önceliklendirilememesi, çok fazla veri-yararsız bilgi gibi faktörler arasındaki bağlantıları bilmek ve aradaki ilişkileri başarılı bir şekilde yönetmektir (Griffiths, 2005: 63).

Bilgi teknolojilerindeki gelişmeler işletme yönetiminde risk algılama ve risklere karşı korunma gereğini doğurmuştur. Böylece iç denetiminde faaliyet alanı genişlemiş ve iç denetim işletme kararlarına destek veren bir birim haline gelmiştir (Demirbaş, 2005: 177).

Risk yönetimi, belirsizlikleri değerlendirme ve yönetme yeteneğini geliştirmek için işletmenin stratejilerini, süreçlerini ve bilgi teknolojisini değerlendirmelidir. İç denetim riskli alanların belirlenmesi ve değerlendirilmesinde işletme yönetimine yardımcı olmalıdır. İç denetçiler, risk değerlendirmesi sonuçlarına dayanarak işletmenin yönetimini, faaliyetlerini ve bilgi teknolojilerini kuşatan kontrollerin uygunluğunu ve etkinliğini değerlendirmektedir (Kurnaz ve Çetinoğlu, 2010: 301). Bir risk yönetimi kurulması, karar verme kabiliyetini artırmakta, bilgi değerlerini korumakta, operasyonları güvenli hale getirmekte, organizasyonun yasa ve yükümlülüklerle uyumunu desteklemektedir. Hedef sadece riski yok etmek değil, kaçınılmaz bir şekilde karşımıza çıkan riskleri yönetebilmek ve olumsuz sonuçlardan kaçınabilmek için fırsatlar oluşturabilmektir. İşletmenin üst yönetimi tarafından işletmenin almaya hazır olduğu risk türünü ve miktarını iç denetim belirlememelidir. İç denetim risk yönetimi süreçlerini uygulama zorunluluğunu dayatmamalı, yönetimin risk yönetimi alanındaki rolünü üstlenmemeli ve risk yönetiminden sorumlu tutulmamalıdır.

İşletmede iç denetim yöneticisi, kontrol çerçevesini ve risk yönetimi tarafından gösterilen alanları incelemelidir. İşletme yönetimi, kontrolleri ve riski değerlendirecek olan süreçleri iyi bir şekilde oluşturmuşsa, iç denetim faaliyeti sırasında kontrol ve risk düzeylerine daha fazla güven duyulabilir. Eğer süreçlerin yeterli olmadığı belirlenirse, iç denetçiler kontrollere ve risklere ilişkin kendi detaylı değerlendirmelerini yapmalıdırlar (Kurnaz ve Çetinoğlu, 2010: 289).

Bilgi teknolojileri kontrolleri bir işletmenin teknoloji kullanımının doğurabileceği risklerin azaltılmasına yardımcı olur. İç denetçinin ise kontroller üzerindeki rolü risk ve kontrol değerlemelerinin sonuçları ile ilgilidir (Alptürk, 2008b: 273).

Günümüzde risk odaklı iç denetim yaklaşımına dayalı bir anlayış vardır. Ancak bazı işletmeler risk odaklı iç denetimden risk yönetimine güvence veren bir denetim anlayışına doğru hareket halindedirler. Risk yönetimi süreçlerinde iç denetim çerçeveleri kontrol süreçleri olgunlaştıkça bu değişim pek çok işletmede yaşanacaktır.

Güvence ve danışmanlık hizmetlerinde bilgi, finansal ve finansal olmayan, geçmiş veya geleceğe yönelik bilgi olarak karşımıza çıkabilir. Elde edilen bilginin güvenilirliği açısından iç denetçi işletmenin yüz yüze olduğu riskleri belirler ve değerlendirerek katkı sağlar. İç denetçiler risk yönetim sürecinin bir gereği olarak risk önceliklendirmesi yapmalı ve karşılaşılan riskleri kontrol etmek ve azaltmak için harcanan çabaları değerlendirmelidir.

2.2.3.2. Kurumsal yönetim ile ilişkilere etkisi

Yönetim anlayışındaki değişimler, küreselleşme, teknolojik gelişmeler, yasal düzenlemeler ve diğer faktörler ile işletmelerin büyümesi sonucu işletme yönetiminde profesyonellik ön plana çıkmıştır. Böylece işletmenin sahipleriyle işletmeyi yönetenler birbirinden ayrılmaya başlamıştır. Sonuç olarak işletmeyi fiilen yöneten yöneticiler hem işletme, hem de toplum için çok kritik görev yapan kişiler konumuna gelmeye başlamıştır. Çünkü profesyonel yöneticiler verdikleri kararlarla sadece kendi işletmeleri üzerinde değil, bütün toplumun kaynak kullanımı üzerinde etkili olabilmektedir. Diğer bir ifadeyle işletmeler, etraflarındaki çıkar gruplarının (paydaşlar) istek ve beklentilerini dikkate alarak faaliyette bulunmak ihtiyacını hissetmeye başlamışlardır (Kurnaz, 2007: 126).

Kurumsal yönetim, risk ve uyumluluk faaliyetlerinin etkinliğinin artırılmasının her geçen gün biraz daha fazla önem kazanmasının yanı sıra birçok işletme bu konulara verimliliği artırmanın yollarını aramaktadır.

İşletmelerde kurumsal yönetim ilkelerinin uygulaması ve yönetim kurulunun denetçilerce desteklenmesi, denetçilerin çalışmalarındaki ve denetim kaynaklarının kullanımındaki etkinliği artırır. Böylece, denetçiler şirketin iş stratejilerini, risk yönetimini değerlendirebilir ve problemler alanlar üzerinde yoğunlaşmak için daha az vakit harcar (Kurnaz, 2007: 38).

Risk odaklı iç denetim yaklaşımı temelde kurumsal yönetim anlayışına dayanır ve kurumsal yönetimin etkin bir biçimde uygulanıp uygulanmadığını saptamaya çalışır. Bu bağlamda Risk odaklı iç denetim, risk yönetimi ve kurumsal yönetim anlayışının ayrılmaz bir parçası durumundadır. Risk odaklı iç denetim sürecinde uygun bir risk yönetim bölümünün kurulması ve risklerin yönetilmesi konusunda iç denetim bölümüne önemli görevler düşmektedir (Uzay, 2003: 228).

Bilgi teknolojileri kontrollerini değerlendirmek, sürekli bir süreçtir. Bilgi teknolojileri gelişmeye devam ettikçe, iş süreçleri de değişir ve çeşitli zayıf noktalar çıktıkça tehditler artar. Burada yönetime düşen sorumluluk kontrol ölçülerini ve raporlamasını yönetmektir. İç denetçiler ise bu raporların geçerliliğini onaylar ve görüş bildirir. İç denetçiler raporlama güvenceleri konusunda yönetimle ve denetim komitesiyle iletişim içinde olmalıdır (Alptürk, 2008b: 274).

Bilgi teknolojileri kurumsal yönetim odaklarını şöyle açıklayabiliriz (Erhan, 2009: 101):

1. *Stratejik odaklanma*: İşletme ve bilgi teknolojileri planlarının bütünleştirilmesi bilgi teknolojileri tarafından yaratılan değerlerin tanımlanması, sürdürülmesi ve doğrulanması bilgi teknolojilerinin kurumsal faaliyetlerle örtüşmesini sağlar.
2. *Değer yaratma*: Bilgi teknolojilerinin değer yaratması, bilgi teknolojilerinin strateji kapsamında taahhüt ettiği kazançları sağlaması, maliyetlerin optimizasyonu ve bilgi teknolojilerinin yapısal değerinin kanıtlanması ile ilgilidir.
3. *Kaynak yönetimi*: Optimal kaynak yatırımı, yazılım, bilgi, altyapı ve insan gibi kritik bilgi teknolojileri kaynaklarının uygun biçimde yönetilmesiyle ilişkilidir.
4. *Risk yönetimi*: Üst düzey yöneticiler ve risk farkındalığı yaratılması, kurumsal bir tutum oluşturma, tanımlanmış riskler için kurumsal saydamlığın sağlanması ve kurum içinde risk yönetim sorumluluklarının yerleştirilmesi ile ilgilidir.
5. *Performans ölçümü*: Geleneksel maliyet yöntemlerinin ötesinde hedeflere ulaşmada stratejinin eyleme dönüştürülmesine hizmet eden kurumsal karnelerin kullanımıyla stratejik sonuçların, proje kapanışları, kaynak kullanımı, süreç başarımları ve hizmet üretiminin izlenmesi ve eğilimlerin gözlenmesidir.

2.3. Kontrol Özdeğerlendirme Sürecindeki Etkiler

Küreselleşen ekonomik yaşamın ihtiyaçları doğrultusunda işletmelerde her türlü kaynağın etkin kullanılması suretiyle; işletmeye değer katma ve işletme hedeflerinin

gerçekleştirilmesine katkıda bulunma ihtiyacı, geleneksel denetimin yerini kontrol öz değerlendirme uygulamalarının almasına neden olmuştur. Günümüzde bilgi teknolojilerinin işletme süreçlerinde kullanımında bütünlüğün sağlanması, yürütülen işlemlerin uygunluğu ve performansının devamlılığını sağlamak otomatize olmuş ve gelişmiş kontrol mekanizmalarına ihtiyaç artmıştır. Kontrollerin değerlendirilme sonuçları denetçilerin yüksek riskli alanlara odaklanmalarını sağlamaktadır (Coderre, 2009: 50).

Günümüzde iç kontrol sisteminin değerlendirilmesinde kontrol odaklı kontrol özdeğerleme yaklaşımlarından risk odaklı kontrol özdeğerleme yaklaşımlarına geçiş olduğu görülmektedir. Kontrol odaklı yaklaşımlarda kontrollerin tasarımından önce risk değerlemesi yapılmamakta, bu da değerlendirme sırasında süreçle ilgili tüm risklerin belirlenmesini zorlaştırmaktadır. Ayrıca kontrol odaklı kontrol özdeğerleme yaklaşımında süreçlerle ilgili yeni riskler ve güncel değişiklikler dikkate alınmamaktadır. Kontrol odaklı kontrol özdeğerleme yaklaşımı kontrollerin riskle ilgili bağlantısından çok yasal düzenlemelere uygunluğuna öncelik vermektedir (Gegin, 2010: 20).

Kontrol öz değerlendirme yaklaşımlarında en çok kullanılan yöntemlerden biri olan grup çalışması kontrol özdeğerlendirme sürecinin önemli bir parçasıdır ve bir sistem geliştirme projesi veya bir tedarik faaliyetinin risk değerlemesi gibi belirli bir projenin veya faaliyetin değerlendirilmesini sağlar (Griffiths, 2005: 54).

2.3.1. Kontrol özdeğerlendirmenin uygulama sürecindeki etkiler

Kontrol özdeğerlendirme yaklaşımında öncelikli olarak işletmenin temel ve destekleyici amaçların belirlenmesi gerekir. Sonrasında da bu amaçların başarılmasına yönelik süreçlerdeki kontrollerin etkinliği incelenir. Bu değerlendirmeler sonucunda kontrollerin güçlü ve zayıf yanları ortaya çıkarılmış olacaktır (Coderre, 2009: 49).

Bilgi teknolojilerindeki gelişmeler, finansal işlemlerin elektronik ortamlarda ve insan faktörünün etkisini azaltarak gerçekleştirilmesini sağlamıştır. Bilgi teknolojileri sayesinde üretilen bilgilerin güvenilirliğinin yüksek düzeyde olması, iç denetimin yalnızca finansal odaklı olmasından uzaklaşmasına neden olmuştur. Elde edilen verilerdeki güvenilirliğin artması ve zaman avantajı sağlaması nedeniyle, Kontrol özdeğerlendirme yaklaşımında da yoğun bir şekilde bilgi teknolojileri kullanımı söz

konusu olmuştur. Yapılan araştırmalar, kontrol öz değerlendirme uygulamalarında yazılım kullanımının gün geçtikçe arttığını göstermektedir. 2003 yılında yapılan Internal Auditor Software Survey araştırmasına göre Kontrol özdeğerlendirme uygulamalarında % 39'luk bir payla Excel kullanımı ön sırada gelmekte iken, CARDmap, CSA Pro, Risk Navigator ve TeamMate gibi programların da kullandıkları belirlenmiştir (McCollum ve Salierno, 2003: 34-35;).

Kontrol öz değerlendirme uygulamaları esnektir. Her bir işletme için farklı uygulamalar söz konusu olabilmektedir. Değerlendirme yapılacak işletme için doğru yöntemin tespiti, işletmenin kültürüne ve çalışmadan beklenen sonuçlara göre yukarıdaki yöntemlerden biri veya birkaçı kullanılabilir. Hangi yöntem belirlenirse belirlensin önemli olan nokta, özdeğerlendirme çalışmasının işletme performansının iyileştirilmesine yönelik olması gerektiğidir. Uygulamada kritik olan unsurlar; özdeğerlendirme uygulamasının üst yönetim tarafından kabul edilmesi, iyi planlanması, değerlendirme ekip veya ekiplerinin oluşturulup, eğitilmesi, planların duyurulması ve uygulanmasıdır (KALDER, 2005: 13).

Kontrol özdeğerlendirmesi, iç kontrol sistemlerinin etkinliği hakkında önemli bilgiler sunar. İç kontrollere rağmen gerçekleşen işlemlere ilişkin verilerin tespit edilmesi, bunların gözden geçirilmesi ve hata ve anormalliklerinin azaltılmasında kontrol özdeğerlendirmenin faydası görülmektedir. Kontrol özdeğerlendirme tasarlanan kontrol testleri aracılığıyla verilerin analizine yardımcı olur. Bu testler COSO çerçevesine dayanmaktadır. Kontroller, bilgilerin gizliliğini, bütünlüğünü, kullanılabilirliğini ve güvenilirliğini garantilemelidir.

2.3.2. İç denetim faaliyetinde kontrol özdeğerlendirmenin rolü

Kontrol özdeğerlendirme, yönetimin risk yönetimi ve kontrolü süreçlerini kurma ve uygulama ve bu sistemin yeterliliğini değerlendirme konularındaki sorumluluk ve görevlerini yerine getirmesinde yönetime yardımcı olarak iç denetim faaliyetinin geleneksel rolünü artırır. Kontrol özdeğerlendirme vasıtasıyla iç denetim birimi ve ilgili iş birimleri kontrol süreçlerinin iyi çalışıp çalışmadığı ve artık risklerin önem düzeyi gibi konularda bilgi üretme konusunda işbirliği yapar. Kontrol özdeğerlendirme programı, işletme içinde kontrol süreçlerini değerlendirme kapsamını arttırmalı, süreç sahiplerinin aldığı düzeltici tedbirlerin kalitesini geliştirmeli ve iç denetim

alışmalarının risk taşıyan süreçler ve olağın dışı durumların incelenmesi üzerinde odaklanmasına yardımcı olmalıdır (TİDE, 2008: 333-334).

Dördüncü Bölüm

Bilgi Teknolojilerinin İç Denetimde Yarattığı Değişimlerin İç Denetim Birimleri Tarafından Değerlendirilmesi: İMKB-100 Araştırması

1. Araştırmanın Amacı

Bilgi teknolojilerinde meydana gelen değişimler işletmelerde iş yapma şekillerini etkilemiş ve dolayısıyla fiziki belgeleme ile yapılan denetim faaliyetleri de geleneksel yaklaşımlardan bilgisayarla gerçekleştirilen denetim yaklaşımlarına doğru kaymıştır. Giderek karmaşıklaşan ve hızla gelişen bilgi teknolojileri çevresinin sağladığı fırsatlar ve yarattığı riskler, iç denetim faaliyetinin faaliyet alanlarının genişlemesine ve yeni denetim türlerinin uygulanmasına neden olmuştur. İşletmelerdeki iş yapma ve bilgiyi işleme şekillerinin gösterdiği hızlı gelişim, ortaya çıkan yeni yaklaşımlar ve genişleyen faaliyet alanları, iç denetimin güvence ve danışmanlık hizmetlerine ilişkin işlevleri ön plana çıkarmıştır.

Araştırmamızın amacı, işletmelerde bilgi teknolojilerindeki değişimler sonucu iç denetimin işlevlerinde ve sürecinde meydana gelen değişimleri araştırmak ve iç denetimden sorumlu tarafların bu değişimlere uyumunu irdeleyerek, değişimleri nasıl değerlendirdiklerini ortaya koymaktır.

2. Evren ve Örneklem

Ana kütle İMKB-100 endeksinde yer alan işletmelerdir. Çünkü bu işletmeler işlem hacimleri, faaliyet konuları ve büyüklükleri, iç denetimi gerektirecek unsurlar içermeleri nedeniyle yaşanan değişimlerin öncüleri durumundadır. Bu amaçla İMKB Hisse Senetleri Piyasası Bilgileri²⁹ kullanılarak bu işletmeler belirlenmiştir. Anketler, işletmelerin internet adreslerinden veya Kamuyu Aydınlatma Platformu³⁰ (KAP)'nın İMKB-100'de işlem gören işletmelere ilişkin yayınladığı genel bilgi formlarından yararlanılarak belirlenen iç denetim alanında sorumluluğu olan iç denetçi, iç denetim

²⁹<http://www.imkb.gov.tr/Data/StocksData.aspx>

³⁰ <http://www.kap.gov.tr/yay/Sirket/sirketListe.aspx>

birimi yöneticisi, denetim koordinatörü, mali işler müdürü, muhasebe müdürü pozisyonunda yer alan isimlere, eğer bu pozisyonlar internette yer almıyorsa genel müdür pozisyonundaki yetkililere gönderilmiştir.

Çalışmamızda anketimizi cevaplayan katılımcılar işletmedeki konumları açısından genel müdür yardımcısı, muhasebe müdürü, mali işler koordinatörü, denetim koordinatörü, iç kontrol koordinatörü, iç kontrol koordinatör yardımcılığı gibi birim bazında müdürlük, koordinatörlük ve koordinatör yardımcılığı görevlerinde bulunmaktadır. Ayrıca genellikle işletmelerde kurmay bir birim olarak görevlendirilen ve koordinatörlüklere eş pozisyonda yer alan iç denetim biriminin yöneticileri, yardımcıları ve birimde çalışan iç denetçiler de çalışmamızda yer almaktadır. Çalışmamızda iç kontrol koordinatör yardımcıları ve iç denetim yönetici yardımcıları yerine getirdikleri görevlerin birbirini tamamlayıcılığı açısından birlikte değerlendirilmiştir.

İMKB 100’de işlem gören bu işletmeler, 01.04.2011-30.06.2011 tarihleri arasında işlem gören en yüksek piyasa değerine sahip ilk 100 şirketi kapsamaktadır. Bu işletmelerin 81 tanesi üretim, ulaştırma-lojistik, elektrik-elektronik-enerji, turizm, inşaat, ticaret, teknoloji, iletişim, madencilik, spor ve diğer sosyal hizmetler sektörünü oluşturmakta iken, 19 tanesi ise bankacılık ve finans sektöründe yer almaktadır. Bankacılık ve finans sektöründeki işletmeler kendi iç yönetmeliklerine ilişkin özellikli durumlar nedeniyle araştırmamızın dışında tutulmuştur. 81 işletmeden 4 tanesi muhasebe ve mali işler bölümlerindeki iş yoğunluğu, 6 tanesi de işletmelerinde iç denetim biriminin bulunmaması nedeniyle anketi cevaplamamışlardır. Kalan 71 işletmeye anketler uygulanmıştır. Geri dönen ve değerlendirilen anket sayısı ise 51’dir.

3. Araştırma Yöntemi

3.1. Verilerin Toplanması

Çalışmamızda veri toplama yöntemi olarak anket tekniği kullanılmıştır. Anket uygulaması pilot uygulamayı da kapsayacak şekilde gerçekleştirilmiştir. 08.05.2011 tarihinde başlayan anket uygulamasında 28.05.2011 tarihinde kadar elde edilen anketler pilot uygulama kapsamında değerlendirilerek, ankette herhangi bir değişiklik gerekip gerekmediği değerlendirilmiş ve elde edilen sonuçlara göre anket uygulamasına devam edilmiştir. Anket uygulaması 16.07.2011 tarihinde tamamen sonlandırılmıştır.

Anket uygulamasının gerçekleştirilmesi sürecinde anket dört şekilde katılımcılara ulaştırılmıştır. Birincisi, internet ortamında hazırlanmış on-line anket linkinin katılımcılara e-mail olarak gönderilmesidir. İkincisi, anket çıktısının katılımcıların adreslerine postayla gönderilmesidir. Üçüncü olarak Türkiye İç Denetçiler Enstitüsü'nün desteği alınmıştır. TİDE'nin düzenlediği Mayıs 2011 Mesleki Gelişim Eğitimlerinde çalışmamızla ilgili olan örnekleme oluşturan katılımcılar tespit edilerek anketi cevaplamaları sağlanmıştır. Son olarak da anket yapılacak kişiler ile önceden randevu alınarak yüzyüze görüşülmüş ve anket formu bu görüşme sırasında katılımcı tarafından cevaplanmıştır.

3.2. Anketin Hazırlanması ve Anket Sorularının İçeriği

Anket soruları, dünyada iç denetim alanındaki önemli kurum ve kuruluşların önderliğinde yürütülmüş olan çeşitli çalışmalardan uyarlanarak hazırlanmıştır. Bu çalışmalar aşağıda belirtilmektedir:

1. A Global Summary Of Common Body Of Knowledge (CBOK) 2006- The Institute Of Internal Auditors (IIA)---Ortak Bilgi Tabanının Küresel Bir Özeti 2006-İç Denetçiler Enstitüsü
2. IT Auditor Benchmarking Study (2009)- The Institute Of Internal Auditors (IIA)/GAIN (Global Audit Information Network)---Bilgi Teknolojileri Denetçileri Kıyaslama Çalışması (2009) İç Denetçiler Enstitüsü/Küresel Denetim Bilgi Ağı
3. Global Auditor Executives Survey (2006)- The Institute Of Internal Auditors (IIA) & ACL Services Ltd.---Küresel Denetçi Yöneticileri Anketi- İç Denetçiler Enstitüsü ve ACL Ltd. ortak çalışması.
4. The Internal Auditor Software Survey (2006)-The Institute Of Internal Auditors (IIA)---İç Denetçiler Yazılım Anketi (2006)-İç Denetçiler Enstitüsü.
5. Continuous Auditing And Monitoring (2010)-KPMG International Cooperative---Sürekli Denetim ve İzleme (2010)- KPMG.
6. SOX Compliance Survey (2004)-ACL Services Ltd. & S.C.I. Research---Sarbanes-Oxley (SOX) Yasası Uyum Anketi (2004)- ACL Ltd. ve Sürekli Denetim Merkezinin görevlendirdiği S.C.I. Research ortak çalışması.

7. XBRL Global Executives Summary (2008)- The Institute Of Internal Auditors (IIA)/GAIN (Global Audit Information Network)--- Genişletilmiş İşletme Raporlama Dili (XBRL) Küresel Yönetici Anketi (2008)-İç Denetçiler Enstitüsü/Küresel Denetim Bilgi Ağı.
8. XBRL Survey Of Chartered Accountants (2006)- Alex Davidson, Artie Robinson and Sue Malthus. Survey of Chartered Accountants Shows XBRL Slow to Catch On, Chartered Accountants Journal, 85 (9): 68-70.- --Yeminli Mali Müşavirler için Genişletilmiş İşletme Raporlama Dili (XBRL) Anketi.

Ankette toplam 72 soru yer almaktadır. Anket soruları katılımcının ve çalıştığı işletmenin demografik özelliklerinin sorulduğu sorularla başlamaktadır (1-15. sorular arası). İkinci bölüm işletmedeki iç denetim biriminin şimdiki ve gelecekteki durumu dikkate alınarak iç denetimin işlevleri, faaliyet alanları ve türlerinde meydana gelen değişimlerin değerlendirilmesi ve iç denetim faaliyetini yerine getirirken karşılaşılan zorlukları içermektedir (16 ve 17. sorular). Üçüncü bölümde bilgi teknolojileri, bilgi teknolojileri denetimi, bilgi teknolojileri uygulamaları ile ilgili sorular (18.-44. sorular arası); dördüncü bölümde sürekli denetim, risk odaklı iç denetim ve kontrol öz değerlendirme ile ilgili sorular (45.-63. sorular arası); beşinci bölümde ise güvence ve danışmanlık hizmetleri, iç kontrol, risk yönetimi ve kurumsal yönetim ile ilgili sorular yer almaktadır (64.-72. sorular arası).

3.3. Araştırma Kısıtları

Anket uygulamasının yapıldığı alanda çalışanlar son derece yoğun bir iş ortamında bulunmaktadır. İş yoğunluğu nedeniyle anket uygulamasına katılma isteği düşmüştür. Bu da anket uygulaması açısından son derece önemli bir kısıtlamadır. İşletmeler anket uygulaması için rica edilen randevu taleplerine geç cevap vermekte veya cevap vermemektedir. Bu durum da anketin uygulama süresini uzatmaktadır.

Ayrıca iç denetçilerin veya iç denetim alanında sorumluluğu olan yöneticilerin bazı konularda günceli takip edememeleri ve bilgi yetersizlikleri de anketin cevaplanma isteğini azaltmıştır. Bu durum da anket uygulaması açısından son derece önemli bir kısıtlamadır.

4. Araştırma Soruları

İMKB-100 endeksinde işlem gören işletmelerde iç denetimden sorumlu tarafların bilgi teknolojilerindeki değişimler sonucu iç denetimin işlevlerinde ve sürecinde meydana gelen değişimleri değerlendirmelerine yönelik hazırlanan bu çalışma “durum tespiti” kapsamında ele alınmıştır.

Bu bağlamda çalışmanın araştırma sorularının içeriği şunları kapsamaktadır:

- İç denetimin işlevlerinde, faaliyet alanlarında ve türlerinde meydana gelen değişimlerin ve iç denetim faaliyetinin yerine getirilmesi sırasında karşılaşılan zorlukların değerlendirilmesi,
- Bilgi teknolojilerindeki gelişmelerle birlikte iç denetimin ön plana çıkan işlevlerinden olan güvence ve danışmanlık hizmetlerinin değerlendirilmesi,
- Sürekli denetim, risk odaklı iç denetim ve kontrol öz değerlendirme yaklaşımlarına ilişkin süreçlerin değerlendirilmesi,
- İç denetimin genişleyen faaliyet alanları olan risk yönetimi, iç kontrol ve kurumsal yönetim süreçlerinin değerlendirilmesi,
- Bilgi teknolojileri uygulamalarının iç denetim ile ilişkilerinin değerlendirilmesi,
- Bilgi teknolojileri denetiminin işletmelerde uygulanma durumunun değerlendirilmesi.

5. İstatistiksel Analiz Bulguları ve Yorumlar

Çalışmamızın anket uygulamasından elde edilen verilere uygulanan güvenilirlik analizi, Komorogov-Smirnov Normallik Varsayımı testi, frekans analizi, çapraz tablo analizi, Kruskal-Wallis Testi ve Spearman’s Rank Order Korelasyonu uygulanmıştır. Yapılan analizlere ilişkin teorik bilgiler Ek-4’te yer almaktadır. Analizlere ilişkin tablolar metin içinde oldukça fazla yer kapladığından ve metni böldüğünden bazıları Ek-1’de verilecektir. Metin içinde analiz sonuçları ile ilgili bilgiler verilirken ilgili tablolara da atıfta bulunulacaktır.

5.1. Güvenilirlik Analizi ve Verilerin Dağılımı

Çalışmamızda elde edilen verilerin değerlendirilmesi SPSS 16.0 istatistik programında gerçekleştirilmiştir. Elde edilen verilerin güvenilirlik analizi sonuçlarına bağlı olarak anket sorularının güvenilirliği 0.964 (% 96,4) olarak bulunmuştur.

Çalışmamızda verilerin normal dağılıp dağılmadığını test amacıyla Kolmogorov-Smirnov (K-S) normallik varsayımı testi uygulanmıştır. 0,05 anlamlılık düzeyine göre Kolmogorov-Smirnov testi için anketimizdeki tüm sorulara verilen cevaplardan elde edilen tüm verilerin p değerlerinin 0,05'ten küçük olması nedeniyle normallik varsayımının reddedildiği, dolayısıyla verilerin normal dağılım göstermediği sonucuna ulaşılmıştır. Kolmogorov-Smirnov testi sonuçları EK-1 Tablo-105'den incelenerek p değerinin 0,05'ten küçük değerleri gösterdiği görülebilir.

5.2. Demografik Sorular İle İlgili Frekans Analizleri

Ankete katılanların ve çalıştıkları işletmelerin demografik özelliklerine ilişkin bulgular bu başlık altında değerlendirilecek olup demografik özelliklere ilişkin gösterim EK-1 Tablo-74'de yapılmıştır.

Ankete katılanların 43'ü (% 84,3) erkek ve 8'i (%15,7) kadın olmak üzere toplam 51 kişiden oluşmaktadır. Katılımcıların 3'ü 30 ve altı yaş grubunda yer alırken, 20'si 31-35 yaş, 14'ü 36-40 yaş, 10'u 41-45 yaş ve 4'ü de 46-50 yaş grubunda yer almaktadır. Katılımcılarının çoğunun 31-35 yaş ve 36-40 yaş olduğu görülmektedir. 32 kişi lisans mezunu iken, 19 kişi de yüksek lisans mezunudur.

Ankete katılanların işletmedeki konumlarına baktığımızda 19 kişi iç denetçi, 10 kişi iç denetim yöneticisi, 7 kişi muhasebe müdürü, 3 kişi genel müdür yardımcısı, 3 kişi mali işler müdürü, 2 kişi denetim koordinatörü, 4 kişi iç kontrol koordinatörü, 2 kişi iç kontrol koordinatör yardımcısı ve 1 kişi iç denetim yöneticisi yardımcısıdır.

Ankete katılanların sahip oldukları mesleki sertifikalara baktığımızda 12 kişi Uluslararası İç Denetçi (CIA), 4 kişi Uluslararası Kamu Denetçisi (CGAP), 1 kişi Kontrol Özdeğerlendirme Sertifikası (CCSA), 1 kişi Uluslararası Finansal Hizmetler Denetçisi (CFSA), 12 kişi Mali Müşavirlik (CA/CPA/ACCA/ACA), 4 kişi Hile Denetçisi (CFE), 1 kişi Sertifikalı Finansal Analist (CFA), 1 kişi Profesyonel Risk Yöneticisi Sertifikası (Associate PRM) ve 1 kişi Kurumsal Yönetim Derecelendirme

Sertifikası sahibidir. Ankete katılanlardan 14 kişinin herhangi bir mesleki sertifikası yoktur.

Katılımcıların 19'u 10 yıl ve üzeri bir zamandır, geri kalan 32 kişinin yarısı (16 kişi) 4-6 yıldır şu an çalıştığı işletmede görev yapmaktadır. Geri kalan 16 kişiden 5'i 7-9 yıldır, 7'si 1-3 yıldır ve 4 kişi de 1 yıldan az bir süredir şu an çalıştığı işletmede görev yapmaktadır.

Bu katılımcıların 1'i işletmelerinde 1 yıldan az bir süredir, 16'sı 1-5 yıldır, 7'si 6-10 yıldır ve bir diğer 16'sı da 11-15 yıldır iç denetim biriminin faaliyet gösterdiğini bildirmiştir. 21 yıl ve üzeri bir süredir işletmelerinde iç denetim biriminin faaliyet gösterdiğini bildirenler ise sadece 4 kişidir.

Ankete katılanların çalıştıkları işletmeler üretim (gıda, kimya, otomotiv, metal eşya, taş, toprak, kağıt, cam) (28 kişi), ulaştırma-lojistik (2 kişi), elektronik-elektrik-enerji (6 kişi), turizm (1 kişi), inşaat (2 kişi), toptan ve perakende ticaret (5 kişi), teknoloji-iletişim (4 kişi), spor ve diğer sosyal hizmetler (yazılı basın vb.) (3 kişi) sektörlerinde faaliyet göstermektedir.

5.3. Çapraz Tablo Analizleri ve Non-Parametrik Testler

Çalışmamızda elde edilen analiz sonuçları “iç denetimin birimi” , “iç denetimin güvence ve danışmanlık hizmetleri işlevleri”, “iç denetim yaklaşımları”, “iç denetimin faaliyet alanları”, “bilgi teknolojileri uygulamaları” ve “bilgi teknolojileri denetimi”olarak gruplanmıştır.

Elde edilen verilerle çapraz tablo analizleri ve non-parametrik testler yapılmıştır. Yapılan çapraz tablo analizleri ankete katılanların işletmedeki konumları açısından ele alınmıştır. Non-parametrik testlerde ise Kruskal-Wallis testi ve Spearman's Rank Order Korelasyonu uygulanmıştır. Yapılan bu testlerden sadece sonuçları anlamlı olanlara çalışmamızda yer verilmiştir.

5.3.1. İç denetim birimi ile ilgili çapraz tablo analizleri ve non-parametrik testler

5.3.1.1. İç denetim birimi ile ilgili çapraz tablo analizleri

İç denetim birimi ile ilgili çapraz tablo analizleri katılımcıların işletmedeki konumları itibarıyla düzenlenmiştir. Ankete katılanlar iç denetim biriminin şimdiki durumunu ve gelecekteki durumunu dikkate alarak “iç denetimin işlevlerinde”, “faaliyet alanlarında” ve “türlerinde” meydana gelen değişimleri değerlendirmişlerdir.

- İç denetimin işlevleri ile katılımcıların konumları arasındaki ilişki:

Güvence hizmetleri:

Tablo-6. Ankete Katılanların İşletmedeki Konumları*Güvence Hizmetlerinin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler

Konum Güvence Hizmetlerindeki Değişimler	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Şimdi--Azaldı Gelecek--Azalacak	0 0	0 0	1 1	0 0	0 0	0 0	0 0	1 1
Şimdi --Aynı kaldı Gelecek-Aynı kalacak	7 8	2 2	1 1	1 1	0 0	0 0	0 0	11 11
Şimdi --Arttı Gelecek--Artacak	12 11	9 9	1 1	6 6	3 3	2 2	4 4	39 38

Tablo-6’da görüldüğü üzere katılımcıların çoğu güvence hizmetlerinin geçmişe oranla arttığını bildirirken (39 kişi), iç denetçi, iç denetim yöneticisi, muhasebe müdürleri ve genel müdür yardımcılarında oluşan 11 kişilik bir katılımcı grubu ise geçmişe oranla bu işlevin aynı kaldığını bildirmiştir. Gelecekte ise yine katılımcıların çoğu (38 kişi) bu işlevin artacağını bildirirken, şimdiki durumda olduğu gibi yine aynı katılımcı grubu aynı kalacağını bildirmiştir.

Danışmanlık hizmetleri:

Tablo-7. Ankete Katılanların İşletmedeki Konumları*Danışmanlık Hizmetlerinin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler

Konum Danışmanlık Hizmetlerindeki Değişimler	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Şimdi—Azaldı	0	0	0	0	0	0	0	0
Gelecek--Azalacak	1	1	0	0	0	0	0	2
Şimdi --Aynı kaldı	8	3	1	1	1	1	1	16
Gelecek-Aynı kalacak	1	0	1	1	0	0	1	4
Şimdi –Arttı	11	8	2	6	2	1	5	35
Gelecek—Artacak	17	10	2	6	3	2	5	45

Tablo-7’de görüldüğü üzere katılımcıların çoğu güvence hizmetlerinin geçmişe oranla arttığını bildirirken (35 kişi), 16 kişi ise geçmişe oranla bu işlevin aynı kaldığını bildirmiştir. Gelecekte ise katılımcıların çoğu (45 kişi) danışmanlık hizmetinin artacağını, 4 kişiden oluşan iç denetçi, genel müdür yardımcısı, muhasebe müdür ve iç kontrol koordinatöründen oluşan bir grup ise aynı kalacağını bildirmiştir.

Özetle, bilgi teknolojilerindeki gelişmelerle birlikte iç denetimin güvence ve danışmanlık hizmetlerinin geçmişe nazaran arttığı ve gelecekte de artacağını söyleyebiliriz. Bu durum güvence ve danışmanlık hizmetlerinin işletmeye sağladığı katma değerın işletmeler tarafından her geçen gün daha iyi anlaşıldığını düşündürmektedir.

- İç denetimin faaliyet alanları ile katılımcıların konumları arasındaki ilişki:

İç kontrol sisteminin izlenmesi ve incelenmesi:

Tablo-8. Ankete Katılanların İşletmedeki Konumları*İç kontrol Sistemini İzleme ve İncelemenin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler

Konum İç kontrol Sistemini İzleme ve İnceleme Değişimler	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Şimdi—Azaldı	1	1	0	0	0	0	0	2
Gelecek--Azalacak	1	1	0	0	0	0	0	2
Şimdi --Aynı kaldı	11	1	2	0	1	1	2	18
Gelecek-Aynı kalacak	6	0	2	0	0	0	0	8
Şimdi –Arttı	7	9	1	7	2	1	4	31
Gelecek—Artacak	12	10	1	7	3	2	6	41

Tablo-8’e göre katılımcıların çoğunluğu (31 kişi) iç denetim sisteminin izleme ve inceleme faaliyetinin geçmişe oranla arttığını, çoğunluğunu iç denetçilerin

oluşturduğu 18 kişilik bir grup ise aynı kaldığını bildirmiştir. Gelecekte ise yine katılımcıların büyük bir kısmı (41 kişi) bu faaliyet alanının artacağını bildirmiştir. Sadece iç denetçi ve genel müdür yardımcılarında oluşan 8 kişilik bir katılımcı grubu ise aynı kalacağı yönünde fikir bildirmiştir.

Risk yönetimi:

*Tablo-9. Ankete Katılanların İşletmedeki Konumları*Risk Yönetimin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler*

Konum Risk yönetimi	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Şimdi--Azaldı	1	1	0	0	0	0	0	2
Gelecek--Azalacak	1	1	1	0	0	0	0	3
Şimdi --Aynı kaldı	11	2	2	0	1	1	1	18
Gelecek-Aynı kalacak	1	0	0	1	0	0	0	2
Şimdi --Arttı	7	8	1	7	2	1	5	31
Gelecek--Artacak	17	10	2	6	3	2	6	46

Tablo-9'a göre katılımcıların çoğunluğu geçmişe oranla risk yönetiminin arttığını, çoğunluğunu iç denetçilerin oluşturduğu 18 kişilik bir grup ise risk yönetiminin aynı kaldığını bildirmiştir. Gelecekte ise katılımcıların çoğu (46 kişi) risk yönetiminin artacağını bildirmiştir.

Kurumsal yönetim:

*Tablo-10. Ankete Katılanların İşletmedeki Konumları*Kurumsal Yönetimin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler*

Konum Kurumsal Yönetimdeki Değişimler	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Şimdi--Azaldı	1	0	0	1	0	0	0	2
Gelecek--Azalacak	2	1	1	1	0	0	0	5
Şimdi --Aynı kaldı	12	4	2	0	1	1	1	21
Gelecek-Aynı kalacak	11	0	1	0	1	1	1	15
Şimdi --Arttı	6	6	1	6	2	1	5	27
Gelecek--Artacak	6	10	1	6	2	1	5	31

Tablo-10'da görüldüğü üzere katılımcıların çoğu kurumsal yönetimin arttığını bildirirken, aynı kaldığını bildiren katılımcıların da sayısı da oldukça fazladır (21 kişi). İç denetçilerin çoğunluğunun kurumsal yönetim alanındaki değişimi aynı kaldığı yönünde değerlendirdiği dikkat çekicidir (12 kişi). Gelecekte ise iç denetim

yöneticilerinin tümünün katıldığı (10 kişi) bir katılımcı grubu kurumsal yönetimin artacağını bildirmiştir (31 kişi). İç denetçilerin çoğunluğunu oluşturduğu 15 kişilik bir katılımcı grubu ise aynı kalacağını bildirmiştir.

Özetle, bilgi teknolojilerindeki gelişmelere paralel olarak değişen iş süreçleri işletmelerin hem risk profillerini belirlemelerini hem de iç kontrol sistemlerini bu riskler doğrultusunda oluşturmalarını gerektirmiştir. Zaten risk yönetimi ve iç kontrol uygulamaları kurumsal yönetim sürecinin de ayrılmaz parçalarıdır. Risk yönetimi, iç kontrol ve kurumsal yönetim faaliyetleri işletmelerde gerçekleştirilmekte ve bu faaliyet alanlarının gerektirdiği süreçlerin uygulanmasına da özen gösterilmektedir. Katılımcıların çoğunluğu bu konuda hem fikirdir. Fakat iç denetçilerin şimdiki durumun değerlendirilmesinde diğer gruplara nazaran biraz daha temkinli davrandıkları dikkat çekmektedir. Geleceğe ilişkin değerlendirmelerde de aynı temkinliliği gösterdikleri söylenebilir. Muhasebe müdürlerinin ve iç kontrol koordinatörlerinin iç denetimin genişleyen faaliyet alanları konusunda yapılan çalışmalarda daha çok yer aldıkları görülmektedir.

- İç denetimin türleri ile katılımcıların konumları arasındaki ilişki:

Finansal denetim:

*Tablo-11. Ankete Katılanların İşletmedeki Konumları*Finansal Denetimin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler*

Konum Finansal Denetimdeki Değişimler	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Şimdi--Azaldı	0	1	0	0	0	0	0	1
Gelecek--Azalacak	1	3	0	0	0	0	0	4
Şimdi --Aynı kaldı	12	2	2	0	1	1	1	19
Gelecek-Aynı kalacak	5	0	1	0	1	1	1	9
Şimdi --Arttı	7	8	1	7	2	1	5	31
Gelecek--Artacak	13	8	2	7	2	1	5	38

Tablo-11’de görüldüğü üzere çoğunluğunu iç denetim yöneticilerinin (8 kişi) ve muhasebe müdürlerinin (7 kişi) oluşturduğu katılımcılar finansal denetimin arttığını bildirmiştir (31 kişi). Çoğunluğunu iç denetçilerin oluşturduğu bir grup ise aynı kaldığını belirtmiştir (19 kişi). Gelecekte ise katılımcıların çoğu finansal denetimin artacağını bildirirken (38 kişi), şimdiki durumun tersi olarak bu kez bu grubun çoğunluğunu iç denetçilerin oluşturduğu dikkat çekmektedir.

Uygunluk denetimi:

*Tablo-12. Ankete Katılanların İşletmedeki Konumları*Uygunluk Denetiminin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler*

Konum Uygunluk Denetimindeki Değişimler	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Şimdi--Azaldı	0	1	0	0	0	0	0	1
Gelecek--Azalacak	1	3	0	0	0	0	0	4
Şimdi --Aynı kaldı	7	1	2	1	0	0	0	11
Gelecek-Aynı kalacak	6	0	2	0	0	0	0	8
Şimdi --Arttı	12	9	1	6	3	2	6	39
Gelecek--Artacak	12	8	1	7	3	2	6	39

Tablo-12’de görüldüğü üzere katılımcıların çoğu uygunluk denetiminin geçmişe oranla arttığını bildirmiştir (39 kişi). Kısmen artacağını bildiren 11 kişi içinde ise iç denetçi ve genel müdür yardımcıları çoğunluktadır. Gelecekte ise çoğunluk (39 kişi) uygunluk denetiminin artacağını bildirmiştir. Kısmen artacağını bildirenler grubunda ise sayı şimdiki durum değerlendirmesine oranla azalmıştır (8 kişi), fakat yine iç denetçiler ve genel müdür yardımcıları bu grup içerisinde.

Faaliyet denetimi:

*Tablo-13. Ankete Katılanların İşletmedeki Konumları*Faaliyet Denetiminin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler*

Konum Faaliyet Denetimindeki Değişimler	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Şimdi--Azaldı	0	0	0	0	0	0	0	0
Gelecek--Azalacak	1	1	0	0	0	0	0	2
Şimdi --Aynı kaldı	8	2	2	1	0	0	0	13
Gelecek-Aynı kalacak	7	2	2	1	0	0	0	12
Şimdi --Arttı	11	9	1	6	3	2	6	38
Gelecek--Artacak	11	8	1	6	3	2	6	37

Tablo-13’de görüldüğü üzere katılımcıların çoğunluğu faaliyet denetiminin geçmişe oranla arttığını bildirmiştir (38 kişi). Kısmen artacağını bildirenler ise iç denetçilerin ve genel müdür yardımcılarının çoğunlukta olduğu 13 kişiden oluşmaktadır. Faaliyet denetiminin azaldığını bildiren olmamıştır. Gelecekte ise katılımcıların çoğu faaliyet denetiminin artacağını bildirirken (37 kişi), kısmen artacağını bildirenler de (12 kişi) bulunmaktadır. Dolayısıyla kısmen de olsa faaliyet denetiminin hem mevcut durumda hem de gelecekte artış eğiliminde olduğu konusunda görüş birliği vardır.

Bilgi teknolojileri denetimi:

*Tablo-14. Ankete Katılanların İşletmedeki Konumları*Bilgi Teknolojileri Denetiminin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler*

Konum BT Denetimindeki Değişimler	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Şimdi--Azaldı	0	0	0	0	0	0	0	0
Gelecek--Azalacak	0	0	0	0	0	0	0	0
Şimdi --Aynı kaldı	2	4	1	1	0	0	0	8
Gelecek-Aynı kalacak	2	1	1	1	0	0	0	5
Şimdi --Arttı	17	6	2	6	3	2	6	42
Gelecek--Artacak	17	9	2	6	3	2	6	45

Tablo-14'e göre katılımların büyük bir çoğunluğu BT denetiminin attığını (42 kişi) ve gelecekte de artacağını bildirmiştir (45 kişi). Aynı kaldığı yönünde az sayıda katılımlar olmakla birlikte BT denetiminin hem mevcut durumda hem de gelecekte artış eğiliminde olduğu konusunda görüş birliği vardır.

Sistem denetimi:

*Tablo-15. Ankete Katılanların İşletmedeki Konumları*Sistem Denetiminin Şimdiki ve Gelecekteki Durumunda Meydana Gelen Değişimler*

Konum Sistem Denetimindeki Değişimler	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Şimdi--Azaldı	0	0	0	0	0	0	0	0
Gelecek--Azalacak	0	0	0	0	0	0	0	0
Şimdi --Aynı kaldı	1	1	1	1	0	0	0	4
Gelecek-Aynı kalacak	8	1	2	1	0	0	0	12
Şimdi --Arttı	18	9	2	6	3	2	6	46
Gelecek--Artacak	11	9	1	6	3	2	6	38

Tablo-15'e göre katılımcıların çoğu (46 kişi) tarafından sistem denetiminin geçmişe oranla arttığı bildirilmiştir. Gelecekte ise artacağını bildirenlerin sayısı biraz düşmekle birlikte yine katılımcıların çoğu (38 kişi) sistem denetiminin artacağını bildirmiştir. Aynı kaldığını bildirenlerin sayısı (12 kişi) ise şimdiki duruma kıyasla artmıştır ve bu artışa neden olanlar iç denetçilerdir.

Özetle, iç denetim türleri açısından işletmelerde finansal, uygunluk, faaliyet, bilgi teknolojileri ve sistem denetimlerinin mevcut durumda büyük bir çoğunlukla gerçekleştirildiği ve ileriki zamanlarda da gerçekleştirilmeye devam edeceği söylenebilir. Özellikle bilgi teknolojileri ve sistem denetimi uygulamalarının diğer denetim türlerine kıyasla daha fazla katılımcı tarafından arttığı ve gelecekte de artacağı

yönünde bildirimde bulunulması dikkat çekmektedir. Dolayısıyla bilgi teknolojilerindeki gelişmeler iç denetim türlerinin çeşitlenmesine yol açmaktadır.

- **Ankete katılanların işletmedeki konumları ile iç denetim görevlerini yerine getirirken karşılaştıkları zorluklar arasındaki ilişkiler:**

*Tablo-16. Ankete Katılanların Konumları*İç Denetim Görevini Yerine Getirirken Karşılaşılan Zorluklar*

Konum Karşılaşılan Zorluklar	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Yetenekli ve yetkili iç denetim personelinin yokluğu	2	1	0	7	1	0	0	11
Bilgi teknolojileri alt yapısının karmaşıklığı	10	5	2	0	0	0	1	18
Kontrollerin eksikliği ve yönetimin veya iş süreçlerinin yarattığı riskler	16	6	1	7	3	2	2	37
Parçalanmış ve eksik veri yapıları	9	3	0	0	2	2	3	19
İç kontrollerin test edilmesini sağlayan uygun teknolojilerin olmaması	10	1	0	1	1	2	6	21

* Ankete katılanlar birden fazla seçenek işaretleyerek soruya cevap verebilmektedir.

Tablo-16'ya göre “Kontrollerin eksikliği ve yönetimin veya iş süreçlerinin yarattığı riskler” karşılaşılan zorluklar arasında birinci sırada gelmektedir (37 kişi). Karşılaşılan bu zorluk iç denetçiler, iç denetim yöneticileri, muhasebe müdürleri, mali işler koordinatörleri ve denetim koordinatörleri tarafından daha çok vurgulanmakla birlikte diğer katımcılar tarafından da bildirilmiştir. İkinci sırada karşılaşılan zorluk ise “İç kontrollerin test edilmesini sağlayan uygun teknolojilerin olmaması”dır (21 kişi). Karşılaşılan bu zorluk iç denetçiler ve iç kontrol koordinatörleri tarafından daha fazla vurgulanırken, genel müdür yardımcılarını bunu bir zorluk olarak görmemektedir. Üçüncü sırada karşılaşılan zorluk ise “Parçalanmış ve eksik veri yapıları”dır (19 kişi). Karşılaşılan bu zorluk iç denetçiler tarafından daha fazla vurgulanmakla birlikte muhasebe müdürleri ve genel müdür yardımcılarını bunu bir zorluk olarak görmemektedir. Ayrıca “Bilgi teknolojileri alt yapısının karmaşıklığı” da önemli bir zorluk olarak görülmektedir (18 kişi). İç denetçiler, iç denetim yöneticileri ve genel müdür yardımcılarını tarafından daha fazla vurgulanmıştır. “Yetenekli ve yetkili iç denetim personelinin yokluğu”nu zorluk olarak bildiren 11 kişinin büyük bir çoğunluğunu muhasebe müdürleri (7 kişi) oluşturmaktadır.

Özetle, iç denetim yöneticileri ve iç denetçiler yukarıda belirtilen zorlukların tümüyle en çok karşılaşılan katılımcılardır. “Kontrollerin eksikliği ve yönetimin veya iş süreçlerinin yarattığı riskler” iç denetim görevinin yerine getirilmesi sırasında en çok

karşılaşılan zorluk olmaktadır. Muhasebe müdürleri, mali işler koordinatörleri ve denetim koordinatörleri için BT altyapısının karmaşıklığı bir zorluk değildir. Uzman personelin varlığı bu karmaşıklığın çözülmesinde yardımcı olacaktır. Ayrıca iç kontrollerin test edilmesini sağlayan uygun bilgi teknolojilerinin olmaması nedeniyle yaşanan sıkıntılar iç denetim faaliyetinin uygulanmasını zorlaştırmaktadır. Bu konuda iç kontrol koordinatörlerinin bu zorluğu en çok vurgulayan grup olduğu dikkat çekicidir. Yetenekli ve yetkili personel açısından iç denetim birimlerinde eksikliklerin olması en çok muhasebe müdürleri açısından zorluk yaratmakta ve iç denetim faaliyetlerinin ağırlaşmasına neden olmaktadır.

5.3.1.2. *İç denetim birimi ile ilgili non-parametrik testler*

Ankete katılanların iç denetim biriminin şimdiki ve gelecekteki durumunu değerlendirmelerinde iç denetimin işlevleri, faaliyet alanları ve türlerindeki değişimler ile katılımcıların konumları arasında anlamlı farklılıkların olup olmadığını görmek için non-parametrik testlerden birisi olan Kruskal-Wallis Testi yapılmış ve yapılan analizlerde bazı anlamlı farklılıklar olduğu görülmüştür. Elde edilen sonuçların Tabloları Ek-1’de yer almaktadır.

İç denetimin işlevlerinden güvence ve danışmanlık hizmetlerinin şimdiki ve gelecekteki durumunun değerlendirilmesi ile ankete katılanların konumları arasında anlamlı farklılık bulunamamıştır.

İç denetimin faaliyet alanlarının şimdiki durumunun değerlendirilmesi ile ankete katılanların konumları arasında anlamlı farklılık bulunamamıştır. **İç denetimin faaliyet alanlarından kurumsal yönetim** açısından gelecekteki durumun değerlendirilmesi ile ankete katılanların konumları arasında anlamlı farklılıklar bulunmuştur. Kurumsal yönetim açısından iç denetim yöneticileri bu faaliyet alanının artacağı, genel müdür yardımcıları bu faaliyet alanının azalacağı yönünde değerlendirmede bulunmuştur (Ek-1 Tablo-75). Bunun nedeni iç denetimin genişleyen faaliyet alanları içerisinde kurumsal yönetimin yerini almış olması ve kurumsal yönetim ilkelerinin dikkate alınarak denetim kaynaklarının daha etkin bir şekilde kullanılabileceğidir.

İç denetimin türlerinin şimdiki ve gelecekteki durumunun değerlendirilmesi ile ankete katılanların konumları arasında anlamlı farklılık bulunamamıştır.

Özetle, bilgi teknolojilerinin işletmelerde yarattığı değişimler iç denetim işlevinin faaliyet alanlarını genişletmiş ve bu alanlarda iç denetimden sorumlu yöneticilerin ve çalışanların sorumlulukları artmıştır. İç denetimin faaliyet alanlarında yerine getirilecek tüm sorumluluklar ve yapılacak tüm çalışmalar iç denetimden beklentileri arttırmakla birlikte özellikle kurumsal yönetim sürecinin de etkinliğinin korunmasını sağlayacaktır.

5.3.2. İç denetimin güvence ve danışmanlık hizmetleri ile ilgili çapraz tablo analizleri ve non-parametrik testler

5.3.2.1. İç denetimin güvence ve danışmanlık hizmetleri ile ilgili çapraz tablo analizleri

İç denetimin BT’deki gelişmeler paralelinde ortaya çıkan işlevlerinden güvence ve danışmanlık hizmetleri ile ilgili çapraz tablo analizleri katılımcıların işletmedeki konumları itibarıyla düzenlenmiştir. Ankete katılanlar “iç denetimden sorumlu tarafların yerine getirdiği güvence hizmetleri”, “güvence hizmetlerinin yapısı”, “güvence sağlamada kullanılan yöntemler”, “danışmanlık hizmeti sağladıkları alanlar”, “danışmanlık hizmetlerinin yapısı” konularını değerlendirmişlerdir.

- Ankete katılanların konumları ile gerçekleştirilen güvence hizmetleri arasındaki ilişki:

Tablo-17. Ankete Katılanların Konumları*Yerine Getirilen Güvence Hizmetlerinin Türleri

Konum Yerine Getirilen Güvence Hizmetlerinin Türleri	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Onaylama	12	1	1	1	1	0	2	18
Finansal tablo denetimi	14	5	2	0	2	1	5	29
İç kontrolün etkinliğini sağlama	19	11	3	7	3	2	5	50
Finansal tabloların gözden geçirilmesi	7	10	2	0	1	1	4	25
WebTrust Hizmetleri	1	0	0	0	0	0	1	2
SysTrust Hizmetleri	1	0	0	0	0	0	0	1
Yatırımlara ilişkin kontroller ve risklerin değerlendirilmesi	2	2	1	0	0	0	1	6
Dijital bilgilerin biriktirilmesi, dağıtılması ve saklanması	3	6	2	0	0	0	2	13
Hile ve yolsuzluk ile ilgili risk değerlendirmesi	6	11	2	6	2	1	5	33
Ticari politika ve prosedür arasındaki uyum	7	10	2	5	2	1	5	32
Kalite sertifikasyonları	3	0	0	0	0	0	0	3
Çevre denetimi	3	4	1	1	0	0	0	9

* Ankete katılanlar birden fazla seçenek işaretleyerek soruya cevap verebilmektedir.

Tablo-17'ye göre en çok gerçekleştirilen ve katılımcıların tümünün belirttiği güvence hizmeti iç kontrolün etkinliğini sağlamaktır (50 kişi). Görüldüğü gibi denetimden sorumlu tüm taraflar hangi konumda olursa olsun önceliği iç kontrolün etkinliğini sağlamaya vermiştir. İkinci sırada hile ve yolsuzluk ile ilgili risklerin değerlendirilmesi (33 kişi) gelmektedir. Bu hizmeti en fazla vurgulayanlar ise iç denetim yöneticileri, muhasebe müdürleri ve iç kontrol koordinatörleri olmuştur. Üçüncü olarak da ticari politika ve prosedürle uyum belirtilmiştir (32 kişi). Bu hizmeti en fazla vurgulayanlar iç denetim yöneticileri, muhasebe müdürleri ve iç kontrol koordinatörleri olmuştur. Ayrıca finansal tablo denetimi (29 kişi) ve finansal tabloların gözden geçirilmesi (25 kişi) de katılımcıların çoğu tarafından vurgulanmıştır. Muhasebe müdürlerinin hiçbirisi finansal tablo denetimini ve finansal tabloların gözden geçirilmesini gerçekleştirmemektedir. İç denetçi ve iç kontrol koordinatörleri finansal tablo denetimi; iç denetim yöneticileri de finansal tabloların gözde geçirilmesi hizmetlerini daha çok vurgulamışlardır. WebTrust ve SysTrust hizmetleri katılımcıların çoğu tarafından gerçekleştirilmemektedir. Kalite sertifikasyonları ve çevre denetimleri ise genellikle iç denetçi ve iç denetim yöneticileri tarafından yerine getirilmektedir. Dijital bilgilerin biriktirilmesi, saklaması ve dağıtılması daha çok iç denetim yöneticilerin vurguladığı bir hizmettir (13 kişi).

Özetle, bilgi teknolojinin gelişimiyle birlikte iç denetim biriminin yerine getirmesi gereken bazı güvence hizmetleri ön plana çıkmıştır. Bunların arasında iç kontrol sisteminin etkinliğini sağlama ilk sırada yer almıştır. Hile ve yolsuzluklar ile ilgili risk değerlendirme hizmetleri de özellikle en çok iç denetim yöneticileri ve muhasebe müdürleri tarafından vurgulanmıştır. Ticari politika ve prosedürler arasındaki uyumu sağlama hizmeti özellikle iç denetim yöneticilerinin vurguladığı bir hizmet olmuştur. Finansal tablo denetimi ve finansal tabloların gözden geçirilmesi gerçekleştirilen güvence hizmetleri arasında muhasebe müdürleri hariç diğer katılımcıların genellikle yerine getirdiklerini bildirdikleri bir hizmet olmuştur. BT alanındaki gelişmelerin etkisini bir kez daha yoğun olarak gördüğümüz güvence hizmetlerinden olan WebTrust ve SysTrust'ın katılımcıların bilgi eksikliğinden dolayı uygulanamamaktadır. Kalite sertifikasyonları ve çevre denetimleri ise işletmelerin yer aldıkları sektörler tarafından da etkilenen güvence hizmetleri olduğundan bu hizmeti yerine getirenlerin sayısı zaten

azdır, dolayısıyla bu da sektörel durumun bir sonucudur. BT alanındaki gelişmeler çoğunlukla güvence hizmetlerinin çeşitliliğini etkilemiştir.

- **Ankete katılanların konumları ile güvence sağlamada kullanılan yöntemler arasındaki ilişki:**

*Tablo-18. Ankete Katılanların Konumları*Güvence Sağlamada Kullanılan Yöntemler*

Yöntemler Konum	Güvence sağlamada kullanılan yöntemler nelerdir?				
	Çoğunlukla periyodik manuel kontroller/standart raporlar	Düzenli yapılan manuel ve otomatik kontrollerin karışımı	Gerçek zamanlı manuel ve otomatik kontrollerin karışımı	Bilmiyorum	Toplam
İç Denetçi	12	5	2	0	19
İç Denetim Yön.	3	4	4	0	11
Genel müdür yrd.	0	0	2	0	2
Muhasebe Md.	1	5	1	0	7
Mali İşler Koord.	1	2	0	0	3
Denetim Koord.	1	1	0	0	2
İç Kontrol Koord.	1	4	0	1	6
Toplam	19	21	9	1	50

* Ankete katılanlar birden fazla seçenek işaretleyerek soruya cevap verebilmektedir.

Tablo-18’de görüldüğü üzere güvence hizmetlerinin sağlanmasında katılımcıların en çok kullandığı yöntem düzenli yapılan manuel ve otomatik kontrollerin karışımıdır (21 kişi). Genel müdür yardımcılarını hariç diğer tüm katılımcıların bu yöntemi kullandığı görülmektedir. Bir diğer en çok kullanılan yöntem de periyodik manuel kontroller ve standart raporlardır (19 kişi). Diğer yöntemlere nazaran en fazla iç denetçinin (12 kişi) bu yöntemi belirttiği dikkat çekmektedir. Genel müdür yardımcılarını bu yöntemi tercih etmemektedir. Gerçek zamanlı manuel ve otomatik kontrollerinin karışımı olarak güvence hizmeti sağladığını bildirenler ise oldukça azdır (9 kişi). Bu kişilerin çoğunluğunu iç denetim yöneticileri ve genel müdür yardımcılarını oluşturmaktadır.

Özetle, gerçek zamanlı kontrollerin az olduğu ve bunlarında yine manuel kontroller ile birlikte gerçekleşiyor olması dikkat çekicidir. Bu durumun nedeninin işlem süreçlerinde tamamen BT’nin kullanılmamasından kaynaklı olabileceğini düşündürmektedir. Çünkü işletmelerde işlem süreçlerinde hala manuel olarak gerçekleştirilen işlemler bulunmakta ve dolayısıyla güvence sağlamada kullanılan kontrollerde de manuel işlemlerin kullanılması sürdürülmektedir.

- Ankete katılanların konumları ile iç denetim biriminin güvence hizmetlerini verebilmesi için yerine getirmesi gereken faaliyetler arasındaki ilişki:

Tablo-19. Ankete Katılanların Konumları*İç Denetim Biriminin Güvence Hizmetlerini Verebilmesi İçin Yerine Getirmesi Gereken Faaliyetler

Konum		İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam	
Güvence Hizmetlerini Verebilmek için yerine Getirilmesi Gereken Faaliyetler	İç denetim işletmede kurumsal yönetim sisteminin yeterliliğini ve etkinliğini değerlendirerek yönetime güvence verir	Katılıyorum	7	2	1	0	1	1	4	16
		Kesinlikle katılıyorum	12	8	6	2	2	1	2	33
İç denetim yöneticisi kararlaştırılan konularda sağlanan ilerlemenin düzenli olarak izlenmesi amacıyla yönetim ve denetim komitesi ile düzenli toplantılar yapar.	Kararsızım	5	0	0	0	1	1	3	10	
	Katılıyorum	2	0	1	0	0	0	1	4	
	Kesinlikle katılıyorum	12	10	6	2	2	1	2	35	
İç denetim birimlerince bütünlüğü, doğruluğu ve tarafsızlığı denetlenip, doğrulanmış bilgi karar vericiler tarafından güvenilir bilgi olarak kabul edilir.	Katılıyorum	7	2	1	0	1	1	4	16	
	Kesinlikle katılıyorum	12	8	6	2	2	1	2	33	
İç denetim, kontrol sistemlerinin (operasyonel kontrol, finansal kontrol) etkinliğini ölçüp değerlendirerek yönetime objektif güvence sağlar.	Kararsızım	1	0	1	0	0	0	0	2	
	Katılıyorum	6	2	0	0	1	1	2	12	
	Kesinlikle katılıyorum	12	8	6	2	2	1	4	35	
İç denetim, işletmede kullanılan bilgi teknolojilerinin güvenliğini ve raporlama imkanlarını içeren muhasebe bilgi sisteminin etkinliğini değerlendirir.	Kararsızım	1	0	1	0	0	0	0	2	
	Katılıyorum	6	2	0	0	1	1	2	12	
	Kesinlikle katılıyorum	12	8	6	2	2	1	4	35	

Tablo-19'dan da görüldüğü gibi katılımcıların neredeyse tamamı (49 kişi) iç denetim biriminin kurumsal yönetim sisteminin yeterliliğinin ve etkinliğinin değerlendirilerek yönetime güvence vermesi gerektiğine inanmaktadır. Üstelik 33 kişi bunun kesinlikle böyle olduğunu belirtirken, hiçbir katılımcı bu konuda kararsızlık göstermemektedir. Bu da bu güvence hizmetinin mutlaka yerine getirilmesi gereken bir faaliyet olduğunu gösterir.

Yine hiç tereddütsüz iç denetim biriminin güvence hizmetini verebilmesi için gereken faaliyetlerden çoğunlukla kabul edilenlerden birisi; iç denetim biriminin

bilginin bütünlüğünü, doğruluğunu ve tarafsızlığını denetlemesi ve sonucunda doğru bilginin karar vericilere ulaştırılmasıdır.

Aslında Tablo-19’da yer alan tüm faaliyetler çoğunlukla iç denetim birimini güvence hizmetini yerine getirmesinde gerekli olarak görmektedir. İç denetim yöneticisinin yönetim kurulu ve denetim komitesi ile düzenli toplantılar yapması, iç kontrol sistemlerinin etkinliğinin ölçülüp değerlendirilerek yönetime objektif bir güvence sağlanması ve bilgi teknolojilerinin güvenliğinin ve muhasebe bilgi sisteminin etkinliğinin değerlendirilmesi konularında katılımcıların tereddütleri vardır.

Katılımcılara göre güvence hizmetleri kapsamında iç denetim birimlerince bütünlüğü, doğruluğu ve tarafsızlığı denetlenip doğrulanmış bilgi güvenilir bilgi olarak değerlendirilmektedir. Ayrıca iç kontrol sistemlerinin etkinliğinin ölçülüp değerlendirilerek yönetime bu konuda güvence verilmesi ve bilgi teknolojilerinin kullanımının çok yüksek olduğu muhasebe bilgi sistemlerinde bu teknolojilerin güvenliğinin sağlanmasını içeren güvence hizmetlerinin yerine getirilmesi, iç denetim biriminin en önemli sorumlulukları olarak görülmektedir.

Katılımcıların güvence hizmetlerinin yerine getirilebilmesi için gerekli görülen faaliyetler konusunda oldukça net olduğu dikkat çekmektedir. Bu da güvence hizmetlerine önem verildiğini ve özen gösterildiğini kanıtlamaktadır.

- **Ankete katılanların konumları ile danışmanlık hizmeti verilen alanlar arasındaki ilişki:**

*Tablo-20. Ankete Katılanların Konumları*Yerine Getirilen Danışmanlık Hizmetleri*

KONUM Yerine Getirilen Danışmanlık Hizmetleri	İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Risk yönetimi	19	9	3	7	3	1	4	46
Elektronik ticaret	0	0	0	0	0	0	0	0
Sistem güvenliği	8	8	1	2	1	1	3	24
Performans ölçümü	7	7	2	3	0	0	1	20
Diğer-Uyum	0	2	0	0	0	1	3	6

* Ankete katılanlar birden fazla seçenek işaretleyerek soruya cevap verebilmektedir.

Tabo-20’de görüldüğü üzere katılımcıların büyük bir kısmı risk yönetimi alanında danışmanlık hizmeti verildiğini belirtmiştir (46 kişi). Sonrasında ise sistem güvenliği (24 kişi) ve performans ölçümü (20 kişi) gelmektedir. Performans ölçümünün mali işler koordinatörleri ve denetim koordinatörleri tarafından gerçekleştirilmediği

dikkat çekmektedir. Ayrıca yerine getirilen faaliyetlerin standart ve çeşitli düzenlemeler ile uyumunu sağlama konusunda da yönetime danışmanlık hizmeti verildiği belirtilmiştir (6 kişi). Elektronik ticaret alanında ise danışmanlık hizmeti verilmemektedir.

Özetle, danışmanlık hizmetleri açısından baktığımızda en fazla yerine getirilen hizmet risk yönetimidir. Bununla birlikte performans ölçümü ve özellikle bilgi teknolojileri açısından önem arz eden sistem güvenliği konularında da üst yönetime danışmanlık hizmeti sağlanmaktadır. Ayrıca işletme faaliyetlerinin ve gerçekleştirilen işlemlerin yasa, yönetmelik, standart gibi belirli kurallar içeren düzenlemelere uyum sağlaması için iç denetim birimi ve sorumluları üst yönetime danışmanlık vermektedir. E-ticaret işlemlerinin işleyişi veya denetimi konusunda ise henüz iç denetim birimlerinin herhangi bir çalışma yapmadıkları görülmektedir. Bunun nedeni işletmelerde e-ticaret işlemlerinin uygulanma oranı geçmişte çok düşükken, şimdilerde çok yaygın olmamakla birlikte çoğunlukla kısmen gerçekleştirilmesi ve iç denetim birimlerinin e-ticaretin örgütlenmesi ve denetlenmesi konularında uzmanlaşmalarının gecikmesidir.

- Ankete katılanların konumları ile iç denetim biriminin danışmanlık hizmetlerini verebilmesi için yerine getirmesi gereken faaliyetler arasındaki ilişki:

Tablo-21. Ankete Katılanların Konumları ile İç Denetim Biriminin Danışmanlık Hizmetlerini Verebilmesi İçin Yerine Getirmesi Gereken Faaliyetler

Konum		İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam	
Danışmanlık Hizmetlerini Verebilmek İçin Yerine Getirilmesi Gereken Faaliyetler	İç denetçi, danışmanlık görevinin iç denetim faaliyetiyle ilgili temel görev planına uygunluğunu göz önünde bulundurur	Kararsızım	1	1	0	0	0	0	2	
		Katılıyorum	8	3	1	0	1	1	4	18
		Kesinlikle katılıyorum	10	7	6	2	2	1	2	30
İç denetçiler risk odaklı bir görev planı uyguladıklarından işletmenin ihtiyaç duyduğu denetim kapsamını belirler	Katılıyorum	9	4	1	0	1	1	2	18	
	Kesinlikle katılıyorum	10	7	6	2	2	1	4	32	
İç denetçiler görev planının izin verdiği ölçüde danışmanlık hizmetini yerine getirmelidirler	Katılmıyorum	1	1	0	0	0	0	0	2	
	Kararsızım	1	1	0	0	0	0	0	2	
	Katılıyorum	7	0	1	0	1	1	2	12	
	Kesinlikle katılıyorum	10	9	6	2	2	1	4	34	
Danışmanlık hizmetleri, iç denetçiler tarafından sunulan ve denetlenenin işletme amaçlarına ulaşmasını sağlayacak tavsiyeleri içerir	Katılıyorum	14	2	1	1	1	1	4	24	
	Kesinlikle katılıyorum	5	9	5	1	2	1	2	25	

Tablo-21’de görüldüğü üzere katılımcıların neredeyse tümü iç denetçilerin danışmanlık hizmetini yerine getirirken risk odaklı bir görev planı uygulayarak işletmenin ihtiyaç duyduğu denetimin kapsamını belirlediğini vurgulamaktadırlar (50 kişi). Aynı şekilde katılımcıların neredeyse tümü danışmanlık hizmetlerinin işletme amaçlarına ulaşmasını sağlayacak tavsiyeleri içerdiğini belirtmektedir. Katılımcıların bu iki konuda herhangi bir kararsızlığı söz konusu değildir.

Tablo-21’de yer alan ifadelerin hepsine katılımcıların katılım gösterdikleri görülmekle birlikte danışmanlık hizmetinin görev planına uygunluğun göz önüne alınması ve görev planının izin verdiği ölçüde danışmanlık hizmeti verilmesi konularında kararsızlığını bildiren katılımcıların olduğu görülmektedir.

Özetle, BT alanında yaşanan gelişmeler ve ortaya çıkan yeni riskler nedeniyle iç denetim sorumluları risk odaklı bir iç denetim planı hazırlayarak işletmenin ihtiyaç duyduğu denetimin kapsamını belirleyip, bu konuda üst yönetime danışmanlık hizmeti vermektedirler. Ayrıca verilen danışmanlık hizmetleri işletmeyi amaçlarına ulaştıracak

tavsiye niteliği taşır. İç denetçiler tarafından verilen bu danışmanlık hizmetleri iç denetim faaliyeti ile ilgili görev planına uygun düzenlenir ve bu görev planının izin verdiği ölçüde danışmanlık hizmeti yerine getirilir. Katılımcıların danışmanlık hizmetlerini yerine getirebilmesi için gerekli görülen faaliyetler konusunda genelde net olduğu ve bu faaliyetlere önem verdiği anlaşılmaktadır.

5.3.2.2. İç denetimin güvence ve danışmanlık hizmetleri ile ilgili non-parametrik testler

İç denetimin güvence ve danışmanlık hizmetlerinin verilebilmesi için yerine getirilmesi gereken faaliyetler ile ankete katılanların konumları arasında anlamlı farklılıkların olup olmadığını görmek için Kruskal-Wallis Testi yapılmıştır. Güvence hizmetlerinin verilebilmesi için yerine getirilmesi gereken faaliyetler ile ankete katılanların konumları arasında anlamlı farklılık bulunamamıştır. Aynı şekilde danışmanlık hizmetlerinin verilebilmesi için yerine getirilmesi gereken faaliyetler ile ankete katılanların konumları arasında da anlamlı farklılık yoktur.

Ayrıca non-parametrik testlerden bir diğeri olan Spearman's Rank Order Korelasyonu da katılanların konumları haricindeki diğer demografik sorulara uygulanmış ve bulunan anlamlı ilişkilere yer verilmiştir. Her biri ayrı ayrı olmak üzere iç denetim biriminin faaliyette bulunduğu süre, BT kullanan iç denetim personeli sayısı ve BT denetiminin uygulandığı süre ile güvence ve danışmanlık hizmetlerinin verilebilmesi için yapılması gereken faaliyetler arasında anlamlı ilişki bulunamamıştır.

Gelişen bilgi teknolojilerinin değiştirdiği işletme süreçleri ile birlikte iç denetimin genişleyen faaliyet alanlarında güvence ve danışmanlık hizmeti sağlanması, belirlenen işletme amaçlarına ulaşılmasında katkı sağlamaktadır. Güvence ve danışmanlık hizmetlerinin verilebilmesi için yerine getirilmesi gereken faaliyetler işletmede bu alanda sorumluluğu bulanan kişilerin konumları veya iç denetim birimine ilişkin diğer özelliklerden bağımsızdır.

5.3.3. İç denetim yaklaşımları ile ilgili çapraz tablo analizleri ve Non-Parametrik Testler

İç denetim yaklaşımları ile ilgili çapraz tablo analizleri katılımcıların işletmedeki konumları itibarıyla hazırlanmıştır. İç denetim yaklaşımları ile ilgili çapraz tablo analizleri sürekli denetim, risk odaklı iç denetim ve kontrol özdeğerlendirme yaklaşımları olmak üzere üç ayrı başlıkta verilecektir.

5.3.3.1. Sürekli denetim ile ilgili çapraz tablo analizleri ve non-parametrik testler

5.3.3.1.1. Sürekli denetim ile ilgili çapraz tablo analizleri

Sürekli denetim yaklaşımı ile ilgili çapraz tablo analizleri katılımcıların işletmedeki konumları itibarıyla düzenlenmiştir. Ankete katılanlar “sürekli denetimin işletmede uygulanma durumunu”, “uygulanmama nedenlerini”, “uygulanmasındaki temel amaçları”, “fayda sağladığı alanlar”, “sürekli denetimi desteklemek amacıyla BT kullanımının yaygınlığı”, “sürekli denetimde veri analizini”, “sürekli izleme faaliyetinde BT kullanımını”, “sürekli izleme kontrollerinin uygulanma durumunu” “kullanılan yazılımları”, “XBRL kullanımını”, “XBRL kullanılan süreçleri”, “XBRL’nin kullanılmama nedenlerini” ve “XBRL hakkında bilinmek istenenleri” değerlendirmişlerdir.

- Ankete katılanların konumları ile sürekli denetimin işletmede uygulanma durumu arasındaki ilişki:

Tablo-22. Ankete Katılanların İşletmedeki Konumları*Sürekli Denetimin Uygulama Durumu

KONUM	İç denetim birimi sürekli denetim yaklaşımını kullanıyor mu?		
	Evet	Hayır	Toplam
İç Denetçi	13	6	19
İç Denetim Yöneticisi	9	2	10
Genel müdür yardımcısı	2	1	3
Muhasebe Müdürü	5	2	7
Mali İşler koordinatörü	2	1	3
Denetim Koordinatörü	1	1	2
İç Kontrol Koordinatörü	5	1	4
Toplam	37	14	51

Tablo-22’de görüldüğü üzere 37 kişi iç denetim biriminde sürekli denetim yaklaşımının uygulandığını, 14 kişi ise uygulanmadığını bildirmiştir. Sürekli denetim yaklaşımının uygulandığını bildiren taraflar arasında her konumdan katılımcı bulunmakla birlikte iç denetçiler, iç denetim yöneticileri, muhasebe müdürleri, iç kontrol koordinatörleri çoğunluktadır.

Ayrıca BT denetiminin uygulandığı süre ve iç denetim biriminin faaliyette bulunduğu süre açısından elde edilen sonuçlarda dikkat çekicidir.

*Tablo-23. Bilgi Teknolojileri Denetiminin Uygulandığı Süre*Sürekli Denetim Uygulama Durumu*

Bilgi teknolojileri denetiminin uygulandığı süre	İç denetim birimi sürekli denetim yaklaşımını kullanıyor mu?		
	Evet	Hayır	Toplam
Hiç uygulanmaz	1	5	6
1 yıldan az	8	0	8
1-3 yıl	13	9	22
4-6 yıl	12	0	12
10 yıl ve üzeri	2	0	2
Toplam	36	14	50

Tablo-23’e göre sürekli denetim yaklaşımının uygulandığını belirten 36 kişinin 13’ü 1-3 yıldır, 12’si ise 4-6 yıldır BT denetiminin yapıldığını bildirmiştir. 8 kişi ise 1 yıldan az bir süredir BT denetiminin uygulandığını belirtmiştir. Sürekli denetim yaklaşımını uygulamadıklarını bildiren 14 kişiden 9’u 1-3 yıldır BT denetimi yaptıklarını belirtmiştir.

*Tablo-24. İç Denetim Biriminin Faaliyette Bulunduğu Süre*Sürekli Denetim Uygulama Durumu*

İç denetim biriminin faaliyette bulunduğu süre	İç denetim birimi sürekli denetim yaklaşımını kullanıyor mu?		
	Evet	Hayır	Toplam
1 yıldan az	1	0	1
1-5 yıl	10	6	16
6-10 yıl	4	3	7
11-15 yıl	12	4	16
16-20 yıl	5	1	6
21 yıl ve üzeri	4	0	4
Bilmiyorum	1	0	1
Toplam	37	14	51

Tablo-24’e bakıldığında sürekli denetim yaklaşımının uygulandığını belirten 37 kişiden 12’si iç denetim biriminin 11-15 yıldır faaliyette olduğunu, 10 kişi de 1-5 yıldır faaliyette olduğunu bildirmiştir.

Özetle, sürekli denetim yaklaşımının uygulanma durumu açısından baktığımızda 5-10 yıllık bir süreçte iç denetim birimi aktif olarak çalışan işletmelerin bu yaklaşımı benimsedikleri söylenebilir. Ayrıca 5 yıllık bir zaman dilimi içinde BT denetimi yapan işletmelerin de bu yaklaşımı benimsedikleri söylenebilir. Dolayısıyla iç denetim biriminin varlığı ve süresi sürekli denetim yaklaşımının benimsenmesinde önemli bir role sahiptir.

- **Ankete katılanların konumları ile sürekli denetimin uygulanmama nedenleri arasındaki ilişki:**

*Tablo-25. Ankete Katılanların İşletmedeki Konumları*Sürekli Denetim Yaklaşımının Uygulanmama Nedenleri*

Sürekli Denetimin Yapılmama Nedenleri	KONUM	İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Önem verilmiyor		1	1	0	1	0	0	0	3
Personel yetersizliği		4	1	0	1	1	1	1	9
Bütçe kısıtları		0	2	0	0	0	0	0	2
Zaman kısıtı		0	1	0	0	0	0	0	1
Uygulanması karmaşık bir yaklaşım		2	2	0	1	0	0	0	5
Bilgisayar sistemleri ve veri yapıları ile ilgili kısıtlar var		5	0	1	1	1	1	1	10
Veri güvenliği ve bütünlüğü ile ilgili sorunlar var		0	2	0	0	0	0	0	2
Veri girişinde sorunlar var		6	2	1	2	1	1	1	14
Bilgi Teknolojileri bölümünden destek alınamaması		5	0	1	0	1	1	1	9

Daha önce belirttiğimiz üzere katılımcıların 14'ü sürekli denetim yaklaşımının kullanılmadığını bildirmişti. Dolayısıyla Tablo-25'e baktığımızda katılımcıların en fazla bildirdiği nedenler arasında veri girişinde sorunlar olduğu bildirilmiştir (14 kişi). Bu nedeni bildirenler arasında iç denetçilerin sayısı fazladır. Sonrasında katılımcılardan 10 kişi bilgisayar sistemleri ve veri yapıları ile ilgili kısıtların olduğunu belirtmiştir. Ancak bu durumu iç denetim yöneticileri bir neden olarak görmezken iç denetçiler bir neden olarak görmektedir. Bunlar dışında sürekli denetim yaklaşımına önem verilmemesi ve bilgi teknolojileri bölümünden destek alınamaması da sürekli denetim yaklaşımının uygulanmama nedenleri arasında yer almıştır. Ayrıca uygulanmasının karmaşık bir yaklaşım olduğunu bildiren katılımcılar da vardır (5 kişi).

Sürekli denetim yaklaşımının uygulanmaması ile ilgili olarak iç denetçiler, muhasebe müdürleri, mali işler koordinatörleri, denetim koordinatörleri ve iç kontrol koordinatörleri BT sistemlerinin kısıtları, BT bölümünden destek alınamaması, veri girişi ile ilgili sorunlar ve personel yetersizliği gibi konulara yönelirken, iç denetim

yöneticileri yaklaşımının karmaşıklığı, veri güvenliği, bütçe kısıtları ve yine veri girişi ile ilgili sorunlara yoğunlaşmışlardır. Çünkü iç denetçileri denetim sürecinin uygulama veya yürütülme kısmında yer aldıkları için BT konusunu ön plana çıkartmak zorundadır.

- **Ankete katılanların konumları ile sürekli denetim yaklaşımının uygulanmasındaki temel amaçlar arasındaki ilişki:**

*Tablo26. Ankete Katılanların İşletmedeki Konumları*Sürekli Denetim Yaklaşımının Uygulanmasındaki Temel Amaçlar*

KONUM		İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Uygulanan önerileri izlemek	Katılmıyorum	1	3	0	0	0	0	2	6
	Katılıyorum	9	5	0	2	0	0	2	18
	Kesinlikle Katılıyorum	3	1	5	0	2	1	1	13
Finansal karakterli bilgilerin doğruluğuna ve güvenilirliğine ilişkin bir görüş oluşturmak	Katılmıyorum	0	0	0	1	0	0	0	1
	Katılıyorum	4	2	0	0	0	0	2	8
	Kesinlikle Katılıyorum	9	7	5	1	2	1	3	28
Sürekli bilgi üzerinde bir dizi güvence hizmeti gerçekleştirmek	Kesinlikle katılmıyorum	1	1	0	0	0	0	0	2
	Kararsızım	0	0	0	0	0	0	2	2
	Katılıyorum	2	1	0	0	0	0	2	5
	Kesinlikle Katılıyorum	10	7	5	2	2	1	1	28
Elektronik ortamda ortaya çıkan verilere ve denetim kanıtlarına odaklanmak	Katılıyorum	2	0	0	1	0	0	2	5
	Kesinlikle Katılıyorum	11	9	5	1	2	1	3	32
Bilgi teknolojilerinin kullanımı sayesinde insan faktöründen kaynaklanan hataları ve zaman kayıplarını engellemek	Katılıyorum	3	1	0	1	0	0	2	7
	Kesinlikle Katılıyorum	10	8	5	1	2	1	3	30
Kontrol zayıflıklarını belirlemek	Katılıyorum	2	2	0	1	0	0	1	6
	Kesinlikle Katılıyorum	11	7	5	1	2	1	4	31
Riskleri gözlemlemek	Katılıyorum	3	2	0	1	0	0	1	7
	Kesinlikle Katılıyorum	10	7	5	1	2	1	4	30
Potansiyel hile faaliyetlerini belirlemek	Katılıyorum	2	0	0	1	0	0	3	6
	Kesinlikle Katılıyorum	11	9	5	1	2	1	2	31

Tablo-26'ya baktığımızda katılımcıların en çok katılım gösterdikleri temel amaçların; “elektronik ortamda ortaya çıkan verilere ve denetim kanıtlarına odaklanmak”, “bilgi teknolojilerinin kullanımı sayesinde insan faktöründen kaynaklanan hataları ve zaman kayıplarını engellemek”, “kontrol zayıflıklarını

belirlemek”, “riskleri gözlemlemek” ve “potansiyel hile faaliyetlerini belirlemek” olduğu görülmektedir. Daha önce sürekli denetim yaklaşımının uygulandığını bildiren 37 kişinin tamamı bunları sürekli denetimin uygulanmasında temel amaçlar olarak görmektedir.

Finansal karakterli bilgilerin doğruluğuna ve güvenilirliğine ilişkin bir görüş oluşturmak da katılımcıların neredeyse tümünün bildirdiği bir diğer amaçtır (36 kişi). Dikkat çekici bir diğer sonuç da sürekli bilgi üzerinde bir dizi güvence hizmeti gerçekleştirmek amacıyla sürekli denetim yaklaşımının uygulandığını belirten 33 kişinin yanı sıra 2 kişinin buna kesinlikle katılmadığını bildirmesi ve bu kişilerin iç denetçi ve iç denetim yöneticisi oluşudur. Uygulanan önerileri izlemek amacıyla sürekli denetim yaklaşımının uygulandığını bildiren 31 kişinin yanı sıra bunu bir amaç olarak görmeyen 6 kişi vardır. Bu kişilerin çoğunluğu iç denetim yöneticisi ve iç kontrol koordinatörüdür.

Özetle, sürekli denetim yaklaşımının uygulanmasındaki temel amaçlar konusunda iç denetim ile ilgili tüm taraflar fikir birliği içindedirler. Bu amaçların BT’nin yarattığı risklere karşı önlem niteliğinde olduğu da dikkat çekmektedir. İşletmeler açısından bilginin güvenliği konusu son derece önemlidir ve hala bu konuda soru işaretleri oluşabilmektedir. Hızlı bir şekilde gerçekleştirilen finansal raporlama sürecinde sürekli denetim yaklaşımını benimsenerek eş zamanlı denetim eylemleri gerçekleştirilmesi hatalara ve hilelere zamanında müdahale edilip, bilginin güvenilirliği konusundaki soru işaretlerinin ortadan kalkmasına, bilgi güvenliğinin artmasına ve BT risklerinin azaltılmasına yardımcı olacaktır. Çünkü sürekli denetim yaklaşımı elektronik ortamda ortaya çıkan veriler ve kanıtlar üzerine odaklanarak, insan faktörünü geri planda bırakmıştır.

- Ankete katılanların konumları ile sürekli denetim yaklaşımının fayda sağladığı alanlar arasındaki ilişki:

Tablo-27. Ankete Katılanların Konumları*Sürekli Denetimin Fayda Sağladığı Alanlar

Konum Sürekli Denetimin Fayda Sağladığı Alanlar	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Kapsamlı güvence sağlaması	11	8	1	5	2	1	4	32
Hileyi önleme ve bulma	13	8	1	5	2	1	5	35
İyi bir yönetim sağlama	11	2	1	5	2	0	3	24
Sürekli süreç iyileştirme	14	6	1	5	2	1	5	34
Maliyet azaltma	9	2	1	0	1	0	2	15

Tablo-27’ye göre sürekli denetim yaklaşımının en fazla fayda sağladığı alan hile önleme ve bulma olarak görülmektedir (35 kişi). Sonrasında ise sürekli süreç iyileştirme (34 kişi) ve kapsamlı güvence sağlama (32 kişi) gelmektedir. Diğer alanlar olarak iyi bir yönetim sağlama denetim koordinatörleri hariç 24 kişi tarafından ve maliyet azaltma muhasebe müdürleri ve denetim koordinatörleri hariç 15 kişi tarafından bildirilmiştir.

Özetle, diğer katılımcıların aksine denetim koordinatörlerine ve muhasebe müdürlerine göre sürekli denetim yaklaşımı işletmeye maliyetlerin azaltılması yönünde bir fayda sağlamamaktadır. Ayrıca denetim koordinatörleri sürekli denetim yaklaşımının iyi bir yönetim sağlamaya da faydası olmadığını düşünmektedir. Aslında sürekli denetim işletmenin yönetim kademesini de denetim sürecine dahil eden bir yaklaşımdır. Hangi konumda olursa olsun tüm iç denetim sorumlularının genelde ortak fikirde oldukları alanlar hile bulma ve önleme, sürekli süreç iyileştirme ve kapsamlı güvence sağlamadır. İşletmelerde bilginin ilgili ve güvenilir olduğu konusunda yönetim kademesinin güvence hizmeti talebinin artması ile birlikte iç denetçilerin güvence hizmetlerinin tüm yönlerini desteklemesi, sürekli denetim yaklaşımının benimsenme eğilimini arttırmıştır.

- Ankete katılanların konumları ile sürekli denetimi desteklemek amacıyla işletmedeki BT kullanımının yaygınlığı arasındaki ilişki:

Tablo-28. Ankete Katılanların İşletmedeki Konumları*Sürekli Denetimi Desteklemek Amacıyla İşletmedeki BT Kullanımının Yaygınlığı

KONUM	Sürekli denetimi desteklemek amacıyla işletmenizdeki bilgi teknolojisi kullanımının yaygınlığı ne düzeydedir?					
	Kurumsal kaynak planlaması gibi standart raporlama sistemleri kullanılır	Denetim ve izleme için tahsis edilmiş araçların kullanımı dikkate alınır	Kısıtlı olarak/pilot uygulama kapsamında denetim ve izleme araçları kullanılır	Geniş bir alanda denetim ve izleme araçları kullanılır	Bilmiyorum	Toplam
İç Denetçi	2	2	7	4	0	15
İç Denetim Yöneticisi	0	5	1	3	0	9
Genel müdür yardımcısı	0	0	1	0	1	2
Muhasebe Müdürü	0	5	0	0	0	5
Mali İşler koordinatörü	0	2	0	0	0	2
Denetim Koordinatörü	0	0	0	1	0	1
İç Kontrol Koordinatörü	0	0	0	3	0	3
Toplam	2	14	9	11	1	37

Tablo-28'e baktığımızda daha önce sürekli denetim yaklaşımının uygulandığını bildiren 37 kişinin 14'ü sürekli denetimde BT kullanımının yaygınlığı açısından denetim ve izleme için ayrılmış BT araçlarının kullanımının dikkate alındığını bildirmiştir. Bu kişilerin çoğunluğunu iç denetim yöneticileri ve muhasebe müdürleri oluşturmaktadır. Sonrasında en çok bildirilen durum geniş bir alanda denetim ve izleme araçlarının kullanıldığıdır (11 kişi). Bir diğer dikkat çeken durum da kısıtlı bir şekilde denetim ve izleme araçları kullanıldığıdır (9 kişi). Bu durumu bildirenler arasında iç denetçilerin çoğunlukta olduğu görülmektedir. Kurumsal kaynak planlaması gibi standart raporlama sistemlerinde BT'nin kullanımının yaygın olduğunu bildiren katılımcılar da vardır ve bunlar iç denetçilerdir (2 kişi).

Ayrıca sürekli denetimde BT'nin kullanım amacına ilişkin olarak katılımcılara verilen "sürekli denetim teknolojisi, risk yönetiminde kullanılabilen teknoloji odaklı sürekli denetim çözümlerini yaygınlaştırmak için oluşturulmuştur" ifadesine verilen cevaplar da dikkat çekmektedir.

Tablo-29. Ankete Katılanların İşletmedeki Konumları*Sürekli Denetimde Kullanılma BT'nin Kullanım Amacı

KONUM	"SÜREKLİ DENETİM TEKNOLOJİSİ, RİSK YÖNETİMİNDE KULLANILABİLEN TEKNOLOJİ ODAKLI SÜREKLİ DENETİM TEKNİKLERİNİ YAYGINLAŞTIRMAK İÇİN OLUŞTURULMUŞTUR" bu ifadeye katılım düzeyinizi ifade ediniz.				
	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle katılıyorum	Toplam
İç Denetçi	2	6	5	0	13
İç Denetim Yöneticisi	1	0	8	0	9
Genel müdür yardımcısı	0	1	0	0	1
Muhasebe Müdürü	0	0	1	4	5
Mali İşler koordinatörü	1	0	0	1	2
Denetim Koordinatörü	0	0	1	0	1
İç Kontrol Koordinatörü	0	0	3	2	5
Toplam	4	7	18	7	36

Tablo-29'a göre genel müdür yardımcıları ve mali işler koordinatörleri hariç katılımcıların çoğunluğu sürekli denetimde kullanılan teknolojilerin risk yönetiminde kullanılabilen teknoloji odaklı sürekli denetim tekniklerini yaygınlaştırmak için oluşturulduğunu düşünmektedir (Katılıyorum-18+Kesinlikle katılıyorum-7= 25 kişi).

Özetle, işletmelerde sürekli denetim yaklaşımının desteklenmesi amacıyla bilgi teknolojileri kullanımı daha çok denetim ve izleme faaliyetlerindedir. Denetim ve izleme araçlarına ilişkin bilgi teknolojisi kullanımı mutlaka geniş bir alanda olmak zorunda değildir. İşletmenin faaliyetlerine bağlı olarak kısıtlı bir alanda da olabilir. İç denetim yöneticileri ve muhasebe müdürleri kısıtlı bir şekilde denetim ve izleme araçları kullanıldığını düşünürken iç denetçiler ve iç kontrol koordinatörleri ise aksine geniş bir alanda denetim ve izleme araçları kullanıldığını düşünmektedir. Bunun nedeni denetim sürecinde çeşitli araç ve yöntemlerin kullanımına ilişkin birim yöneticilerinin beklentilerinin daha yüksek olması olabilir. Ayrıca katılımcıların çoğu sürekli denetimde kullanılan BT'nin risk yönetiminde kullanılabilen BT odaklı sürekli denetim tekniklerini yaygınlaştırmak için oluşturulduğunu düşünmektedir.

- Ankete katılanların konumları ile sürekli denetimde veri analizinin kullanım yeri arasındaki ilişki:

*Tablo-30. Ankete Katılanların İşletmelerindeki Konumları *Sürekli Denetimde Veri Analizinin Kullanım Yeri*

KONUM Veri Analizinin Kullanım Yeri	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Denetim faaliyetinin yürütülmesinde	13	8	1	5	2	1	2	32
Hile bulma programlarında	5	8	0	0	1	1	4	19
Denetim planlama sürecinde	5	8	1	0	1	1	1	17
Risk değerlendirme sürecinde	5	8	1	5	2	1	3	25
Denetim raporlarında	7	6	0	0	1	1	2	17
Bilmiyorum	0	0	0	0	0	0	1	1

Tablo-30'a göre katılımcıların çoğu sürekli denetimde veri analizinin denetim faaliyetinin yürütülmesinde kullanıldığını bildirmiştir (32 kişi). Sonrasında 25 kişi risk değerlendirme sürecinde veri analizini kullandıklarını bildirmiştir. Bu kişilerin çoğunluğunu iç denetim yöneticileri ve muhasebe müdürleri oluşturmaktadır. Ayrıca hile bulma programlarında da veri analizi kullanımı yüksektir (19 kişi). Burada da iç denetim yöneticileri ve iç kontrol koordinatörlerinin çoğunlukta olduğu görülmektedir. Denetimin planlama sürecinde (17 kişi) ve denetim raporlarında (17 kişi) veri analizinin kullanıldığını belirten katılımcılar da olmuştur.

Sürekli denetimde veri analizi çalışmaları iç denetçiler tarafından sürekli denetim faaliyetlerinin gelişimini sürdürebilmek için önemlidir. Bu doğrultuda katılımcıların çoğunluğu denetim faaliyetinin yürütülmesi, risk değerlendirme ve hile bulma programlarında veri analizini kullandıklarını bildirmişlerdir. Özellikle hile bulma ile ilgili çalışmalarda diğer katılımcılara nazaran iç denetçiler, iç denetim yöneticileri ve iç kontrol koordinatörleri tarafından veri analizinin daha çok kullanıldığı görülmektedir.

- Ankete katılanların konumları ile sürekli izleme faaliyetinde BT kullanımı ve sürekli izleme kontrollerini uygulama durumları arasındaki ilişki:

*Tablo-31. Ankete Katılanların Konumları*Sürekli İzleme Faaliyetinde BT Kullanımı*

KONUM	İşletmenizin herhangi bir biriminde veya sürecinde iç kontroller üzerinde sürekli izleme gerçekleştirmek amacıyla bilgi teknolojileri kullanılıyor mu?			
	Evet	Hayır	Bilmiyorum	Toplam
İç Denetçi	11	2	0	13
İç Denetim Yöneticisi	4	5	0	9
Genel müdür yardımcısı	1	0	1	2
Muhasebe Müdürü	0	0	5	5
Mali İşler koordinatörü	1	0	1	2
Denetim Koordinatörü	1	0	0	1
İç Kontrol Koordinatörü	5	0	0	5
Toplam	23	7	7	37

Tablo-31'e göre sürekli denetim yaklaşımının uygulandığını bildiren katılımcıların çoğunluğu sürekli izleme faaliyetinde BT'nin kullanıldığını belirtmiştir. Bu katılımcılar arasında muhasebe müdürleri hariç iç denetçilerin ve iç kontrol koordinatörlerinin çoğunlukta olduğu dikkat çekmektedir. Ayrıca sürekli izleme kontrollerinin uygulanması ile ilgili olarak da katılımcıların fikirleri alınmıştır.

*Tablo-32. Ankete Katılanların Konumları*Sürekli İzleme Kontrollerinin Uygulama Durumları*

KONUM	Yönetim/iş süreci sahipleri sürekli izleme kontrollerini uyguluyorlar mı?			
	Evet	Hayır	Bilmiyorum	Toplam
İç Denetçi	7	7	0	14
İç Denetim Yöneticisi	8	0	0	8
Genel müdür yardımcısı	1	0	1	2
Muhasebe Müdürü	0	0	5	5
Mali İşler koordinatörü	1	0	1	2
Denetim Koordinatörü	1	0	0	1
İç Kontrol Koordinatörü	3	2	0	5
Toplam	21	9	7	37

Tablo-32'ye göre herhangi bir yönetim veya iş sürecinde bu süreç sahipleri tarafından sürekli izleme kontrollerinin çoğunlukla uygulandığı görülmektedir (21 kişi). İç denetim yöneticileri, katılımı yüksek olan gruptur. Bu durumu bildirenler arasında muhasebe müdürleri yoktur, çünkü muhasebe müdürleri bu duruma ilişkin bilgi sahibi olmadıklarını bildirmişlerdir.

Sürekli denetimin uygulanmasıyla birlikte sürekli izleme faaliyetleri de ortaya çıkmıştır. Sürekli denetim yaklaşımını benimseyen işletmelerde yönetim veya iş süreci sahipleri sürekli izleme kontrollerini de uygulamaktadırlar. Bu açıdan baktığımızda iç denetim yöneticilerinin ve iç kontrol koordinatörlerinin katılımların yüksek olduğu dikkat çekmektedir. Bu da doğal bir sonuçtur. Çünkü işletmedeki veri türlerinin, bilgi sistemlerinin, işlem süreçlerinin tümünün veya bunlardan herhangi birinin performansının ölçülmesini kapsayan sürekli izleme faaliyetleri iç denetim ve iç kontrol sorumlularının birlikte çalışmalarıyla gerçekleşmektedir. Ayrıca sürekli denetimde kullanılan bilgi teknolojilerinin risk yönetiminde kullanılan teknoloji odaklı sürekli denetim çözümlerini de yaygınlaştırdığı kabul edilmektedir. Bu konuda da bu kez iç denetçilerin ve yine iç kontrol koordinatörlerinin çoğunlukla katılımlarının yüksek olduğu görülmektedir. Çünkü elektronik veri ve kanıtlara dayanan sürekli denetim teknolojilerini risk yönetimi süreçlerinde bizzat yer alarak uygulayanlar iç denetçiler ve iç kontrol koordinatörleridir.

- Ankete katılanların konumları ile veri bulma, veri analizi ve sürekli denetim süreçlerinde kullanılan yazılımlar arasındaki ilişki:

Tablo-33. Ankete Katılanların İşletmedeki Konumları*Veri Bulma, Veri Analizi ve Sürekli Denetim Sürecinde Kullanılan Yazılımlar

KONUM Yazılımlar		İç Denetçi	İç Denetim Yöneticisi	Muhasebe Md	Gn Md. Yrd	Mali İşler Koord.	Denetim Koord.	İç Kontrol	Toplam
Access	Veri Bulma	3	5	0	0	0	0	2	10
	Veri Analizi	5	7	0	0	1	1	2	16
	Sürekli Denetim	0	0	5	0	1	0	0	6
ACL	Veri Bulma	7	1	0	1	0	1	0	10
	Veri Analizi	8	1	0	1	0	1	0	11
	Sürekli Denetim	8	1	4	1	0	1	2	17
IDEA	Veri Bulma	1	0	0	0	0	0	0	1
	Veri Analizi	-	-	-	-	-	-	-	-
	Sürekli Denetim	0	0	3	0	0	0	1	4
Excel	Veri Bulma	5	7	1	1	0	0	1	15
	Veri Analizi	8	9	1	1	1	1	3	24
	Sürekli Denetim	10	7	5	0	1	0	1	24
Monarch	Veri Bulma	-	-	-	-	-	-	-	-
	Veri Analizi	1	0	0	0	0	0	0	1
	Sürekli Denetim	0	0	2	0	0	0	1	3
Oracle	Veri Bulma	9	5	0	1	0	0	3	18
	Veri Analizi	11	6	0	1	0	1	3	22
	Sürekli Denetim	8	5	3	1	0	0	3	20
AS/400 Query	Veri Bulma	3	0	0	0	0	0	0	3
	Veri Analizi	1	0	0	0	0	0	0	1
	Sürekli Denetim	0	0	2	0	0	0	2	4
Crystal Reports	Veri Bulma	2	0	0	0	0	0	0	2
	Veri Analizi	1	0	0	0	0	0	0	1
	Sürekli Denetim	0	0	0	0	0	0	1	1
People Soft	Veri Bulma	1	0	0	0	0	0	0	1
	Veri Analizi	-	-	-	-	-	-	-	-
	Sürekli Denetim	0	0	0	0	0	0	1	1
SAP	Veri Bulma	1	0	0	0	0	0	1	2
	Veri Analizi	2	0	2	0	0	0	1	5
	Sürekli Denetim	1	0	0	0	0	0	1	2
SAS	Veri Bulma	-	-	-	-	-	-	-	-
	Veri Analizi	1	0	0	0	0	0	0	1
	Sürekli Denetim	0	0	0	0	0	0	1	1
Datas	Veri Bulma	1	0	0	0	0	0	0	1
	Veri Analizi	-	-	-	-	-	-	-	-
	Sürekli Denetim	0	0	0	0	0	0	1	1
TeamMate	Veri Bulma	2	0	0	0	0	0	0	2
	Veri Analizi	3	0	0	0	0	0	0	3
	Sürekli Denetim	0	0	0	0	0	0	1	1

Tablo-33'e göre veri bulma, veri analizi ve sürekli denetim süreçlerinde kullanılan yazılımlardan katılımcılar tarafından en çok bildirilenler Access, ACL, Excel, Oracle ve SAP olmuştur. Bu yazılımlar içinde veri bulma ve veri analiz süreçleri açısından Excel ve Oracle'ın daha çok bildirildiği görülmektedir. Sürekli denetim sürecinde ise Excel ve Oracle ile birlikte ACL'in de kullanımının yüksek olduğu

görülmektedir. Sürekli denetim sürecinde bunların dışında Access ve IDEA'nın da kullanıldığı görülmektedir. Kullanımı az da olsa katılımcılar tarafından bahsedilen diğer yazılımlar Monarch, AS/400 Query, Crystal Reports, People Soft, SAS, Datas ve TeamMate'dir.

Veri analizi, veri bulma ve sürekli denetim süreçlerinde işletmelerin kullandığı birçok yazılım olabilir. Katılımcılar tarafından yapılan değerlendirmelerde en çok bilinen ve kullanılan yazılımlar Access, ACL, Excel, Oracle ve SAP olmuştur. Bu konularda bilgili olan tarafların genellikle iç denetçiler, iç denetim yöneticileri, muhasebe müdürleri ve iç kontrol koordinatörleri olduğu görülmektedir.

- **Ankete katılanların konumları ile XBRL'nin kullanımı ve kullanılan süreçler arasındaki ilişki:**

*Tablo-34. Ankete Katılanların İşletmedeki Konumları*XBRL Kullanımı*

KONUM	İşletmenizdeki herhangi bir süreçte XBRL ye başvuruldu mu?			
	Evet	Hayır	Bilmiyorum	Toplam
İç Denetçi	1	14	4	19
İç Denetim Yöneticisi	0	6	5	11
Genel müdür yardımcısı	0	1	2	3
Muhasebe Müdürü	0	1	6	7
Mali İşler koordinatörü	0	1	2	3
Denetim Koordinatörü	0	1	1	2
İç Kontrol Koordinatörü	0	1	5	6
Toplam	1	25	25	51

Tablo-34'den katılımcıların büyük bir kısmının ya XBRL'yi kullanmadığı ya da XBRL ile ilgili bilgi sahibi olmadığı görülmektedir. Sadece 1 kişi XBRL'nin kullanıldığını bildirmiştir. Bu kişinin XBRL kullanımının hangi süreçlerde gerçekleştirdiğine dair bilgiler aşağıdaki Tablo-35'de görülmektedir.

*Tablo-35. XBRL kullananlar*İşletmede XBRL Kullanılan Süreçler*

İşletmede XBRL Kullanılan Süreçler	İşletmenizdeki herhangi bir süreçte XBRL ye başvuruldu mu? sorusuna EVET Cevabı Verenlerin Sayısı
Finansal raporlama	1
Finansal tabloların standartlara uygun hazırlanması	1
Performans ölçümünde	1
Verinin bilgiye dönüştürülmesinde	1
TOPLAM	1

Tablo-35'e göre XBRL finansal raporlama, finansal tabloların standartlara uygun hazırlanması, performans ölçümü, verinin bilgiye dönüştürülmesi gibi süreçlerde kullanılabilir.

Raporlama dilleri açısından uygulamada en yaygın kullanılan XBRL'nin ülkemizdeki işletmelerde kullanımı konusunda bilgi ve teknik uzmanlık konusunda yetersizliklerin olması, mevcut raporlama sisteminden memnun olunması ve yönetim tarafından onaylanmadığı gerekçeleri ile kullanımının olmadığı görülmüştür.

- **Ankete katılanların konumları ile XBRL'nin kullanılmama nedenleri ve XBRL hakkında bilinmek istenenler arasındaki ilişki:**

*Tablo-36. Ankete Katılanların İşletmedeki Konumları*XBRL'nin Kullanmama Nedenleri*

KONUM XBRL'yi Kullanmama Nedenleri	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Yönetim tarafından onaylanmaması	2	0	0	1	0	-	0	3
İstek yapılmasını beklemek	2	1	0	0	0	-	0	3
Yeterli teknik uzmanlığın olmaması	1	1	0	0	0	-	0	2
İşletmenin küçük olması	-	-	-	-	-	-	-	-
XBRL hakkında bilgi yetersizliği	13	6	1	0	1	1	1	23
Mevcut raporlama sisteminden memnun olunması	1	4	1	0	0	-	0	6
Bilmiyorum	3	0	0	0	0	-	0	3

Tablo-36'ya göre daha önce XBRL'nin kullanılmadığını bildiren 25 kişinin 23'ü XBRL hakkında yeterli bilgiye sahip olmadıklarından ötürü kullanılmadığını bildirmiştir. En önemli neden olarak bilgi yetersizliği görülmektedir. Bunun haricinde mevcut raporlama sisteminden memnun olunması, yönetim tarafından onaylanmaması, istek yapılmasının beklenmesi, yeterli teknik uzmanlığın olmaması gibi nedenler de bildirilmiştir. İç denetçilerin ve iç denetim yöneticilerinin XBRL'nin kullanılmama nedenlerine genelde katılım gösterdikleri görülmektedir. Ayrıca katılımcıların XBRL ile ilgili bilmek istediği konular da kendilerine sorulmuştur. Alınan cevaplar aşağıda Tablo-37'de görülmektedir.

Tablo-37. Ankete Katılanların İşletmelerindeki Konumları*XBRL İle İlgili Bilmek İstenilen veya Bilinmesi Gereken Bilgiler

KONUM XBRL ile İlgili Bilmek İstenilen veya Bilinmesi gereken Bilgiler	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
XBRL'nin güvenilirliğinin nasıl sağlandığı	15	6	2	6	3	1	2	35
XBRL sürecinde iç denetçinin rolü	18	9	2	1	2	2	5	39
XBRL'nin bilgi teknolojileri ve muhasebe açısından rolü	15	5	2	1	1	1	4	29
XBRL'nin denetimin planlanmasındaki rolü	17	7	2	1	1	2	5	35
XBRL'nin Kurumsal Kaynak Planlaması ile ilişkisi	13	1	1	0	1	1	2	19
XBRL ile ilgili denetim riskleri	16	6	2	0	1	2	5	32
İç kontrollerin anlaşılması	15	6	2	0	1	1	3	28
Finansal raporlama sürecine kattığı değer	10	4	2	1	0	0	2	19
Bilgi teknolojisi ile ilgili riskler ve kurulması gereken kontroller	15	5	2	6	2	1	2	33
XBRL'nin uygulanma süreci, avantajları, dezavantajları ve maliyetlere etkisi	10	2	1	1	0	1	3	18

Tablo-37'ye bakıldığında katılımcıların XBRL ile ilgili bilmek istediği en önemli konunun XBRL sürecinde iç denetçinin rolünün ne olduğudur. Ayrıca XBRL sürecinin güvenliğinin nasıl sağlanacağı, XBRL'nin denetim planlamasındaki rolü, bilgi teknolojisi ile ilgili riskler ve kurulması gereken kontroller ve XBRL ile ilgili denetim riskleri diğer önde gelen konular arasında yer almaktadır. Bu konuları hemen hemen her konumdan katılımcı vurgulamıştır. Fakat XBRL ile ilgili denetim riskleri muhasebe müdürleri açısından merak edilen bir konu değildir. Bunlar dışında XBRL'nin kurumsal kaynak planlaması ile ilişkisi, finansal raporlama sürecine kattığı değer ve iç kontrollerin anlaşılması gibi konularda daha ziyade uygulamanın içinde yer alana iç denetçilerce merak edilen konular olmakla beraber mali işler koordinatörleri, muhasebe müdürleri, mali işler koordinatörleri tarafından pek fazla ilgi görmemiştir.

5.3.3.1.2. Sürekli denetim ile ilgili non-parametrik testler

Her biri için ayrı ayrı olmak üzere “sürekli denetim yaklaşımının uygulanmasının temel amaçları” ve “sürekli denetimde BT kullanmanın amacı” ile ankete katılanların konumları arasında anlamlı farklılıkların olup olmadığını görmek için Kruskal-Wallis Testi yapılmıştır.

Sürekli denetim yaklaşımının uygulanmasının temel amaçlarından birisi olan uygulanan önerileri izleme ile ankete katılanların konumları arasında anlamlı farklılıklar bulunmuştur (Ek-1 Tablo-76). Muhasebe müdürleri, mali işler

koordinatörleri ve denetim koordinatörleri sürekli denetimin temel amacını uygulanan önerileri izlemek olarak görürken, iç denetim yöneticileri aksi yönde bildirimde bulunmuştur. Çünkü iç denetim yöneticileri sürekli denetim yaklaşımının uygulanmasında elektronik veri ve kanıtlar üzerine daha çok odaklanmaktadırlar. BT kaynaklarının ve BT risklerinin değerlendirilmesinde iç denetim birimlerinin sorumluluk ve görevleri diğer yöneticilere göre daha fazladır.

Sürekli denetimde BT'nin kullanım amacı ile ankete katılanların konumları arasında anlamlı farklılıklar bulunmuştur (Ek-1 Tablo-77). Muhasebe müdürleri sürekli denetimde kullanılan teknolojilerin risk yönetiminde kullanılabilen teknoloji odaklı sürekli denetim tekniklerini yaygınlaştırmak için oluşturulduğunu düşünürken, genel müdür yardımcıları aksi yönde düşünmektedirler.

Kruskal-Wallis Testi dışında bir diğer non-parametrik test olarak uygulanan Spearman's Rank Order Korelasyonu sonuçlarına göre sürekli denetimde BT kullanım amacı ile ankete katılanların işletmedeki çalışma süreleri arasında anlamlı ilişki bulunmuştur (Ek-1 Tablo-78). Ankete katılanların işletmede çalışma süreleri arttıkça, sürekli denetimde kullanılan teknolojilerin risk yönetiminde kullanılabilen teknoloji odaklı sürekli denetim tekniklerini yaygınlaştırmak için oluşturulduğu düşüncesi kuvvetlenmektedir.

5.3.3.2. Risk odaklı iç denetim ile ilgili çapraz tablo analizleri ve non-parametrik testler

5.3.3.2.1. Risk odaklı iç denetim ile ilgili çapraz tablo analizleri

Risk odaklı iç denetim yaklaşımı ile ilgili çapraz tablo analizleri katılımcıların işletmedeki konumları itibarıyla düzenlenmiştir. Ankete katılanlar “risk odaklı iç denetim yaklaşımının uygulanma durumunu” ve “risk odaklı iç denetim yaklaşımının bileşenlerini” değerlendirmişlerdir.

- Ankete katılanların konumları ile risk odaklı iç denetim yaklaşımının uygulanma durumu arasındaki ilişki:

Tablo-38. Ankete Katılanların İşletmedeki Konumları*Risk Odaklı İç Denetim Yaklaşımının Uygulanması

Konum	İç denetim birimi Risk odaklı iç denetim yaklaşımını kullanıyor mu?		
	Evet	Hayır	Toplam
İç Denetçi	16	3	19
İç Denetim Yöneticisi	10	1	11
Genel müdür yardımcısı	3	0	3
Muhasebe Müdürü	6	1	7
Mali İşler koordinatörü	3	0	3
Denetim Koordinatörü	2	0	2
İç Kontrol Koordinatörü	6	0	6
Toplam	46	5	51

Tablo-38'e bakıldığında katılımcıların çoğunluğu risk odaklı iç denetim yaklaşımının kullanıldığını bildirmiştir (46 kişi). Risk odaklı iç denetim yaklaşımının uygulanmadığını bildirenler de vardır fakat sayıları oldukça azdır (5 kişi). Genel müdür yardımcılarının, mali işler koordinatörlerinin, denetim koordinatörlerinin ve iç kontrol koordinatörlerinin tümü risk odaklı iç denetim yaklaşımının uygulandığını bildirmiştir.

İşletmeler risk odaklı iç denetim yaklaşımına olumlu bakmaktadır ve işletmelerinde uygulayanların çokluğu dikkat çekmektedir. Çünkü işletmelerde bilgi teknolojileri yoğun bir çalışma ortamı vardır ve bu ortamın oluşturduğu risklerin ölçülmesi ve yönetilmesinde yeni yöntemler geliştirilmesi gerekmiş, dolayısıyla geleneksel yöntemlerle yapılan iç denetim faaliyetleri genişlemiş ve risk odaklı iç denetim yaklaşımı benimsenmiştir.

- Ankete katılanların konumları ile risk odaklı iç denetim sürecinin bileşenleri arasındaki ilişki:

Tablo-39. Ankete Katılanların Konumları*Risk Odaklı İç Denetim Yaklaşımının Bileşenleri

KONUM		İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Risk odaklı iç denetim süreci bileşenleri	İç denetçi işletme içindeki olası risk alanlarını araştırmak durumundadır	Katılmıyorum	1	0	1	0	0	0	2
		Kararsızım	2	0	0	0	0	0	2
		Katılıyorum	4	1	0	1	0	2	9
		Kesinlikle katılıyorum	12	9	6	2	2	4	37
Risk tanımlamasında işletme bünyesinde bulunan riskler her risk seviyesine göre (düşük, orta, yüksek) değerlendirilir ve risk alanları tablosunda gösterilir	Katılmıyorum	1	0	1	0	0	0	0	2
	Kararsızım	2	2	0	0	0	0	0	4
	Katılıyorum	1	1	0	0	0	0	1	3
	Kesinlikle katılıyorum	15	7	6	2	3	2	5	40
Risk faktörleri tespit edildikten sonra bu faktörlerin toplam risk içindeki nispi önemini belirlemek gerekir.	Katılmıyorum	1	0	1	0	0	0	0	2
	Kararsızım	3	3	0	0	0	0	0	6
	Katılıyorum	0	0	0	0	0	0	3	3
	Kesinlikle katılıyorum	15	7	6	2	3	2	3	38
Belirlenen riskler derecelerine bağlı olarak sıraya konulur.	Katılmıyorum	2	1	1	0	0	0	0	4
	Kararsızım	2	0	0	0	0	0	0	2
	Katılıyorum	0	2	0	0	0	0	3	5
	Kesinlikle katılıyorum	15	7	6	2	3	2	3	38
Risklerle ilgili sonuçlar yönetim kuruluna, denetim komitesine ve diğer ilgililere iletilir.	Katılmıyorum	1	0	1	0	0	0	0	2
	Kararsızım	2	0	0	0	0	0	0	2
	Katılıyorum	11	4	4	2	2	1	1	25
	Kesinlikle katılıyorum	5	6	1	0	1	1	5	19

Tablo-39’da görüldüğü üzere tabloda yer alan ifadelerin her biri bir risk odaklı iç denetim yaklaşımı bileşenini temsil etmektedir. Bunlar sırasıyla işletme hakkında bilgi toplama, risk tanımlama, risk ölçümü, risk önceliklendirme ve sonuçların raporlanmasıdır. Ankete katılanların çoğu genelde bu bileşenlere ait ifadelere katılım göstermişlerdir.

Katılımcıların çoğu iç denetçinin işletme içindeki olası risk alanlarını araştırması gerektiğini vurgulayarak risk odaklı iç denetim yaklaşımının ilk bileşeni olan işletme hakkında bilgi toplamaya katılımı vurgulamıştır (Katılıyorum-9+Kesinlikle katılıyorum-37= 46 kişi). Bu konuda kararsızlar ve aksi yönde düşünenler olsa bile bunlar sayıca oldukça azdır.

Yine katılımcıların çoğu ikinci bileşen olarak ele alınan risk tanımlama ile ilgili olarak işletme bünyesinde bulunan riskleri her risk seviyesine göre (düşük, orta, yüksek)

değerlendirilip, risk alanları tablosunun oluşturulması konusuna katılmaktadırlar (Katılıyorum-3+Kesinlikle katılıyorum-40= 43 kişi).

Katılımcıların çoğu risk ölçümünün risk yönetiminin bir bileşeni olduğunu kabul etmiştir. Risk faktörleri tespit edildikten sonra bu faktörlerin toplam risk içindeki nispi önemini belirlenmesi gerektiğini de düşünmektedirler (Katılıyorum-3+Kesinlikle katılıyorum-38= 41 kişi). Bu bileşen ile ilgili olarak kararsızların sayılarının biraz daha arttığı görülmekle birlikte bunların iç denetçi ve iç denetim yöneticilerinden oluşması dikkat çekicidir.

Risk derecelendirmesi veya risk değerlendirme ile ilgili olarak ise risklerin derecelerine bağlı olarak sıraya konulması gerektiği vurgulanmaktadır (Katılıyorum-5+Kesinlikle katılıyorum-38= 43 kişi).

Son olarak risklerle ilgili sonuçların yönetim kuruluna, denetim komitesine ve diğer ilgililere iletilmesi ile ilgili olarak ortaya konulan sonuçların raporlanması bileşeni de katılımcılar tarafından çoğunlukla kabul edilmektedir (Katılıyorum-25+Kesinlikle katılıyorum-19= 44 kişi). Bu konuda kararsızlığa kapılan veya bu bileşene katılmayan katılımcıların çok az olduğu görülmektedir. Bu kişiler arasında iç denetçilerin yer alması dikkat çekicidir.

Özetle, risk odaklı iç denetim bileşenleri açısından baktığımızda katılımcıların genellikle katılımlarının yüksek olduğu görülmüştür. Ayrıca risk odaklı iç denetim yaklaşımı çoğunlukla uygulanan bir iç denetim yaklaşımı olduğu için bu yaklaşımın bileşenleri ile ilgili değerlendirmelere de katılım yüksek olmuştur. İç denetim sorumluları denetim faaliyetini yerine getirirken geçmiş faaliyetlerin değerlendirilmesinden ziyade risk odaklı denetim yaklaşımının bileşenleri doğrultusunda gelecekle ilgili faaliyetleri yönetebilmektedir.

5.3.3.2.2. Risk odaklı iç denetim ile ilgili non-parametrik testler

Risk odaklı iç denetim yaklaşımının bileşenleri ile ankete katılanların konumları arasında anlamlı farklılıkların olup olmadığını görmek için Kruskal-Wallis Testi yapılmıştır. Risk odaklı iç denetim yaklaşımı bileşenleri ile ankete katılanların konumları arasında anlamlı farklılık bulunamamıştır. Fakat BT kullanan iç denetim personeli sayısı ile risk odaklı iç denetim yaklaşımı bileşenleri arasında anlamlı farklılıklar bulunmuştur (Ek-1 Tablo-79). BT kullanan iç denetim personeli sayısı 7-9

kişi arasında olanlar iç denetçinin olası risk alanlarını araştırması gerektiğini savunurken, BT kullanan iç denetim personeli olmayanlar aksi yönde görüş bildirmektedir.

BT kullanan iç denetim personeli sayısı 7-9 kişi arasında olanlar risk tanımlama ile ilgili olarak işletme bünyesinde bulunan riskleri her risk seviyesine göre değerlendirilip, risk alanları tablosunun oluşturulması gerektiğini bildirirken, BT kullanan iç denetim personeli olmayanlar aksi yönde görüş bildirmektedir.

BT kullanan iç denetim personeli sayısı 7-9 kişi arasında olan katılımcılar risk tespit edildikten sonra bu faktörlerin toplam risk içindeki nispi öneminin belirlenmesi gerektiğini vurgularken, BT kullanan iç denetim personeli olmayanlar aksi yönde görüş bildirmektedir.

BT kullanan iç denetim personeli sayısı 7-9 kişi arasında olan katılımcılar risk değerlendirme ile ilgili olarak risklerin derecelerine bağlı olarak sıraya konulması gerektiğini düşünürken, BT kullanan iç denetim personeli olmayanlar aksi yönde görüş bildirmektedir.

BT kullanan iç denetim personeli sayısı 7-9 kişi arasında olanlar risklerle ilgili sonuçların yönetim kuruluna, denetim komitesine ve diğer ilgililere iletilmesi gerektiğini bildirirken, BT kullanan iç denetim personeli olmayanlar aksi yönde görüş bildirmektedir.

Özetle, işletmede çalışan personel arasında BT kullanımının yaygın olması denetim faaliyetinin risk odaklı iç denetim yaklaşımının bileşenleri doğrultusunda gerçekleştirilmesinde etkili olmaktadır.

Kruskal-Wallis Testi dışında bir diğer non-parametrik test olarak uygulanan Spearman's Rank Order Korelasyonu sonuçlarına göre Risk odaklı iç denetim yaklaşımı bileşenlerinden sonuçların raporlanması bileşeni ile iç denetim biriminin faaliyet gösterdiği süre arasında anlamlı ilişki bulunmuştur (Ek-1 Tablo-80). Buna göre iç denetim faaliyetinin uygulandığı süre arttıkça, risklerle ilgili sonuçların yönetim kurulu, denetim komitesi veya diğer ilgililere iletimine katılım düzeyi de artmaktadır.

5.3.3.3. Kontrol öz değerlendirme ile ilgili çapraz tablo analizleri ve non-parametrik testler

5.3.3.3.1. Kontrol öz değerlendirme ile ilgili çapraz tablo analizleri

Kontrol özdeğerlendirme yaklaşımı ile ilgili çapraz tablo analizleri katılımcıların işletmedeki konumları itibarıyla düzenlenmiştir. Ankete katılanlar “Kontrol özdeğerlendirme yaklaşımının uygulanma durumunu”, “uygulanma nedenlerini”, “uygulanmama nedenlerini” ve hangi yaklaşımların uygulandığını” değerlendirmişlerdir.

- **Ankete katılanların konumları ile kontrol özdeğerlendirme yaklaşımının uygulanma durumu arasındaki ilişki:**

Tablo-40. Ankete Katılanların İşletmedeki Konumları*Kontrol Özdeğerlendirme Yaklaşımının Uygulanması

Konum	Kontrol öz değerlendirme yaklaşımı işletmenizde uygulanıyor mu?		
	Evet	Hayır	Toplam
İç Denetçi	6	13	19
İç Denetim Yöneticisi	8	3	11
Genel müdür yardımcısı	0	2	2
Muhasebe Müdürü	1	6	7
Mali İşler koordinatörü	1	2	3
Denetim Koordinatörü	1	1	2
İç Kontrol Koordinatörü	5	1	6
Toplam	22	28	50

Tablo-40’da görüldüğü üzere kontrol özdeğerlendirme yaklaşımını uygulayanlar (22 kişi) ve uygulamayanlar (28 kişi) hemen hemen eşittir denilebilir. İç denetim yöneticileri çoğunlukla kontrol özdeğerlendirmenin uygulandığını bildirirken, iç denetçiler çoğunlukla uygulanmadığını bildirmektedir. İç kontrol koordinatörleri çoğunlukla uygulandığını bildirirken, muhasebe müdürleri de çoğunlukla uygulanmadıklarını bildirmektedir.

Özetle, kontrol özdeğerleme yaklaşımının henüz yaygınlık göstermediği anlaşılmaktadır. Bunun nedeni günümüzde risk odaklı iç denetim yaklaşımının daha fazla benimsenmiş olamasıdır. Çünkü artık denetim faaliyetleri sadece geçmiş döneme ait hataların incelenmesi ve belirli bir faaliyete veya şahsa yönelik yürütülen çalışmaları denetleme işi değildir. Denetim risk odaklı yapılmaya başlanmıştır ve işletmelerde geçmiş faaliyetlerin değerlendirilmesinden çok, geleceğin daha iyi yönetilmesine odaklanılmaktadır.

- Ankete katılanların konumları ile kontrol özdeğerlendirme yaklaşımının uygulanma nedenleri arasındaki ilişki:

Tablo-41. Ankete Katılanların Konumları*Kontrol Öz Değerlendirme Yaklaşımının Uygulanma Nedenleri

KONUM		İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd.	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Denetimin kapsamını genişletmek	Katılıyorum	2	2	0	-	0	0	4	8
	Kesinlikle Katılıyorum	4	6	1	-	1	1	1	14
Yasalara uyum sağlamak	Katılmıyorum	1	0	0	-	0	0	0	1
	Katılıyorum	1	2	0	-	0	0	3	6
	Kesinlikle Katılıyorum	4	6	1	-	1	1	2	15
Bir iş sürecinin yeniden yapılanma sürecini izlemek	Katılıyorum	2	2	0	-	0	0	1	5
	Kesinlikle Katılıyorum	4	6	1	-	1	1	4	17
Amaçların başarılmasını sağlamak	Katılıyorum	1	2	0	-	0	0	1	4
	Kesinlikle Katılıyorum	5	6	1	-	1	1	3	17
Katılımcıların öğrenme sürecini geliştirmek	Katılıyorum	2	2	0	-	0	0	1	5
	Kesinlikle Katılıyorum	4	6	1	-	1	1	4	17
Etkin bir iç kontrol ve risk yönetimi için her düzeyde sorumlulukların yerine getirilmesi konusunda yönetime yardımcı olmak	Katılıyorum	2	2	0	-	0	0	1	5
	Kesinlikle Katılıyorum	4	6	1	-	1	1	4	17
Planlama stratejilerini desteklemek	Katılıyorum	2	3	0	-	0	0	3	8
	Kesinlikle Katılıyorum	4	5	1	-	1	1	2	14

Tablo-41’de görüldüğü üzere denetimin kapsamını genişletmek, etkin bir iç kontrol ve risk yönetimi için her düzeyde sorumlulukların yerine getirilmesi konusunda yönetime yardımcı olmak, bir iş sürecinin yeniden yapılanma sürecini izlemek, öğrenme sürecini geliştirmek ve planlama stratejilerini geliştirmek gibi nedenlere katılımcıların çoğunlukla ve en yüksek düzeyde katılım gösterdiği nedenlerdir.

Kontrol özdeğerleme yaklaşımını uygulayanlar açısından en önemli neden denetimin kapsamını genişletmektir. Bununla birlikte bir iş sürecinin yeniden yapılanmasını sağlamak ve amaçların başarılmasını sağlamak da kontrol özdeğerlemenin gerçekleştirilme nedenleri arasındadır. Ayrıca etkin bir iç kontrol ve risk yönetimi için her düzeyde sorumlulukların yerine getirilmesi konusunda yönetime yardımcı olmanın da kontrol özdeğerlendirmenin benimsenmesi ile yakından ilgili olduğu söylenebilir. Bu konulara katılımı en yüksek grupların iç denetçiler, iç denetim yöneticileri ve iç kontrol kordinatörleri olduğu dikkat çekmektedir.

- Ankete katılanların konumları ile kontrol özdeğerlendirme yaklaşımının uygulanmama nedenleri arasındaki ilişki:

Tablo-42. Ankete Katılanların Konumları*Kontrol Öz Değerlendirme Yaklaşımı Uygulanmama Nedenleri

KONUM Kontrol Özdeğerlendirme Uygulanmama Nedenleri	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Uygulama yönteminin bilinmemesi	10	2	1	5	2	1	1	22
İşletme yönetiminin bu uygulamaya sıcak bakmaması	4	0	1	1	0	0	0	6
Yaklaşımın karmaşık olması	0	1	0	0	0	0	0	1

Tablo-42’de görüldüğü üzere kontrol özdeğerlendirme yaklaşımını uygulamayan katılımcıların çoğunlukla bu yaklaşımın uygulanma yöntemini bilmemeleri nedeniyle kontrol özdeğerlendirme yaklaşımını uygulamadıkları görülmektedir (22 kişi).

Kontrol özdeğerlendirme yaklaşımın uygulanma yönteminin bilinmemesi bu yaklaşımın en önemli uygulanmama nedenidir. Hemen her konumdan katılımcı bu konuda aynı fikirdeyken, iç denetçilerin ve muhasebe müdürlerinin çoğunluğu oluşturdukları görülmektedir.

- Ankete katılanların konumları ile uygulanan kontrol özdeğerlendirme yaklaşımları arasındaki ilişki:

Tablo-43. Ankete Katılanların Konumları*Kontrol Öz Değerlendirme Yaklaşımı Türleri

KONUM Kontrol Özdeğerlendirme Uygulanmama Nedenleri	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam	İç Denetçi
Grup Çalışması	3	6	-	1	0	-	0	0	10
Anket	4	5	-	0	1	-	4	1	13
Yönetici Analizleri	2	5	-	1	0	-	1	0	9

Tablo-43’de görüldüğü üzere ankete katılanlardan kontrol öz değerlendirme yaklaşımının uygulandığını bildirenler kontrol özdeğerlendirme türlerinden en çok anket (13 kişi) ve sonrasında da grup çalışmasını (10 kişi) kullandıklarını bildirmiştir. Anketi kullandıklarını bildirenlerin çoğunluğunu iç kontrol koordinatörleri ve iç denetim yöneticilerinden oluşmaktadır. Grup çalışmasını kullandıklarını bildirenlerin çoğunluğunu ise iç denetim yöneticileri oluşturmaktadır. Bunlar haricinde yönetici analizlerini kullananlar da bulunmaktadır (9 kişi).

Kontrol özdeğerlendirme yaklaşımı henüz yaygınlık göstermemekle birlikte bu yaklaşımı uygulayan işletmelerde kontrol özdeğerleme yaklaşımı olarak genellikle anket ve sonrasında da grup çalışması ve yönetici analizleri kullanıldığı görülmektedir. Grup çalışması yaklaşımının da kendi içinde çeşitleri vardır. Grup çalışmasını kullananlar riske, kontrole veya sürece dayalı olarak grup çalışmasını uygulamaktadır.

5.3.3.3.2. Kontrol öz değerlendirme ile ilgili non-parametrik testler

Kontrol özdeğerlendirme yaklaşımının uygulanma nedenleri ile ankete katılanların konumları arasında anlamlı farklılıkların olup olmadığını görmek için Kruskal-Wallis Testi yapılmıştır. Ankete katılanların konumları ile kontrol özdeğerlendirmenin uygulanma nedenleri arasında anlamlı farklılık bulunamamıştır.

Kruskal-Wallis Testi dışında bir diğer non-parametrik test olarak uygulanan Spearman's Rank Order Korelasyonu sonuçlarına göre Kontrol özdeğerlendirme yaklaşımının uygulanma nedenleri ile ankete katılanların çalıştıkları işletmelerdeki çalışma süreleri arasında anlamlı ilişki bulunmuştur (Ek-1 Tablo-81). Buna göre;

Katılımcıların işletmedeki çalışma süresi arttıkça, yasalara uyum sağlama nedeniyle kontrol özdeğerlendirme uygulama düzeyleri azalmaktadır.

Katılımcıların işletmedeki çalışma süresi arttıkça, iş sürecinin yapılmasını izleme açısından kontrol özdeğerlendirme düzeyi azalmaktadır.

Katılımcıların işletmedeki çalışma süresi arttıkça, amaçların başarılması konusunda katılım düzeyi azalmaktadır.

Katılımcıların işletmedeki çalışma süresi arttıkça, katılımcıların öğrenme sürecini geliştirme açısından katılım düzeyleri azalmaktadır.

Katılımcıların işletmedeki çalışma süresi arttıkça, etkin bir iç kontrol ve risk yönetimi için yönetime destek verme açısından katılım düzeyleri düşmektedir.

Özetle, katılımcıların işletmedeki çalışma süresi arttıkça kontrol özdeğerlendirme yaklaşımının uygulanma nedenlerinde aksi yönde bir değişim görülmektedir. Bunun nedeni iç denetimden sorumlu tarafların bu yaklaşımın uygulama süreci hakkında bilgilerinin yetersiz oluşudur. Ayrıca işletmedeki çalışma süresi arttıkça, yeni bir yaklaşımın benimsenmesi konusunda da istekliliğin azalması ve mevcut düzenin değiştirilmek istenmemesi sözkonusu olabilir. Çünkü benimsenecek

yeni bir yaklaşım tüm denetim sürecini değiştirebilir ve bu yeni süreci öğrenmeye iç denetim faaliyetini gerçekleştiren taraflar istekli olmayabilir.

5.3.3.4. İç denetim yaklaşımları doğrultusunda iç denetim sürecinde kullanılan araç ve gereçlerle ilgili çapraz tablo analizleri

İç denetim yaklaşımları doğrultusunda gerçekleştirilen iç denetim uygulama sürecinde kullanılabilecek araç ve gereçlere dair şimdiki ve gelecekteki durumun değerlendirilmesi ile ilgili çapraz tablo analizleri katılımcıların işletmedeki konumları itibarıyla düzenlenmiştir. Ankete katılanlar sürekli denetim, risk odaklı iç denetim ve kontrol özdeğerlendirme yaklaşımlarında kullanılabilecek araç ve gereçlerin hem mevcut durumda hem de gelecekteki kullanımlarına ilişkin değerlendirmelerde bulunmuşlardır.

Tablo-44. Ankete Katılanların Konumları*İç Denetim Faaliyetinde Kullanılan Araç ve Teknikler (Şimdi)

Konum		İç Denetçi	İç Den. Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Sürekli denetim teknikleri	Hiç kullanılmıyor	1	1	0	0	0	0	0	2
	Kullanılmıyor	5	2	2	0	1	1	1	12
	Kısmen kullanılıyor	0	0	0	1	0	0	0	1
	Kullanılıyor	10	7	1	1	0	1	2	22
	Çok kullanılıyor	3	0	4	0	2	0	3	12
Veri inceleme-veri analizi	Kullanılmıyor	1	2	1	0	0	0	0	4
	Kısmen kullanılıyor	7	1	2	1	1	1	1	14
	Kullanılıyor	5	4	1	0	0	1	4	15
	Çok kullanılıyor	6	3	3	1	2	0	1	16
Veri madenciliği	Hiç kullanılmıyor	7	1	1	0	1	0	2	12
	Kullanılmıyor	4	2	3	0	0	1	0	10
	Kısmen kullanılıyor	3	4	1	2	2	1	3	16
	Kullanılıyor	2	1	0	0	0	0	1	4
	Çok kullanılıyor	3	2	2	0	0	0	0	7
Risk odaklı iç denetim planı	Kullanılmıyor	1	0	1	0	0	0	0	2
	Kısmen kullanılıyor	1	1	0	0	0	0	0	2
	Kullanılıyor	7	1	1	0	1	1	2	13
	Çok kullanılıyor	10	8	5	2	2	1	4	32
Bilgisayar destekli denetim teknikleri	Hiç kullanılmıyor	3	0	0	0	0	0	2	5
	Kullanılmıyor	2	0	1	0	0	1	1	5
	Kısmen kullanılıyor	2	4	0	0	0	0	1	7
	Kullanılıyor	8	3	5	2	2	0	0	20
	Çok kullanılıyor	4	3	1	0	1	1	2	12
Denetim uzman sistemleri	Hiç kullanılmıyor	5	1	0	0	1	0	3	10
	Kullanılmıyor	9	2	6	0	2	1	1	21
	Kısmen kullanılıyor	2	3	0	2	0	1	1	9
	Kullanılıyor	1	1	0	0	0	0	0	2
	Çok kullanılıyor	2	3	1	0	0	0	1	7
Genelleştirilmiş denetim yazılımı	Hiç kullanılmıyor	5	1	0	0	1	0	3	10
	Kullanılmıyor	9	2	6	0	2	2	2	23
	Kısmen kullanılıyor	2	4	0	2	0	0	0	8
	Kullanılıyor	1	1	0	0	0	0	0	2
	Çok kullanılıyor	2	2	1	0	0	0	1	6
Analitik inceleme prosedürleri	Hiç kullanılmıyor	4	1	0	0	1	0	0	6
	Kullanılmıyor	1	0	1	0	0	0	1	3
	Kısmen kullanılıyor	7	2	0	1	1	1	0	12
	Kullanılıyor	5	3	1	0	0	1	2	12
	Çok kullanılıyor	2	4	5	1	1	0	3	16
Kıyaslama	Hiç kullanılmıyor	4	1	0	0	1	0	1	7
	Kullanılmıyor	3	3	2	1	0	0	1	10
	Kısmen kullanılıyor	7	1	2	1	0	1	0	12
	Kullanılıyor	3	3	0	0	1	1	2	10
	Çok kullanılıyor	2	2	3	0	1	0	2	10
İstatistiksel örnekleme	Hiç kullanılmıyor	0	1	0	0	0	0	0	1
	Kullanılmıyor	1	0	1	0	0	0	1	3
	Kısmen kullanılıyor	7	0	1	0	1	1	1	11
	Kullanılıyor	1	3	1	0	0	0	0	5
	Çok kullanılıyor	10	6	4	2	2	1	4	29
Uygulama yazılımı ve eşleme	Hiç kullanılmıyor	4	2	0	0	1	0	3	10
	Kullanılmıyor	9	2	6	2	1	1	1	22
	Kısmen kullanılıyor	4	2	0	0	1	1	1	9
	Kullanılıyor	0	2	0	0	0	0	0	2
	Çok kullanılıyor	2	2	1	0	0	0	1	6

Tablo-44. Ankete Katılanların Konumları*İç Denetim Faaliyetinde Kullanılan Araç ve Teknikler (Şimdi) (Devam)

İç denetim Faaliyetinde Kullanılan Araç ve Teknikler		KONUM		İç Denetçi	İç Den. Yön.	Gn Md. Yrd.	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol	Toplam
Süreç modelleme	Hiç kullanılmıyor			2	3	5	0	1	0	2	13
	Kullanılmıyor			11	2	1	2	1	1	1	19
	Kısmen kullanılıyor			1	2	0	0	0	0	0	3
	Kullanılıyor			3	2	0	0	1	1	2	9
	Çok kullanılıyor			2	1	1	0	0	0	1	5
Bütünleşik test tekniği	Hiç kullanılmıyor			4	3	0	0	1	0	3	11
	Kullanılmıyor			8	3	6	1	1	1	1	21
	Kısmen kullanılıyor			2	2	0	0	1	1	1	7
	Kullanılıyor			2	1	0	1	0	0	0	4
	Çok kullanılıyor			1	1	1	0	0	0	1	4
Veri testi tekniği	Hiç kullanılmıyor			1	3	0	0	0	0	2	6
	Kullanılmıyor			11	2	1	1	1	1	1	18
	Kısmen kullanılıyor			2	2	2	0	1	1	1	9
	Kullanılıyor			3	2	0	1	0	0	1	7
	Çok kullanılıyor			2	1	4	0	1	0	1	9
Paralel simülasyon tekniği	Hiç kullanılmıyor			6	2	0	0	1	0	3	12
	Kullanılmıyor			8	5	6	1	1	1	1	23
	Kısmen kullanılıyor			2	2	0	0	1	1	1	7
	Kullanılıyor			1	0	0	1	0	0	0	2
	Çok kullanılıyor			1	1	1	0	0	0	1	4
Elektronik çalışma kağıtları	Hiç kullanılmıyor			4	0	0	0	1	0	3	8
	Kullanılmıyor			11	2	6	2	2	2	2	27
	Kısmen kullanılıyor			1	0	0	0	0	0	0	1
	Kullanılıyor			2	4	0	0	0	0	0	6
	Çok kullanılıyor			1	3	1	0	0	0	1	6
Akış şeması yazılımları	Hiç kullanılmıyor			1	0	0	0	0	0	0	1
	Kullanılmıyor			11	4	1	2	1	1	2	22
	Kısmen kullanılıyor			2	1	1	0	0	0	2	6
	Kullanılıyor			2	3	0	0	0	1	1	7
	Çok kullanılıyor			3	2	5	0	2	0	1	13
Denegeli Ölçüm Kartı	Hiç kullanılmıyor			5	2	0	0	1	0	4	12
	Kullanılmıyor			8	3	6	2	1	1	0	21
	Kısmen kullanılıyor			2	0	0	0	0	0	0	2
	Kullanılıyor			3	3	0	0	1	1	2	10
	Çok kullanılıyor			1	2	1	0	0	0	0	4

Tablo-44'e göre mevcut durumda katılımcıların en çok kullandığı araç risk odaklı iç denetim planıdır (Kullanılıyor-13+Çok kullanılıyor-32= 46 kişi). Ayrıca tablodan da görülmektedir ki bu 46 kişinin 32'si bu aracın çok kullanıldığını bildirmiştir. Sonrasında BDDT'lerini çoğunlukla kullandığını bildiren katılımcılar bunlar içerisinde de özellikle istatistiksel örnekleme, analitik inceleme prosedürleri, kıyaslama, süreç modelleme, veri testi tekniği, akış şemaları yazılımlarını, balans skor kart ve elektronik çalışma kağıtlarının en çok kullanıldığını belirtmiştir. Sürekli denetim tekniklerini de çoğunlukla kullandıklarını bildiren katılımcılar özellikle veri analizini de oldukça kullandıkları anlaşılmaktadır. Bu araç ve tekniklerin kullanımı konusunda genel

olarak baktığımızda iç denetçilerin, iç denetim yöneticilerinin, iç kontrol koordinatörlerinin ve muhasebe müdürlerinin daha fazla bilgi sahibi olduğunu anlıyoruz.

Tablo-45. Ankete Katılanların Konumları*İç Denetim Faaliyetinde Kullanılan Araç ve Teknikler (Gelecekte)

İç denetim Faaliyetinde Kullanılan Araç ve Teknikler		Konum	İç Denetçi	İç Den. Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol	Toplam
Sürekli denetim teknikleri	Kullanılmayacak		1	0	1	0	0	0	0	2
	Kısmen kullanılacak		1	0	0	0	0	0	0	1
	Kullanılacak		7	3	0	0	1	1	2	14
	Çok kullanılacak		10	7	6	2	2	1	4	32
Veri inceleme-veri analizi	Kullanılmayacak		1	0	1	0	0	0	0	2
	Kısmen kullanılacak		1	0	1	0	0	0	0	2
	Kullanılacak		7	3	0	0	1	1	2	14
	Çok kullanılacak		10	7	5	2	2	1	4	31
Veri madenciliği	Hiç kullanılmayacak		0	0	1	0	0	0	0	1
	Kullanılmayacak		1	0	1	0	0	0	0	2
	Kısmen kullanılacak		6	4	2	0	0	1	1	14
	Kullanılacak		5	2	0	0	1	1	4	13
	Çok kullanılacak		7	4	3	2	2	0	1	19
Risk odaklı iç denetim planı	Hiç kullanılmayacak		1	0	1	0	0	0	0	2
	Kullanılacak		3	1	0	0	0	0	1	5
	Çok kullanılacak		15	9	6	2	3	2	5	42
	Kullanılmayacak		1	0	1	0	0	0	0	2
Bilgisayar destekli denetim teknikleri	Kısmen kullanılacak		0	0	0	0	0	0	2	2
	Kullanılacak		8	1	0	0	1	1	2	13
	Çok kullanılacak		10	9	6	2	2	1	2	32
	Kullanılmayacak		1	0	1	0	0	0	0	2
Denetim uzman sistemleri	Kısmen kullanılacak		7	2	0	0	1	1	4	15
	Kullanılacak		9	2	0	1	1	1	1	15
	Çok kullanılacak		2	6	6	1	1	0	1	17
	Kullanılmayacak		6	0	1	0	1	0	1	9
Genelleştirilmiş denetim yazılımı	Kısmen kullanılacak		0	0	0	0	0	0	2	2
	Kullanılacak		10	4	0	1	0	2	2	19
	Çok kullanılacak		3	6	6	1	2	0	1	19
	Kullanılmayacak		1	0	1	0	0	0	0	2
Analitik inceleme prosedürleri	Kısmen kullanılacak		5	0	0	0	1	0	1	7
	Kullanılacak		10	3	0	1	1	2	2	19
	Çok kullanılacak		3	7	6	1	1	0	3	21
	Kullanılmayacak		1	1	1	0	0	0	0	3
Kıyaslama	Kısmen kullanılacak		6	0	1	0	1	0	1	9
	Kullanılacak		10	2	0	1	1	2	2	18
	Çok kullanılacak		2	7	5	1	1	0	3	19
	Kullanılmayacak		1	0	1	0	0	0	0	2
İstatistiksel örnekleme	Kısmen kullanılacak		1	0	0	0	0	0	0	1
	Kullanılacak		6	2	0	0	1	1	2	12
	Çok kullanılacak		11	8	6	2	2	1	4	34
	Kullanılmayacak		1	0	1	0	0	0	0	2
Uygulama yazılımı ve eşleme	Kısmen kullanılacak		8	1	2	0	2	1	4	18
	Kullanılacak		8	3	0	1	0	1	1	14
	Çok kullanılacak		2	6	4	1	1	0	1	15
	Kullanılmayacak		1	0	1	0	0	0	0	2
Süreç modelleme	Kısmen kullanılacak		3	3	3	0	0	0	2	11
	Kullanılacak		11	0	0	1	1	1	2	16
	Çok kullanılacak		4	7	3	1	2	1	2	20
	Kullanılmayacak		1	0	1	0	0	0	0	2

Tablo-45. Ankete Katılanların Konumları*İç Denetim Faaliyetinde Kullanılan Araç ve Teknikler (Gelecekte) (Devam)

İç denetim Faaliyetinde Kullanılan Araç ve Teknikler		KONUM	İç Denetçi	İç Den. Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kon. Koord.	Toplam
Bütünleşik test tekniği	Kullanılmayacak		5	0	1	0	1	0	1	8
	Kısmen kullanılacak		10	4	2	0	1	2	3	22
	Kullanılacak		1	0	0	1	0	0	1	3
	Çok kullanılacak		3	6	4	1	1	0	1	16
Veri testi tekniği	Kullanılmayacak		1	0	1	0	0	0	0	2
	Kısmen kullanılacak		1	2	2	0	0	0	2	7
	Kullanılacak		9	3	0	0	2	2	3	19
	Çok kullanılacak		8	5	4	2	1	0	1	21
Paralel simülasyon tekniği	Hiç kullanılmayacak		0	1	0	0	0	0	0	1
	Kullanılmayacak		6	1	1	0	1	0	1	10
	Kısmen kullanılacak		8	3	3	1	0	1	2	18
	Kullanılacak		3	1	0	0	1	1	2	8
Elektronik çalışma kağıtları	Çok kullanılacak		2	4	3	1	1	0	1	12
	Kullanılmayacak		1	0	1	0	0	0	0	2
	Kısmen kullanılacak		1	1	2	0	0	0	2	6
	Kullanılacak		13	1	0	1	1	2	3	21
Akış şeması yazılımları	Çok kullanılacak		4	8	4	1	2	0	1	20
	Kullanılmayacak		1	0	1	0	0	0	0	2
	Kısmen kullanılacak		1	1	1	1	0	0	0	4
	Kullanılacak		7	1	0	0	1	0	2	11
Denegeli Ölçüm Kartı	Çok kullanılacak		10	8	5	1	2	2	4	32
	Kullanılmayacak		2	1	1	0	0	0	0	4
	Kısmen kullanılacak		6	2	2	1	1	1	3	16
	Kullanılacak		7	0	0	0	0	0	1	8
	Çok kullanılacak		4	7	4	1	2	1	2	21

Tablo-45'e göre katılımcıların gelecekle ilgili değerlendirmelerine bakıldığında hemen hemen tüm araç ve teknikler açısından kullanılacaklarına dair katılımların yüksek olduğu görülmektedir. Yine iç denetçilerin, iç denetim yöneticilerinin ve iç kontrol koordinatörlerinin katılımları diğer katılımcılara nazaran daha yüksektir.

5.3.4. İç denetimin faaliyet alanları ile ilgili çapraz tablo analizleri ve non-parametrik testler

İç denetim faaliyet alanları ile ilgili çapraz tablo analizleri katılımcıların işletmedeki konumları itibarıyla hazırlanmıştır. İç denetim faaliyet alanları ile ilgili çapraz tablo analizleri risk yönetimi, iç kontrol ve kurumsal yönetim olmak üzere üç ayrı başlıkta verilecektir.

5.3.4.1. Risk yönetimi ile ilgili çapraz tablo analizleri ve non-parametrik testler

5.3.4.1.1. Risk yönetimi ile ilgili çapraz tablo analizleri

Risk yönetimi ile ilgili çapraz tablo analizleri katılımcıların işletmedeki konumları itibarıyla düzenlenmiştir. Ankete katılanlar “risk yönetiminin uygulanma durumu” ve “risk yönetimi bileşenlerini” değerlendirmişlerdir.

- **Ankete katılanların konumları ile risk yönetiminin uygulanma durumu arasındaki ilişki:**

Tablo-46. Ankete Katılanların Konumları*İşletmelerinde Risk Yönetimi Uygulama Durumu

KONUM	İşletmenizde Risk yönetimi uygulanıyor mu?		
	Evet	Hayır	Toplam
İç Denetçi	16	3	19
İç Denetim Yöneticisi	9	0	9
Genel müdür yardımcısı	2	0	2
Muhasebe Müdürü	6	1	7
Mali İşler koordinatörü	3	0	3
Denetim Koordinatörü	2	0	2
İç Kontrol Koordinatörü	6	0	6
Toplam	44	4	48

Tablo-46’ya göre ankete katılanların büyük bir çoğunluğu risk yönetiminin uygulandığını bildirmiştir (44 kişi). Risk yönetiminin uygulanmadığını bildiren 4 kişi vardır ve bunların 3’ü iç denetçidir. Denetim faaliyetlerinin risk odaklı hale gelmesi risk yönetim sürecinin uygulanmasını yaygınlaştırmıştır. Zaten daha önce de bildirildiği üzere iç denetim birimleri tarafından yerine getirilen danışmanlık hizmetleri kapsamında risk yönetimi ilk sırada yer almaktadır. Dolayısıyla bu durum da yine işletmelerde risk yönetimi uygulamalarının gerçekleştirildiğini ispatlamaktadır.

- Ankete katılanların konumları ile risk yönetiminin bileşenleri arasındaki ilişki:

Tablo-47. Ankete Katılanların Konumları*Risk Yönetimi Bileşenleri

Risk yönetimi Bileşenleri		Konum	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Kontrol ortamı, risklerin kurumda çalışan kişiler tarafından nasıl görüntülenmesi ve yönlendirilmesi gerektiğine dair bir temel oluşturur.	Katılmıyorum		1	0	1	0	0	0	0	2
	Kararsızım		2	0	0	0	0	0	0	2
	Katılıyorum		10	2	0	1	1	1	4	19
	Kesinlikle Katılıyorum		5	8	6	1	2	1	2	25
Yönetim risk stratejisini göz önünde bulundurarak hedefleri belirler.	Katılmıyorum		1	0	1	0	0	0	0	2
	Kararsızım		10	0	0	1	1	1	1	14
	Katılıyorum		3	3	0	0	0	0	1	7
	Kesinlikle Katılıyorum		4	7	6	1	2	1	4	25
Belirsizliklerin risk mi fırsat mı olduğu konusunda çalışmalar yapılır	Katılmıyorum		1	0	1	0	0	0	0	2
	Kararsızım		6	0	0	0	1	1	1	9
	Katılıyorum		7	3	0	1	0	0	1	12
	Kesinlikle Katılıyorum		4	7	6	1	2	1	4	25
Riskler tanımlandıktan sonra bunların işletme üzerindeki olası etkileri ve meydana gelme olasılıkları değerlendirir.	Katılmıyorum		1	0	1	0	0	0	0	2
	Kararsızım		4	0	0	0	1	0	1	6
	Katılıyorum		9	3	0	1	0	1	1	15
	Kesinlikle Katılıyorum		4	7	6	1	2	1	4	25
Belirlenen risklerin kurumun risk kapasitesi ve risk toleransı içinde olup olmadığı belirlenir.	Katılmıyorum		1	0	1	0	0	0	0	2
	Kararsızım		4	0	0	0	1	0	1	6
	Katılıyorum		9	3	0	1	0	1	3	17
	Kesinlikle Katılıyorum		4	7	6	1	2	1	2	23
Riske verilecek karşılıkların etkili bir biçimde yerine getirilmesi ve devam eden risklerin risk kapasitesi sınırları içinde yönetilmesi için politika ve prosedürler oluşturulur.	Katılmıyorum		1	0	1	0	0	0	0	2
	Kararsızım		4	0	0	0	1	0	1	6
	Katılıyorum		7	2	0	1	0	1	1	12
	Kesinlikle Katılıyorum		6	8	6	1	2	1	4	28
Kişilerin sorumluluklarını yerine getirmesi için ilgili bilgi belli bir biçimde ve belli zaman aralıkları ile tanımlanır ve iletilir.	Katılmıyorum		1	0	1	0	0	0	0	2
	Kararsızım		5	0	0	0	1	0	1	7
	Katılıyorum		8	3	0	1	0	1	1	14
	Kesinlikle Katılıyorum		4	7	6	1	2	1	4	25
Risk yönetiminin uygulanması izlenir ve etkinliğini arttırmak için gerektiğinde ayarlamalar yapılır.	Katılmıyorum		1	0	1	0	0	0	0	2
	Kararsızım		4	0	0	0	1	0	1	6
	Katılıyorum		9	3	0	1	0	1	3	17
	Kesinlikle Katılıyorum		3	7	6	1	2	1	2	22

Tablo-47’de görülen ifadelerin her biri bir risk yönetimi bileşenini temsil etmektedir. Bunlar sırasıyla kontrol ortamı, hedef belireme, risk tanımlama, risk

değerleme, risk tutumu, kontrol faaliyetleri, bilgi-iletişim ve izlemedir. Katılımcılar risk yönetimi bileşenlerine dair ifadelerinde genelde katılım göstermişlerdir.

Katılımcıların büyük bir çoğunluğu kontrol ortamı bileşeni doğrultusunda risklerin kurumda çalışan kişiler tarafından nasıl görüntülenmesi ve yönlendirilmesi gerektiğine dair bir temel oluşturulması gerektiğini vurgulamışlardır (Katılıyorum-19+Kesinlikle katılıyorum-25= 44 kişi).

İkinci bileşen olan hedef belirlemeye ilişkin olarak yönetim risk stratejisini göz önünde bulundurarak hedeflerin belirlenmesi gerektiğine katılımcıların katılımı yüksek olmuştur (Katılıyorum-7+Kesinlikle katılıyorum-25= 32 kişi). Bu bileşenin uygulanmasına yönelik kararsızlığını bildiren katılımcılar da olmuştur ve kararsızlar arasında iç denetçiler fazladır.

Katılımcılar risk tanımlama bileşeni doğrultusunda belirsizliklerin risk mi fırsat mı olduğu konusunda çalışmalar yapılması gerektiğini vurgulamaktadır (Katılıyorum-12+Kesinlikle katılıyorum-25= 37 kişi).

Risk değerlendirme bileşeni açısından katılımcıların çoğu riskler tanımlandıktan sonra bunların işletme üzerindeki olası etkilerinin ve meydana gelme olasılıklarının değerlendirilmesi gerektiğini bildirmişlerdir (Katılıyorum-15+Kesinlikle katılıyorum-25= 40 kişi). Kararsızlığını bildirenler ise 6 kişidir. Hedef belirleme ve risk tanımlama bileşenlerine göre kararsızların sayısı düşmüştür.

Belirlenen risklerin kurumun risk kapasitesi ve risk toleransı içinde olup olmadığını belirlenmesine olanak sağlayan risk tutumu da katılımcıların çoğunluğunun katılım gösterdiği bileşenlerdendir (Katılıyorum-13+Kesinlikle katılıyorum-27= 40 kişi).

Katılımcılar kontrol faaliyetleri bileşeni doğrultusunda riske verilecek karşılıkların etkili bir biçimde yerine getirilmesine ve devam eden risklerin risk kapasitesi sınırları içinde yönetilmesi için politika ve prosedürler oluşturulmasına katılımlarını bildirmişlerdir (Katılıyorum-12+Kesinlikle katılıyorum-28= 40 kişi).

Kişilerin sorumluluklarının yerine getirmeleriyle ilgili bilginin belli bir biçimde ve belli zaman aralıkları ile tanımlanması ve iletilmesi doğrultusunda oluşturulan bilgi-iletişim bileşenine katılımlarını bildirmişlerdir (Katılıyorum-14+Kesinlikle katılıyorum-25= 39 kişi).

Son bileşen olan izleme bileşeni açısından ise katılımcıların çoğu risk yönetiminin uygulanma sürecinin izlendiğini ve izleme faaliyetinin etkinliğini arttırmak için gerektiğinde ayarlamalar yapıldığını vurgulamışlardır (Katılıyorum-17+Kesinlikle katılıyorum-22= 39 kişi).

Özetle, katılımcıların risk yönetimi bileşenlerine genellikle katılım gösterdikleri görülmektedir. Bilgi teknolojilerindeki gelişmelerle birlikte işletmelerde değişen risk profillerinin belirlenmesi ve gerekli çözümlerinin geliştirilmesi için risk yönetimi sürecinin uygulanması gerekmiştir. Bu gelişmelerle birlikte işletmelerde yapılan denetim faaliyetleri geçmiş olaylardan ziyade risklere odaklanmış ve iç denetim faaliyetinin kapsamı genişleyerek risk yönetimi faaliyet alanını da kapsamaya başlamıştır. Ayrıca iç denetim birimlerinin üst yönetime sağladığı danışmanlık hizmetlerinde de risk yönetimi ilk sırada yer almaktadır.

5.3.4.1.2. Risk yönetimi ile ilgili non-parametrik testler

Risk yönetiminin bileşenleri ile ankete katılanların konumları arasında anlamlı farklılıkların olup olmadığını görmek için Kruskal-Wallis Testi yapılmıştır. Ankete katılanların konumları ile risk yönetimi bileşenleri arasında anlamlı farklılık bulunamamıştır. Fakat BT denetiminin uygulandığı süre ve BT kullanan iç denetim personeli sayısı ile risk yönetimi bileşenlerinden bazıları arasında anlamlı farklılıklar bulunmuştur.

BT denetiminin uygulandığı süre ile risk yönetimi bileşenlerinden birisi olan kontrol ortamı arasında anlamlı farklılıklar bulunmuştur (Ek-1 Tablo-82). 4-6 yıldır BT denetimi uygulayanlar risklerin kurumda çalışan kişiler tarafından nasıl görüntülenmesi ve yönlendirilmesi gerektiğine dair bir temel oluşturulduğunu bildirirken, BT denetimini uygulamayanlar aksi yönde bildirimde bulunmuştur.

BT denetiminin uygulandığı süre ile risk yönetimi bileşenlerinden birisi olan hedef belirleme arasında anlamlı farklılıklar bulunmuştur (Ek-1 Tablo-82). 1 yıldan az bir süredir BT denetimi uygulayanlar yönetimin işletme hedeflerini risk stratejisini göz önünde bulundurarak hedefleri belirlediğini bildirirken, BT denetimini uygulamayanlar aksi yönde bildirimde bulunmuştur.

BT denetiminin uygulandığı süre ile risk yönetimi bileşenlerinden birisi olan risk tanımlama arasında anlamlı farklılıklar bulunmuştur (Ek-1 Tablo-82). 1 yıldan az bir

süredir BT denetimi uygulayanlar belirsizliklerin risk mi fırsat mı olduğu konusunda çalışmalar yapıldığını bildirirken, BT denetimini uygulamayanlar aksi yönde bildirimde bulunmuştur.

BT denetiminin uygulandığı süre ile risk yönetimi bileşenlerinden birisi olan kontrol faaliyetleri arasında anlamlı farklılıklar bulunmuştur (Ek-1 Tablo-82). 1 yıldan az bir süredir BT denetimi uygulayanlar riske verilecek karşılıkların etkili bir biçimde yerine getirilmesi ve devam eden risklerin risk kapasitesi sınırları içinde yönetilmesi için politika ve prosedürler oluşturulduğunu bildirirken, BT denetimini uygulamayanlar aksi yönde bildirimde bulunmuştur.

Özetle, BT denetimini uygulamaya başlayan işletmeler risk yönetimi sürecini gerçekleştirmektedir. BT denetimi uygulamayan işletmeler ise risk yönetim sürecinin uygulanması konusunda gereken çabayı göstermemektedir.

BT kullanan iç denetim personeli sayısı ile risk yönetimi bileşenlerinden sırasıyla kontrol ortamı, hedef belirleme, risk tanımlama, risk değerlendirme ve kontrol faaliyetleri arasında anlamlı farklılıklar bulunmuştur.

BT kullanan iç denetim personeli sayısı 7-9 kişi olanlar, kontrol ortamı bileşeni doğrultusunda risklerin kurumda çalışan kişiler tarafından nasıl görüntülenmesi ve yönlendirilmesi gerektiğine dair bir temel oluşturduğunu bildirirken, BT kullanan iç denetim personeli olmayanlar aksi yönde bildirimde bulunmuştur (Ek-1 Tablo-83).

BT kullanan iç denetim personeli sayısı 7-9 kişi olanlar, hedef belirleme bileşeni doğrultusunda yönetimin risk stratejisini göz önünde bulundurarak hedefleri belirlediğini bildirirken, BT kullanan iç denetim personeli olmayanlar aksi yönde bildirimde bulunmuştur (Ek-1 Tablo-83).

BT kullanan iç denetim personeli sayısı 7-9 kişi olanlar, risk tanımlama bileşeni doğrultusunda belirsizliklerin risk mi fırsat mı olduğu konusunda çalışmalar yapıldığını bildirirken, BT kullanan iç denetim personeli olmayanlar aksi yönde bildirimde bulunmuştur (Ek-1 Tablo-83).

BT kullanan iç denetim personeli sayısı 7-9 kişi olanlar, risk değerlendirme bileşeni doğrultusunda riskler tanımlandıktan sonra bunların işletme üzerindeki olası etkilerinin ve meydana gelme olasılıklarının değerlendirildiğini bildirirken, BT kullanan iç denetim personeli olmayanlar aksi yönde bildirimde bulunmuştur (Ek-1 Tablo-83).

BT kullanan iç denetim personeli sayısı 7-9 kişi arasında ve 10 kişi üzerinde olanlar, kontrol faaliyetleri bileşeni doğrultusunda riske verilecek karşılıkların etkili bir biçimde yerine getirilmesi ve devam eden risklerin risk kapasitesi sınırları içinde yönetilmesi için politika ve prosedürler oluşturulduğunu bildirirken, BT kullanan iç denetim personeli olmayanlar aksi yönde bildirimde bulunmuştur (Ek-1 Tablo-83).

Özetle, BT kullanan iç denetim personeli sayısı yeterli olduğu takdirde risk yönetimi sürecinin uygulanışı risk yönetimi bileşenleri doğrultusunda gereken titizlikle gerçekleştirilebilmektedir. Çünkü iç denetim biriminde yeterli sayıda personel olduğunda gerçekleştirilecek süreçlerde personel sıkıntısı yaşanmamakta ve personelin çeşitli süreçlerde uzmanlaşması daha kolay sağlanabilmektedir.

Kruskal-Wallis Testi dışında bir diğer non-parametrik test olarak uygulanan Spearman's Rank Order Korelasyonu sonuçlarına göre risk yönetimi bileşenleri ile iç denetim biriminin faaliyet gösterdiği süre ve BT kullanan iç denetim personeli sayısı arasında da anlamlı ilişkiler bulunmuştur.

İç denetim birimini faaliyet gösterdiği süre ile risk yönetimi bileşenlerinden hedef belirleme arasında yapılan analize göre iç denetim biriminin faaliyet gösterdiği süre arttıkça, yönetimin risk stratejisini göz önünde bulundurarak hedefleri belirleme durumu da artmaktadır (Ek-1 Tablo-84).

BT kullanan iç denetim personeli sayısı ile risk yönetimi bileşenlerinin tümü arasında anlamlı ilişkiler bulunmuştur. BT kullanan iç denetim personeli sayısı ile risk yönetimi bileşenlerinden kontrol ortamı arasında yapılan analize göre BT kullanan iç denetim personeli sayısı arttıkça, risklerin kurumda çalışan kişiler tarafından nasıl görüntülenmesi ve yönlendirilmesi gerektiğine dair bir temel oluşturulması durumu artmaktadır (Ek-1 Tablo-85).

BT kullanan iç denetim personeli sayısı ile risk yönetimi bileşenlerinden hedef belirleme arasında yapılan analize göre BT kullanan iç denetim personeli sayısı arttıkça, yönetimin risk stratejisini göz önünde bulundurarak hedefleri belirleme durumu da artmaktadır (Ek-1 Tablo-85).

BT kullanan iç denetim personeli sayısı ile risk yönetimi bileşenlerinden risk tanımlama arasında yapılan analize göre BT kullanan iç denetim personeli sayısı arttıkça, belirsizliklerin risk mi fırsat mı olduğu konusunda çalışmalar da artmaktadır (Ek-1 Tablo-85).

BT kullanan iç denetim personeli sayısı ile risk yönetimi bileşenlerinden risk değerlendirme arasında yapılan analize göre BT kullanan iç denetim personeli sayısı arttıkça, riskler tanımlandıktan sonra bunların işletme üzerindeki olası etkileri ve meydana gelme olasılıklarının değerlendirilmesi de artmaktadır (Ek-1 Tablo-85).

BT kullanan iç denetim personeli sayısı ile risk yönetimi bileşenlerinden risk tutumu arasında yapılan analize göre BT kullanan iç denetim personeli sayısı arttıkça, belirlenen risklerin kurumun risk kapasitesi ve risk toleransı içinde olup olmadığı belirlemesi durumu da artmaktadır (Ek-1 Tablo-85).

BT kullanan iç denetim personeli sayısı ile risk yönetimi bileşenlerinden kontrol faaliyetleri arasında yapılan analize göre BT kullanan iç denetim personeli sayısı arttıkça, riske verilecek karşılıkların etkili bir biçimde yerine getirilmesi ve devam eden risklerin risk kapasitesi sınırları içinde yönetilmesi için politika ve prosedürler oluşturulması da artmaktadır (Ek-1 Tablo-85).

BT kullanan iç denetim personeli sayısı ile risk yönetimi bileşenlerinden bilgi-iletişim arasında yapılan analize göre BT kullanan iç denetim personeli sayısı arttıkça, kişilerin sorumluluklarını yerine getirmesi için ilgili bilginin belli bir biçimde ve belli zaman aralıkları ile tanımlanması ve iletilmesi de artmaktadır (Ek-1 Tablo-85).

BT kullanan iç denetim personeli sayısı ile risk yönetimi bileşenlerinden izleme arasında yapılan analize göre BT kullanan iç denetim personeli sayısı arttıkça, risk yönetiminin uygulanması izlenmesi ve etkinliğini arttırmak için gerektiğinde ayarlamalar yapılması da artmaktadır (Ek-1 Tablo-85).

Özetle, iç denetim birimi işletmede uzun zamandır faaliyet gösteriyorsa risk yönetim sürecinde yönetimin risk stratejisini göz önünde bulundurarak hedefleri belirlemesi sağlanmaktadır. Ayrıca işletme BT kullanan iç denetim birimi personelinin yeterli sayıda olması da risk yönetim sürecinin tüm aşamalarının eksiksiz ve kısıtsız bir şekilde yerine getirilmesinde etkili olmaktadır. Personel sayısının yeterliliği iç denetim faaliyetine verilen önemi de göstermektedir.

5.3.4.2. İç kontrol sistemi ile ilgili çapraz tablo analizleri

İç kontrol sistemlerinde BT kontrollerinin durumu ile ilgili çapraz tablo analizleri katılımcıların işletmedeki konumları itibarıyla düzenlenmiştir. Kruskal-Wallis

testi ve Spearman's Rank Order Korelasyonu uygulandığında anlamlı sonuçlar elde edilememiştir.

*Tablo-48. Ankete Katılanların Konumları*İç Kontrol Sistemlerinde BT Kontrollerinin Durumu*

İç Kontrol Sistemlerinde BT Kontrollerinin Durumu	Konum	İç Denetçi	İç Denetim Yöneticisi	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
İşletme yedeklenmiş dosyaları koruyor mu?	Evet	18	2	10	7	3	2	6	48
	Hayır	0	0	0	0	0	0	0	0
Dosyalara erişim sınırlandırılmış mı?	Evet	18	2	10	7	3	2	6	48
	Hayır	0	0	0	0	0	0	0	0
Kullanılan bir arşivleme sistemi var mı?	Evet	18	2	10	7	3	2	6	48
	Hayır	0	0	0	0	0	0	0	0
Donanım arıza ve kayıplarına karşı alınmış önlem var mı?	Evet	18	2	10	7	3	2	6	48
	Hayır	0	0	0	0	0	0	0	0
Acil durumlar için yedek sistem bulunduruluyor mu?	Evet	17	2	10	7	3	2	6	47
	Hayır	1	0	0	0	0	0	0	1
Veritabanına girmek için şifre var mı?	Evet	18	2	10	7	3	2	6	48
	Hayır	0	0	0	0	0	0	0	0
Bu şifreler düzenli olarak değiştiriliyor mu?	Evet	17	2	10	6	3	2	6	46
	Hayır	1	0	0	1	0	0	0	2
Kullanıcılar belirlenerek ayrı ayrı şifre verilmiş mi?	Evet	17	2	9	7	3	2	6	46
	Hayır	1	0	0	0	0	0	0	1
Virüs ve çeşitli saldırılara karşı önlem alınmış mı?	Evet	18	2	10	7	3	2	6	48
	Hayır	0	0	0	0	0	0	0	0
Veritabanına girebilen eski işletme çalışanları var mı?	Evet	15	1	9	6	2	2	3	38
	Hayır	3	1	1	1	1	0	3	10

Tablo-48'e baktığımızda katılımcılar iç kontrol sistemlerinde yer alan BT kontrollerinin çoğunlukla uygulandığını bildirmişlerdir. Katılımcılar işletmenin yedeklenmiş dosyaları koruduğunu onaylanmıştır (Evet= 48 kişi).

Katılımcılar dosyalara erişimin sınırlandırılmış olduğunu bildirmişlerdir (Evet= 48 kişi).

Katılımcılar kullanılan bir arşivleme sistemi olduğunu bildirmişlerdi (Evet= 48 kişi).

Katılımcılar donanım arıza ve veri kayıplarına karşı önlem alındığını bildirmişlerdir (Evet= 48 kişi).

Katılımcılar çoğunlukla acil durumlar için yedek sistem bulundurulduğunu bildirmiştir (Evet=47 Kişi, Hayır=1 Kişi).

Katılımcılar veritabanına girmek için şifre oluşturulduğunu bildirmiştir (Evet= 46 kişi). Ayrıca bu şifrelerin 46 kişi değiştirildiğini bildirirken 2 kişi de değiştirilmediğini bildirmiştir. Bu iki kişiden 1'i iç denetçi diğeri de muhasebe müdürüdür.

Katılımcılar kullanıcılara ayrı ayrı şifreler verildiğini bildirmiştir (Evet= 46 kişi).

Katılımcılar virüs ve çeşitli saldırılara karşı önlem alındığını bildirmiştir (Evet= 48 kişi).

Veritabanına girebilen eski işletme çalışanları olup olmadığı sorulduğunda 38 katılımcı olduğunu, 10 katılımcı da olmadığını bildirmiştir. Bu 10 kişilik grubu denetim koordinatörleri hariç iç denetçilerin ve iç kontrol koordinatörlerinin çoğunlukta olduğu diğer katılımcılar oluşturmaktadır.

Özetle, genellikle işletmelerin iç kontrol sistemleri üzerinde BT kontrollerini oluşturdukları görülmektedir. İşletmeler yedekleme, arşivleme, şifreleme, veri kayıplarını önleme, veri güvenliği ve sistemlere erişimleri kısıtlama gibi konularda iç kontrol sistemlerinde gerekli çalışmaları yapmışlardır. Fakat veritabanlarına erişim ile ilgili bir konu dikkat çekicidir. Eski çalışanlar halen veritabanlarına ulaşabilmektedir ve bu da iç kontrol sisteminin güvenilirliğini ve ayrıca veri ve bilgi güvenliğini tehdit eden bir durumdur.

5.3.4.3. Kurumsal yönetim ile ilgili çapraz tablo analizleri ve non-parametrik testler

5.3.4.3.1. Kurumsal yönetim ile ilgili çapraz tablo analizleri

Kurumsal yönetim ile ilgili çapraz tablo analizleri katılımcıların işletmedeki konumları itibariyle düzenlenmiştir. Ankete katılanlar kurumsal yönetim kapsamında iç denetimin rolünü değerlendirmişlerdir.

Tablo-49. Ankete Katılanların İşletmedeki Konumları*Kurumsal Yönetim Kapsamında İç Denetimin Rolü

Kurumsal Yönetim Anlayışında İç Denetimin Rolü		Konum	İç Denetçi	İç Den. Yön.	Gn Md. Yrd	Muh. Md.	Mali İşler Koord.	Denetim Koord.	İç Kon. Koord.	Toplam
İç denetim, kurumsal yönetim sisteminin bütünleştirici bir parçasıdır.	Katılmıyorum		6	0	0	1	1	1	3	12
	Kararsızım		5	1	0	0	0	0	0	6
	Katılıyorum		0	0	3	0	0	0	1	4
	Kesinlikle Katılıyorum		7	1	8	6	2	1	2	27
İç denetim, kontrol sistemlerinin (operasyonel kontrol, finansal kontrol) etkinliğini ölçüp değerlendirerek yönetime objektif güvence sağlar.	Katılmıyorum		1	0	0	1	0	0	0	2
	Katılıyorum		10	1	3	0	1	1	2	18
	Kesinlikle Katılıyorum		7	1	8	6	2	1	4	29
İç denetim, işletme bilgi teknolojisi sisteminin güvenliğini ve raporlama imkanlarını içeren muhasebe bilgi sisteminin etkinliğini değerlendirir.	Katılmıyorum		1	0	0	1	0	0	0	2
	Kararsızım		0	0	0	0	0	0	2	2
	Katılıyorum		10	1	4	0	1	1	2	19
	Kesinlikle Katılıyorum		7	1	7	6	2	1	2	26
İç denetim, profesyonel yöneticilere yetki devrinde güvence sağlar.	Katılmıyorum		1	0	0	1	0	0	0	2
	Kararsızım		10	1	0	0	1	1	1	14
	Katılıyorum		1	0	4	0	0	0	3	8
	Kesinlikle Katılıyorum		6	1	7	6	2	1	2	25
İç denetim faaliyeti; zamanı ve emeğini, kurum çapında düzgün risk yönetimi süreçlerinin kurulmasına ve uygulanmasına katkıda bulunan danışmanlık faaliyetlerine harcar.	Katılmıyorum		5	0	0	1	1	1	1	9
	Kararsızım		6	1	1	0	0	0	0	8
	Katılıyorum		3	0	4	0	0	0	1	8
	Kesinlikle Katılıyorum		4	1	6	6	2	1	4	24
İç denetim, risk değerlendirme sürecinin etkin bir şekilde çalıştığı konusunda yönetim kuruluna ve yönetime objektif güvence sağlar.	Katılmıyorum		1	0	0	1	0	0	0	2
	Kararsızım		3	0	0	0	1	0	1	5
	Katılıyorum		8	1	4	0	0	1	1	15
	Kesinlikle Katılıyorum		6	1	7	6	2	1	4	27
Kurumsal yönetim anlayışının işletmede oluşması değerinin artırılması ve kalitesinin sürdürülebilmesi için iç denetimin kurumsal yönetim anlayışına işlevsellik kazandırır.	Katılmıyorum		1	0	0	1	0	0	0	2
	Kararsızım		4	0	0	0	1	0	1	6
	Katılıyorum		9	1	5	0	0	1	1	17
	Kesinlikle Katılıyorum		4	1	6	6	2	1	4	24

Tablo-49'a göre katılımcıların büyük bir çoğunluğu iç denetimin kontrol sistemlerinin etkinliğini ölçüp değerlendirerek yönetime objektif güvence sağladığını bildirmiştir (Katılıyorum-18 + Kesinlikle katılıyorum-29= 47 kişi).

Katılımcıların çoğu iç denetimin işletme bilgi teknolojisi sisteminin güvenliğini ve raporlama imkanlarını içeren muhasebe bilgi sisteminin etkinliğini değerlendirdiğini bildirmiştir (Katılıyorum-19 + Kesinlikle katılıyorum-26= 45 kişi).

Katılımcıların çoğu iç denetimin risk değerlendirme sürecinin etkin bir şekilde çalıştığı konusunda yönetim kuruluna ve yönetime objektif güvence sağladığını bildirmiştir (Katılıyorum-15 + Kesinlikle katılıyorum-27= 42 kişi).

Katılımcıların çoğu kurumsal yönetim anlayışının işletmede oluşması, değerinin artırılması ve kalitesinin sürdürülebilmesi için iç denetimin kurumsal yönetim anlayışına işlevsellik kazandırdığını düşünmektedir (Katılıyorum-17 + Kesinlikle katılıyorum-24= 41 kişi).

İç denetimin profesyonel yöneticilere yetki devrinde güvence sağladığı konusunda da katılımcılardan çoğu katılımını bildirirken (Katılıyorum-8 + Kesinlikle katılıyorum-25= 33 kişi), bu konuda kararsızlarında olduğu dikkat çekmektedir (14 kişi).

Katılımcıların çoğu iç denetim faaliyetinin zamanını ve emeğini, kurum çapında düzgün risk yönetimi süreçlerinin kurulmasına ve uygulanmasına katkıda bulunan danışmanlık faaliyetlerine harcadığını bildirmiştir (Katılıyorum-8 + Kesinlikle katılıyorum-25= 33 kişi).

Katılımcıların çoğunluğu iç denetimin kurumsal yönetim sisteminin bütünleştirici bir parçası olduğunu bildirmiştir (Katılıyorum-4 + Kesinlikle katılıyorum-27= 31 kişi). Aksi yönde fikir bildirenler ise 12 kişidir.

Özetle, kurumsal yönetim kapsamında iç kontrol sistemlerinin etkinliğini ölçüp değerlendirmesi ve risk değerlendirme sürecinde etkinlik sağlaması konularında yönetime objektif güvence sağlayan iç denetim biriminin önemi büyüktür. Ayrıca işletmedeki bilgi teknolojisi sistemlerinin güvenliğini sağlama ve raporlama imkanlarını geliştirme açısından muhasebe bilgi sisteminin etkinliğini incelemek için iç denetim biriminin faaliyet göstermesi gereklidir. İç denetim faaliyetini gerçekleştiren taraflar, iç denetim faaliyetlerinin yerine getirilmesinin kurumsal yönetim anlayışının işletmede oluşması, işletmeye katma değer sağlaması ve kalitesinin sürdürülmesi vasıtasıyla işletmede işlevsellik kazandığını düşünmektedir.

5.3.4.3.2. Kurumsal yönetim ile ilgili non-parametrik testler

Kurumsal yönetim kapsamında iç denetimin rolü ile ankete katılanların konumları arasında anlamlı farklılıkların olup olmadığını görmek için Kruskal-Wallis Testi yapılmıştır. Ankete katılanların konumları ile kurumsal yönetim kapsamında iç

denetimin rolü arasında anlamlı farklılık bulunamamıştır. Fakat BT denetiminin uygulandığı süre ile kurumsal yönetim kapsamında iç denetimin rolü arasında anlamlı farklılıklar bulunmuştur. Bulunan sonuçlara göre;

BT denetiminin uygulandığı süre 10 yıl ve üzerinde olanlar iç denetimin kurumsal yönetim sisteminin bütünleştirici bir parçası olduğunu bildirirken, 1-3 yıl arasında olanlar aksi yönde bildirimde bulunmuştur (Ek-1 Tablo-86).

BT denetiminin uygulandığı süre 10 yıl ve üzerinde olanlar iç denetimin kontrol sistemlerinin etkinliğini ölçüp değerlendirerek yönetime objektif güvence sağladığını bildirirken, 1-3 yıl arasında olanlar aksi yönde bildirimde bulunmuştur (Ek-1 Tablo-86).

BT denetiminin uygulandığı süre 10 yıl ve üzerinde olanlar iç denetimin işletme bilgi teknolojisi sisteminin güvenliğini ve raporlama imkanlarını içeren muhasebe bilgi sisteminin etkinliğini değerlendirdiğini bildirirken, BT denetiminin uygulamayanlar aksi yönde bildirimde bulunmuştur (Ek-1 Tablo-86).

BT denetiminin uygulandığı süre 10 yıl ve üzerinde olanlar iç denetimin profesyonel yöneticilere yetki devrinde güvence sağladığını bildirirken, 1-3 yıl arasında olanlar aksi yönde bildirimde bulunmuştur (Ek-1 Tablo-86).

BT denetimini 1 yıldan az bir süredir uygulayanlar iç denetim faaliyetinin zamanı ve emeğini, kurum çapında düzgün risk yönetimi süreçlerinin kurulmasına ve uygulanmasına katkıda bulunan danışmanlık faaliyetlerine harcadığını bildirirken, 1-3 yıl olanlar aksi yönde bildirimde bulunmuştur (Ek-1 Tablo-86).

BT denetiminin uygulandığı süre 4-6 yıl olanlar iç denetimin risk değerlendirme sürecinin etkin bir şekilde çalıştığı konusunda yönetim kuruluna ve yönetime objektif güvence sağladığını bildirirken, BT denetimin uygulanmadığını bildirenler aksi yönde bildirimde bulunmuşlardır (Ek-1 Tablo-86).

Özetle, kurumsal yönetim kapsamında iç denetimin kazandığı rollerden en çok göze çarpanlardan olan iç kontrolün etkinliğini sağlama ve risk değerlendirme sürecinde güvence sağlama, BT denetimlerinin uzun süredir yapıldığı işletmelerde mutlaka ortaya çıkmaktadır. BT denetimini uzun yıllardan beri uygulayan işletmelerde iç denetimin öneminin kurumsal yönetim süreci bağlamında daha iyi anlaşıldığı söylenebilir. İç denetimin kurum içinde öneminin kavranması ve kuruma mal edilmesi açısından BT denetimi önemli bir rol oynamaktadır. Çünkü klasik anlamda BT uygulamalarına yer

vermeyen işletmelerde iç denetim daha dar kapsamda uygulanmakta ve işletmenin bütününe yayılamamaktadır.

Kruskal-Wallis Testi dışında bir diğer non-parametrik test olarak uygulanan Spearman's Rank Order Korelasyonu sonuçlarına göre kurumsal yönetim kapsamında iç denetimin rolü ile iç denetim biriminin faaliyet gösterdiği süre, BT kullanan iç denetim personeli sayısı ve BT denetiminin uygulandığı süre arasında anlamlı ilişkiler bulunmuştur.

İç denetim biriminin faaliyet gösterdiği süre arttıkça, iç denetim faaliyeti zamanının ve emeğinin, kurum çapında düzgün risk yönetimi süreçlerinin kurulmasına ve uygulanmasına katkıda bulunan danışmanlık faaliyetlerine harcandığı bildirilmiştir (Ek-1 Tablo-87).

BT kullanan iç denetim personeli sayısı arttıkça, iç denetimin kurumsal yönetimin bir parçası olduğu bildirilmiştir (Ek-1 Tablo-88).

BT kullanan iç denetim personeli sayısı arttıkça, iç denetimin kontrol sistemleri konusunda yönetime güvence sağladığı bildirilmiştir (Ek-1 Tablo-88).

BT kullanan iç denetim personeli sayısı arttıkça, iç denetim biriminin muhasebe bilgi sisteminin etkinliğini değerlendirdiği hakkında katılım düzeyleri artmıştır (Ek-1 Tablo-88).

BT kullanan iç denetim personeli sayısı arttıkça, iç denetimin yetki devrinde yöneticilere güvence sağlaması konusunda katılım düzeyleri de artmaktadır (Ek-1 Tablo-88).

BT kullanan iç denetim personeli sayısı arttıkça, kurumsal yönetim risk yönetimi ile iç içe geçmiş bir anlayış olduğundan iç denetim biriminin risk yönetimi sürecinde danışmanlık hizmeti sunduğu konusunda katılım düzeyleri artmaktadır (Ek-1 Tablo-88).

BT kullanan iç denetim personeli sayısı arttıkça, iç denetimin risk yönetimi sürecinde yönetime güvence sağlaması açısından katılım düzeyleri artmaktadır (Ek-1 Tablo-88).

BT kullanan iç denetim personeli sayısı arttıkça, iç denetimin kurumsal yönetim anlayışına işlevsellik kazandırdığı fikrine katılımlar artmıştır (Ek-1 Tablo-88).

BT Denetiminin uygulanma süresi arttıkça, iç denetim biriminin muhasebe bilgi sisteminin etkinliğini değerlendirmesi fikrine katılımlar artmıştır (Ek-1 Tablo-89).

Özetle, BT kullanan iç denetim personeli sayısı yeterli olduğunda kurumsal yönetim kapsamında iç denetim birimleri gerçekleştirmeleri gereken tüm faaliyetleri herhangi bir kısıtla karşılaşmaksızın yerine getirebilmektedirler. Kurumsal yönetim kapsamında iç denetimin kazandığı rollerden en çok göze çarpanlar iç kontrolün etkinliğini sağlama ve risk değerlendirme sürecinde güvence sağlama, BT denetimlerinin uzun süredir yapıldığı işletmelerde mutlaka ortaya çıkmaktadır.

5.3.5. Bilgi teknolojileri uygulamaları ile ilgili çapraz tablo analizleri ve non-parametrik testler

5.3.5.1. Bilgi teknolojileri uygulamaları ile ilgili çapraz tablo analizleri

Bilgi teknolojileri uygulamaları ile ilgili çapraz tablo analizleri katılımcıların işletmedeki konumları itibarıyla düzenlenmiştir. Ankete katılanlar “bilgi teknolojilerinin kimler tarafından kullanıldığını”, “bilgi teknolojilerinin geçmiş ve şimdiki kullanımlarını”, “bilgi teknolojilerinin değerlemesi sırasındaki uygulamaları”, “bilgi teknolojileri kontrollerini”, “bilgi teknolojilerinin kullanımının artmasını engelleyen durumları”, “iç denetim ile ilişkileri yönünden elektronik ticaret, internet, elektronik veri değişimi, kurumsal kaynak planlama ve veri işleme teknolojilerini” değerlendirmişlerdir.

- Ankete katılanların konumları ile BT’ni kullanan taraflar arasındaki ilişki:

Tablo-50. Ankete Katılanların İşletmedeki Konumları * BT Kullananlar

Konum BT Kullananlar	İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
BT Uzmanları	17	6	1	7	3	2	6	42
İç denetçiler	14	10	2	1	1	1	5	34
Muhasebe	2	5	1	1	1	0	2	12
Satın Alma	2	3	0	0	1	0	2	8
Satış-Pazarlama	1	4	0	0	1	0	2	8
ERP Kullanıcıları	1	0	0	0	0	0	0	1
Uzman personel	1	0	0	0	0	0	0	1

* Ankete katılanlar birden fazla seçenek işaretleyerek soruya cevap verebilmektedir.

Tablo-50’ye göre katılımcıların çoğu işletmelerde birinci sırada bilgi teknolojileri uzmanlarının (42 kişi), ikinci sırada iç denetçilerin (34 kişi) ve üçüncü sırada muhasebe birimi çalışanlarının (12 kişi) bilgi teknolojilerini kullandığını

bildirmiştir. İç denetçiler en çok BT uzmanları ve kendileri; iç denetim yöneticileri iç denetçiler; muhasebe müdürleri, mali işler koordinatörleri, denetim koordinatörleri, iç kontrol koordinatörleri BT uzmanları tarafından BT kullanıldığını bildirmişlerdir. Ayrıca satın alma birimi, pazarlama-satış birimi, ERP kullanıcıları ve uzman personel katılımcılar tarafından bildirilen diğer BT kullanıcılarıdır.

İşletmelerde özellikle BT alanında uzmanlık gerektiren süreçlerdeki işleyişin devamlılığı ve kontrolü açısından BT uzmanlarının, BT süreçlerini denetlemeye yönelik çalışmalarda iç denetçilerin ve finansal işlemlerin kayıtları ve finansal tabloların hazırlanması gibi süreçlerde muhasebe birimi çalışanlarının BT teknolojilerini yaygın olarak kullandığı söylenebilir. Bunlar haricinde pazarlama ve satın alma birimlerinde de stok işlemlerinin yürütülmesi ve takibi açısından BT kullanımı yaygındır.

- **Ankete katılanların konumları ile BT uygulamalarının geçmiş ve şimdiki kullanımları arasındaki ilişki:**

İnternet:

*Tablo-51. Ankete Katılanların İşletmedeki Konumları*İnternetin Geçmişteki ve Şimdiki Kullanımı*

Konum		İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
İnternet	GEÇMİŞ	Kısmen uygulandı	4	1	1	0	0	0	6
		Uygulandı	0	2	0	0	0	2	4
		Hep uygulandı	15	8	6	3	3	2	41
	ŞİMDİ	Kısmen uygulanıyor	1	0	1	0	0	2	4
		Uygulanıyor	1	0	0	0	0	0	1
		Hep Uygulanıyor	17	11	6	3	3	2	46

Tablo-51’de görüldüğü üzere katılımcıların çoğu internetin geçmişte de uygulandığını bildirmiştir (Uygulandı-4+Hep Uygulandı-41= 45 kişi). 6 kişi ise kısmen uygulandığını belirtmiştir ve çoğunluğu iç denetçilerden oluşmaktadır. Şimdiki durum için katılımcıların çoğu internetin kullanıldığını bildirmiştir (Uygulanıyor-1+Hep Uygulanıyor-46= 47kişi). Kısmen kullanıldığını bildiren kişi sayısı 4’tür ve bu kez bu toplam içinde iç denetçilerin sayısı azalmıştır.

Intranet:

Tablo-52. Ankete Katılanların İşletmedeki Konumları*Intranetin Geçmişteki ve Şimdiki Kullanımı

Konum Intranet		İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
GEÇMİŞ	Hiç uygulanmadı	2	1	0	1	1	1	1	7
	Uygulanmadı	1	0	1	0	0	0	0	2
	Kısmen uygulandı	2	2	0	0	0	0	0	4
	Uygulandı	1	1	0	0	0	0	2	4
	Hep uygulandı	13	7	6	2	2	1	3	34
ŞİMDİ	Hiç uygulanmıyor	0	0	0	1	0	0	0	1
	Kısmen uygulanıyor	1	0	1	0	0	0	0	2
	Uygulanıyor	2	1	0	0	0	0	0	3
	Hep Uygulanıyor	16	10	6	2	3	2	6	45

Tablo-52’de görüldüğü üzere katılımcıların çoğu intranetin geçmişte kullanıldığını bildirmişlerdir (Uygulandı-4+Hep Uygulandı-34= 38 kişi). Şimdiki durumda ise intranetin kullanım durumunun daha da arttığı görülmektedir (Uygulanıyor-3+Hep Uygulanıyor-45= 48 kişi).

Extranet:

Tablo-53. Ankete Katılanların İşletmedeki Konumları*Extranetin Geçmişteki ve Şimdiki Kullanımı

Konum Extranet		İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
GEÇMİŞ	Hiç uygulanmadı	7	2	0	2	1	1	3	16
	Uygulanmadı	6	0	1	0	1	1	2	11
	Kısmen uygulandı	3	6	0	1	0	0	1	11
	Uygulandı	1	2	0	0	0	0	0	3
	Hep uygulandı	1	0	6	0	1	0	0	8
ŞİMDİ	Hiç uygulanmıyor	2	1	0	1	1	1	3	9
	Uygulanmıyor	2	1	1	0	0	0	0	4
	Kısmen uygulanıyor	6	7	0	2	0	0	2	17
	Uygulanıyor	5	0	0	0	1	1	1	8
	Hep Uygulanıyor	3	1	6	0	1	0	0	11

Tablo-53’de görüldüğü üzere toplam 27 kişi tarafından extranetin geçmişte kullanılmadığını bildirilmiştir (Hiç uygulanmadı-16+Uygulanmadı-11= 27 kişi). Bu kişiler çoğunlukla iç denetçiler, genel müdür yardımcıları, mali işle koordinatörleri, denetim koordinatörleri, iç kontrol koordinatörlerinden oluşmaktadır. Kısmen kullanıldığını

bildiren 11 kişi vardır ve bunların çoğunluğu iç denetim yöneticilerinden oluşmaktadır. Extranetin geçmişte kullanıldığını bildiren kişiler ise toplam 11 kişidir ve bunların çoğunluğunu muhasebe müdürleri oluşturmaktadır. Şimdiki durumda ise extranetin kullanımında bir artış olmakla birlikte (Uygulanıyor-8+Hep uygulanıyor-18= 19 kişi), kısmen kullanımının da arttığı görülmektedir (17 kişi). Extranetin arttığı bildirenler arasında muhasebe müdürleri, iç denetçiler ve mali koordinatörler çoğunluktadır. Kısmen uygulandığını bildirenler arasında geçmişte olduğu gibi yine iç denetim yöneticilerinin ve onlarla birlikte iç denetçilerin fazla olduğu görülmektedir. Extranetin uygulanmadığını bildiren kişi sayısı ise 13'e (Hiç uygulanmıyor-9+Uygulanmıyor-4= 13 kişi) düşmüştür.

Elektronik veri değişimi:

*Tablo-54. Ankete Katılanların İşletmedeki Konumları*Elektronik Veri Değişiminin Geçmişteki ve Şimdiki Kullanımı*

Elektronik Veri Değişimi / Konum		İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
GEÇMİŞ	Hiç uygulanmadı	0	0	0	1	0	0	0	1
	Uygulanmadı	2	2	0	0	0	1	1	6
	Kısmen uygulandı	8	5	1	1	2	1	2	20
	Uygulandı	3	1	0	0	0	0	2	6
	Hep uygulandı	6	2	6	1	1	0	1	17
ŞİMDİ	Uygulanmıyor	1	0	1	0	0	0	0	2
	Kısmen uygulanıyor	5	6	0	1	1	1	2	16
	Uygulanıyor	1	1	0	0	0	0	0	2
	Hep Uygulanıyor	12	3	6	2	2	1	4	30

Tablo-54'e göre katılımcıların yarısı tarafından elektronik veri değişiminin geçmişte uygulandığı bildirilmiştir (Uygulandı-6+Hep uygulandı-17= 23 kişi). Kısmen uygulandığını bildiren sayısı da yüksektir (20 kişi). Kısmen uygulandığını bildiren kişiler daha çok iç denetçiler, iç denetim yöneticileri ve mali işler koordinatörlerinden oluşmaktadır. Uygulandığını bildirenler arasında ise muhasebe müdürleri ve iç denetçiler çoğunluktadır. Şimdiki durumda ise uygulanmadığını bildirenlerin sayısı geçmişe kıyasla azalmıştır (2 kişi). Kısmen uygulandığını bildirenlerin sayısı (16 kişi) ise uygulandığını bildirenlerin sayısının yarısı kadardır (Uygulanıyor-2+ Hep uygulanıyor-30= 32 kişi).

Elektronik ticaret:

*Tablo-55. Ankete Katılanların İşletmedeki Konumları*Elektronik Ticaretin Geçmişteki ve Şimdiki Kullanımı*

Konum Elektronik Veri Değişimi		İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
GEÇMİŞ	Hiç uygulanmadı	9	2	5	2	2	1	3	24
	Uygulanmadı	0	1	0	0	0	0	0	1
	Kısmen uygulandı	7	7	1	1	1	1	2	20
	Uygulandı	3	0	0	0	0	0	0	3
	Hep uygulandı	0	0	0	0	0	0	1	1
ŞİMDİ	Hiç uygulanmıyor	6	0	0	2	0	0	2	10
	Kısmen uygulanıyor	4	9	2	1	0	1	2	19
	Uygulanıyor	7	0	0	0	2	1	1	11
	Hep Uygulanıyor	2	1	5	0	1	0	1	10

Tablo-55'e baktığımızda geçmişte e-ticaretin uygulanmadığı (Hiç uygulanmadı-24+ Uygulanmadı-1= 25 kişi) ve kısmen uygulandığı dikkat çekmektedir (20 kişi). İç denetçiler, muhasebe müdürleri, iç kontrol koordinatörleri ve mali işler koordinatörleri uygulanmadığını bildiren grup içinde ağırlıktadır. Kısmen uygulandığını bildirenler ise daha çok iç denetim yöneticilerinden ve iç denetçilerden oluşmaktadır. Şimdiki durumda ise e-ticaretin uygulanmadığını bildirenlerin sayısı oldukça düşmüştür (10 kişi). Bu kişilerin çoğunluğunu iç denetçiler oluşturmaktadır. E-ticaretin uygulandığını bildirenler ise artmıştır (Uygulanıyor-11+Hep uygulanıyor-10= 21 kişi). Bu kişiler içinde iç denetim yöneticileri çoğunluktadır. Kısmen kullanıldığını uygulanmakta olduğunu bildirenler ise geçmişteki durumdan farklı değildir (19 kişi).

Kurumsal kaynak planlama:

*Tablo-56. Ankete Katılanların İşletmedeki Konumları*Kurumsal Kaynak Planlamasının Geçmişteki ve Şimdiki Kullanımı*

Konum Kurumsal Kaynak planlama		İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
GEÇMİŞ	Hiç uygulanmadı	5	1	0	2	0	0	0	8
	Uygulanmadı	6	5	1	0	0	2	2	16
	Kısmen uygulandı	3	3	0	1	1	0	1	9
	Uygulandı	3	1	1	0	1	0	2	8
	Hep uygulandı	1	0	5	0	1	0	1	8
ŞİMDİ	Hiç uygulanmıyor	0	0	0	1	0	0	0	1
	Uygulanmıyor	2	1	1	0	0	0	0	4
	Kısmen uygulanıyor	8	6	0	2	1	1	2	20
	Uygulanıyor	0	3	0	0	0	0	0	3
	Hep Uygulanıyor	8	0	6	0	2	1	4	21

Tablo-56'ya baktığımızda katılımcıların çoğu geçmişte kurumsal kaynak planlamanın uygulanmadığını bildirmiştir (Hiç uygulanmadı-8+ Uygulanmadı-16= 24 kişi). Uygulandığını bildirenler 16 kişidir (Uygulandı-8+Hep uygulandı-8) ve çoğunluğu muhasebe müdürleri ve iç denetçilerden oluşmaktadır. Şimdiki durumda ise geçmişteki durumun tersine döndüğü görülmektedir. Kurumsal kaynak planlamasını uygulayanlar artmıştır (Uygulanıyor-3+Hep uygulanıyor-21= 24 kişi). Uygulandığını bildirenlerin çoğunluğu iç denetçi, muhasebe müdürleri ve iç kontrol koordinatörlerinden oluşmaktadır. Kısmen uygulandığını bildirenler de oldukça artmış (20 kişi), fakat uygulanmadığını bildirenler ise oldukça azalmıştır (Hiç uygulanmıyor-1+Uygulanmıyor-4= 5 kişi).

Elektronik veri işleme:

*Tablo-57. Ankete Katılanların İşletmedeki Konumları*Elektronik Veri İşlemenin Geçmişteki ve Şimdiki Kullanımı*

Elektronik Veri İşleme		Konum	İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
GEÇMİŞ	Hiç uygulanmadı		0	0	0	1	0	0	0	1
	Uygulanmadı		6	1	0	0	2	1	1	11
	Kısmen uygulandı		3	3	1	0	0	1	2	10
	Uygulandı		3	2	0	0	0	0	2	7
	Hep uygulandı		7	5	6	2	1	0	1	22
ŞİMDİ	Hiç uygulanmıyor		0	0	0	1	0	0	0	1
	Uygulanmıyor		1	0	1	0	0	0	0	2
	Kısmen uygulanıyor		2	1	0	0	0	0	1	4
	Uygulanıyor		2	5	0	0	0	1	1	9
	Hep Uygulanıyor		14	5	6	2	3	1	4	35

Tablo-57'de görüldüğü üzere elektronik veri işlemenin katılımcıların çoğu tarafından geçmişte uygulandığı görülmektedir (Uygulandı-7+Hep uygulandı-22= 29 kişi). Bu kişiler çoğunlukla iç denetçi, muhasebe müdürü ve iç denetim yöneticilerinden oluşmaktadır. Uygulanmadığını bildiren 12 kişinin 6'sı da iç denetçilerdir ve iç denetim yöneticileri ve muhasebe müdürleri hariç diğer katılımcıların da bu grupta yer aldığı görülmektedir. Şimdiki durumda ise katılımcıların büyük bir kısmı uygulandığını bildirmiştir (Uygulanıyor-9+Hep uygulanıyor-35= 44 kişi). Kısmen uygulandığı (4 kişi) veya uygulanmadığı (Hiç uygulanmıyor-1+Uygulanmıyor-2= 3 kişi) yönündeki katılımlar geçmişe kıyasla oldukça düşmüştür.

Bilgi teknolojilerinde yaşanan gelişmelerin ve işletmelerin bu teknolojileri hemen hemen her süreçte kullanıyor olmaları iç denetim bölümlerini de bu

teknolojilerin kullanımı ve işlem süreçleri açısından takip etmeye yöneltmiştir. İşletmelerde bilgi teknolojileri kullanımının iç denetim açısından bazı sonuçlar ortaya çıkardığı söylenebilir. Öncelikle belirtmek gerekir ki, internet, intranet, extranet, elektronik veri değişimi, elektronik ticaret, kurumsal kaynak planlaması ve veri işleme teknolojileri işletmelerde çokça kullanılan ve işlem süreçlerine doğrudan veya dolaylı şekilde etkileri olan teknolojilerdir. Özellikle internet, intranet elektronik veri değişimi ve elektronik veri işleme geçmiş ve şimdiki değerlendirmelerde en yüksek kullanımlara sahip BT uygulamalarıdır. Geçmişe kıyasla şimdiki durumda kullanımı artan BT uygulamaları ise extranet, e-ticaret ve kurumsal kaynak planlamasıdır.

• **Ankete katılanların konumları ile e-ticaret-iç denetim arasındaki ilişki:**

*Tablo-58. Ankete Katılanların İşletmedeki Konumları *E-ticaret-İç Denetim İlişkisi*

E-ticaret ve İç Denetim İlişkisine Yönelik Katılım Düzeyleri		Konum	İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md	Mali İşler Koord	Denetim Koord	İç Kontrol Koord	Toplam
Elektronik ticaret iç kontrolün etkinliğine ilişkin asıl riskleri bünyesinde barındırır.	Katılmıyorum		6	2	0	0	1	1	1	11
	Kararsızım		8	1	2	1	1	1	3	17
	Katılıyorum		3	2	1	0	0	0	0	6
	Kesinlikle Katılıyorum		2	5	4	1	1	0	2	15
Elektronik formlar ve elektronik ticaret kapsamındaki çevrimiçi işlemler, iç kontrolün etkinliğini doğrulamak amacıyla ticari işlem dokümanının bütünlüğünü sağlar.	Kararsızım		10	2	2	1	1	1	2	19
	Katılıyorum		8	4	1	0	1	1	4	19
	Kesinlikle Katılıyorum		1	4	4	1	1	0	0	11
Geleneksel kağıt dokümanlardan elektronik ticarete geçiş iç kontrol zayıflıklarını artırır.	Kesinlikle katılmıyorum		3	7	0	1	1	0	0	12
	Katılmıyorum		2	1	0	0	0	1	2	6
	Kararsızım		12	1	7	1	2	1	4	28
	Katılıyorum		2	1	0	0	0	0	0	3

Tablo-58'e bakıldığında katılımcılar geleneksel kağıt dokümanlardan elektronik ticarete geçilmesinin iç kontrol zayıflıklarını arttıracak konusunda bazı tereddütler yaşamakla (Kararsızım=28 kişi) birlikte iç kontrolün zayıfladığını tetikleyeceği fikrine katılımcıların çok azı katılımda bulunmuştur (Katılıyorum=3 kişi) . Bu duruma katılmadığını bildirenler ise 18 kişidir (Kesinlikle katılmıyorum-12+Katılmıyorum-6= 12 kişi) ve çoğunluğunu iç denetim yöneticileri oluşturmaktadır.

Dolayısıyla bu doğrultuda elektronik formların ve elektronik ticaret kapsamındaki çevrimiçi işlemlerin iç kontrolün etkinliğini doğrulayarak dokümanların bütünlüğünü sağladığı düşünülmektedir (Kesinlikle katılıyorum-11+Katılıyorum-19= 30

kişi). Bu duruma katıldığını bildirenlerin çoğunluğunu iç denetçilerin, iç denetim yöneticilerinin, muhasebe müdürlerinin ve iç kontrol koordinatörlerinin oluşturduğu görülmektedir. Kararsızlığını bildirilenlerin sayısı ise 19 kişidir ve çoğunluğu iç denetçilerden oluşmaktadır.

Elektronik ticaretin iç kontrolün etkinliğine ilişkin asıl riskleri bünyesinde barındırması ise denetim koordinatörleri hariç çoğu katılımcı tarafından kabul edilmektedir (Katılıyorum-6+Kesinlikle katılıyorum-15= 21 kişi). Bu konuda kararsızlığını (17 kişi) ve katılmadığını (11 kişi) bildirenlerin sayıları da çok düşük sayılmaz. Kararsızlığını bildiren grupta iç denetçilerin (8 kişi) ve iç kontrol koordinatörlerinin (3 kişi) çoğunlukta olduğu görülmektedir.

Özetle, e-ticaret uygulamalarının belgeleme ve işlemlerin çevrimiçi olarak gerçekleştirilmesi açısından iç kontrolün etkinliğini olumsuz yönde etkilemeyeceği düşünülürken, bir yandan da elektronik ticaret işlemlerinin asıl riskleri içinde barındığı kabul edilmektedir.

- Ankete katılanların konumları ile internet-iç denetim arasındaki ilişki:

Tablo-59. Ankete Katılanların İşletmedeki Konumları *İnternet-İç Denetim İlişkisi

İnternet ile İç Denetim İlişkisine Yönelik Katılım Düzeyleri		Konum	İç Denetçi	İç Denetim Yn	Gn Md. Yrd	Muhasebe Md	Mali İşler Kord	Denetim Kord	İç Kontrol Kord	Toplam
İşletmemizin finansal tabloları ve raporları internet erişim sayfamızdan yayınlanmaktadır.	Kesinlikle Katılmıyorum		6	0	0	1	0	0	0	7
	Katılmıyorum		1	0	1	0	0	0	0	2
	Katılıyorum		6	0	0	0	1	1	2	11
	Kesinlikle Katılıyorum		6	11	6	1	2	1	3	30
İnternet vasıtasıyla eş zamanlı veri ve bilgi alış verişi sağlanmaktadır.	Katılmıyorum		1	0	1	0	0	0	0	2
	Karasızım		0	2	0	0	0	0	0	2
	Katılıyorum		12	1	0	1	1	1	3	19
	Kesinlikle Katılıyorum		6	8	6	1	2	1	3	27
İşletmemizde internet ortamında yayınlanan finansal tabloların hazırlanması sürecinde XBRL kullanılmaktadır.	Kesinlikle Katılmıyorum		6	0	0	1	0	0	1	8
	Katılmıyorum		6	2	1	0	1	1	1	12
	Karasızım		5	8	6	1	2	1	3	26
	Katılıyorum		0	0	0	0	0	0	1	1
İşletmemizde XBRL, veri transferinin eş zamanlı gerçekleşmesini sağlayarak eş zamanlı raporlama ve sürekli denetimin gerçekleşmesini sağlamaktadır.	Kesinlikle Katılmıyorum		6	0	0	1	0	0	1	8
	Katılmıyorum		6	2	1	0	1	1	1	12
	Karasızım		5	8	6	1	2	1	3	26
	Katılıyorum		0	0	0	0	0	0	1	1
İşletmemizde risklere karşı iç denetim mekanizmaları oluşturulurken internet teknolojisinin yapılandırılması, yönetimi ve kontrolü gibi alanlar da tanımlanır.	Kesinlikle Katılmıyorum		6	0	0	1	0	0	0	7
	Katılmıyorum		1	0	1	0	0	0	0	2
	Karasızım		0	1	0	0	0	0	0	1
	Katılıyorum		7	3	1	0	1	1	2	15
İşletmemizde iç denetçiler anormalliklerin takip edilmesi ve hataların tanımlanması süreçlerinde elektronik çalışma kağıtlarını kullanırlar.	Kesinlikle Katılmıyorum		6	0	0	1	0	0	4	7
	Katılmıyorum		2	1	1	0	1	0	0	5
	Karasızım		7	2	6	0	2	2	4	23
	Katılıyorum		1	2	0	0	0	0	1	4
İşletmemizde iç denetçiler anormalliklerin takip edilmesi ve hataların tanımlanması süreçlerinde elektronik çalışma kağıtlarını kullanırlar.	Kesinlikle Katılmıyorum		2	6	0	1	0	0	1	10
	Katılmıyorum		2	6	0	1	0	0	1	10
	Karasızım		7	2	6	0	2	2	4	23
	Katılıyorum		1	2	0	0	0	0	1	4

Tablo-59’da görüldüğü üzere katılımcıların büyük bir çoğunluğu internet vasıtasıyla veri ve bilgi alışverişi sağlandığını kabul etmektedir (Katılıyorum-19+Kesinlikle katılıyorum-27= 46 kişi). Zaten internet BT uygulamaları arasında en yaygın olarak kullanıldır ve bu daha önce de katılımcılar tarafından belirtilmiştir. Dolayısıyla işletmenin finansal tablolarının ve raporlarının internet erişim sayfasından yayınladığını vurgulamıştır (Katılıyorum-11+Kesinlikle katılıyorum-30= 41 kişi). Bu

durum da internet kullanımının yaygınlığını doğrulamaktadır. Kararsızlığını bildiren katılımcılardan 6'sının iç denetçi olması dikkat çekicidir. Bu kişilerin konu hakkında bilgi eksikliği söz konusu olabilir.

Katılımcıların çoğunluğunun desteklediği konulardan biri de risklere karşı iç denetim mekanizmalarını oluştururken internet tabanlı teknoloji kullanımının yönetimi ve kontrolünü tanımlandığını bildirmiştir (Katılıyorum-15+Kesinlikle katılıyorum-25= 40 kişi). Bu konuda aksi düşünce içinde olan 9 kişi vardır ve bunların 7'si iç denetçilerdir. Dolayısıyla bu kişilerin internet dikkate alınarak yapılan çalışmalarla ilgili bazı endişeleri olduğu söylenebilir.

Katılımcıların hemen hemen yarısı işletmenin internet ortamında yayınlanan finansal tablolarının hazırlanması sürecinde Genişletilebilir İşletme Raporlama Dilinin (XBRL) kullanılmadığını vurgulamıştır (Kesinlikle katılmıyorum-8+Katılmıyorum-12= 20 kişi). Bu konuda kararsız kalanların da (26 kişi) çoğunlukta olduğu görülmektedir. İşletmelerde her ne kadar internet yoğun olarak kullanılsa da internet tabanlı raporlama dillerinden biri olan XBRL' nin kullanımı açısından yaygınlığın olmadığı görülmektedir.

Aynı şekilde katılımcılar XBRL vasıtasıyla veri transferinin eş zamanlı olarak gerçekleşmesinin sağlanarak eş zamanlı raporlama ve sürekli denetim süreçlerinin gerçekleşmesine destek olmadığını düşünmektedir (Kesinlikle katılmıyorum-8+Katılmıyorum-12= 20 kişi). Bu konuda kararsız kalanlar da çoğunlukta (26 kişi). Sürekli denetimin çoğunlukla yerine getirildiğini belirten işletmelerin sürekli denetimde yaygın olarak kullanılan yazılımlardan biri olan XBRL'yi kullanmadıkları veya bu konuda yeterli bilgiye sahip olmadıkları anlaşılmaktadır.

Özetle, işletmeler finansal tablo ve raporları internet erişim sayfalarından yayınlamaya ve aynı zamanda internet vasıtasıyla eş zamanlı veri ve bilgi alış verişi sağlayarak zaman ve kaynak tasarrufu sağlamaktadırlar. Fakat internet kullanımının sağladığı kolaylıklardan faydalanırken, işletmedeki iç denetim mekanizmasında internet teknolojisinin kullanımı ve kontrolü ile ilgili konularda endişelerin olduğu dikkat çekmektedir. Daha önce yaygın olarak kullanıldığı bildirilen internet uygulamalarının genelde tabloların yayınlanması ve bilgi alış verişi ile sınırlı olduğu anlaşılmaktadır. Raporlama veya sürekli denetim süreçlerinde ise internet tabanlı teknolojilerin kullanımı konusunda sıkıntılar vardır.

- Ankete katılanların konumları ile elektronik veri değişimi-iç denetim arasındaki ilişki:

Tablo-60. Ankete Katılanların İşletmedeki Konumları*Elektronik Veri Değişimi-İç Denetim İlişkisi

Elektronik Veri Değişimi ile İç Denetim İlişkisine Yönelik Katılım Düzeyleri		Konum	İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
İşletmemiz elektronik veri değişimi yardımıyla iş ilişkilerini elektronik ortamda devam ettirir.	Kesinlikle katılmıyorum	6	0	0	0	0	0	0	0	6
	Katılmıyorum	2	0	1	0	1	0	0	0	4
	Kararsızım	1	1	0	0	0	1	3	6	
	Katılıyorum	8	3	0	1	1	1	2	16	
	Kesinlikle katılıyorum	2	6	6	1	1	0	1	17	
Elektronik veri değişimi, iç denetçilerimizin muhasebe bilgi sisteminde denetim uygulaması yapmasına yardımcı olur.	Kesinlikle katılmıyorum	6	0	0	0	0	0	0	0	6
	Katılmıyorum	1	1	0	0	0	0	0	0	2
	Kararsızım	7	1	0	0	2	2	4	16	
	Katılıyorum	3	2	1	1	0	0	1	8	
	Kesinlikle katılıyorum	2	6	6	1	1	0	1	17	
Elektronik veri değişimi, iç denetçilerin iç kontrol sisteminin etkinliğini ve yeterliliğini belirlemeye uygun denetim süreçlerini uygulamasını sağlar.	Kesinlikle Katılmıyorum	6	0	0	0	0	0	0	0	6
	Kararsızım	7	1	0	0	2	2	2	14	
	Katılıyorum	3	3	1	1	0	0	3	11	
	Kesinlikle katılıyorum	3	6	6	1	1	0	1	18	

Tablo-60’da görüldüğü üzere katılımcıların çoğu elektronik veri değişimi yardımıyla iş ilişkilerini elektronik ortamda sürdürdüklerini belirtmiştir (Katılıyorum-16+Kesinlikle katılıyorum-17= 33 kişi). Bu katılımcıların çoğunluğu iç denetçiler, iç denetim yöneticileri ve muhasebe müdürlerinden oluşmaktadır. Bu duruma katılmadığını belirtenler ise iç denetçiler, muhasebe müdürleri ve mali işler koordinatörleri olmak üzere 10 kişiden oluşmaktadır ve katılmayanların çoğunluğunu iç denetçiler (8 kişi) oluşturmaktadır.

Elektronik veri değişiminin iç kontrol sisteminin etkinliğini ve yeterliliğini belirlemeye uygun denetim süreçlerinin uygulamasını sağladığı görüşünde olan katılımcıların sayısı katılımcıların yarısından fazladır (Katılıyorum-11+Kesinlikle katılıyorum-18= 29 kişi). Bu kişilerin çoğunluğunu iç denetim yöneticileri, muhasebe müdürleri ve iç kontrol koordinatörlerinden oluşmaktadır. Bu duruma katılmadığını bildiren 6 kişi vardır ve bunlar iç denetçilerdir. Bu konuda kararsız kaldığını bildiren 14 kişinin çoğunluğu yine iç denetçilerdir. İç denetçilerin kararsız olmasının nedeni bu konuda bilgilerinin yeterli olmaması olabileceği gibi elektronik veri değişiminin iç

kontrol sisteminin etkinliğini ve yeterliliğini belirlemeye uygun denetim süreçlerini barındırmadığını düşünmeleri de olabilir.

Katılımcıların çoğunluğunun katılım gösterdiği konulardan birisi de elektronik veri değişiminin muhasebe bilgi sisteminde denetim uygulaması yapılmasına yardımcı olduğudur (Katılıyorum-8+ Kesinlikle katılıyorum-17= 25 kişi). Bu konuda kararsız olduğunu bildirenler ise 16 kişidir. Bu kişiler muhasebe müdürleri ve genel müdür yardımcıları hariç diğer katılımcıları kapsamaktadır. Katılmadığını bildiren 8 kişi ise iç denetçi (7 kişi) ve iç denetim yöneticisinden (1 kişi) oluşmaktadır.

Özetle, iç denetim alanında sorumluluğu olan taraflar açısından elektronik veri değişimi iç kontrolün etkinliğini ve yeterliliğini belirlemeye uygun denetim süreçlerinin uygulamasını sağladığından iç denetim faaliyetini önemli ölçüde desteklemektedir. Bununla birlikte iç denetim yöneticileri ve muhasebe müdürlerinin çoğunlukla elektronik veri değişimi sayesinde muhasebe bilgi sisteminin de denetiminin yapıldığını vurgulamaktadırlar. Dolayısıyla hem işletme içi hem de diğer iş ilişkilerinin tamamıyla elektronik ortamda yürütülmesi iç denetim birimlerinin denetim faaliyetlerini bu doğrultuda yönlendirmelerine neden olmaktadır.

- **Ankete katılanların konumları ile kurumsal kaynak planlama-iç denetim arasındaki ilişki:**

*Tablo-61. Ankete Katılanların İşletmedeki Konumları*Kurumsal Kaynak Planlaması-İç Denetim İlişkisi*

Kurumsal Kaynak Planlaması ile İç Denetim İlişkisine Yönelik Katılım Düzeyleri		Konum							
		İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Kurumsal kaynak planlaması işletmemizdeki izleme faaliyetlerinin verimliliğini arttırmıştır	Kesinlikle katılmıyorum	6	0	0	0	0	0	0	6
	Kararsızım	1	2	1	0	0	0	2	6
	Katılıyorum	9	1	0	1	2	1	2	16
	Kesinlikle katılıyorum	3	7	6	1	1	1	2	21
İşletmemizde iç kontrol sistemi güvenliğini sağlamak için riskleri azaltmak amacıyla WebTrust, SysTrust gibi güvenlik sistemleri kullanılır	Kesinlikle katılmıyorum	7	1	0	0	0	1	1	10
	Katılmıyorum	7	1	0	0	2	1	2	13
	Kararsızım	1	5	0	2	0	0	2	10
	Katılıyorum	2	2	1	0	0	0	1	6
	Kesinlikle katılıyorum	2	1	6	0	1	0	0	10
Kurumsal kaynak planlaması işletmemizde süreçlerin otomatikleşmesini sağlamıştır.	Kesinlikle katılmıyorum	6	0	0	0	0	0	0	6
	Katılmıyorum	5	0	0	0	1	1	1	8
	Kararsızım	3	1	1	0	0	0	4	9
	Katılıyorum	2	2	0	1	1	0	0	6
	Kesinlikle katılıyorum	3	7	6	1	1	1	1	20

Tablo-61'den görüldüğü üzere kurumsal kaynak planlamasının işletmedeki izleme faaliyetlerinin verimliliğini arttırdığı çoğu katılımcı tarafından kabul görmüştür (Katılıyorum-16+Kesinlikle katılıyorum-21= 37 kişi). Aksini düşünenler ise 6 kişidir ve hepsi iç denetçidir.

Çoğunluğunu muhasebe müdürlerinin ve iç denetim yöneticilerinin olduğu 26 katılımcı, kurumsal kaynak planlamasının, süreçlerin otomatikleşmesine katkı sağladığını düşünmektedir. Aksini düşünenler ise çoğunluğu iç denetçi olmakla birlikte toplam 16 kişidir. Kararsız olduğunu bildiren 9 kişi içinde iç denetçiler (3 kişi) ve iç kontrol koordinatörleri (3 kişi) çoğunluktadır.

Bunlar dışında katılımcılar iç kontrol sisteminin güvenilirliğini sağlamak için riskleri azaltmak amacıyla Webtrust, Systrust gibi güvenlik sistemlerinin kullanımına çoğunlukla katılmadıklarını bildirmiştir (Kesinlikle katılmıyorum-10+Katılmıyorum-13= 23 kişi). Daha önce güvence ve danışmanlık hizmetlerinin yerine getirilişi sırasında WebTrust ve SysTrust hizmetlerinin yerine getirilmediğine dair bir sonuca ulaşmıştık. Bunu destekler nitelikte katılımcıların çoğu iç kontrol sisteminin güvenilirliğini sağlamak için riskleri azaltmak adına bu hizmetleri kapsayan sistemlerin kullanılmadığını bildirmişlerdir. Kararsızlığını bildiren 10 kişi arasında ise çoğunluğun iç denetim yöneticilerinden oluşması dikkat çekicidir. Yukarıdaki ifadeye katıldığını bildiren 16 kişi bulunmaktadır. Burada muhasebe müdürlerinin tümünün (7 kişi) bu konuda katılımını bildirdiği görülmektedir.

Sonuç olarak, kurumsal kaynak planlaması, izleme faaliyetlerine ve işletmedeki iş süreçlerinin otomatikleşmesine önemli katkılar sağlamaktadır. Dolayısıyla kurumsal kaynak planlamasının kontrole ve raporlamaya odaklanmış bir uygulama olduğu söylenebilir. Kurumsal kaynak planlamasının iç kontrol sistemine odaklı olması beraberinde sistemin güvenilirliğini sağlamak, riskleri azaltmak ve etkin ve verimli çalışmasını sağlamak amacıyla çeşitli güvenlik sistemlerinin kurulmasını gerektirmesine rağmen uygulamada durumun böyle olmadığı ayrıca bir bilgi yetersizliği olduğu da dikkat çekmektedir.

- Ankete katılanların konumları ile elektronik veri işleme-iç denetim arasındaki ilişki:

Tablo-62. Ankete Katılanların İşletmedeki Konumları*Elektronik Veri İşleme-İç Denetim İlişkisi

Elektronik Veri İşleme ile İç Denetim İlişkisine Yönelik Katılım Düzeyleri		Konum	İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
İşletmemizde elektronik veri işleme teknolojileri sayesinde iç kontrol sistemi bilgisayarda yazılım düzeyinde bulunmaktadır.	Katılmıyorum		8	1	1	1	0	0	0	11
	Kararsızım		5	2	0	0	1	1	5	14
	Katılıyorum		2	0	6	0	2	0	0	10
	Kesinlikle katılıyorum		4	7	0	1	0	1	1	14
İşletmemizde finansal bilgiler ve denetim kanıtlarının çoğu elektronik ortamda tutulmaktadır.	Katılmıyorum		6	0	1	0	1	1	1	10
	Kararsızım		0	0	0	0	0	0	1	1
	Katılıyorum		7	2	6	1	1	0	0	17
	Kesinlikle katılıyorum		6	8	0	1	1	1	4	21
Gerçek zamanlı elektronik veri işleme sistemleri denetim tekniklerimizi yenilememize neden olmuştur.	Katılmıyorum		6	0	1	0	1	1	1	10
	Kararsızım		0	0	0	0	0	0	1	1
	Katılıyorum		2	3	0	0	0	0	0	5
	Kesinlikle katılıyorum		11	7	6	2	2	1	4	33
İşletmemizde elektronik veri işleme teknolojilerinin kullanımı hatalı işlemleri azaltmıştır.	Katılmıyorum		6	0	1	0	1	1	1	10
	Kararsızım		7	4	0	2	0	0	1	14
	Katılıyorum		2	3	0	0	0	0	0	5
	Kesinlikle katılıyorum		4	2	6	0	2	1	4	19
İşletmemizde elektronik veri işleme teknolojilerinin kullanımıyla ortaya çıkan güvenlik açıkları bilgi güvenliğini tehdit etmektedir.	Kesinlikle katılmıyorum		0	0	0	0	0	0	2	2
	Katılmıyorum		2	0	1	0	0	0	0	3
	Kararsızım		2	1	5	0	1	0	1	10
	Kesinlikle katılıyorum		6	2	0	0	1	1	1	11
	Kesinlikle katılıyorum		9	7	0	2	1	1	2	22

Tablo-62'ye baktığımızda işletmelerin finansal bilgilerinin ve denetim kanıtlarının çoğunun elektronik ortamda tutulduğunu katılımcıların çoğunun vurguladığı görülmektedir (Kesinlikle katılıyorum-21+Katılıyorum-17= 38 kişi). Bu kez iç denetim yöneticileri ve muhasebe müdürleri ile birlikte iç denetçilerin de katılımlarının yüksek olduğu görülmektedir. Katılmadığını bildirenler 10 kişidir ve bunların 6'sı iç denetçidir.

Aynı şekilde katılımcıların çoğu gerçek zamanlı elektronik veri işleme sistemlerinin denetim tekniklerini yenilemelerine neden olduğunu belirtmiştir (Kesinlikle katılıyorum-35+Katılıyorum-5= 38 kişi). Üstelik bu duruma 35 kişi

kesinlikle katıldığını bildirmektedir. Bu duruma katılmadığını bildirenler ise 10 kişidir ve bunların 6'sı iç denetçidir.

Katılımcıların çoğunlukla vurguladığı bir diğer nokta da elektronik veri işleme teknolojilerinin kullanımıyla ortaya çıkan güvenlik açıklarının bilgi güvenliğini tehdit etmesidir (Kesinlikle katılıyorum-22+Katılıyorum-11= 33 kişi). Muhasebe müdürlerinin çoğu ve iç denetim yöneticisinin de yer aldığı 10 kişilik bir grup bu konuda kararsız olduğunu bildirmiştir. Aksini bildirenler ise sadece 5 kişidir.

Katılımcıların çoğu işletmelerinde veri işleme teknolojileri sayesinde iç kontrol sisteminin bilgisayarlarda yazılım düzeyinde bulunduğunu bildirmiştir (Kesinlikle katılıyorum-14+Katılıyorum-10= 24 kişi). Katılanlar arasında muhasebe müdürleri ve iç denetim yöneticileri çoğunluktadır. İç kontrol koordinatörlerinin tümünün (4 kişi) ve iç denetçilerin (5 kişi) çoğunlukta olduğu 14 kişi ise kararsızlığını bildirmiştir. Katılmadığını bildirenler 11 kişidir ve bunların 8'i iç denetçidir.

Katılımcıların çoğu işletmede elektronik veri işleme teknolojilerinin kullanımının hatalı işlemleri azalttığını vurgulamaktadır (Kesinlikle katılıyorum-19+Katılıyorum-5= 24 kişi). İç denetçi, iç denetim yöneticisi ve genel müdür yardımcılarının çoğunlukta olduğu 14 kişilik grup ise kararsızlığını bildirmiştir. Katılmadığını bildirenler 10 kişidir ve bunların 6'sı iç denetçidir.

Özetle, elektronik veri işleme sistemlerinin kullanımı işletmelerde finansal bilgi ve kanıtların çoğunun elektronik ortamda saklanmasını gerektirmektedir. Gerçek zamanlı sistemlerin kullanılması işletmelerin denetim tekniklerini yenilemesini gerektirmiştir. Ayrıca yapılan değerlendirmelere göre elektronik veri işleme sistemleri sayesinde iç kontrol sistemi bilgisayarda yazılım düzeyine gelmiş ve hatalı işlem sayısı azalmıştır. Fakat elektronik veri işlemenin bilgi güvenliği konusunda oluşturduğu endişeler sürmektedir. Bu durum iç kontrol sisteminin önemini bir kez daha göstermektedir.

- Ankete katılanların konumları ile BT'nin değerlendirilmesi sırasındaki uygulamalar arasındaki ilişki:

Tablo-63. Ankete Katılanların Konumları* BT'nin Değerlendirilmesi Sırasındaki Uygulamalar

Konum		İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
İç Denetim Biriminin Bilgi Teknolojilerini Değerlendirmesi Sırasındaki Uygulamaları	Bilgi Teknolojileri kullanımının verimliliğinin /etkinliğinin/ekonomikliğinin değerlendirilmesi yapılır	Hiç yapılmaz	0	1	0	0	0	0	1
	Bazen yapılır	3	2	1	0	0	0	0	6
	Yapılır	12	2	0	1	1	1	2	19
	Hep yapılır	4	6	6	2	2	1	4	25
Politikalar ve düzenlemelerle uyumluluğunun değerlendirilmesi yapılır.	Hiç yapılmaz	0	1	0	0	0	0	0	1
	Yapılmaz	1	0	1	0	0	0	0	2
	Bazen yapılır	1	0	0	0	0	0	0	1
	Yapılır	12	4	0	1	1	1	4	23
Bilgi teknolojilerine dayalı sistemlerde iç kontrolün değerlendirilmesi yapılır	Hep yapılır	5	6	6	2	2	1	2	24
	Hiç yapılmaz	0	1	0	0	0	0	0	1
	Bazen yapılır	3	1	1	0	0	0	0	5
	Yapılır	7	1	0	1	0	0	1	10
Finansal tabloların gösteriminde eşitliğin ve muhasebe bilgi sisteminin doğruluğunun ve tamlığının değerlendirilmesi yapılır	Hep yapılır	9	8	6	2	3	2	5	35
	Hiç yapılmaz	6	0	0	1	0	0	0	7
	Bazen yapılır	6	1	1	0	1	1	1	11
	Yapılır	3	3	0	0	0	0	3	9
	Hep yapılır	4	7	6	2	2	1	2	24

Tablo-63'e göre katılımcıların büyük bir çoğunluğu BT değerlendirilmesi sırasında en çok gerçekleştirilen uygulamanın politika ve düzenlemelerle uyumluluğun değerlendirilmesi olduğunu bildirmiştir (Yapılır-23+Hep yapılır-24= 47 kişi). Sonrasında BT'ne dayalı sistemlerde iç kontrolün değerlendirilmesinin yapılması çoğu katılımcı tarafından bildirilmiştir (Yapılır-10+Hep yapılır-35= 45 kişi). Ayrıca BT kullanımının verimliliğinin/etkinliğinin/ekonomikliğinin değerlendirilmesi de katılımcıların çoğunlukla bildirdiği uygulamalardandır (Yapılır-19+Hep yapılır-25= 44 kişi). Finansal tabloların gösteriminde eşitliğin ve muhasebe bilgi sisteminin doğruluğunun ve tamlığının değerlendirilmesinin yapılması ise 33 katılımcı (Yapılır-19+Hep yapılır-25= 33 kişi) tarafından bildirilmiştir. Bu uygulamada bazen yapıldığı yönündeki bildirimlerin diğer uygulamalara nazaran arttığı dikkat çekmektedir (11 kişi).

Özetle, işletmede kullanılan BT'nin değerlendirilmesi sırasında gerçekleştirilecek faaliyetler, bu teknolojilerin işletmenin politika ve düzenlemelerine uyumlu olmasını kapsar. BT'nin etkinliğinin ve verimliliğinin değerlendirmesi, gerçekleşen işlemlerin doğruluğunun onaylanmasını ve dolayısıyla işletmenin iç kontrol

sisteminin değerlendirmesini sağlamaktadır. İşletmeler bilgi teknolojilerini kullanırken başarılı bir muhasebe bilgi sistemini amaç edinmelidir. Kullanılan bilgi teknolojilerinden en fazla faydayı elde etmeleri için muhasebe bilgi sisteminin ve bu sistemin çıktıları olan finansal tabloların doğruluğunun yine BT değerlendirmeleri sırasında dikkate alınması gerekecektir.

- **Ankete katılanların konumları ile BT kontrollerinin performansı arasındaki ilişki:**

*Tablo-64. Ankete Katılanların İşletmedeki Konumları *BT Kontrollerinin Performansı*

BT kontrollerinin Performansı		Konum	İç Denetçi	İç Denetim Yön.	Gn Md. Yrd.	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Kontrollerin etkinliği test edilir	Bazen yapılır	2	1	1	0	0	0	0	0	4
	Yapılır	12	1	0	1	1	1	1	4	20
	Hep yapılır	5	8	6	2	2	1	2	2	26
Riskler ve risk yönetimi süreci değerlendirilir.	Yapılmaz	1	0	1	0	0	0	0	0	2
	Bazen yapılır	1	0	0	0	0	0	0	0	1
	Yapılır	11	1	0	1	1	1	1	4	19
Genel kontrollerin etkinliği test edilir.	Hep yapılır	6	9	6	2	2	1	2	2	28
	Yapılmaz	1	0	1	0	0	0	0	0	2
	Bazen yapılır	1	0	0	0	0	0	0	0	1
Uygulamalar içindeki kontroller test edilir	Yapılır	12	2	0	1	1	1	1	2	19
	Hep yapılır	5	8	6	2	2	1	4	4	28
	Bazen yapılır	3	2	1	0	0	0	0	0	6
Uygulama kontrolleri ve genel kontroller değerlendirilir	Yapılır	11	0	0	1	1	1	1	2	16
	Hep yapılır	5	8	6	2	2	1	4	4	28
	Yapılmaz	1	0	1	0	0	0	0	0	2
Uygulama kontrolleri ve genel kontroller değerlendirilir	Bazen yapılır	0	1	0	0	0	0	0	0	1
	Yapılır	13	1	0	1	1	1	1	4	21
	Hep yapılır	4	8	6	2	2	1	2	2	25

Tablo-64'e göre katılımcıların çoğu BT kontrollerinin performansının ölçümü açısından risklerin ve risk yönetimi sürecinin değerlendirildiğini (Yapılır-19+Hep yapılır-28= 47 kişi) ve genel kontrollerin test edildiğini (Yapılır-19+Hep yapılır-28= 47 kişi) bildirmektedir. Ayrıca BT kontrollerinin performansının ölçümü açısından kontrollerin etkinliğinin test edilmesi (Yapılır-20+Hep yapılır-26=46 kişi) ve uygulama ve genel kontrollerin değerlendirilmesi de (Yapılır-21+Hep yapılır-25=46 kişi) katılımcıların çoğu tarafından yapıldığı bildirilmiştir. Uygulamaların içindeki kontrollerin test edilmesi de katılımcıların çoğu tarafından yapılmaktadır (Yapılır-16+Hep yapılır-28=44 kişi).

Özetle iç denetim birimi ve iç denetimden sorumlu taraflar, BT kontrolleri ile ilgili sorumluluğu bulunan birimlerle etkileşim halindedir ve BT ile ilgili yenilikler ortaya çıktıkça bu teknolojilerin kullanım amaçlarından, karşı karşıya olduğu risklerden

ve değerlendirilmesinden sorumludurlar. Denetçiler edindikleri bilgiler ve yapılan değerlendirmeler sonucunda mevcut BT kontrollerini düzeltmeli, geliştirmeli veya yenilerini oluşturabilmelidir. BT kontrollerinin performansının değerlendirilmesi sırasında risk yönetimi sürecinin de değerlendirilmesi gerekebilir.

- **Ankete katılanların konumları ile BT kullanımının artmasını engelleyen durumlar arasındaki ilişki:**

*Tablo-65. Ankete Katılanların İşletmedeki Konumları*BT Kullanımının Artmasını Engelleyen Durumlar*

BT Kullanımının Artmasını Engelleyen Durumlar	Konum	İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Veri analizi yazılımlarını kullanacak kalifiye personel olmayışı		8	1	0	7	3	2	3	24
Veri erişiminde bilgi teknolojilerine bağımlılık		2	6	1	0	0	0	4	13
Bilgi sistemlerinin/ işletme birimlerinin/ global faaliyetlerin denetlenme gerekliliği		3	6	1	0	0	0	1	11
Veri bütünlüğü, güvenilirliği ve doğruluğu ile ilgili konular		14	4	1	0	1	2	3	25
Bilgi teknolojisi ile ilgili konuların önceliği yoktur		1	6	1	0	0	0	0	8
Bütçe kısıtları		1	2	0	7	1	0	0	11

* Ankete katılanlar birden fazla seçenek işaretleyerek soruya cevap verebilmektedir.

Tablo-65'e bakıldığında muhasebe müdürleri hariç katılımcıların çoğu veri bütünlüğü, güvenilirliği ve doğruluğu ile ilgili konuları BT kullanımının artmasını engelleyen durumlar arasında ilk sırada belirtmiştir (25 kişi). Sonrasında ise veri analizi yazılımlarını kullanacak kalifiye personel olmayışı gelmektedir (24 kişi). Burada ise muhasebe müdürlerinin, mali işler koordinatörlerinin ve denetim koordinatörlerinin tümünün katılım göstermesi dikkat çekmektedir. Veri erişiminde bilgi teknolojilerine bağımlılık da 13 katılımcı tarafından bildirilmiştir. Bu katılımcıların çoğunluğu iç denetim yöneticileri ve iç kontrol koordinatörleridir. Bilgi sistemlerinin/işletme birimlerinin/global faaliyetlerin denetlenme gerekliliği (11 kişi) ve bütçe kısıtları (11 kişi) bir diğer durumdur. Bütçe kısıtlarının en çok muhasebe müdürleri tarafından bildirildiği görülmektedir.

Özetle, veri bütünlüğü, güvenilirliği ve doğruluğu konusundaki endişeler BT kullanımının artmasının önündeki en önemli engellerden birisi olarak görülmektedir. Kalifiye personelin olmayışı da bu endişelerin artmasına ve dolayısıyla BT kullanımının artmasına engel olmaktadır. Bazı işletmeler açısından ise mali konular önem taşıyabilmektedir, dolayısıyla bütçe kısıtları nedeniyle BT alımları veya yenilemeleri

ertelenebilmektedir. Kalifiye personel yetersizliği ve bütçe kısıtları muhasebe müdürlerinin en çok öncelik verdiği konulardır.

5.3.5.2. Bilgi teknolojileri uygulamaları ile ilgili non-parametrik testler

Her biri için ayrı ayrı olmak üzere “bilgi teknolojileri uygulamalarının geçmiş ve şimdiki kullanımlarının değerlendirilmesi” ve “iç denetim ile ilişkileri yönünden elektronik ticaret, internet, elektronik veri değişimi, kurumsal kaynak planlama ve veri işleme teknolojileri” ile ankete katılanların konumları arasında anlamlı farklılıkların olup olmadığını görmek için Kruskal-Wallis Testi yapılmıştır.

BT uygulamalarından extranet ve elektronik ticaretin şimdiki kullanımlarının değerlendirilmesi ile ankete katılanların konumları arasında anlamlı farklılık bulunmuştur (Ek-1 Tablo-90). Muhasebe müdürleri mevcut durumda extranetin kullanıldığı, iç kontrol koordinatörleri ise kullanılmadığı yönünde bildirimde bulunmuştur. Elektronik ticaret açısından ise mali işler koordinatörleri bu uygulamanın kullanıldığı, genel müdür yardımcıları ise kullanılmadığı yönünde bildirimde bulunmuştur. Geçmişteki değerlendirmeler baktığımızda **BT uygulamalarından extranetin ve kurumsal kaynak planlamasının geçmişteki** kullanımlarının değerlendirilmesi ile ankete katılanların konumları arasında anlamlı farklılıklar bulunmuştur (Ek-1 Tablo- 90). Extranet açısından muhasebe müdürleri geçmişte de bu BT uygulamasını kullandıkları, denetim koordinatörleri ise kullanmadıkları yönünde bildirimde bulunmuştur. Kurumsal kaynak planlaması açısından bakıldığında muhasebe müdürleri geçmişte de bu BT uygulamasını kullandıkları, genel müdür yardımcıları ise kullanmadıkları yönünde bildirimde bulunmuştur.

Ankete katılanların konumları ile **iç denetim ile ilişkisi yönünden e-ticaretin değerlendirilmesi** arasında anlamlı farklılıklar bulunamamıştır. Fakat ankete katılanların yaşları açısından anlamlı farklılıklar olduğu dikkat çekmiştir (Ek-1 Tablo-91). 36-40 yaş grubundaki katılımcılar elektronik ticaretin iç kontrolün etkililiğine ilişkin asıl riskleri bünyesinde barındırdığını vurgularken, 30 yaş ve altı katılımcılar aksi yönde fikir bildirmişlerdir. Aynı şekilde 36-40 yaş grubundaki katılımcılar elektronik formların ve elektronik ticaret kapsamındaki çevrimiçi işlemlerin iç kontrolün etkinliğini doğrulamak amacıyla işlem bütünlüğü sağladığını belirtirken, 30 yaş ve altı katılımcılar aksini belirtmişlerdir. 30 yaş ve altı gruptaki katılımcılar geleneksel kağıt

dokümanlardan elektronik ticarete geçişin iç kontrol zayıflıklarını arttırdığını bildirirken, 36-40 yaş gurubu katılımcılar arttırmadığı yönünde düşünceye sahiptirler.

Ankete katılanların konumları ile **iç denetim ile ilişkisi yönünden internetin değerlendirilmesi** arasında anlamlı farklılık bulunmamıştır, fakat ankete katılanların yaşları açısından anlamlı farklılıkların olduğu dikkat çekmiştir (Ek-1 Tablo-92). 36-40 yaş grubundaki katılımcılar finansal tabloların internet erişim sayfasından yayınlandığını, 30 yaş ve altı grubundaki katılımcılar yayınlanmadığını bildirmiştir. Ayrıca 36-40 yaş grubundaki katılımcılar internet vasıtasıyla eş zamanlı veri sağladıkları, 46-50 yaş grubundaki katılımcılar sağlamadıklarını bildirmiştir. 36-40 yaş grubundaki katılımcılar finansal tabloların hazırlanmasında XBRL kullanıldığını, 30 yaş ve altı grubundaki katılımcılar kullanılmadığını bildirmiştir. Yine 36-40 yaş grubundaki katılımcılar eş zamanlı veri transferi sayesinde eş zamanlı raporlama ve sürekli denetim yapıldığı, 30 yaş ve altı grubundaki katılımcılar yapılmadığı yönünde bildirimde bulunmuştur. 36-40 yaş grubundaki katılımcılar iç denetim mekanizmalarının oluşturulması sırasında internet teknolojisinin tanımladığını, 30 yaş ve altı grubundaki katılımcılar tanımlanmadığı yönünde bildirimde bulunmuştur.

Ankete katılanların konumları ile **iç denetim ile ilişkisi yönünden elektronik veri değişiminin değerlendirilmesi** arasında anlamlı farklılıklar bulunmuştur (Ek-1 Tablo-93). Muhasebe müdürleri elektronik veri değişimi vasıtasıyla iş ilişkilerini sürdürdüklerini, iç denetçiler aksi yönde bildirimde bulunmuştur. Muhasebe müdürleri elektronik veri değişiminin iç denetçilerin muhasebe bilgi sistemini denetlemesine yardımcı olduğu, iç denetçiler ise olmadığı yönünde bildirimde bulunmuştur. Muhasebe müdürleri elektronik veri değişiminin iç denetçilerin iç kontrol sistemini denetlemesine yardımcı olduğu, denetim koordinatörleri ise olmadığı yönünde bildirimde bulunmuştur.

Ankete katılanların konumları ile **iç denetim ile ilişkisi yönünden kurumsal kaynak planlamasının değerlendirilmesi** arasında anlamlı farklılıklar bulunmuştur (Ek-1 Tablo-94). Muhasebe müdürlerinin riskleri azaltmak amacıyla çeşitli güvenlik sistemlerini kullandıkları, denetim koordinatörleri ve iç kontrol koordinatör yardımcılarını kullanmadıkları yönünde bildirimde bulunmuştur. Muhasebe müdürleri kurumsal kaynak planlamasının işlerin otomatikleşmesine katkı sağladığı, iç denetçiler ise sağlamadığı yönünde bildirimde bulunmuştur.

Ankete katılanların konumları ile **iç denetim ile ilişkisi yönünden elektronik veri işlemenin değerlendirilmesi** arasında anlamlı farklılıklar bulunmuştur (Ek-1 Tablo-95). Genel müdür yardımcıları elektronik veri işlemenin yarattığı güvenlik açıklarının bilgi güvenliğini tehdit ettiğini, muhasebe müdürleri ise etmediği yönünde bildirimde bulunmuştur.

Özetle, işletmede pek çok süreçte kullanılan BT uygulamaları, özellikle iç kontrol sisteminin etkinliği ve verimliliği, iç kontrol sisteminde ortaya çıkan risklerin tespiti, bilgi güvenliğinin sağlanması, iş ilişkilerinin ve iş süreçlerinin elektronik ortama taşınması, finansal raporlama gibi konularda iç denetimden sorumlu tarafların endişe duymasına neden olabilmektedir. Fakat finansal tabloların kısa zamanda hazırlanması ve yayınlanması, iç kontrol sisteminin denetlenmesi, eş zamanlı veri alışverişi ile sağlanan kaynak ve zaman tasarrufu, izleme faaliyetlerinin verimliliğinin artması gibi konularda BT'nin sağladığı faydalar da inkar edilememektedir.

Kruskal-Wallis Testi dışında bir diğer non-parametrik test olarak uygulanan Spearman's Rank Order Korelasyonu sonuçlarına göre "İç denetim ile ilişkileri yönünden elektronik ticaret, internet, elektronik veri değişimi, kurumsal kaynak planlama ve veri işleme teknolojileri" ile BT kullanan iç denetim personeli sayısı ve BT denetiminin uygulandığı süre arasında anlamlı ilişkiler bulunmuştur.

BT kullanan iç denetim personel sayısı ile internet-iç denetim ilişkisi yönünden "İnternet vasıtasıyla eş zamanlı veri ve bilgi alışverişi sağlanmaktadır" ifadesi arasında yapılan analizde BT kullanan iç denetim personel sayısı arttıkça, internet vasıtasıyla eş zamanlı bilgi alış verişi de artmaktadır (Ek-1 Tablo-96). "İşletmemizde internet ortamında yayınlanan finansal tabloların hazırlanması sürecinde XBRL kullanılmaktadır" ifadesi ile yapılan analizde BT kullanan iç denetim personel sayısı arttıkça, internet ortamında yayınlanmak için hazırlanan finansal tabloların hazırlanmasında XBRL kullanımına ilişkin katılım düzeyi de artmaktadır (Ek-1 Tablo-96). "İşletmemizde risklere karşı iç denetim mekanizmaları oluşturulurken internet teknolojisinin yapılandırılması, yönetimi ve kontrolü gibi alanlar da tanımlanır" ifadesi ile yapılan analizde BT kullanan iç denetim personel sayısı arttıkça, iç denetim mekanizmaları oluşturulurken internet teknolojisinin yapılandırılması, yönetimi ve kontrolü gibi alanların tanımlandığına katılımları da artmaktadır (Ek-1 Tablo-96).

BT kullanan iç denetim personel sayısı ile elektronik veri işleme-iç denetim ilişkisi yönünden “*İşletmemizde finansal bilgiler ve denetim kanıtlarının çoğu elektronik ortamda tutulmaktadır*” ifadesi arasında yapılan analizde BT kullanan iç denetim personel sayısı arttıkça, işletmelerde finansal bilgilerin ve denetim kanıtlarının elektronik ortamda tutulmasına katılım düzeyleri de artmıştır (Ek-1 Tablo-96). “*İşletmemizde elektronik veri işleme teknolojilerinin kullanımı hatalı işlemleri azaltmıştır*” ifadesi ile yapılan analizde BT kullanan iç denetim personel sayısı arttıkça, hatalı işlemlerin elektronik veri işleme teknolojilerinin kullanımına bağlı olarak azaldığı fikrine katılımları da artmıştır (Ek-1 Tablo-96).

BT denetiminin uygulandığı süre ile elektronik veri işleme-iç denetim ilişkisi yönünden “*İşletmemizde elektronik veri işleme teknolojilerinin kullanımı hatalı işlemleri azaltmıştır*” ifadesi arasında yapılan analizde BT denetiminin uygulandığı süre arttıkça hatalı işlemlerin elektronik veri işleme teknolojilerinin kullanımına bağlı olarak azaldığı fikrine katılımları da artmıştır (Ek-1 Tablo-97).

Özetle, BT kullanılan işletmelerde iç denetim birimlerinde çalışan kişilerin sayıca yeterli olması özellikle internet ve elektronik veri işlemeye dayalı BT uygulamalarının kullanılarak veri ve bilgi alış verişinin hızlanması, finansal tabloların hazırlanması sürecinde son teknolojinin kullanılarak tabloların internet ortamında yayınlanması, internetin kullanımının iç kontrol mekanizması oluşturulurken tanımlanması ve gerekli kontrollerin oluşturulması gibi konularda çalışabilecek ve uzmanlaşacak personelin bulunmasına yardımcı olabilir. İşletmelerdeki BT kaynaklarını denetlemeye yönelik gerçekleştirilen BT denetimlerinde ise bu denetimin uygulandığı süre arttıkça elektronik veri işleme sayesinde gerçekleştirilen işlemlerdeki hataların da azalacağı söylenebilir.

5.3.6. Bilgi teknolojileri denetimi ile ilgili çapraz tablo analizleri ve non-parametrik testler

5.3.6.1. Bilgi teknolojileri denetimi ile ilgili çapraz tablo analizleri

BT denetimi ile ilgili çapraz tablo analizleri katılımcıların işletmedeki konumları itibarıyla düzenlenmiştir. Ankete katılanlar “BT denetiminin uygulanma süresi”, “BT denetiminin yapılma nedenleri”, “iç denetim planlama faaliyetlerinin BT denetimini kapsama durumu”, “BT denetiminin etkinliği”, “BT denetimini etkileyen konular” ve “BT denetiminin uygulanmasını kolaylaştıran teknolojik yenilikler” konularını değerlendirmişlerdir.

- Ankete katılanların konumları ile BT denetiminin uygulanma süresi arasındaki ilişki:

Tablo-66. Ankete Katılanların İşletmedeki Konumları*BT Denetiminin Uygulandığı Süre

Konum	Bilgi teknolojileri denetiminin uygulandığı süre					
	Hiç uygulanmaz	1 yıldan az	1-3 yıl	4-6 yıl	10 yıl ve üzeri	Toplam
İç Denetçi	1	1	11	4	1	18
İç Denetim Yöneticisi	1	3	4	3	0	11
Genel müdür yardımcısı	2	1	0	0	0	3
Muhasebe Müdürü	2	1	0	4	0	7
Mali İşler koordinatörü	0	1	2	0	0	3
Denetim Koordinatörü	0	0	2	0	0	2
İç Kontrol Koordinatörü	0	1	3	1	1	6
Toplam	6	8	22	12	2	50

Tablo-66’da görüldüğü üzere katılımcıların çoğu 1-3 yıldır BT denetiminin uygulandığını bildirmektedir (22 kişi). Sonrasında ise 4-6 yıldır BT denetimini uygulayanların çoğunlukta olduğu görülmektedir (12 kişi). Genel müdür yardımcılarını hariç diğer katılımcıların genelde bu iki seçenek arasında durumlarını belirttikleri görülmektedir. Genel müdür yardımcıları ise BT denetiminin yapılmadığını bildirmektedir.

Özetle, BT denetiminin uygulanma süresinin çok eskilere dayanmadığı görülmekle birlikte yapılan analizlerde genellikle geçtiğimiz 5 yıllık bir süreçte BT denetiminin arttığı ve işletmelerin bu konuda biraz daha bilinçlendiği söylenebilir.

- Ankete katılanların konumları ile BT denetiminin yapılma gerekliliğine ilişkin nedenler arasındaki ilişki:

Tablo-67. Ankete Katılanların İşletmedeki Konumları*BT Denetiminin Yapılma Gerekliliğine İlişkin Nedenler

BT Denetiminin Yapılmasının Nedenleri		Konum	İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Sistemlerin kesintisiz çalışmasını sağlar.	Katılmıyorum		0	0	0	0	0	0	1	1
	Kararsızım		1	1	1	0	0	0	0	3
	Katılıyorum		5	1	1	0	1	1	1	10
	Kesinlikle katılıyorum		12	8	3	1	2	1	4	31
Beklenmedik durumlar karşısında iş sürekliliğini sağlar.	Katılmıyorum		0	0	0	0	0	0	1	1
	Kararsızım		1	4	2	0	0	0	0	7
	Katılıyorum		6	2	0	0	1	1	2	12
	Kesinlikle katılıyorum		11	3	3	1	2	1	3	24
Bilgi teknoloji risklerine karşı önlem almayı sağlar	Kararsızım		0	2	1	0	0	0	0	3
	Katılıyorum		5	0	1	0	1	1	3	11
	Kesinlikle katılıyorum		13	8	3	1	2	1	3	31
Teknolojik alt yapının ihtiyaçlarını karşılamada optimum çözüm olup olmadığını bulmayı sağlar.	Kararsızım		5	0	2	0	1	1	2	11
	Katılıyorum		2	4	0	0	0	0	2	8
	Kesinlikle katılıyorum		11	6	3	1	2	1	2	26
Bilgi-işlem departmanındaki kişilere bağımlı olmamayı sağlar.	Katılmıyorum		1	1	0	0	0	0	1	3
	Kararsızım		0	0	1	0	0	0	3	4
	Katılıyorum		2	8	0	0	0	0	0	10
	Kesinlikle katılıyorum		15	1	4	1	3	2	2	28
Kullanıcıların sistem veya uygulama kaçaklarını görmesini ve bu kaçakları kötüye kullanmalarını önlemeyi sağlar	Kararsızım		1	1	1	0	0	0	0	3
	Katılıyorum		0	2	0	0	0	0	3	5
	Kesinlikle katılıyorum		17	7	4	1	3	2	3	37
İşletme bilgilerinin güvenliğini sağlar.	Kararsızım		0	0	1	0	0	0	0	1
	Katılıyorum		2	1	1	0	0	0	0	4
	Kesinlikle katılıyorum		16	9	3	1	3	2	6	40

Tablo-67’de görüldüğü üzere katılımcıların büyük bir çoğunluğu işletme bilgilerinin güvenilirliğinin sağlanması için BT denetiminin yapılması gerektiğini bildirmiştir (Katılıyorum-4+Kesinlikle katılıyorum-40= 44 kişi).

BT risklerine karşı önlem almayı sağlaması açısından BT denetiminin yapılması gerektiğini bildirenler de oldukça fazladır (Katılıyorum-11+Kesinlikle katılıyorum-31= 42 kişi). Aynı şekilde kullanıcıların sistem veya uygulama kaçaklarını görmesini ve bu kaçakları kötüye kullanmalarını önlemesini sağlamak için de BT denetiminin yapılması gerektiğini düşünenler çoktur (Katılıyorum-5+Kesinlikle katılıyorum-37= 42 kişi).

Katılımcıların büyük bir çoğunluğu sistemlerin kesintisiz çalışması için BT denetiminin yapılması gerektiğini bildirmektedir (Katılıyorum-10+Kesinlikle katılıyorum-31= 41 kişi).

BT denetiminin beklenmedik durumlar karşısında iş sürekliliğini sağlaması nedeniyle yapılması gerektiğine 36 kişi katıldığını bildirirken (Katılıyorum-12+Kesinlikle katılıyorum-24), 7 kişi bu konuda kararsız olduğunu belirtmiştir. Kararsız grubun çoğunluğunu iç denetim yöneticileri (4 kişi) oluşturmaktadır.

Teknolojik alt yapının ihtiyaçlarını karşılamada optimum düzeyde olup olmadığını ortaya çıkarması açısından BT denetiminin yapılması gerektiğini vurgulayan katılımcılar 34 kişidir (Katılıyorum-8+Kesinlikle katılıyorum-26). Bu katılımcılar içinde hemen hemen her konumdan katılımcı olmakla birlikte iç denetçilerin ve iç denetim yöneticilerinin ağırlıkta olduğu görülmektedir. Bu konuda kararsız olduğunu bildiren 11 kişinin içinde genel müdür yardımcıları ve iç denetim yöneticileri yoktur.

Özetle, hangi konumda olursa olsun katılımcılar BT denetiminin yapılma nedeni olarak bilgi güvenilirliğinin sağlanmasını görmektedir. Bununla birlikte sistemdeki açıkları yakalamak ve bu açıkların kötüye kullanılmasını önlemek, sistemlerin kesintisiz çalışmasını sağlamak ve iş sürekliliğini devam ettirebilmek de BT denetiminin yapılmasındaki diğer önemli nedenlerdir. İç denetim alanında sorumluluk taşıyan yönetici ve çalışanlar özellikle iç denetim yöneticileri, muhasebe müdürleri ve iç denetçiler bu nedenlerin önemi doğrultusunda BT konusunda çalışmalar yapmaktadır.

- **Ankete katılanların konumları ile iç denetim planlama faaliyetlerinin BT denetimini kapsama durumu arasındaki ilişki:**

*Tablo-68. Ankete Katılanların İşletmelerindeki Konumları*İç Denetim Planlama Faaliyetlerinin BT Denetimini Kapsama Durumu*

KONUM	İşletmenizde iç denetim planlama faaliyetlerine Bilgi teknolojileri denetimi faaliyetleri dahil midir?			
	Evet	Hayır	Bilmiyorum	Toplam
İç Denetçi	18	1	0	19
İç Denetim Yöneticisi	9	2	0	11
Genel müdür yardımcısı	0	2	1	3
Muhasebe Müdürü	0	7	0	7
Mali İşler koordinatörü	3	0	0	3
Denetim Koordinatörü	2	0	0	2
İç Kontrol Koordinatörü	6	0	0	6
Toplam	38	12	1	51

Tablo-68'e bakıldığında katılımcıların çoğunluğu BT denetiminin iç denetimin planlama faaliyetine dahil olduğunu bildirmiştir (38 kişi). Muhasebe müdürleri ve genel müdür yardımcıları bu grupta yer almazken, iç denetçilerin (18 kişi) ve iç denetim yöneticilerinin (9 kişi) neredeyse tümü ve diğer katılımcılar bu grupta yer almaktadır. BT denetiminin iç denetimin planlama faaliyetine dahil olmadığını bildirenler ise 12 kişidir ve çoğunluğu muhasebe müdürlerinden oluşmaktadır.

Özetle, iç denetimin planlama faaliyetleri sırasında denetimin kapsamı, planı ve gerekli güvence seviyesi belirlenirken, BT denetimine ilişkin faaliyetler de ele alınmaktadır. Özellikle iç denetim birimlerinde görevli olan iç denetçiler, iç denetim yöneticileri, iç kontrol koordinatörleri ve yardımcıları bu faaliyetlerin planlanmasında ve uygulanmasında esas sorumluluk sahibidirler. Özellikle muhasebe müdürleri ve genel müdür yardımcıları gibi işletmede genel veya belli bir bölüme yönelik öncelikli sorumlulukları bulunan katılımcılarda iç denetime yönelik sorumlulukların benimsenmesinde bazen zayıflıklar olduğu görülmektedir.

- **Ankete katılanların konumları ile BT denetiminin etkinliği arasındaki ilişki:**

*Tablo-69. Ankete Katılanların Konumları*BT Denetiminin Etkinliği*

Konum	İşletmenizdeki Bilgi teknolojileri denetim faaliyetlerinin etkinliğini değerlendiriniz.					
	Hiç etkin değil	Etkin değil	Kısmen etkin	Etkin	Tamamıyla etkin	Toplam
İç Denetçi	1	0	12	5	1	19
İç Denetim Yöneticisi	0	2	1	5	3	11
Genel müdür yardımcısı	0	2	1	0	0	3
Muhasebe Müdürü	2	0	5	0	0	7
Mali İşler koordinatörü	0	0	2	1	0	3
Denetim Koordinatörü	0	0	1	1	0	2
İç Kontrol Koordinatörü	0	0	2	4	0	6
Toplam	3	4	24	16	4	51

Tablo-69'a baktığımızda katılımcıların çoğu BT denetiminin kısmen etkin bir şekilde gerçekleştirildiğini bildirmektedir (24 kişi). Bu kişiler çoğunlukla muhasebe müdürleri ve iç denetçilerden oluşmaktadır. BT denetiminin etkin bir şekilde gerçekleştirildiğini bildirenler ise 20 kişidir (Etkin-16+Tamamıyla etkin-4). İç denetim yöneticilerinin ve iç kontrol koordinatörlerinin çoğunluğunun bu grupta yer alması dikkat çekmektedir.

Ayrıca sürekli denetimin uygulanması ve sürekli izleme faaliyetlerinin gerçekleştirilmesi açısından BT denetiminin etkinliğinin değerlendirildiği sonuçları aşağıdaki Tablo-70 ve Tablo 71’den görebilmek mümkündür.

*Tablo-70. Sürekli Denetimin Uygulanma Durumu*BT Denetim Faaliyetlerinin Etkinliği*

İç denetim birimi sürekli denetim yaklaşımını kullanıyor mu?	İşletmenizdeki Bilgi teknolojileri denetim faaliyetlerinin etkinliğini değerlendiriniz.					
	Hiç etkin değil	Etkin değil	Kısmen etkin	Etkin	Tamamıyla etkin	Toplam
Evet	0	1	17	15	4	37
Hayır	3	3	7	1	0	14
Toplam	3	4	24	16	4	51

Tablo-70’e baktığımızda sürekli denetimin uygulandığını bildiren 37 kişiden 17’sinin BT denetimini kısmen, 19’unun da etkin bir şekilde uyguladığı görülmektedir.

*Tablo-71. Sürekli İzleme Gerçekleştirmek Amacıyla BT Kullanımı*BT Denetimi Faaliyetlerinin Etkinliği*

İşletmenizin herhangi bir biriminde veya sürecinde iç kontroller üzerinde sürekli izleme gerçekleştirmek amacıyla bilgi teknolojileri kullanılıyor mu?	İşletmenizdeki Bilgi teknolojileri denetim faaliyetlerinin etkinliğini değerlendiriniz.				
	Etkin değil	Kısmen etkin	Etkin	Tamamıyla etkin	Toplam
Evet	0	9	14	0	23
Hayır	0	2	1	4	7
Bilmiyorum	1	6	0	0	7
Toplam	1	17	15	4	37

Tablo-71’e baktığımızda işletmenin herhangi bir biriminde veya sürecinde iç kontroller üzerinde sürekli izleme faaliyetini gerçekleştirmek amacıyla bilgi teknolojileri kullanıldığını bildiren 23 kişiden 14’ü BT denetiminin etkin olduğunu, 9’u ise kısmen etkin olduğunu bildirmiştir. İç kontroller üzerinde sürekli izleme faaliyetini gerçekleştirmek amacıyla bilgi teknolojilerinin kullanılmadığını belirten 7 kişinin 5’i BT denetiminin etkin olduğunu, 2’si etkin olmadığını bildirmiştir.

Özetle, BT denetiminin etkin bir şekilde uygulanması ile ilgili bazı sorunlar olduğu bu nedenle uygulamanın genelde kısmen gerçekleştiği görülmektedir. Bu nedenle hala işletmelerin BT denetiminin uygulanmasına ilişkin tamamlamaları gereken eksiklikler olduğu söylenebilir. Ayrıca BT denetiminin etkinliği konusunda iç denetçilerin ve iç denetim yöneticileri hariç diğer katılımcıların daha fazla beklentileri olduğu, iç denetim yöneticilerinin ise gerçekleşen süreçten daha memnun oldukları görülmektedir.

- Ankete katılanların konumları ile BT denetimini etkileyen konular arasındaki ilişki:

Tablo-72. Ankete Katılanların Konumları*BT Denetimini Etkileyen Konular

Konum BT Denetimini Etkileyen Konular	İç Denetçi	İç Denetim Yön.	Gn Md. Yrd	Muhasebe Md.	Mali İşler Koord.	Denetim Koord.	İç Kontrol Koord.	Toplam
Bilgi teknolojilerinin sahip olduğu kısıtlar	8	7	1	0	1	1	3	21
Veri güvenliği ve gizliliği	9	1	0	7	2	0	4	23
Bilgi teknolojilerinin karmaşıklığı	13	10	2	0	1	2	2	30

* Ankete katılanlar birden fazla seçenek işaretleyerek soruya cevap verebilmektedir.

Tablo-72’ye göre BT denetimini etkileyen konular arasında “bilgi teknolojilerinin karmaşıklığı” katılımcıların en fazla bildirdiği konular arasında yer almaktadır (30 kişi). Bilgi teknolojilerinin karmaşıklığı muhasebe müdürleri ve iç kontrol koordinatörleri hariç diğer katılımcıların bildirdiği bir konudur. İkinci sırada ise “veri güvenliği ve gizliliği” konusu yer almaktadır (23 kişi) ve katılımcıların çoğunluğunu muhasebe müdürleri, iç kontrol koordinatörleri ve iç denetçiler oluşturmaktadır. Bilgi teknolojilerinin sahip olduğu kısıtlar ise 21 kişi tarafından belirtilmiştir ve muhasebe müdürleri hariç diğer gruptaki katılımcıları burada görebiliriz.

Özetle, bilgi teknolojilerinin karmaşıklığı iç denetim ile ilgili sorumluluğu bulunan taraflarca BT denetimini etkileyen en önemli konu olarak görülmektedir. Bilgi teknolojilerinin karmaşıklığı ve sahip olduğu kısıtlar BT denetimini etkileyebilmektedir. Katılımcılar arasında BT karmaşıklığı ve BT kısıtları ile ilgili konular iç denetçileri ve iç denetim yöneticilerini daha fazla etkilemektedir. Çünkü BT denetiminin gerçekleştirilmesinde bizzat onlar görev almaktadır. BT kullanımı birçok kolaylığı sağlamakla birlikte güvenlik sorunlarını da beraberinde getirmektedir. Veri güvenliği ise iç kontrol koordinatörleri ve muhasebe müdürleri tarafından daha fazla vurgulanmıştır. Çünkü veri güvenliği ve gizliliği iç kontrol sisteminin ve muhasebe bilgi sisteminin etkin bir şekilde çalışması açısından oldukça önemlidir.

- Ankete katılanların konumları ile BT denetiminin uygulanmasını kolaylaştıran teknolojik yenilikler arasındaki ilişki:

Tablo-73. Ankete Katılanların Konumları*BT Denetiminin Uygulanmasını Kolaylaştıran Teknolojik Yenilikler

Konum	İç Denetçi	İç Denetim Yân	Gn Md. Yrd	Muhasebe Md	Mali İşler Koord	Denetim Koord.	İç Kontrol Koord.	Toplam
Sürekli denetim tekniklerinin ve yazılımlarının kullanımı (ACL,IDEA, Acsess vs.)	18	10	2	6	3	2	3	44
Çevrimiçi (on-line) sistemlerin kullanımı	5	5	1	6	2	1	3	23
İstatistiksel analiz yazılımları kullanımı	9	8	1	6	2	1	1	28
Elektronik çalışma kağıtları yazılımlarının kullanımı	3	2	0	0	0	0	0	5
Bilgi teknolojileri denetim alanlarında rehberlik sağlanması	7	1	0	1	1	1	3	14
Bilmiyorum	0	0	0	0	0	0	1	1

* Ankete katılanlar birden fazla seçenek işaretleyerek soruya cevap verebilmektedir.

Tablo-73’de görüldüğü üzere katılımcıların çoğu (44 kişi) tarafından sürekli denetim tekniklerinin ve yazılımlarının kullanımı BT denetiminin uygulanmasını kolaylaştıran yenilikler arasında görülmektedir. Sonrasında istatistiksel analiz yazılımlarının kullanımı katılımcılar (28 kişi) tarafından bildirilmiştir. Özellikle muhasebe müdürleri ve iç denetim yöneticilerinin çoğu katılım göstermektedir. Çevrim-içi sistemlerin kullanımı da üçüncü sırada yer almaktadır (23 kişi). Bu guruba tüm katılımcılardan bildirimler geldiği görülmekle birlikte muhasebe müdürleri sayı olarak en fazla katılımı göstermiştir. Bilgi teknolojileri denetimi alanında sağlanan danışmanlıklar da bir diğer kolaylık olarak görülebilir (14 kişi). Özellikle iç denetçilerin katılımları burada dikkat çekmektedir.

Özetle BT’deki gelişmelerle gündeme gelen sürekli denetim yaklaşımı beraberinde sürekli denetimin gerçekleştirilmesinde kullanılacak denetim tekniklerinin oluşmasına neden olmuştur. Bu nedenle iç denetim alanında doğrudan sorumluluğu olan iç denetçiler ve iç denetim yöneticileri açısından sürekli denetim tekniklerinin ve yazılımlarının kullanımı BT’nin kullanımını kolaylaştıran yenilikler arasındadır. Çevrim-içi sistemlerin kullanımı ve istatistiksel analiz yazılımları da BT denetimleri açısından kolaylık sağlayan yeniliklerdir ve yapılacak denetimler sırasında iç denetçiler tarafından sıklıkla kullanılmaktadır. Ayrıca muhasebe müdürleri de sorumlu oldukları birimin BT’ni kullanarak bilgi üretmesinden kaynaklanan sorumlulukları nedeniyle BT’ni kolaylaştıran yeniliklerden yararlanmaktadır.

5.3.6.2. Bilgi teknolojileri denetimi ile ilgili non-parametrik testler

“BT denetiminin yapılma nedenleri” ve “BT denetiminin etkinliğinin değerlendirilmesi” ile ankete katılanların konumları arasında anlamlı farklılıkların olup olmadığını görmek için Kruskal-Wallis Testi yapılmıştır.

BT denetiminin yapılma nedenlerinden “*Bilgi-işlem departmanındaki kişilere bağımlı olmamayı sağlar*” ile ankete katılanların konumları arasında anlamlı farklılıklar bulunmuştur (Ek-1 Tablo-98). Genel müdür yardımcısı, mali işler koordinatörleri ve denetim koordinatörleri BT denetiminin yapılma nedenini bilgi-işlem departmanından ayrı çalışabilme imkanı sağlaması yönüyle ele alırken, iç denetim yönetici yardımcılarının katılımları bu yönde değildir. Ayrıca belirtelim ki, BT denetiminin uygulanma nedeni ile BT denetiminin uygulanma süresi açısından da Kruskal-Wallis testi sonuçları dikkat çekici bulunmuştur (Ek-1 Tablo-99). 1-3 yıldır BT denetimi gerçekleştirenler BT denetiminin yapılma nedenini bilgi-işlem departmanından ayrı çalışabilme imkanı sağlaması yönüyle ele alırken, 10 yıl ve üzerinde bir süredir BT denetimini gerçekleştirenlerin katılımları bu yönde değildir.

Ankete katılanların konumları ile BT denetiminin etkinliğinin değerlendirilmesi arasında anlamlı farklılık bulunmuştur. (Ek-1 Tablo-100). İç denetim yöneticileri BT denetiminin etkin olduğu, genel müdür yardımcıları ise etkin olmadığı yönünde bildirimde bulunmuştur. Ayrıca BT teknolojileri denetiminin uygulandığı süre ile BT denetiminin etkinliğinin değerlendirilmesi arasında anlamlı farklılık bulunmuştur (Ek-1 Tablo-101). BT denetimini 1-3 yıldır uygulayanlar BT denetiminin etkin olduğu, BT denetiminin hiç uygulanmadığını bildirenler ise BT denetimin etkin olmadığı yönünde bildirimde bulunmuştur.

Kruskal-Wallis Testi yanı sıra bir diğer non-parametrik test olarak uygulanan Spearman’s Rank Order Korelasyonu sonuçlarına göre BT denetiminin etkinliği ile iç denetim biriminin faaliyet gösterdiği süre, BT kullanan iç denetim personeli sayısı ve BT denetiminin uyguladığı süre arasında anlamlı ilişkiler bulunmuştur.

İç denetim birimini faaliyet gösterdiği süre ile BT denetiminin etkinliği arasında yapılan analize göre iç denetim birimini faaliyet gösterdiği süre arttıkça, BT denetiminin etkinliği de artmaktadır (Ek-1 Tablo-102).

BT kullanan iç denetim personel sayısı ile BT denetiminin etkinliği arasında yapılan analize göre BT kullanan iç denetim personel sayısı arttıkça, BT denetiminin etkinliği de artmaktadır (Ek-1 Tablo-103).

BT denetiminin uygulandığı süre ile BT denetiminin etkinliği arasında yapılan analize göre BT denetiminin uygulandığı süre arttıkça, BT denetiminin etkinliği de artmaktadır (Ek-1 Tablo-104).

Sonuç olarak, BT denetiminin etkinliği, iç denetim biriminin gelişmişliği ve çalışan personelin uzmanlığından etkilenmektedir. BT denetiminin yapılma nedenleri açısından bakıldığında ise iç denetim birimi yöneticileri BT denetimlerini bilgi işlem birimine bağımlı olarak gerçekleştirmekten rahatsız olmaz iken, diğer yöneticiler bu denetimlerin bilgi-işlem biriminden bağımsız gerçekleştirilmesinden yanadırlar. Bilgi-işlem birimi BT denetimleri sırasında kullanılan teknolojiler hakkında teknik destek sağlayabilir fakat BT denetimi iç denetim türlerinden birisi olduğu için iç denetim birimleri tarafından gerçekleştirilmelidir. Bir diğer dikkat çekici nokta da BT denetimini ortalama olarak 5 yıldan az bir zamandan beri gerçekleştirenler bilgi-işlem departmanına bağımlı olmadan birim bazında bu denetimleri gerçekleştirebilmekte iken, daha uzun sürelerden beri BT denetimi yapanlar bu konuda bilgi işlem departmanından destek almaktan rahatsızlık duymamaktadırlar. Dolayısıyla BT denetimini yeni gerçekleştirmeye başlayanlar BT ile ilgili konularda daha bilgili olduklarından bilgi-işlem biriminin desteğine ihtiyaç duymamaktadırlar.

Genel Değerlendirme ve Sonuç

Bilgi teknolojilerini her alanda kullanan işletmeler gerçek zamanlı sistemler sayesinde finansal performanslarını ve risk durumlarını daha iyi yönetebilmektedir. Finansal raporların hazırlanmasındaki çabukluk, finansal verilerin denetiminin olaylar geçip gittikten sonra değil, gerçekleştiği an yapılmasını gerektirmiştir. Dolayısıyla geleneksel denetim yaklaşımları, işletmelerin anlık olarak değişen durumlarını takip etmede ve değerlendirmede yetersiz kalmıştır. Bilgi teknolojilerinde meydana gelen değişimlerin işletmelerde iş yapma biçimlerini ve işletmelerin risk yapılarını değiştirmesi iç denetim faaliyetinin işlevlerini, faaliyet alanlarını ve yaklaşımlarını etkilemiştir. İç denetim sürecinde bilgi teknolojilerine odaklı yaklaşımlar benimsenmiş ve iç denetimin gerçekleştirildiği faaliyet alanları genişlemiştir.

İşletmelerde bilgi teknolojilerindeki değişimler sonucu iç denetimin işlevlerinde ve sürecinde meydana gelen değişimleri araştırmak ve iç denetimden sorumlu tarafların bu değişimlere uyumunu irdeleyerek, değişimleri nasıl değerlendirdiklerini ortaya koymak amacıyla gerçekleştirdiğimiz çalışmamızda işletmelerde iç denetimin işlevlerinin ve sürecinin bilgi teknolojilerindeki gelişmelerden etkilenmekle birlikte iç denetim ile ilgili birimlerde hem yapısal hem de bilgi açısından bazı eksikliklerin olduğu görülmüştür. Özellikle iç denetim birimlerini kurmay kademedeki iç denetçi ve iç denetim yöneticilerinden oluşturan işletmelerin oldukça az olduğu, birçok işletmede muhasebe, mali işler gibi birimlerde de iç denetimi ilgilendiren faaliyetlerin gerçekleştirildiği görülmektedir.

İşletmeler çoğunlukla bilgi teknolojilerindeki değişimler doğrultusunda iç denetim faaliyetlerini yapılandırmaya gayret etmişlerdir. Fakat bu süreçte bilgi ve mesleki eğitim açısından var olan eksiklikler, bilgi teknolojilerindeki gelişmelerin etkisiyle ortaya çıkmış olan güvence ve danışmanlık hizmetlerinin ve iç denetim yaklaşımlarının uygulanış biçimini etkilemiştir.

Bilgi teknolojilerindeki gelişmelerin, gelişimini hızlandırdığı güvence hizmetleri konusunda işletmelerde genellikle iç kontrolün etkinliğini sağlamaya, hile ve yolsuzluğun önlenmesine ve finansal tablo denetimi yapmaya yönelik çalışmalara yer verildiği, bilgi teknolojilerinin yoğun olarak kullanıldığı WebTrust ve SysTrust

hizmetlerinin henüz kullanılmadığı görülmüştür. İç denetimden sorumlu taraflar bilgi teknolojilerinin yoğun olarak kullanıldığı güvence hizmetlerinden olan WebTrust ve SysTrust hizmetlerine ilişkin bilgi sahibi değildir. Bu güvence hizmetlerine ilişkin aldıkları bir eğitim veya herhangi bir sertifikaları bulunmamaktadır. Dolayısıyla gelişimi hızla devam eden güvence hizmetleri konusunda iç denetim birimlerinde eksik uygulamalar bulunmaktadır. Bilgi teknolojilerinin yoğun olarak kullanıldığı güvence hizmetlerinin yaygın olmaması, güvence hizmetlerinin gerçekleştirilmesi sırasında manuel kontrollerden ve kısıtlı olarak gerçek zamanlı kontrollerden yararlanılmasına neden olmuştur.

Bilgi teknolojilerinde yaşanan gelişmelerin işletmelerde oluşan risk profilleri açısından etkili olması iç denetim birimlerinin üst yönetime sağladığı danışmanlık hizmetlerini geliştirmiştir. Özellikle risk yönetimi ve sistem güvenliği konularında iç denetim birimleri risk odaklı bir iç denetim planı hazırlayarak işletmenin ihtiyaç duyduğu denetimin kapsamını belirleyerek bu konuda üst yönetime danışmanlık hizmeti sunmaktadır. Bunlar haricinde işletmelerde çeşitli standart, yönetmelik ve düzenlemelere uyum sağlama amacıyla da danışmanlık hizmeti sunulmaktadır. Fakat bilgi teknolojileri uygulamalarından olan ve yurt dışında önemli çalışmalar yapıldığı e-ticaret uygulamaları açısından ülkemizdeki işletmelerde henüz iç denetim birimleri e-ticaret işlemlerinin örgütlenmesi ve denetlenmesi konularında herhangi bir danışmanlık hizmeti sağlamamaktadırlar. Bu durumun nedeni işletmelerde e-ticaret işlemlerine karşı temkinli yaklaşılması ve e-ticaret uygulamalarının kısıtlı gerçekleştirilmesi olabilir.

Son yıllarda bilgi teknolojilerinde yaşanan gelişmeler iç denetimin etkinliğini artırma çabalarını ön plana çıkarmıştır. Bu çabalar sürekli denetim, risk odaklı iç denetim ve kontrol özdeğerlendirme gibi yeni denetim yaklaşımlarını gündeme getirmiştir. İşletmelerde geleneksel denetim yaklaşımı henüz tam olarak terk edilmemekle birlikte yeni denetim yaklaşımlarına doğru bir yönelme olduğu da görülmektedir. İşletmelerde bu yeni yaklaşımların eksiksiz olarak uygulandığını söylemek ise mümkün değildir. Özellikle iç denetim yaklaşımlarının uygulanma süreçlerinde kullanılan yazılımlar, raporlama dilleri, bilgisayar destekli denetim teknikleri açısından iç denetim birimlerinde tam anlamıyla uyumun sağlanamadığı ve bilgi eksiklikleri nedeniyle bu konulara ilişkin herhangi bir çalışma yapılamadığı görülmüştür.

Sürekli denetim yaklaşımı bilgi teknolojilerinin yarattığı risklere karşı anlık denetimleri gerçekleştirmeyi ve gereken önlemleri almayı sağlar. Çalışmamızdan çıkan sonuçlara göre işletmeler elektronik ortamdan çıkan veri ve kanıtlara odaklanmak, hile faaliyetlerini belirlemek, kontrol zayıflıklarını önlemek, riskleri gözlemlemek, insan faktöründen kaynaklanan hataları önlemek ve güvence hizmetlerini gerçekleştirmek gibi amaçlarla sürekli denetim yaklaşımını uygulamaktadırlar. Bu amaçlar doğrultusunda sürekli denetim yaklaşımını benimseyen işletmeler kapsamlı güvence sağlama, hile önleme ve bulma ve sürekli süreç iyileştirme gibi faydalar elde etmektedirler. Özellikle son yıllarda üst yönetimin iç denetim biriminden güvence sağlama konusunda beklentilerinin artması ve sürekli denetim yaklaşımının da güvence hizmetlerinin tüm yönlerini desteklemesi nedeniyle iç denetçiler bu yaklaşımın uygulanması yönündeki çalışmalara destek vermektedirler. Fakat sürekli denetim yaklaşımının uygulanması konusunda henüz uzmanlaşamadıkları görülmektedir. Sürekli denetim yaklaşımını benimsenmesi veri analizi ve sürekli denetimin uygulanma sürecinde birtakım yazılımların, raporlama dillerinin ve bilgisayar destekli denetim tekniklerinin kullanımını gerektirmektedir. Yurtdışındaki işletmelerde kullanımları oldukça yaygın olan yazılımların (ACL, IDEA, Monarch, AS/400 Query, Crystal Reports, People Soft, SAS, Datas, TeamMate, vb.) ülkemizde henüz bilinmediği veya çok az kullanıldığı görülmüştür. Yine yurtdışında sürekli denetimin uygulanma fırsatını arttırdığı için yaygın bir şekilde kullanılan raporlama dillerinin (XBRL) ülkemizde henüz kullanılmadığı görülmektedir. Çalışmamıza katılan işletmelerin bildirdiğinin aksine sürekli denetimin olmazsa olmazlarından olan bu yazılım ve raporlama dillerinin eksikliğinin sürekli denetimin tam anlamıyla uygulanmasını güçleştirdiği düşünülmektedir. Bilgisayar destekli denetim teknikleri açısından ise uzun zamandır bilinen ve pek çok işletme tarafından kullanılan tekniklerin kullanımına devam edilmekte, genelleştirilmiş denetim yazılımı, veri testi tekniği, süreç modelleme, paralel simülasyon gibi yeni tekniklerin henüz yaygınlaşmadığı görülmektedir.

İşletmelerde çalışma ortamlarında bilgi teknolojilerinin yoğun bir şekilde kullanımı riskli alanları araştırmayı, riskleri düzeylerine göre tanımlamayı ve sınıflandırmayı gerektirmiştir. Bu durumda işletmelerin risk odaklı iç denetim yaklaşımını kullanarak riskler ve çözüm yollarına ilişkin bilgileri üst yönetime ve denetim komitesine bildikleri görülmüştür. Mevcut durum itibarıyla risk odaklı iç

denetimi benimseyen işletmelerin gerçekleştirdiği çalışmalar riskleri ortaya çıkarmaya yönelik olmakla birlikte kurumsal yönetim ve risk yönetimi gibi faaliyet alanları üzerine odaklanmayı gerektirmektedir. Çünkü risk odaklı iç denetim yaklaşımı bu faaliyet alanlarına ilişkin sürecin çıktılarından faydalanmaktadır.

İç kontrol sisteminin etkinliğinin ve verimliliğinin değerlendirilmesinde detaylı çalışmalar yapılması kontrol özdeğerlendirme yaklaşımının ortaya çıkışını sağlamıştır. Bu yaklaşım ülkemizdeki işletmelerce henüz bilinmemektedir. Kontrol özdeğerlendirme yaklaşımı doğrultusunda uygulanan grup çalışmaları, anketler, yönetici analizleri sadece iç denetçilerden oluşan bir ekibin bu çalışmayı yürütmediğini işletme yönetici ve çalışanlarının da sürece dahil edildiğini göstermektedir. Az sayıda işletmenin ana hatlarıyla uygulamaya çalıştığı bu yaklaşımın işletme amaçlarının başarılmasına, etkin bir iç kontrol için her düzeyde sorumluluklarının yerine getirilmesine ve iş süreçlerinin yeniden yapılandırılmasına katkı sağladığı düşünülmektedir.

İşletmelerde bilgi teknolojilerinin yaygın bir şekilde kullanımının değiştirdiği ve çeşitlendirdiği işletme riskleri bu risklerden korunma ihtiyacını arttırmış ve dolayısıyla iç denetimin faaliyet alanlarını genişletmiştir. Bu doğrultuda iç denetim faaliyetleri risk yönetimi, iç kontrol ve kurumsal yönetim alanlarına genişlemiştir. İşletmeler risk yönetimi ve iç kontrol açısından gerçekleştirdikleri uygulamalarda geçmişe nazaran gelişme gösterdiklerinden dolayı iç denetim birimleri de bu alanlarda çalışmaları desteklemektedirler. Bu gelişmeler iç denetim birimlerinin üst yönetime sağladığı danışmanlık hizmetleri açısından risk yönetiminin ve güvence hizmetleri açısından da iç kontrolün etkinliğinin sağlanması ile ilgili çalışmaların ilk sırada yer almasına neden olmuştur. İşletmeler iç kontrol sistemlerinde bilgi teknolojisi kontrollerine yer vererek, iç kontrol sisteminin güvenilirliğini ve etkinliğini artırma çabalarını doğrulamaktadır. Kurumsal yönetim süreci açısından ise iç denetim birimleri sürecin kalitesini ve sürekliliğini sağlama adına işletmelere katkı sağlamaktadır. Risk ve uyum faaliyetlerinin etkinliğinin arttırılmasında işletme yönetimine danışmanlık sağlanmaktadır.

Bilgi teknolojileri uygulamaları işletmelerde hemen hemen her süreçte karşımıza çıkmakta ve ilgili süreçteki işlemlerin gerçekleşmesinde kolaylıklar sağlamaktadır. BT uygulamalarından internet ve intranetin işletmeler tarafından oldukça yoğun bir şekilde kullanılmaktadır. Bunlar dışında elektronik veri değişimi, kurumsal kaynak planlaması

ve elektronik veri işleme günümüzde geçmişe oranla kullanımı yaygınlaşan BT uygulamalarıdır. Elektronik ticaret ise işletmeler tarafından daha temkinli yaklaşılan ve dolayısıyla kısmen gerçekleştirilen bir uygulamadır. Bu BT uygulamalarının işletmelerde hemen hemen her süreçte kullanılıyor olmaları iç denetim birimlerinin de bu teknolojileri kullanmaları ve işlem süreçlerini takip etmelerini gerektirmiştir.

İç denetim birimleri e-ticaret uygulamalarının iç kontrolün etkinliğini olumsuz yönde etkilemediğini düşünmekle birlikte BT ile ilgili risklere açık bir süreç olduğu için bu uygulamalara temkinli yaklaşmaktadır. Fakat bu temkinliliğin gereği olarak henüz bu süreçlere ilişkin özel denetim prosedürleri geliştirmiş değildir.

Eş zamanlı veri-bilgi alışverişi ve kaynak tasarrufu açısından günümüzde işletmeler finansal tablolarını internet erişim sayfalarından yayınlamayı tercih etmektedirler. Fakat internet kullanımının sağladığı kolaylıklardan faydalanırken, iç denetim mekanizmasında internet kullanımı ve ilgili teknolojinin kontrolü konularında endişeler yaşanmaktadır. Dolayısıyla finansal raporlama ve sürekli denetim süreçlerinde internet tabanlı teknolojilerin kullanımı konusunda sıkıntılar vardır. Özellikle internet kullanımı ile ilişkili WebTrust güvence hizmetlerinin veya XBRL gibi raporlama dillerinin işletmelerimizde henüz kullanılmaması internet kullanımı ile ilgili oluşturulması gereken iç denetim mekanizması konusundaki şüpheleri doğrulamaktadır.

İç denetim faaliyetini önemli ölçüde destekleyen BT uygulamalarından birisi de elektronik veri değişimidir. Hem işletme içi hem de işletme dışı işlemlerin tamamıyla elektronik ortamda yürütülmesi iç denetim birimlerinin denetim faaliyetlerini elektronik ortamda ve elektronik kanıtlarla gerçekleştirmelerine neden olmaktadır. Elektronik veri değişimi uygulamaları iç kontrolün etkinliği ve güvenilirliği düşünülerek oluşturulduğundan iç denetim birimlerine denetim süreci boyunca kolaylık sağlamaktadır.

Kurumsal kaynak planlaması, iç kontrol sistemine odaklı bir uygulamadır. Bu nedenle iç kontrol sisteminin güvenilirliğini sağlamak, riskleri azaltmak ve etkin ve verimli çalışmasını sağlamak amacıyla çeşitli güvenlik sistemlerinin kurulmasını gerektirmektedir. Fakat işletmelerin kurumsal kaynak planlaması uygulamaları açısından güvence elde edebilecekleri WebTrust ve SysTrust gibi hizmetleri henüz kullanmamaları güvenlik ve risklere karşı önlemler alma konularını olumsuz yönde etkileyebilir.

Elektronik veri işleme sistemlerinin kullanımı gerçek zamanlı sistemlerin kullanımını gerektirmekte ve bu durum denetim tekniklerinin de bu doğrultuda yenilenmesini gündeme getirmektedir. Elektronik veri işleme gibi gerçek zamanlı sistemlerde gerçek zamanlı kontrollere ihtiyaç olması ve işletmelerimizde bu kontrollerin yeterli düzeyde olmaması bilgi güvenliği konusunda endişelerin oluşmasına neden olmaktadır.

Bilgi teknolojilerindeki gelişmeler ve işletmelerde bilgi teknolojileri uygulamalarının yaygınlaşması iç denetim türlerinin çeşitlenmesine yol açmış, finansal denetim, uygunluk denetimi, faaliyet denetimi gibi uzun zamandan beri gerçekleştirilen iç denetim türlerinin yanı sıra sistem denetimi ve BT denetimi gibi yeni denetim türleri ortaya çıkmıştır. Sürekli denetim yaklaşımını benimseyen işletmelerin iç denetim faaliyetleri kapsamında BT denetimlerini de yürütmekte olduğunu görmekteyiz ve yapılan bu BT denetimleri etkin bir şekilde yerine getirilmeye çalışılmaktadır. Fakat sürekli denetim sürecinin uygulanışındaki eksiklerin bu denetimin gerçekleştirilme biçimini de etkilediği söylenebilir. Bu nedenle işletmelerin BT denetiminin etkinliğini yeniden değerlendirmeleri gerekmektedir. BT denetimi geçtiğimiz 5 yıllık bir süreçte artış göstermiştir. Çünkü işletmelerdeki BT uygulamalarının çeşitliliği de artmıştır. BT denetimleri bilginin güvenliğini sağlamak, sistemlerdeki açıkları yakalamak ve bu açıkların kötüye kullanılmasını engellemek amacıyla gerçekleştirilmektedir. BT denetiminin etkinliği, iç denetim biriminin gelişmişliği ve çalışan personelin uzmanlığından etkilenmektedir. Bu nedenle BT denetimleri bilgi-işlem biriminden bağımsız gerçekleştirilmektedir. Bilgi-işlem birimi BT denetimleri sırasında kullanılan teknolojiler hakkında teknik destek sağlayabilir, zaten BT denetiminin uygulama sürecinde yer alan iç denetçiler de bilgi işlem departmanından destek alınmasından rahatsızlık duymamaktadır.

İç denetim birimlerinin işletmelerdeki bilgi teknolojileri uygulamaları ve bu uygulamalar sonucunda ortaya çıkan yeni yaklaşımlar, genişleyen faaliyet alanları ve ön plana çıkan işlevler bakımından bilgi eksiklikleri vardır. Bu eksiklikler mesleki gelişimin sürekliliğinin sağlanması adına yapılacak eğitimlerle ortadan kaldırılabilir. Bu konuda iç denetim alanında sorumluluğu bulunan mesleki birliklere önemli görevler düşmektedir.

İç denetim alanında mesleki gelişim ve yeniliklere uyum sağlama adına yapılan çalışmalar olmakla birlikte, bu çalışmalara katılan meslek mensuplarının sayısını arttırmak önemlidir. Ayrıca sadece iç denetim birimleri ve sorumluları değil, işletme yöneticileri de iç denetim faaliyetinin önemini anlamalarını sağlayacak çalışmalara dahil edilmelidir. Böylece işletme yöneticileri işletme organizasyonu içinde iç denetim birimlerinin nerede bulunması gerektiği, sorumluluklarının neler olduğu, hangi çalışmaları ne şekilde gerçekleştirdikleri bakımından daha bilinçli değerlendirmeler yapabileceklerdir.

Ekler Listesi

Ek-1. Elde Edilen Analiz Sonuçlarına İlişkin Tablolar.....	259
Ek-2. Anket Formu	286
Ek-3. İMKB 100 Şirketlerinin Listesi	296
Ek-4. Araştırma Sorularının Testinde Kullanılan İstatistiksel Analizler İle İlgili Bilgiler.....	299

Ek-1. Elde Edilen Analiz Sonuçlarına İlişkin Tablolar

Tablo-74. Ankete Cevap Verenlerin ve Çalıştıkları İşletmelerin Demografik Özellikleri

		f	%
CİNSİYET	Bay	43	84,3
	Bayan	8	15,7
	TOPLAM	51	100,0
YAŞ	30 ve altı yaş	3	5,9
	31-35 yaş	20	39,2
	36-40 yaş	14	27,5
	41-45 yaş	10	19,6
	46-50 yaş	4	7,8
	TOPLAM	51	100,0
EĞİTİM	Lisans	32	62,7
	Lisansüstü (Master)	19	37,3
	TOPLAM	51	100,0
İŞLETMEDEKİ ÇALIŞMA SÜRESİ	1 yıldan az	4	7,8
	1-3 yıl	7	13,7
	4-6 yıl	16	31,4
	7-9 yıl	5	9,8
	10 yıl ve üzeri	19	37,3
	TOPLAM	51	100,0
İŞLETMEDEKİ KONUMU	İç Denetçi	19	37,3
	İç Denetim Yöneticisi	10	19,6
	Muhasebe Müdürü	7	13,7
	Genel müdür yardımcısı	3	5,9
	Mali İşler koordinatörü	3	5,9
	Denetim Koordinatörü	2	3,9
	İç Kontrol Koordinatörü	4	7,8
	İç Kontrol Koordinatörü Yardımcısı	2	3,9
	İç Denetim Yöneticisi Yardımcısı	1	2,0
	TOPLAM	51	100,0
BİLGİ TEKNOLOJİLERİ KULLANAN İÇ DENETİM PERSONELİ SAYISI	Hiç yok	3	5,9
	1-3 kişi	30	58,8
	4-6 kişi	9	17,6
	7-9 kişi	2	3,9
	10 kişi ve üstü	5	9,8
	Bilmiyorum	2	3,9
	TOPLAM	51	100,0
SERTİFİKALI İÇ DENETÇİNİZ VAR MI?	Evet	31	60,8
	Hayır	19	37,3
	Bilmiyorum	1	2,0
	TOPLAM	51	100,0
MESLEKİ SERTİFİKALARINIZ	Uluslararası İç Denetçi (CIA)	12	23,5
	Uluslararası Kamu Denetçisi (CGAP)	4	7,8
	Kontrol Özdeğerlendirme Sertifikası (CCSA)	1	2,0
	Uluslararası Finansal Hizmetler Denetçisi (CFSA)	1	2,0
	Kamu Muhasebesi / Mali Müşavirlik (CA/CPA/ACCA/ACA)	12	23,5
	Hile Denetçisi (CFE)	4	7,8
	Sertifikalı Finansal Analist (CFA)	1	2,0
	Profesyonel Risk Yöneticisi Sertifikası (Associate PRM)	1	27,5
	Kurumsal Yönetim Derecelendirme Sertifikası	1	2,0
	Sertifikası Yok	14	2,0
	TOPLAM	51	100,0

Tablo-74. Ankete Cevap Verenlerin ve Çalıştıkları İşletmelerin Demografik Özellikleri (Devam)

		f	%
İÇ DENETİM BİRİMİNİN FAALİYET GÖSTERDİĞİ SÜRE	1 yıldan az	1	2,0
	1-5 yıl	16	31,4
	6-10 yıl	7	13,7
	11-15 yıl	16	31,4
	16-20 yıl	6	11,8
	21 yıl ve üzeri	4	7,8
	Bilmiyorum	1	2,0
	TOPLAM	51	100,0
İÇ DENETİM BİRİMİNİN RAPOR SUNDUĞU MERCİ	Yönetim Kurulu	35	68,6
	Genel Müdür	11	21,6
	Denetim Komitesi	5	9,8
	TOPLAM	51	100,0
FAALİYET GÖSTERİLEN SEKTÖR	Üretim-İmalat	28	54,9
	Ulaştırma-Lojistik	2	3,9
	Elektrik-Elektronik-Enerji	6	11,8
	Turizm	1	2,0
	İnşaat	2	3,9
	Toptan ve Perakende Ticaret	5	9,8
	Teknoloji-İletişim	4	7,8
	Spor ve Diğer Sosyal Hizmet	3	5,9
	TOPLAM	51	100,0

Tablo-75. Ankete Katılanların İşletmedeki Konumları ile İç Denetim Biriminin İç Denetimin İşlevleri, Faaliyet Alanları ve Türleri Açısından Gelecekteki Durumunda Meydana Gelen Değişimlerin Değerlendirilmesinin Kruskal-Wallis Testi Sonuçları

	İşletmenizdeki konumunuz	N	Mean Rank**	Asymp. Sig.
Kurumsal yönetim-GELECEK	İç Denetçi	19	19,21	0,050*
	İç Denetim Yöneticisi	11	33,00	
	Muhasebe Müdürü	7	31,29	
	Genel müdür yardımcısı	3	17,33	
	Mali İşler koordinatörü	3	28,33	
	Denetim Koordinatörü	2	24,50	
	İç Kontrol Koordinatörü	6	32,17	
	Toplam	51		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

**Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-76. Ankete Katılanların İşletmedeki Konumları ile Sürekli Denetimin Kullanımındaki Temel Amaçlar Arasında Kruskal-Wallis Testi Sonuçları

	İşletmenizdeki konumunuz	N	Mean Rank**	Asymp. Sig.*
Uygulanan önerileri izlemek	İç Denetçi	13	18,15	0,011*
	İç Denetim Yöneticisi	9	13,22	
	Muhasebe Müdürü	5	31,00	
	Genel müdür yardımcısı	2	15,50	
	Mali İşler koordinatörü	2	31,00	
	Denetim Koordinatörü	1	31,00	
	İç Kontrol Koordinatörü	5	13,80	
	Toplam	37		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

**Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-77. Ankete Katılanların İşletmedeki Konumları ile Sürekli Denetimde Kullanılma BT'nin Kullanım Amacı Arasında Kruskal-Wallis Testi Sonuçları

	İşletmenizdeki konumunuz	N	Mean Rank**	Asymp. Sig.*
"SÜREKLİ DENETİM TEKNOLOJİSİ, RİSK YÖNETİMİNDE KULLANILABİLEN TEKNOLOJİ ODAKLI SÜREKLİ DENETİM ÇÖZÜMLERİNİ YAYGINLAŞTIRMAK İÇİN OLUŞTURULMUŞTUR" bu ifadeye katılım düzeyinizi ifade ediniz.	İç Denetçi	13	11,96	0,009*
	İç Denetim Yöneticisi	9	18,50	
	Muhasebe Müdürü	5	30,50	
	Genel müdür yardımcısı	1	8,00	
	Mali İşler koordinatörü	2	17,75	
	Denetim Koordinatörü	1	20,50	
	İç Kontrol Koordinatörü/Yönetmeni	5	25,50	
	Total	36		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

**Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-78. Ankete Katılanların İşletmedeki Çalışma Süreleri Ve Sürekli Denetimde BT Kullanım Amacı Spearman's Rank Order Korelasyonu

	Çalışma süresi-Spearman rho
SÜREKLİ DENETİM TEKNOLOJİSİ, RİSK YÖNETİMİNDE KULLANILABİLEN TEKNOLOJİ ODAKLI SÜREKLİ DENETİM ÇÖZÜMLERİNİ YAYGINLAŞTIRMAK İÇİN OLUŞTURULMUŞTUR" bu ifadeye katılım düzeyinizi ifade ediniz.	0,477*

*Korelasyon katsayısı 0,30-0,49 aralığında ise iki değişken arasındaki ilişki orta derecededir.

Tablo-79. BT Kullanan İç Denetim Personeli Sayısı ile Risk Odaklı İç Denetim Yaklaşımı Bileşenleri Arasında Kruskal-Wallis Testi Sonuçları

	Bilgi teknolojilerini kullanan iç denetim personelinin sayısı	N	Mean Rank**	Asymp.Sig.*
İç denetçi işletme içindeki olası risk alanlarını araştırmak durumundadır	Hiç yok	2	1,50	0,042*
	1-3 kişi	30	25,50	
	4-6 kişi	9	29,44	
	7-9 kişi	2	32,00	
	10 kişi ve üstü	5	27,40	
	Bilmiyor	2	20,50	
	Toplam	50		
Risk tanımlamasında işletme bünyesinde bulunan riskler her risk seviyesine göre (düşük, orta, yüksek) değerlendirilir ve risk alanları tablosunda gösterilir	Hiç yok	2	1,50	0,010*
	1-3 kişi	30	27,12	
	4-6 kişi	9	21,56	
	7-9 kişi	2	29,50	
	10 kişi ve üstü	5	25,20	
	Bilmiyor	1	29,50	
	Toplam	49		
Risk faktörleri tespit edildikten sonra bu faktörlerin toplam risk içindeki nispi önemini belirlemek gerekir.	Hiç yok	2	1,50	0,003*
	1-3 kişi	30	28,15	
	4-6 kişi	9	17,61	
	7-9 kişi	2	30,50	
	10 kişi ve üstü	5	25,50	
	Bilmiyor	1	30,50	
	Toplam	49		
Belirlenen riskler derecelerine bağlı olarak sıraya konulur.	Hiç yok	2	2,50	0,004*
	1-3 kişi	30	28,12	
	4-6 kişi	9	17,83	
	7-9 kişi	2	30,50	
	10 kişi ve üstü	5	24,90	
	Bilmiyor	1	30,50	
	Toplam	49		
Risklerle ilgili sonuçlar yönetim kuruluna, denetim komitesine ve diğer ilgililere iletilir.	Hiç yok	2	1,50	0,001*
	1-3 kişi	29	20,62	
	4-6 kişi	9	34,11	
	7-9 kişi	2	39,00	
	10 kişi ve üstü	5	30,20	
	Bilmiyor	1	39,00	
	Toplam	48		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

**Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-80. İç Denetim Biriminin Faaliyet Gösterdiği Süre ve Risk Odaklı İç Denetim Yaklaşımı Bileşenleri Spearman's Rank Order Korelasyonu

	İç Denetim Biriminin Faaliyet Gösterdiği Süre-Spearman rho
Risklerle ilgili sonuçlar yönetim kuruluna, denetim komitesine ve diğer ilgililere iletilir.	0,402*

*Korelasyon katsayısı 0,30-0,49 aralığında ise iki değişken arasındaki ilişki orta derecededir.

Tablo-81. İşletmedeki Çalışma Süresi ve Kontrol Özdeğerlendirme Yaklaşımının Uygulanma Nedenleri Spearman's Rank Order Korelasyonu

	İç Denetim Biriminin Faaliyet Gösterdiği Süre-Spearman rho
Yasalara uyum sağlamak	-0,437*
Bir iş sürecinin yeniden yapılanma sürecini izlemek	-0,462*
Amaçların başarılmasını sağlamak	-0,506*
Katılımcıların öğrenme sürecini geliştirmek	-0,462*
Etkin bir iç kontrol ve risk yönetimi için her düzeyde sorumlulukların yerine getirilmesi konusunda yönetime yardımcı olmak	-0,462*

*Negatif korelasyon: İki değişken arasında biri artarken diğeri azalan ters orantılı bir ilişki vardır. -0,49 ile -0,30 aralığı orta derece ve -0,50 ile -1,00 aralığı yüksek ilişki olarak kabul edilir.

Tablo-82. BT Denetiminin Uygulandığı Süre ile Risk Yönetimi Bileşenleri Arasında Kruskal-Wallis Testi Sonuçları

	BT denetiminin uygulandığı süre:	N	Mean Rank**	Asymp. Sig.*
Kontrol ortamı, risklerin kurumda çalışan kişiler tarafından nasıl görüntülenmesi ve yönlendirilmesi gerektiğine dair bir temel oluşturur.	Hiç uygulanmaz	4	18,25	0,027*
	1 yıldan az	8	29,62	
	1-3 yıl	21	18,69	
	4-6 yıl	12	31,42	
	10 yıl ve üzeri	2	24,25	
	Toplam	47		
Yönetim risk stratejisini göz önünde bulundurarak hedefleri belirler.	Hiç uygulanmaz	4	18,25	0,048*
	1 yıldan az	8	31,81	
	1-3 yıl	21	18,95	
	4-6 yıl	12	29,00	
	10 yıl ve üzeri	2	27,25	
	Toplam	47		
Belirsizliklerin risk mi fırsat mı olduğu konusunda çalışmalar yapılır	Hiç uygulanmaz	4	18,25	0,042*
	1 yıldan az	8	32,75	
	1-3 yıl	21	19,19	
	4-6 yıl	12	29,00	
	10 yıl ve üzeri	2	21,00	
	Toplam	47		
Riske verilecek karşılıkların etkili bir biçimde yerine getirilmesi ve devam eden risklerin risk kapasitesi sınırları içinde yönetilmesi için politika ve prosedürler oluşturulur.	Hiç uygulanmaz	4	17,75	0,016*
	1 yıldan az	8	31,56	
	1-3 yıl	21	18,43	
	4-6 yıl	12	30,75	
	10 yıl ve üzeri	2	24,25	
	Toplam	47		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

**Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-83. BT Kullanan İç Denetim Personeli Sayısı ile Risk Bileşenleri Arasında Kruskal-Wallis Testi Sonuçları

	BT kullanan iç denetim personelinin sayısı	N	Mean Rank**	Asymp. Sig.*
Kontrol ortamı, risklerin kurumda çalışan kişiler tarafından nasıl görüntülenmesi ve yönlendirilmesi gerektiğine dair bir temel oluşturur.	Hiç yok	2	1,50	0,043*
	1-3 kişi	29	23,14	
	4-6 kişi	9	26,22	
	7-9 kişi	2	36,00	
	10 kişi ve üstü	5	31,60	
	Bilmiyor	1	36,00	
	Toplam	48		
Yönetim risk stratejisini göz önünde bulundurarak hedefleri belirler.	Hiç yok	2	1,50	0,025*
	1-3 kişi	29	22,10	
	4-6 kişi	9	30,67	
	7-9 kişi	2	36,00	
	10 kişi ve üstü	5	29,60	
	Bilmiyor	1	36,00	
	Toplam	48		
Belirsizliklerin risk mi fırsat mı olduğu konusunda çalışmalar yapılır	Hiç yok	2	1,50	0,040*
	1-3 kişi	29	22,53	
	4-6 kişi	9	29,83	
	7-9 kişi	2	36,00	
	10 kişi ve üstü	5	28,60	
	Bilmiyor	1	36,00	
	Toplam	48		
Riskler tanımlandıktan sonra bunların işletme üzerindeki olası etkileri ve meydana gelme olasılıkları değerlendirir.	Hiç yok	2	1,50	0,048*
	1-3 kişi	29	22,79	
	4-6 kişi	9	29,33	
	7-9 kişi	2	36,00	
	10 kişi ve üstü	5	28,00	
	Bilmiyor	1	36,00	
	Toplam	48		
Riske verilecek karşılıkların etkili bir biçimde yerine getirilmesi ve devam eden risklerin risk kapasitesi sınırları içinde yönetilmesi için politika ve prosedürler oluşturulur.	Hiç yok	2	1,50	0,009*
	1-3 kişi	29	21,60	
	4-6 kişi	9	30,06	
	7-9 kişi	2	34,50	
	10 kişi ve üstü	5	34,50	
	Bilmiyor	1	34,50	
	Toplam	48		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

**Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-84. İç Denetim Biriminin Faaliyet Gösterdiği Süre ve Risk Yönetimi Bileşenleri Spearman's Rank Order Korelasyonu

	İç Denetim Biriminin Faaliyet Gösterdiği Süre-Spearman rho
Yönetim risk stratejisini göz önünde bulundurarak hedefleri belirler.	0,322*

*Korelasyon katsayısı 0,30-0,49 aralığında ise iki değişken arasındaki ilişki orta derecededir.

Tablo-85. BT Kullanan İç Denetim Personeli Sayısı ve Risk Yönetimi Bileşenleri Spearman's Rank Order Korelasyonu

	BT Kullanan İç Denetim Personeli Sayısı-Spearman rho
Kontrol ortamı, risklerin kurumda çalışan kişiler tarafından nasıl görüntülenmesi ve yönlendirilmesi gerektiğine dair bir temel oluşturur.	0,404*
Yönetim risk stratejisini göz önünde bulundurarak hedefleri belirler.	0,461*
Belirsizliklerin risk mi fırsat mı olduğu konusunda çalışmalar yapılır	0,421*
Riskler tanımlandıktan sonra bunların işletme üzerindeki olası etkileri ve meydana gelme olasılıkları değerlendirir.	0,401*
Belirlenen risklerin kurumun risk kapasitesi ve risk toleransı içinde olup olmadığı belirlenir.	0,347*
Riske verilecek karşılıkların etkili bir biçimde yerine getirilmesi ve devam eden risklerin risk kapasitesi sınırları içinde yönetilmesi için politika ve prosedürler oluşturulur.	0,539**
Kişilerin sorumluluklarını yerine getirmesi için ilgili bilgi belli bir biçimde ve belli zaman aralıkları ile tanımlanır ve iletilir.	0,368*
Risk yönetiminin uygulanması izlenir ve etkinliğini arttırmak için gerektiğinde ayarlamalar yapılır.	0,328*

*Korelasyon katsayısı 0,30-0,49 aralığında ise iki değişken arasındaki ilişki orta derecededir.

**Korelasyon katsayısı 0,50-1,00 aralığında ise iki değişken arasındaki ilişki yüksek derecededir.

Tablo-86. BT Denetiminin Uygulandığı Süre İle Kurumsal Yönetim Kapsamında İç Denetimin Rolü Açısından Kruskal-Wallis Testi Sonuçları

	BT denetiminin uygulandığı süre:	N	Mean Rank**	Asymp. Sig.*
İç denetim, kurumsal yönetim sisteminin bütünleştirici bir parçasıdır.	Hiç uygulanmaz	5	23,90	0,013*
	1 yıldan az	8	27,50	
	1-3 yıl	21	17,83	
	4-6 yıl	12	32,58	
	10 yıl ve üzeri	2	35,50	
	Toplam	48		
İç denetim, kontrol sistemlerinin (operasyonel kontrol, finansal kontrol) etkinliğini ölçüp değerlendirerek yönetime objektif güvence sağlar.	Hiç uygulanmaz	5	21,30	0,043*
	1 yıldan az	8	28,75	
	1-3 yıl	21	19,17	
	4-6 yıl	12	30,67	
	10 yıl ve üzeri	2	34,50	
	Toplam	48		
İç denetim, işletme bilgi teknolojisi sisteminin güvenliğini ve raporlama imkanlarını içeren muhasebe bilgi sisteminin etkinliğini değerlendirir.	Hiç uygulanmaz	5	17,80	0,026*
	1 yıldan az	8	26,44	
	1-3 yıl	21	19,79	
	4-6 yıl	12	32,33	
	10 yıl ve üzeri	2	36,00	
	Toplam	48		
İç denetim, profesyonel yöneticilere yetki devrinde güvence sağlar.	Hiç uygulanmaz	5	19,00	0,013*
	1 yıldan az	8	28,69	
	1-3 yıl	21	18,57	
	4-6 yıl	12	32,46	
	10 yıl ve üzeri	2	36,00	
	Toplam	48		
İç denetim faaliyeti; zamanı ve emeğini, kurum çapında düzgün risk yönetimi süreçlerinin kurulmasına ve uygulanmasına katkıda bulunan danışmanlık faaliyetlerine harcar.	Hiç uygulanmaz	5	19,30	0,042*
	1 yıldan az	8	31,69	
	1-3 yıl	21	19,05	
	4-6 yıl	12	30,71	
	10 yıl ve üzeri	2	28,75	
	Toplam	48		
İç denetim, risk değerlendirme sürecinin etkin bir şekilde çalıştığı konusunda yönetim kuruluna ve yönetime objektif güvence sağlar.	Hiç uygulanmaz	5	17,80	0,028*
	1 yıldan az	8	30,38	
	1-3 yıl	21	19,45	
	4-6 yıl	12	32,08	
	10 yıl ve üzeri	2	25,25	
	Toplam	48		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

**Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-87. İç Denetim Biriminin Faaliyet Gösterdiği Süre ve Kurumsal Yönetim Spearman's Rank Order Korelasyonu

	İç Denetim Biriminin Faaliyet Gösterdiği Süre-Spearman rho
İç denetim faaliyeti; zamanı ve emeğini, kurum çapında düzgün risk yönetimi süreçlerinin kurulmasına ve uygulanmasına katkıda bulunan danışmanlık faaliyetlerine harcar.	0,313

Tablo-88. BT Kullanan İç Denetim Personeli Sayısı ve Kurumsal Yönetim Spearman's Rank Order Korelasyonu

	BT Kullanan İç Denetim Personeli Sayısı-Spearman rho
İç denetim, kurumsal yönetim sisteminin bütünleştirici bir parçasıdır.	0,346
İç denetim, kontrol sistemlerinin (operasyonel kontrol, finansal kontrol) etkinliğini ölçüp değerlendirerek yönetime objektif güvence sağlar.	0,422
İç denetim, işletme bilgi teknolojisi sisteminin güvenliğini ve raporlama imkanlarını içeren muhasebe bilgi sisteminin etkinliğini değerlendirir.	0,374
İç denetim, profesyonel yöneticilere yetki devrinde güvence sağlar.	0,438
İç denetim faaliyeti; zamanı ve emeğini, kurum çapında düzgün risk yönetimi süreçlerinin kurulmasına ve uygulanmasına katkıda bulunan danışmanlık faaliyetlerine harcar.	0,445
İç denetim, risk değerlendirme sürecinin etkin bir şekilde çalıştığı konusunda yönetim kuruluna ve yönetime objektif güvence sağlar.	0,516
Kurumsal yönetim anlayışının işletmede oluşması değerinin artırılması ve kalitesinin sürdürülebilmesi için iç denetimin kurumsal yönetim anlayışına işlevsellik kazandırır.	0,385

Tablo-89. BT Denetiminin Uygulandığı Süre ve Kurumsal Yönetim Spearman's Rank Order Korelasyonu

	BT Denetiminin Uygulandığı Süre-Spearman rho
İç denetim, işletme bilgi teknolojisi sisteminin güvenliğini ve raporlama imkanlarını içeren muhasebe bilgi sisteminin etkinliğini değerlendirir.	0,330

Tablo-90. Ankete Katılanların İşletmedeki Konumları İle Bilgi Teknolojilerinin Geçmişteki Kullanımı Arasında Kruskal-Wallis Testi Sonuçları

	İşletmenizdeki konumunuz	N	Mean Rank**	Asymp. Sig.*
Extranet-Geçmiş	İç Denetçi	18	20,89	0,008*
	İç Denetim Yöneticisi	10	29,50	
	Muhasebe Müdürü	7	42,14	
	Genel müdür yardımcısı	3	16,67	
	Mali İşler koordinatörü	3	25,33	
	Denetim Koordinatörü	2	15,25	
	İç Kontrol Koordinatörü	6	17,08	
	Toplam	49		
Kurumsal Kaynak Planlaması-Geçmiş	İç Denetçi	18	20,36	0,007*
	İç Denetim Yöneticisi	10	21,15	
	Muhasebe Müdürü	7	40,21	
	Genel müdür yardımcısı	3	12,67	
	Mali İşler koordinatörü	3	37,33	
	Denetim Koordinatörü	2	16,50	
	İç Kontrol Koordinatörü	6	30,42	
	Toplam	49		
Extranet-Şimdi	İç Denetçi	18	26,08	0,048*
	İç Denetim Yöneticisi	10	21,45	
	Muhasebe Müdürü	7	39,36	
	Genel müdür yardımcısı	3	16,33	
	Mali İşler koordinatörü	3	27,83	
	Denetim Koordinatörü	2	19,75	
	İç Kontrol Koordinatörü	6	15,58	
	Toplam	49		
Elektronik Ticaret-Şimdi	İç Denetçi	19	23,63	0,041*
	İç Denetim Yöneticisi	10	22,55	
	Muhasebe Müdürü	7	38,21	
	Genel müdür yardımcısı	3	10,33	
	Mali İşler koordinatörü	3	38,50	
	Denetim Koordinatörü	2	27,50	
	İç Kontrol Koordinatörü	6	21,92	
	Toplam	50		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

** Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-91. Ankete Katılanların Yaşları ile E-ticaret ve İç Denetim İlişğine Yönelik Katılım Düzeyleri Arasında Kruskal-Wallis Testi Sonuçları

	Yaşınız	N	Mean Rank	Asymp. Sig.*
Elektronik ticaret iç kontrolün etkililiğine ilişkin asıl riskleri bünyesinde barındırır.	30 ve altı yaş	3	15,33	0,013*
	31-35 yaş	20	17,88	
	36-40 yaş	13	36,12	
	41-45 yaş	10	25,75	
	46-50 yaş	3	31,50	
	Toplam	49		
Elektronik formlar ve elektronik ticaret kapsamındaki çevrimiçi işlemler, iç kontrolün etkililiğini doğrulamak amacıyla ticari işlem dokümanının bütünlüğünü sağlar	30 ve altı yaş	3	16,33	0,001*
	31-35 yaş	20	16,65	
	36-40 yaş	13	34,15	
	41-45 yaş	10	31,20	
	46-50 yaş	3	29,00	
	Toplam	49		
Geleneksel kağıt dokümanlardan elektronik ticarete geçiş iç kontrol zayıflıklarını artırır.	30 ve altı yaş	3	32,50	0,012*
	31-35 yaş	20	29,75	
	36-40 yaş	13	14,58	
	41-45 yaş	10	27,15	
	46-50 yaş	3	23,83	
	Toplam	49		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

** Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-92. Ankete Katılanların Yaşları ile İnternet ile İç Denetim İlişkisine Yönelik Katılım Düzeyleri Arasında Kruskal-Wallis Testi Sonuçları

	Yaşınız	N	Mean Rank**	Asymp. Sig.*
İşletmemizin finansal tabloları ve raporları internet erişim sayfamızdan yayınlanmaktadır.	30 ve altı	3	7,67	0,000*
	31-35	20	19,42	
	36-40	14	34,04	
	41-45	10	33,45	
	46-50	3	17,50	
	Toplam	50		
İnternet vasıtasıyla eş zamanlı veri ve bilgi alış verişi sağlanmaktadır.	30 ve altı	3	14,00	0,014*
	31-35	20	22,05	
	36-40	14	33,71	
	41-45	10	28,00	
	46-50	3	13,33	
	Toplam	50		
İşletmemizde internet ortamında yayınlanan finansal tabloların hazırlanması sürecinde XBRL kullanılmaktadır.	30 ve altı	3	7,83	0,001*
	31-35	20	19,82	
	36-40	14	34,46	
	41-45	9	27,17	
	46-50	2	14,50	
	Toplam	48		
İşletmemizde XBRL, veri transferinin eş zamanlı gerçekleşmesini sağlayarak eş zamanlı raporlama ve sürekli denetimin gerçekleşmesini sağlamaktadır.	30 ve altı	3	7,83	0,001*
	31-35	20	19,82	
	36-40	14	34,46	
	41-45	9	27,17	
	46-50	2	14,50	
	Toplam	48		
İşletmemizde risklere karşı iç denetim mekanizmaları oluşturulurken internet teknolojisinin yapılandırılması, yönetimi ve kontrolü gibi alanlar da tanımlanır.	30 ve altı	3	8,67	0,003*
	31-35	20	20,50	
	36-40	14	34,57	
	41-45	10	30,00	
	46-50	3	18,33	
	Toplam	50		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

** Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-93. Ankete Katılanların İşletmedeki Konumları ile Elektronik Veri Değişimi ile İç Denetim İlişkisine Yönelik Katılım Düzeyleri Arasında Kruskal-Wallis Testi Sonuçları

	İşletmenizdeki konumunuz	N	Mean Rank**	Asymp. Sig.*
İşletmemiz elektronik veri değişimi yardımıyla iş ilişkilerini elektronik ortamda devam ettirir.	İç Denetçi	19	17,34	0,015
	İç Denetim Yöneticisi	10	33,30	
	Muhasebe Müdürü	7	36,36	
	Genel müdür yardımcısı	2	32,75	
	Mali İşler koordinatörü	3	24,67	
	Denetim Koordinatörü	2	19,00	
	İç Kontrol Koordinatörü	6	21,75	
	Toplam	49		
Elektronik veri değişimi, iç denetçilerimizin muhasebe bilgi sisteminde denetim uygulaması yapmasına yardımcı olur.	İç Denetçi	19	16,39	0,003
	İç Denetim Yöneticisi	10	32,70	
	Muhasebe Müdürü	7	39,21	
	Genel müdür yardımcısı	2	34,75	
	Mali İşler koordinatörü	3	24,67	
	Denetim Koordinatörü	2	16,50	
	İç Kontrol Koordinatörü	6	22,58	
	Toplam	49		
Elektronik veri değişimi, iç denetçilerin iç kontrol sisteminin etkinliğini ve yeterliliğini belirlemeye uygun denetim süreçlerini uygulamasını sağlar.	İç Denetçi	19	16,58	0,003
	İç Denetim Yöneticisi	10	33,45	
	Muhasebe Müdürü	7	38,43	
	Genel müdür yardımcısı	2	33,25	
	Mali İşler koordinatörü	3	22,50	
	Denetim Koordinatörü	2	13,50	
	İç Kontrol Koordinatörü	6	24,25	
	Toplam	49		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

** Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-94. Ankete Katılanların İşletmedeki Konumları ile Kurumsal Kaynak Planlaması ile İç Denetim İlişkisine Yönelik Katılım Düzeyleri Arasında Kruskal-Wallis Testi Sonuçları

	İşletmenizdeki konumunuz	N	Mean Rank**	Asymp. Sig.*
İşletmemizde iç kontrol sistemi güvenliğini sağlamak için riskleri azaltmak amacıyla WebTrust, SysTrust gibi güvenlik sistemleri kullanılır.	İç Denetçi	19	18,32	0,003*
	İç Denetim Yöneticisi	10	28,25	
	Muhasebe Müdürü	7	43,36	
	Genel müdür yardımcısı	2	28,50	
	Mali İşler koordinatörü	3	26,17	
	Denetim Koordinatörü	2	11,25	
	İç Kontrol Koordinatörü	6	22,17	
	Toplam	49		
Kurumsal kaynak planlaması işletmemizde süreçlerin otomatikleşmesini sağlamıştır.	İç Denetçi	19	15,89	0,003*
	İç Denetim Yöneticisi	10	34,85	
	Muhasebe Müdürü	7	36,57	
	Genel müdür yardımcısı	2	33,00	
	Mali İşler koordinatörü	3	25,50	
	Denetim Koordinatörü	2	25,00	
	İç Kontrol Koordinatörü	6	21,00	
	Toplam	49		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

** Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-95. Ankete Katılanların İşletmedeki Konumları ile Elektronik Veri İşleme ile İç Denetim İlişkisine Yönelik Katılım Düzeyleri Arasında Kruskal-Wallis Testi Sonuçları

	İşletmenizdeki konumunuz	N	Mean Rank**	Asymp. Sig.*
İşletmemizde elektronik veri işleme teknolojilerinin kullanımıyla ortaya çıkan güvenlik açıkları bilgi güvenliğini tehdit etmektedir.	İç Denetçi	19	25,92	0,024*
	İç Denetim Yöneticisi	10	31,50	
	Muhasebe Müdürü	6	9,42	
	Genel müdür yardımcısı	2	37,50	
	Mali İşler koordinatörü	3	23,00	
	Denetim Koordinatörü	2	29,25	
	İç Kontrol Koordinatörü/Yönetmeni	6	18,25	
	Toplam	48		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

** Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-96. BT Kullanan İç Denetim Personeli Sayısı ve BT Uygulamaları Spearman's Rank Order Korelasyonu

		BT Kullanan İç Denetim Personeli Sayısı- Spearman rho
İİTERNET	İnternet vasıtasıyla eş zamanlı veri ve bilgi alış verişı sağlanmaktadır.	0,400*
	İşletmemizde internet ortamında yayınlanan finansal tabloların hazırlanması sürecinde XBRL kullanılmaktadır.	0,363*
	İşletmemizde risklere karşı iç denetim mekanizmaları oluşturulurken internet teknolojisinin yapılandırılması, yönetimi ve kontrolü gibi alanlar da tanımlanır.	0,415*
EVİ	İşletmemizde finansal bilgiler ve denetim kanıtlarının çoğu elektronik ortamda tutulmaktadır.	0,617**
	İşletmemizde elektronik veri işleme teknolojilerinin kullanımı hatalı işlemleri azaltmıştır.	0,531**

*Korelasyon katsayısı 0,30-0,49 aralığında ise iki değişken arasındaki ilişki orta derecededir.

**Korelasyon katsayısı 0,50-1,00 aralığında ise iki değişken arasındaki ilişki yüksek derecededir.

Tablo-97. BT Denetiminin Uygulandığı Süre ve BT Uygulamaları Spearman's Rank Order Korelasyonu

		BT Denetiminin Uygulandığı Süre-Spearman rho
EVİ	İşletmemizde elektronik veri işleme teknolojilerinin kullanımı hatalı işlemleri azaltmıştır.	0,301*

*Korelasyon katsayısı 0,30-0,49 aralığında ise iki değişken arasındaki ilişki orta derecededir.

Tablo-98. Ankete Katılanların İşletmedeki Konumları ile BT Denetiminin Yapılmasının Nedenleri Arasında Kruskal-Wallis Testi Sonuçları

	İşletmenizdeki konumunuz	N	Mean Rank	Asymp. Sig.
Bilgi-işlem departmanındaki kişilere bağımlı olmamayı sağlar.	İç Denetçi	18	27,75	0,006
	İç Denetim Yöneticisi	10	13,35	
	Muhasebe Müdürü	5	26,30	
	Genel müdür yardımcısı	1	31,50	
	Mali İşler koordinatörü	3	31,50	
	Denetim Koordinatörü	2	31,50	
	İç Kontrol Koordinatörü	6	13,58	
	Toplam	45		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

** Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-99. BT Denetiminin Uygulandığı Süre ile BT Denetiminin Yapılmasının Nedenleri Arasında Kruskal-Wallis Testi Sonuçları

	İşletmenizdeki bilgi teknolojileri denetiminin uygulandığı süre:	N	Mean Rank**	Asymp. Sig.*
Bilgi-işlem departmanındaki kişilere bağımlı olmamayı sağlar.	1 yıldan az	8	18,56	0,047*
	1-3 yıl	22	26,48	
	4-6 yıl	12	20,38	
	10 yıl ve üzeri	2	7,25	
	Toplam	44		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

** Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-100. Ankete Katılanların Konumları ile Bilgi Teknolojileri Denetiminin Etkinliğinin Değerlendirilmesi Arasında Kruskal-Wallis Testi Sonuçları

	İşletmenizdeki konumunuz	N	Mean Rank**	Asymp. Sig.*
İşletmenizdeki Bilgi teknolojileri denetim faaliyetlerinin etkinliğini değerlendiriniz. () Hiç etkin değil () Etkin değil () Kısmen etkin () Etkin () Tamamıyla etkin	İç Denetçi	19	25,42	0,026*
	İç Denetim Yöneticisi	11	34,23	
	Muhasebe Müdürü	7	14,50	
	Genel müdür yardımcısı	3	10,17	
	Mali İşler koordinatörü	3	26,17	
	Denetim Koordinatörü	2	29,50	
	İç Kontrol Koordinatörü/Yönetmeni	6	32,83	
	Toplam	51		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

** Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-101. Bilgi Teknolojileri Denetimin Yapıldığı Süre ile Bilgi Teknolojileri Denetiminin Etkinliğinin Değerlendirilmesi Arasında Kruskal-Wallis Testi Sonuçları

	İşletmenizdeki bilgi teknolojileri denetiminin uygulandığı süre:	N	Mean Rank**	Asymp. Sig.*
İşletmenizdeki Bilgi teknolojileri denetim faaliyetlerinin etkinliğini değerlendiriniz. () Hiç etkin değil () Etkin değil () Kısmen etkin () Etkin () Tamamıyla etkin	Hiç uygulanmaz	6	3,75	0,001*
	1 yıldan az	8	32,50	
	1-3	22	26,82	
	4-6	12	28,75	
	10 yıl ve üzeri	2	28,75	
	Toplam	50		

* Asymp. Sig (p değeri) < 0,05 olduğunda gruplar arasında anlamlı farklılıklar vardır.

** Mean Rank değeri, en yüksek ve en düşük ortalamaya sahip olan grupları göstermektedir.

Tablo-102. İç Denetim Biriminin Faaliyet Gösterdiği Süre ve BT Denetimi Etkinliği Spearman's Rank Order Korelasyonu

	İç Denetim Biriminin Faaliyet Gösterdiği Süre-Spearman rho
İşletmenizdeki Bilgi teknolojileri denetim faaliyetlerinin etkinliğini değerlendiriniz. () Hiç etkin değil () Etkin değil () Kısmen etkin () Etkin () Tamamıyla etkin	0,300*

*Korelasyon katsayısı 0,30-0,49 aralığında ise iki değişken arasındaki ilişki orta derecededir.

Tablo-103. BT Kullanan İç Denetim Personeli Sayısı ve BT Denetiminin Etkinliği Spearman's Rank Order Korelasyonu

	BT Kullanan İç Denetim Personeli Sayısı-Spearman rho
İşletmenizdeki Bilgi teknolojileri denetim faaliyetlerinin etkinliğini değerlendiriniz. () Hiç etkin değil () Etkin değil () Kısmen etkin () Etkin () Tamamıyla etkin	0,300*

*Korelasyon katsayısı 0,30-0,49 aralığında ise iki değişken arasındaki ilişki orta derecededir.

Tablo-104. BT Denetiminin Uygulandığı Süre ve BT Denetiminin Etkinliği Spearman's Rank Order Korelasyonu

	BT Denetiminin Uygulandığı Süre-Spearman rho
İşletmenizdeki Bilgi teknolojileri denetim faaliyetlerinin etkinliğini değerlendiriniz. () Hiç etkin değil () Etkin değil () Kısmen etkin () Etkin () Tamamıyla etkin	0,310*

*Korelasyon katsayısı 0,30-0,49 aralığında ise iki değişken arasındaki ilişki orta derecededir.

Tablo-105. Anket Sorularının Normal Dağılım Varsayımı Testi-Kolmogorov-Smirnov Testi

Normal Dağılım Testi			
	Kolmogorov-Smirnov		
	Statistic	df	Sig.
S1-Cinsiyetiniz	,508	51	,000
S2-Yaşınız	,237	51	,000
S3-Eğitim düzeyiniz	,405	51	,000
S5-İşletmenizdeki çalışma süreniz	,235	51	,000
S6-İşletmenizdeki konumunuz	,248	51	,000
S7-Meslekî Sertifikanız/Sertifikalarınız	,189	51	,000
S8-İşletmeniz faaliyetinde bulunduğunuz sektör	,319	51	,000
S12-İşletmenizdeki iç denetim biriminin faaliyetinde bulunduğunuz süre	,192	51	,000
S13-İç denetim biriminin hazırladığı raporları sunduğunuz merci	,369	51	,000
S14-Sertifikalı İç Denetçiniz var mı	,387	51	,000
S15-Bilgi teknolojilerini kullanan iç denetim personelinin sayısı	,348	51	,000

Tablo-105. Anket Sorularının Normal Dağılım Varsayımı Testi-Kolmogorov-Smirnov Testi (Devam)

	Statistic	df	Sig.
S16- İç Denetim Biriminizin şimdiki durumunu dikkate alarak iç denetimin işlevlerinde, faaliyet alanlarında ve türlerinde meydana gelen değişimlerle ilgili fikrinizi belirtiniz.			
Güvence hizmeti	,473	50	,000
Danışmanlık hizmeti	,431	50	,000
İç kontrol sisteminin izlenmesi ve incelenmesi	,377	50	,000
Risk Yönetimi	,388	50	,000
Kurumsal yönetim	,346	50	,000
Finansal Denetim	,401	50	,000
Uygunluk Denetimi	,480	50	,000
Faaliyet denetim	,461	50	,000
Bilgi Teknolojileri Denetimi	,507	50	,000
Sistem Denetimi	,535	50	,000
S16- İç Denetim Biriminizin gelecekteki durumunu dikkate alarak iç denetimin işlevlerinde, faaliyet alanlarında ve türlerinde meydana gelen değişimlerle ilgili fikrinizi belirtiniz.			
Güvence hizmeti	,454	50	,000
Danışmanlık hizmeti	,514	50	,000
İç kontrol sisteminin izlenmesi ve incelenmesi	,479	50	,000
Risk Yönetimi	,523	50	,000
Kurumsal yönetim	,370	50	,000
Finansal Denetim	,457	50	,000
Uygunluk Denetimi	,468	50	,000
Faaliyet denetim	,449	50	,000
Bilgi Teknolojileri Denetimi	,529	50	,000
Sistem Denetimi	,471	50	,000
S17-İç denetim görevini yerine getirirken karşılaştığınız zorluklar nelerdir? (Birden fazla seçeneği işaretleyebilirsiniz)			
Yetenekli ve yetkili iç denetim personelinin yokluğu	,478	49	,000
Bilgi teknolojileri alt yapısının karmaşıklığı	,407	49	,000
Kontrollerin eksikliği ve yönetimin veya iş süreçlerinin yarattığı riskler	,469	49	,000
Parçalanmış ve eksik veri yapıları	,397	49	,000
İç kontrollerin test edilmesini sağlayan uygun teknolojilerin olmaması	,376	49	,000
S18-İşletmenizde kimler Bilgi teknolojilerini kullanıyor?			
Bilgi Teknolojileri uzmanları	,507	50	,000
İç denetçiler	,431	50	,000
Muhasebe-diğer	,471	50	,000
Satın alma-diğer	,507	50	,000
Satış-diğer	,507	50	,000
ERP Kullanıcıları-diğer	,536	50	,000
Uzman personel- diğer	,536	50	,000
S19-İşletmenizde bilgi teknolojilerinin geçmişteki kullanım düzeylerini belirtiniz.			
İnternet	,476	48	,000
İntranet	,384	48	,000

Tablo-105. Anket Sorularının Normal Dağılım Varsayımı Testi-Kolmogorov-Smirnov Testi (Devam)

	Statistic	df	Sig.
Extranet	,191	48	,000
Elektronik Veri Değişimi	,260	48	,000
Elektronik Ticaret	,313	48	,000
Kurumsal Kaynak Planlaması	,226	48	,000
Veri İşleme Teknolojileri	,248	48	,000
S19-İşletmenizde bilgi teknolojilerinin şu andaki kullanım düzeylerini belirtiniz.			
İnternet	,525	48	,000
İntranet	,500	48	,000
Extranet	,193	48	,000
Elektronik Veri Değişimi	,372	48	,000
Elektronik Ticaret	,243	48	,000
Kurumsal Kaynak Planlaması	,273	48	,000
Veri İşleme Teknolojileri	,387	48	,000
S 20-İç denetim faaliyetinizin bilgi teknolojisi stratejisinin niteliği nedir ? (Tek bir seçenek işaretleyiniz)	,426	49	,000
S21- İç denetim biriminizin bilgi teknolojilerini değerlendirmesi sırasındaki uygulamaları ile ilgili fikrinizi belirtiniz.			
Bilgi Teknolojileri kullanımının verimliliğinin /etkinliğinin/ekonomikliğinin değerlendirilmesi yapılır	,293	49	,000
Politikalar ve düzenlemelerle uyumluluğunun değerlendirilmesi yapılır	,281	49	,000
Bilgi teknolojilerine dayalı sistemlerde iç kontrolün değerlendirilmesi yapılır	,414	49	,000
Finansal tabloların gösteriminde eşitliğin ve muhasebe bilgi sisteminin doğruluğunun ve tamlığının değerlendirilmesi yapılır	,280	49	,000
S22-Bilgi teknolojilerinin değerlendirilmesinde bazı kontroller ve testler uygulanabilir. Lütfen aşağıdaki değerlendirme kontrollerini ve testlerini dikkate alarak biriminizin performansı hakkında fikrinizi belirtiniz.			
Kontrollerin etkinliğinin test edilir	,336	49	,000
Riskler ve risk yönetimi süreci değerlendirilir.	,335	49	,000
Genel kontrollerin etkinliği test edilir.	,335	49	,000
Uygulamalar içindeki kontroller test edilir	,354	49	,000
Uygulama kontrolleri ve genel kontroller değerlendirilir	,300	49	,000
S23-İç denetim sürecinde bilgi teknolojilerinin kullanımının artmasını engelleyen durumlar nelerdir?			
Veri analizi yazılımlarını kullanacak kalifiye personel olmayışı	,344	49	,000
Veri erişiminde bilgi teknolojilerine bağımlılık	,459	49	,000
Bilgi sistemlerinin/ işletme birimlerinin/ global faaliyetlerin denetlenme gerekliliği	,478	49	,000
Veri bütünlüğü, güvenilirliği ve doğruluğu ile ilgili konular	,344	49	,000
Bilgi teknolojisi ile ilgili konuların önceliği yoktur	,506	49	,000
Bütçe kısıtları	,478	49	,000
S24-İşletmenizde bilgi teknolojileri denetiminin uygulandığı süre:	,235	49	,000
S 25-İşletmenizde bilgi teknolojileri denetimi yapılmasının nedenleri ile ilgili olarak aşağıdaki ifadelerle katılım düzeylerinizi belirtiniz.			
Sistemlerin kesintisiz çalışmasını sağlar.	,382	47	,000

Tablo-105. Anket Sorularının Normal Dağılım Varsayımı Testi-Kolmogorov-Smirnov Testi (Devam)

	Statistic	df	Sig.
Beklenmedik durumlar karşısında iş sürekliliğini sağlar.	,314	47	,000
Bilgi teknoloji risklerine karşı önlem almayı sağlar	,390	47	,000
Teknolojik alt yapının ihtiyaçlarını karşılamada optimum çözüm olup olmadığını bulmayı sağlar.	,337	47	,000
Bilgi-işlem departmanındaki kişilere bağımlı olmamayı sağlar.	,357	47	,000
Kullanıcıların sistem veya uygulama kaçaklarını görmesini ve bu kaçakları kötüye kullanmalarını önlemeyi sağlar.	,462	47	,000
İşletme bilgilerinin güvenliğini sağlar.	,493	47	,000
S26-İşletmenizde iç denetim planlama faaliyetlerine Bilgi teknolojileri denetimi faaliyetleri dahil midir?	,484	47	,000
S27-İşletmenizdeki Bilgi teknolojileri denetim faaliyetlerinin etkinliğini değerlendiriniz.	,274	47	,000
S28-İşletmenizde Bilgi teknolojileri denetimini etkileyen konular nelerdir? (Birden fazla seçeneği işaretleyebilirsiniz)			
Bilgi teknolojilerinin sahip olduğu kısıtlar	,376	49	,000
Veri güvenliği ve gizliliği	,355	49	,000
Bilgi teknolojileri sistemlerinin karmaşıklığı	,397	49	,000
S29-Bilgi teknolojileri denetimlerinin uygulanmasını kolaylaştıran teknolojik yenilikler nelerdir? (Birden fazla seçenek işaretleyebilirsiniz)			
Sürekli denetim tekniklerinin ve yazılımlarının kullanımı (ACL,IDEA, Acsess vs.)	,529	49	,000
Çevrimiçi (on-line) sistemlerin kullanımı	,355	49	,000
İstatistiksel analiz yazılımları kullanımı	,376	49	,000
Elektronik çalışma kağıtları yazılımlarının kullanımı	,529	49	,000
Bilgi teknolojileri denetim alanlarında rehberlik sağlanması	,449	49	,000
Bilmiyorum	,536	49	,000
S30-İşletmenizdeki herhangi bir süreçte XBRL ye başvuruldu mu?	,337	47	,000
S37- Elektronik ticaret ve iç denetim ilişkisini belirten aşağıdaki ifadelerle katılım düzeylerinizi belirtiniz.			
Elektronik ticaret iç kontrolün etkililiğine ilişkin asıl riskleri bünyesinde barındırır.	,242	47	,000
Elektronik formlar ve elektronik ticaret kapsamındaki çevrimiçi işlemler, iç kontrolün etkililiğini doğrulamak amacıyla ticari işlem dokümanının bütünlüğünü sağlar	,245	47	,000
Geleneksel kağıt dokümanlardan elektronik ticarete geçiş iç kontrol zayıflıklarını artırır.	,357	47	,000
S38-Elektronik ticaretin örgütlenmesi sırasında iç denetçinin üzerine düşen görevlerin yerine getirilmesini belirten aşağıdaki ifadeler hakkında fikrinizi belirtiniz.			
İşlemlerin değerini tespit etmeli	,300	47	,000
Hissedar ve diğer hak sahiplerini tanımlamalı	,330	47	,000
Değişim yönetimi sürecini gözden geçirmeli	,226	47	,000
Onay sürecini incelemeli	,311	47	,000
Açık anahtar sertifikalarına ilişkin politikaları değerlendirmeli	,384	47	,000
Dijital imza prosedürlerini gözden geçirmeli	,343	47	,000

Tablo-105. Anket Sorularının Normal Dağılım Varsayımı Testi-Kolmogorov-Smirnov Testi (Devam)

	Statistic	df	Sig.
Alıcı, tedarikçi ve sertifikalandırma yetkilisiyle yapılan hizmet düzeyi anlaşmalarını incelemeli	,308	47	,000
Kalite güvencesi politikasını araştırmalı	,308	47	,000
Elektronik ticaret faaliyetlerinde özel hayat ve bilgiler politikasını ve bu politikaya uyumu değerlendirmeli.	,365	47	,000
Arızaları müdahale yeteneğini incelemeli ve değerlendirmeli.	,270	47	,000
S39-Elektronik ticaret faaliyetlerinin denetiminin temel unsurlarının yerine getirilme durumları hakkında fikrinizi belirtiniz.			
Üst yönetimin belirlediği tarz da dahil iç kontrol yapısını değerlendirmek	,296	47	,000
Hedef ve amaçlara ulaşabileceği konusunda makul güvence sağlamak	,296	47	,000
Risklerin kabul edilebilir olup olmadığını tespit etmek	,244	47	,000
Bilgi akışını anlamak	,293	47	,000
Arayüz sorunlarını incelemek	,257	47	,000
İş devamlılığı ve felaket sonrası toparlama planlarını değerlendirmek	,264	47	,000
S40-İç denetim yöneticisinin bir elektronik ticaret işinin yürütülmesinde ilgilenmesi gereken konular aşağıda sıralanmıştır. Bunların yerine getirilme durumları hakkında fikrinizi belirtiniz.			
Elektronik ticaret projesi ve programı	,227	47	,000
Elektronik ticaret sisteminin planlama, tasarım ve uygulamasının kurum stratejileriyle bütünleşmesi	,253	47	,000
Sistemin performansı, güvenliği, güvenilirliği ve kullanıma hazırlığı	,234	47	,000
Sistemin işlevselliği	,246	47	,000
İdari ve hukuki koşullar	,246	47	,000
Donanım ve yazılımın güvenilirliği	,221	47	,000
İşlem süreçlerinin güncelliği, doğruluğu ve tamlığı	,261	47	,000
Kontrol ortamı	,287	47	,000
Risk değerlendirmesi	,282	47	,000
İnternetle ilgili riskler	,257	47	,000
Bilgi gizliliği	,244	47	,000
Sözleşmenin denetim haklarını içermesi	,298	47	,000
S41- İnternet kullanımı ve iç denetim arasındaki ilişkiyi ortaya koyan aşağıdaki ifadelere katılım düzeyinizi belirtiniz.			
İşletmemizin finansal tabloları ve raporları internet erişim sayfamızdan yayınlanmaktadır.	,317	44	,000
İnternet vasıtasıyla eş zamanlı veri ve bilgi alış verişi sağlanmaktadır.	,306	44	,000
İşletmemizde internet ortamında yayınlanan finansal tabloların hazırlanması sürecinde XBRL kullanılmaktadır.	,296	44	,000
İşletmemizde XBRL, veri transferinin eş zamanlı gerçekleşmesini sağlayarak eş zamanlı raporlama ve sürekli denetimin gerçekleşmesini sağlamaktadır.	,296	44	,000
İşletmemizde risklere karşı iç denetim mekanizmaları oluşturulurken internet teknolojisinin yapılandırılması, yönetimi ve kontrolü gibi alanlar da tanımlanır.	,314	44	,000
İşletmemizde iç denetçiler anormalliklerin takip edilmesi ve hataların tanımlanması süreçlerinde elektronik çalışma kağıtlarını kullanırlar.	,257	44	,000
S42- Elektronik Veri Değişimi ve iç denetim arasındaki ilişkiyi ortaya koyan aşağıdaki ifadelere katılım düzeyinizi belirtiniz.			

Tablo-105. Anket Sorularının Normal Dağılım Varsayımı Testi-Kolmogorov-Smirnov Testi (Devam)

	Statistic	df	Sig.
İşletmemiz elektronik veri değişimi yardımıyla iş ilişkilerini elektronik ortamda devam ettirir.	,252	44	,000
Elektronik veri değişimi, iç denetçilerimizin muhasebe bilgi sisteminde denetim uygulaması yapmasına yardımcı olur.	,191	44	,000
Elektronik veri değişimi, iç denetçilerin iç kontrol sisteminin etkinliğini ve yeterliliğini belirlemeye uygun denetim süreçlerini uygulamasını sağlar.	,191	44	,000
S43- Kurumsal Kaynak Planlaması ve iç denetim arasındaki ilişkiyi ortaya koyan aşağıdaki ifadelerle katılım düzeyinizi belirtiniz			
Kurumsal kaynak planlaması işletmemizdeki izleme faaliyetlerinin verimliliğini arttırmıştır.	,268	44	,000
İşletmemizde iç kontrol sistemi güvenliğini sağlamak için riskleri azaltmak amacıyla WebTrust, SysTrust gibi güvenlik sistemleri kullanılır.	,212	44	,000
Kurumsal kaynak planlaması işletmemizde süreçlerin otomatikleşmesini sağlamıştır.	,238	44	,000
S44- Elektronik Veri İşleme ve iç denetim arasındaki ilişkiyi ortaya koyan aşağıdaki ifadelerle katılım düzeyinizi belirtiniz			
İşletmemizde elektronik veri işleme teknolojileri sayesinde iç kontrol sistemi bilgisayarda yazılım düzeyinde bulunmaktadır.	,217	44	,000
İşletmemizde finansal bilgiler ve denetim kanıtlarının çoğu elektronik ortamda tutulmaktadır.	,273	44	,000
Gerçek zamanlı elektronik veri işleme sistemleri denetim tekniklerimizi yenilememize neden olmuştur.	,401	44	,000
İşletmemizde elektronik veri işleme teknolojilerinin kullanımı hatalı işlemleri azaltmıştır.	,242	44	,000
İşletmemizde elektronik veri işleme teknolojilerinin kullanımıyla ortaya çıkan güvenlik açıkları bilgi güvenliğini tehdit etmektedir.	,276	44	,000
S45-İç denetim birimi sürekli denetim yaklaşımını kullanıyor mu?	,454	51	,000
S46-45. SORUYA CEVAP HAYIR İSE, neden kullanmıyor? (Birden fazla seçeneği işaretleyebilirsiniz)			
Önem verilmiyor	,478	14	,000
Personel yetersizliği	,407	14	,000
Bütçe kısıtları	,510	14	,000
Zaman kısıtı	,534	14	,000
Uygulanması karmaşık bir yaklaşım	,407	14	,000
Bilgisayar sistemleri ve veri yapıları ile ilgili kısıtlar var	,443	14	,000
Veri güvenliği ve bütünlüğü ile ilgili sorunlar var	,510	14	,000
Bilgi Teknolojileri bölümünden destek alınamaması	,407	14	,000
S47-45. SORUYA CEVAP EVET İSE, sürekli denetim yaklaşımının kullanımındaki temel amaçlarınızı belirten ifadeleri önem sırasına göre sıralayınız.			
Uygulanan önerileri izlemek	,323	36	,000
Finansal karakterli bilgilerin doğruluğuna ve güvenilirliğine ilişkin bir görüş oluşturmak	,479	36	,000
Sürekli bilgi üzerinde bir dizi güvence hizmeti gerçekleştirmek	,427	36	,000
Elektronik ortamda ortaya çıkan verilere ve denetim kanıtlarına odaklanmak	,525	36	,000

Tablo-105. Anket Sorularının Normal Dağılım Varsayımı Testi-Kolmogorov-Smirnov Testi (Devam)

	Statistic	df	Sig.
Bilgi teknolojilerinin kullanımı sayesinde insan faktöründen kaynaklanan hataları ve zaman kayıplarını engellemek	,504	36	,000
Kontrol zayıflıklarını belirlemek	,515	36	,000
Riskleri gözlemlmek	,504	36	,000
Potansiyel hile faaliyetlerini belirlemek	,515	36	,000
S48-İşletmenizin herhangi bir biriminde veya sürecinde iç kontroller üzerinde sürekli izleme gerçekleştirmek amacıyla bilgi teknolojileri kullanılıyor mu?	,391	36	,000
S49-Yönetim/iş süreci sahipleri sürekli izleme kontrollerini uyguluyorlar mı?	,359	36	,000
S50-"SÜREKLİ DENETİM TEKNOLOJİSİ, RİSK YÖNETİMİNDE KULLANILABİLEN TEKNOLOJİ ODAKLI SÜREKLİ DENETİM ÇÖZÜMLERİNİ YAYGINLAŞTIRMAK İÇİN OLUŞTURULMUŞTUR" bu ifadeye katılım düzeyinizi ifade ediniz.	,292	36	,000
S51-Sürekli denetimin fayda sağladığı alanlar hangileridir? (Birden fazla seçeneği işaretleyebilirsiniz)			
Kapsamlı güvence sağlaması	,525	36	,000
Hileyi önleme ve bulma	,538	36	,000
İyi bir yönetim sağlama	,424	36	,000
Sürekli süreç iyileştirme	,539	36	,000
Maliyet azaltma	,381	36	,000
S52-Sürekli denetimi desteklemek amacıyla işletmenizdeki bilgi teknolojisi kullanımının yaygınlığı ne düzeydedir? Tek seçenek	,246	36	,000
S53-Bilgi teknolojileri tabanlı sürekli denetim araçlarının kullanımı konusunda iç denetim biriminizdeki farkındalık durumu nedir? (Birden fazla seçenek işaretleyebilirsiniz)			
Oracle GRC	,272	34	,000
SAP GRC	,490	34	,000
Oversight	,537	34	,000
Approva Bizrights	,539	34	,000
ACL	,297	34	,000
Idea	,461	34	,000
Diğer-SIRON AML	,530	34	,000
S54- İç denetim biriminizde veri analizi ne zaman kullanılır? (Birden fazla seçenek işaretleyebilirsiniz)			
Denetim faaliyetinin yürütülmesinde	,523	34	,000
Hile bulma programlarında	,353	34	,000
Sürekli denetim yaklaşımında	,472	34	,000
Denetim planlama sürecinde	,353	34	,000
Risk değerlendirme sürecinde	,429	34	,000
Denetim raporlarında	,353	34	,000
Bilmiyorum	,539	34	,000
S55- Veri Bulma, Veri Analizi ve Sürekli Denetim için hangi yazılımları kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)			
Access-veri bulma	,452	36	,000

Tablo-105. Anket Sorularının Normal Dağılım Varsayımı Testi-Kolmogorov-Smirnov Testi (Devam)

	Statistic	df	Sig.
Access-veri analizi	,367	36	,000
Access-sürekli denetim	,504	36	,000
ACL-veri bulma	,452	36	,000
ACL-veri analizi	,438	36	,000
ACL-sürekli denetim	,352	36	,000
IDEA-veri bulma	,538	36	,000
IDEA-sürekli denetim	,525	36	,000
Excel-veri bulma	,381	36	,000
Excel-veri analizi	,424	36	,000
Excel-sürekli denetim	,424	36	,000
Monarch-veri analizi	,538	36	,000
Monarch-sürekli denetim	,534	36	,000
Oracle-veri bulma	,338	36	,000
Oracle-veri analizi	,395	36	,000
Oracle-sürekli denetim	,367	36	,000
AS/400 Query-veri bulma	,534	36	,000
AS/400 Query-veri analizi	,538	36	,000
AS/400 Query-sürekli denetim	,525	36	,000
Crystal Reports-veri bulma	,539	36	,000
Crystal Reports-veri analizi	,538	36	,000
Crystal Reports-sürekli denetim	,538	36	,000
People Soft-veri bulma	,538	36	,000
People Soft-sürekli denetim	,538	36	,000
SAP-veri bulma	,539	36	,000
SAP-veri analizi	,515	36	,000
SAP-sürekli denetim	,539	36	,000
SAS-veri analizi	,538	36	,000
SAS-sürekli denetim	,538	36	,000
Datas-veri bulma	,538	36	,000
Datas-sürekli denetim	,538	36	,000
TeamMate-veri bulma	,539	36	,000
TeamMate-veri analizi	,534	36	,000
TeamMate-sürekli denetim	,538	36	,000
S56-İç denetim birimi Risk odaklı iç denetim yaklaşımını kullanıyor mu?	,534	48	,000
S57-Risk odaklı iç denetim süreci hakkında işletmenizdeki durum ile ilgili katılım düzeylerinizi belirtiniz			
İç denetçi işletme içindeki olası risk alanlarını araştırmak durumundadır	,439	48	,000
Risk tanımlamasında işletme bünyesinde bulunan riskler her risk seviyesine göre (düşük, orta, yüksek) değerlendirilir ve risk alanları tablosunda gösterilir	,481	48	,000
Risk faktörleri tespit edildikten sonra bu faktörlerin toplam risk içindeki nispi önemini belirlemek gerekir.	,463	48	,000
Belirlenen riskler derecelerine bağlı olarak sıraya konulur.	,454	48	,000

Tablo-105. Anket Sorularının Normal Dağılım Varsayımı Testi-Kolmogorov-Smirnov Testi (Devam)

	Statistic	df	Sig.
Risklerle ilgili sonuçlar yönetim kuruluna, denetim komitesine ve diğer ilgililere iletilir.	,273	48	,000
S58-Kontrol öz değerlendirme yaklaşımı işletmenizde uygulanıyor mu?	,361	46	,000
S63-İç denetim faaliyetinde kullanılan araç ve tekniklerin kullanım derecelerini belirtiniz (Şimdi)			
Sürekli denetim teknikleri	,311	46	,000
Veri inceleme-Veri analizi	,202	46	,000
Veri madenciliği	,187	46	,000
Kontrol özdeğerlendirme	,198	46	,000
Risk odaklı iç denetim planı	,395	46	,000
Bilgisayar Destekli Denetim Teknikleri	,270	46	,000
Denetim uzman sistemleri (otomatik risk analizi, sistem yazılımı, kontrol hedefleri yazılımı)	,290	46	,000
Genelleştirilmiş denetim yazılımı	,313	46	,000
Analitik inceleme prosedürleri	,184	46	,000
Kıyaslama (Benchmarking)	,142	46	,020
İstatistiksel örnekleme	,368	46	,000
Uygulama yazılımı izleme ve eşleme	,287	46	,000
Süreç modelleme	,283	46	,000
Bütünleşik test tekniği	,288	46	,000
Veri testi tekniği	,229	46	,000
Paralel simülasyon tekniği	,299	46	,000
Elektronik çalışma kağıtları	,394	46	,000
Akış şeması yazılımları	,280	46	,000
Balance Score Card (Balans Skor Kartı)	,308	46	,000
S63-İç denetim faaliyetinde kullanılan araç ve tekniklerin kullanım derecelerini belirtiniz (Gelecekte)			
Sürekli denetim teknikleri	,393	46	,000
Veri inceleme-Veri analizi	,380	46	,000
Veri madenciliği	,235	46	,000
Kontrol özdeğerlendirme	,342	46	,000
Risk odaklı iç denetim planı	,509	46	,000
Bilgisayar Destekli Denetim Teknikleri	,395	46	,000
Denetim uzman sistemleri (otomatik risk analizi, sistem yazılımı, kontrol hedefleri yazılımı)	,222	46	,000
Genelleştirilmiş denetim yazılımı	,276	46	,000
Analitik inceleme prosedürleri	,259	46	,000
Kıyaslama (Benchmarking)	,232	46	,000
İstatistiksel örnekleme	,416	46	,000
Uygulama yazılımı izleme ve eşleme	,235	46	,000
Süreç modelleme	,252	46	,000
Bütünleşik test tekniği	,308	46	,000
Veri testi tekniği	,260	46	,000

Tablo-105. Anket Sorularının Normal Dağılım Varsayımı Testi-Kolmogorov-Smirnov Testi (Devam)

	Statistic	df	Sig.
Paralel simülasyon tekniği	,236	46	,000
Elektronik çalışma kağıtları	,243	46	,000
Akış şeması yazılımları	,399	46	,000
Balance Score Card (Balans Skor Kartı)	,277	46	,000
S64- Güvence hizmetleri ile ilgili aşağıdaki ifadelerle ilişkin katılım düzeylerinizi belirtiniz.			
İç denetim işletmede kurumsal yönetim sisteminin yeterliliğini ve etkinliğini değerlendirerek yönetime güvence verir.	,428	49	,000
İç denetim yöneticisi kararlaştırılan konularda sağlanan ilerlemenin düzenli olarak izlenmesi amacıyla yönetim ve denetim komitesi ile düzenli toplantılar yapar.	,439	49	,000
İç denetim birimlerince bütünlüğü, doğruluğu ve tarafsızlığı denetlenip, doğrulanmış bilgi karar vericiler tarafından güvenilir bilgi olarak kabul edilir.	,428	49	,000
İç denetim, kontrol sistemlerinin (operasyonel kontrol, finansal kontrol) etkinliğini ölçüp değerlendirerek yönetime objektif güvence sağlar.	,436	49	,000
İç denetim, işletmede kullanılan bilgi teknolojilerinin güvenliğini ve raporlama imkanlarını içeren muhasebe bilgi sisteminin etkinliğini değerlendirir.	,436	49	,000
S65- İç denetim birimi olarak hangi güvence hizmetlerini sağlıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz)			
Onaylama	,407	49	,000
Finansal tablo denetimi	,376	49	,000
İç kontrolün etkinliğini sağlama	,536	49	,000
Finansal tabloların gözden geçirilmesi	,344	49	,000
WebTrust Hizmetleri	,540	49	,000
SysTrust Hizmetleri	,536	49	,000
Yatırımlara ilişkin kontroller ve risklerin değerlendirilmesi	,529	49	,000
Dijital bilgilerin biriktirilmesi, dağıtılması ve saklanması	,469	49	,000
Hile ve yolsuzluk ile ilgili risk değerlendirmesi	,407	49	,000
Ticari politika ve prosedür arasındaki uyum	,407	49	,000
Kalite sertifikasyonları	,539	49	,000
Çevre denetimi	,497	49	,000
Diğer	,540	49	,000
S66-Güvence sağlamada kullanılan yöntemler nelerdir? (Tek bir seçenek işaretleyiniz)			
	,240	49	,000
S67- Danışmanlık hizmetleri ile ilgili aşağıdaki ifadelerle ilişkin katılım düzeylerinizi belirtiniz			
İç denetçi, danışmanlık görevinin iç denetim faaliyetiyle ilgili temel görev planına uygunluğunu göz önünde bulundurur.	,373	49	,000
İç denetçiler risk odaklı bir görev planı uyguladıklarından işletmenin ihtiyaç duyduğu denetim kapsamını belirler.	,407	49	,000
İç denetçiler görev planının izin verdiği ölçüde danışmanlık hizmetini yerine getirmelidirler	,395	49	,000
Danışmanlık hizmetleri, iç denetçiler tarafından sunulan ve denetlenenin işletme amaçlarına ulaşmasını sağlayacak tavsiyeleri içerir	,344	49	,000
S68- İç denetim birimi olarak hangi alanlarda danışmanlık hizmeti sağlıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz)			
Risk yönetimi	,529	49	,000

Tablo-105. Anket Sorularının Normal Dağılım Varsayımı Testi-Kolmogorov-Smirnov Testi (Devam)

	Statistic	df	Sig.
Sistem güvenliği	,355	49	,000
Performans ölçümü	,407	49	,000
Uyum - Diğer	,522	49	,000
S69- İç denetçilerin bilgi teknolojileri üzerindeki kontrolleri incelerken kullanacağı iç kontrol sistemleri ile ilgili olarak aşağıdaki ifadeleri cevaplayınız.			
Acil durumlar için yedek sistem bulunduruluyor mu?	,537	47	,000
Bu şifreler düzenli olarak değiştiriliyor mu?	,540	47	,000
Kullanıcılar belirlenerek ayrı ayrı şifre verilmiş mi?	,537	47	,000
Veritabanına girebilen eski işletme çalışanları var mı?	,493	47	,000
S70-İşletmeniz Risk yönetimi uygulanıyor mu?	,533	47	,000
S71-Risk yönetimi bileşenleri hakkında işletmenizdeki durum ile ilgili katılım düzeylerinizi belirtiniz.			
Kontrol ortamı, risklerin kurumda çalışan kişiler tarafından nasıl görüntülenmesi ve yönlendirilmesi gerektiğine dair bir temel oluşturur.	,300	47	,000
Yönetim risk stratejisini göz önünde bulundurarak hedefleri belirler.	,321	47	,000
Belirsizliklerin risk mi fırsat mı olduğu konusunda çalışmalar yapılır	,310	47	,000
Riskler tanımlandıktan sonra bunların işletme üzerindeki olası etkileri ve meydana gelme olasılıkları değerlendirir.	,304	47	,000
Belirlenen risklerin kurumun risk kapasitesi ve risk toleransı içinde olup olmadığı belirlenir.	,279	47	,000
Riske verilecek karşılıkların etkili bir biçimde yerine getirilmesi ve devam eden risklerin risk kapasitesi sınırları içinde yönetilmesi için politika ve prosedürler oluşturulur.	,343	47	,000
Kişilerin sorumluluklarını yerine getirmesi için ilgili bilgi belli bir biçimde ve belli zaman aralıkları ile tanımlanır ve iletilir.	,306	47	,000
Risk yönetiminin uygulanması izlenir ve etkinliğini arttırmak için gerektiğinde ayarlamalar yapılır.	,279	47	,000
S72- Kurumsal yönetim anlayışı kapsamında işletmenizde iç denetimin rolü hakkında katılım düzeylerinizi belirtiniz.			
İç denetim, kurumsal yönetim sisteminin bütünleştirici bir parçasıdır.	,344	49	,000
İç denetim, kontrol sistemlerinin (operasyonel kontrol, finansal kontrol) etkinliğini ölçüp değerlendirerek yönetime objektif güvence sağlar.	,346	49	,000
İç denetim, işletme bilgi teknolojisi sisteminin güvenliğini ve raporlama imkanlarını içeren muhasebe bilgi sisteminin etkinliğini değerlendirir.	,312	49	,000
İç denetim, profesyonel yöneticilere yetki devrinde güvence sağlar.	,320	49	,000
İç denetim faaliyeti; zamanı ve emeğini, kurum çapında düzgün risk yönetimi süreçlerinin kurulmasına ve uygulanmasına katkıda bulunan danışmanlık faaliyetlerine harcar.	,299	49	,000
İç denetim, risk değerlendirme sürecinin etkin bir şekilde çalıştığı konusunda yönetim kuruluna ve yönetime objektif güvence sağlar.	,327	49	,000
Kurumsal yönetim anlayışının işletmede oluşması değerinin artırılması ve kalitesinin sürdürülebilmesi için iç denetimin kurumsal yönetim anlayışına işlevsellik kazandırır.	,292	49	,000

NOT: 31., 32., 33., 34., 59., 60., 61. ve 62. sorularda yeterli veri olmadığı için hesaplama yapılamamıştır.

Ek-2. Anket Formu

Sayın Katılımcı,

Bu anket formu Anadolu Üniversitesi Sosyal Bilimler Enstitüsü Muhasebe Doktora Programında "**Bilgi Teknolojilerinin İç Denetimde Yarattığı Değişimler ve İç Denetim Birimlerinin Değişimlere Uyumu: Bir Uygulama**" adlı doktora tezi ile ilgili hazırlanmıştır. Anketin amacı, *bilgi teknolojilerindeki değişimlerin iç denetimin işlevlerinde ve iç denetim sürecindeki etkilerini ve iç denetim birimlerinin bu değişimlere uyumunu* ortaya koymaktır. Bu amaçla anketimiz iç denetçilere ve iç denetim alanında sorumluluğu olan yöneticilere uygulanmaktadır.

Anketin amacına ulaşabilmesi için siz katılımcıların cevaplarına ihtiyaç duyulmaktadır. Değerli zamanınızı ayırarak bu anketi cevaplandıracağınızı umut ediyoruz.

Anket çalışmamızın uygulanmasında ve sizlere ulaşmamızda verdiği destekten ötürü Türkiye İç Denetçiler Enstitüsüne (TİDE) teşekkürlerimizi sunuyoruz. Araştırma sonucunda elde edilen bulgular kesinlikle gizli tutulacak ve ulaşılan sonuçlar işletme adı belirtmeksizin istatistiki analizler şeklinde araştırmada kullanılacaktır. Anketi cevaplarken aklınıza takılan herhangi bir soru veya belirtmek istediğiniz bir tavsiye olursa aşağıdaki iletişim adreslerinden bize ulaşabilirsiniz.

Değerli zamanınızı ayırdığınız için teşekkür eder, çalışmalarınızda başarılar dileriz.

Prof. Dr. Saime ÖNCE

Anadolu Üniversitesi, İ.İ.B.F., İşletme Bölümü

GSM: 05056882359

e-mail: sonce@anadolu.edu.tr

Araş. Gör. Burcu İŞGÜDEN

Balıkesir Üniversitesi, Bandırma İ.İ.B.F.

GSM: 05324023241-05063030769

e-mail: burcuisguden@yahoo.com

Fax: 0266 738 0946

1.Cinsiyetiniz: Bay ()

Bayan ()

2.Yaşınız:

3.Eğitim düzeyiniz:

4.Mezun olduğunuz bölüm:

5.İşletmenizdeki çalışma süreniz:

6.İşletmenizdeki konumunuz:

7.Meslekî Sertifika/Sertifikalarınız:

8.İşletmenizin faaliyette bulunduğu sektör:

9.İşletmenin faaliyette bulunduğu süre:

10. İşletmenizin işlem gördüğü borsa:

11.İşletmenizin hukuku statüsü:

12.İşletmenizde iç denetim biriminin faaliyette bulunduğu süre:

13.İç denetim biriminin hazırladığı raporları sunduğu merci:

14.Sertifikalı İç Denetçiniz var mı? ()Evet ()Hayır

15.Bilgi teknolojilerini kullanan iç denetim personelinin sayısı:

16.İç Denetim Biriminizin şimdiki durumunu ve gelecekteki durumunu dikkate alarak iç denetimin işlevlerinde, faaliyet alanlarında ve türlerinde meydana gelen değişimlerle ilgili fikrinizi belirtiniz.

(1=Arttı/Artacak, 2=Aynı kaldı/Aynı Kalacak, 3=Azaldı/Azalacak)	Şimdi			Gelecekte		
	1	2	3	1	2	3
Güvence hizmeti						
Danışmanlık hizmeti						
İç kontrol sisteminin izlenmesi ve incelenmesi						
Risk Yönetimi						
Kurumsal yönetim						
Finansal Denetim						
Uygunluk Denetimi						
Faaliyet denetim						
Bilgi Teknolojileri Denetimi						
Sistem Denetimi						

17.İç denetim görevini yerine getirirken karşılaştığınız zorluklar nelerdir? (Birden fazla seçeneği işaretleyebilirsiniz)

() Yetenekli ve yetkili iç denetim personelinin yokluğu

() Bilgi teknolojileri alt yapısının karmaşıklığı

() Kontrollerin eksikliği ve yönetimin veya iş süreçlerinin yarattığı riskler

() Parçalanmış ve eksik veri yapıları

() İç kontrollerin test edilmesini sağlayan uygun teknolojilerin olmaması

18.İşletmenizde kimler Bilgi teknolojilerini kullanıyor?

() Bilgi teknolojisi uzmanları () İç denetçiler () Diğer

19.İşletmenizde bilgi teknolojilerinin geçmişteki ve şu andaki kullanım düzeylerini belirtiniz.

(1= Hiç uygulanmıyor, 2= Uygulanmıyor, 3= Kısmen uygulanıyor, 4= Uygulanıyor, 5= Hep uygulanıyor.)

Geçmiş					Bilgi teknolojileri	Şimdi				
1	2	3	4	5		1	2	3	4	5
					İnternet					
					İntranet					
					Extranet					
					Elektronik veri değişimi					
					Elektronik ticaret					
					Kurumsal kaynak planlaması					
					Veri İşleme teknolojileri					

20.İç denetim faaliyetinizin bilgi teknolojisi stratejisinin niteliği nedir ? (Tek bir seçenek işaretleyiniz)

- () Deneyssel/erken uygulayıcı – önde gideriz, yeni araçları ve yaklaşımları aktif bir şekilde araştırırız.
 () Temel – ileriye bakıyoruz, fakat diğerler işletmelerin yeni teknoloji ile ne yapacağını görmek için bekliyoruz.
 () Muhafazakar – herkes kullandığı zaman biz de bir şeyler uygulayacağız.
 () Uygulanabilir değil – iç denetim işlerimizde bilgi teknolojisi tabanlı araçlar kullanmıyoruz
 () Diğer (Lütfen belirtiniz)

21.İç denetim biriminizin bilgi teknolojilerini değerlendirmesi sırasındaki uygulamaları ile ilgili fikrinizi belirtiniz.

(1=Hiç yapılmaz, 2= Yapılmaz, 3= Bazen yapılır, 4=Yapılır, 5= Hep yapılır)	1	2	3	4	5
Bilgi Teknolojileri kullanımının verimliliğinin /etkinliğinin/ekonomikliğinin değerlendirilmesi yapılır					
Politikalar ve düzenlemelerle uyumluluğunun değerlendirilmesi yapılır					
Bilgi teknolojilerine dayalı sistemlerde iç kontrolün değerlendirilmesi yapılır					
Finansal tabloların gösteriminde eşitliğin ve muhasebe bilgi sisteminin doğruluğunun ve tamlığının değerlendirilmesi yapılır					

22.Bilgi teknolojilerinin değerlendirilmesinde bazı kontroller ve testler uygulanabilir. Lütfen aşağıdaki değerlendirme kontrollerini ve testlerini dikkate alarak biriminizin performansı hakkında fikrinizi belirtiniz.

(1=1=Hiç yapılmaz, 2= Yapılmaz, 3= Bazen yapılır, 4=Yapılır, 5= Hep yapılır)	1	2	3	4	5
Kontrollerin etkinliğinin test edilir					
Riskler ve risk yönetimi süreci değerlendirilir.					
Genel kontrollerin etkinliği test edilir.					
Uygulamalar içindeki kontroller test edilir					
Uygulama kontrolleri ve genel kontroller değerlendirilir					

23.İç denetim sürecinde bilgi teknolojilerinin kullanımının artmasını engelleyen durumlar nelerdir?

(Birden fazla seçenek işaretleyebilirsiniz)

- () Veri analizi yazılımlarını kullanacak kalifiye personel olmayışı
 () Veri erişiminde bilgi teknolojilerine bağımlılık
 () Bilgi sistemlerinin/ işletme birimlerinin/ global faaliyetlerin denetlenme gerekliliği
 () Veri bütünlüğü, güvenilirliği ve doğruluğu ile ilgili konular
 () Bilgi teknolojisi ile ilgili konuların önceliği yoktur
 () Bütçe kısıtları
 () Diğer (Lütfen belirtiniz)

24.İşletmenizde **bilgi** **teknolojileri** **denetiminin** **uygulandığı**
süre:.....

25.İşletmenizde bilgi teknolojileri denetimi yapılmasının nedenleri ile ilgili olarak aşağıdaki ifadelere katılım düzeylerinizi belirtiniz.

(1= Kesinlikle Katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle Katılıyorum)	1	2	3	4	5
Sistemlerin kesintisiz çalışmasını sağlar.					
Beklenmedik durumlar karşısında iş sürekliliğini sağlar.					
Bilgi teknoloji risklerine karşı önlem almayı sağlar					
Teknolojik alt yapının ihtiyaçlarını karşılamada optimum çözüm olup olmadığını bulmayı sağlar.					
Bilgi-işlem departmanındaki kişilere bağımlı olmamayı sağlar.					
Kullanıcıların sistem veya uygulama kaçaklarını görmesini ve bu kaçakları kötüye kullanmalarını önlemeyi sağlar.					
İşletme bilgilerinin güvenliğini sağlar.					

26.İşletmenizde iç denetim planlama faaliyetlerine Bilgi teknolojileri denetimi faaliyetleri dahil midir?
☐ Evet ☐ Hayır ☐ Bilmiyorum

27.İşletmenizdeki Bilgi teknolojileri denetim faaliyetlerinin etkinliğini değerlendiriniz.

☐ Hiç Etkin Değil ☐ Etkin Değil ☐ Kısmen Etkin ☐ Etkin ☐ Tamamıyla etkin

28.İşletmenizde Bilgi teknolojileri denetimini etkileyen konular nelerdir? (Birden fazla seçeneği işaretleyebilirsiniz)

☐ Bilgi teknolojilerinin sahip olduğu kısıtlar ☐ Veri güvenliği ve gizliliği
☐ Bilgi teknolojileri sistemlerinin karmaşıklığı ☐ Diğer (Lütfen belirtiniz)

29.Bilgi teknolojileri denetimlerinin uygulanmasını kolaylaştıran teknolojik yenilikler nelerdir? (Birden fazla seçenek işaretleyebilirsiniz)

☐ Sürekli denetim tekniklerinin ve yazılımlarının kullanımı (ACL,IDEA, Access vs.)
☐ Çevrimiçi (on-line) sistemlerin kullanımı
☐ İstatistiksel analiz yazılımları kullanımı
☐ Elektronik çalışma kağıtları yazılımlarının kullanımı
☐ Bilgi teknolojileri denetim alanlarında rehberlik sağlanması
☐ Diğer (Lütfen belirtiniz)

30.İşletmenizdeki herhangi bir süreçte XBRL'ye başvuruldu mu?

☐ Evet ☐ Hayır ☐ Bilmiyorum

(Cevabınız **HAYIR** ise 35. soruya geçiniz)----- (Cevabınız **BİLMİYORUM** ise sadece 36. soruya geçiniz)

31. 30. SORUYA CEVABINIZ EVET İSE işletmenizde hangi süreçlerde XBRL'yi kullanıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz)

☐ Sadece finansal raporlama ☐ Finansal tabloların standartlara uygun hazırlanması
☐ Performans ölçümünde ☐ Verinin bilgiye dönüştürülmesinde
☐ Diğer (Lütfen belirtiniz)

32. 30. SORUYA CEVABINIZ EVET İSE XBRL'yi kullanma sebebiniz nedir? (Birden fazla seçeneği işaretleyebilirsiniz)

☐ Düşük eğitim maliyetleri ☐ Ticari yazılımların kullanılabilir olması ☐ İzlenebilir bilgi izleri yaratması
☐ Esnek / Genişletilebilir olması ☐ Veri Değişimi sağlama ☐ Otomatik veri sağlama
☐ Zaman tasarrufu ☐ Diğer (Lütfen belirtiniz)

33. 30. SORUYA CEVABINIZ EVET İSE İşletmeniz XBRL formatında mali rapor yayımladı mı?

☐ Evet ☐ Hayır ☐ Bilmiyorum

(Cevabınız **HAYIR** veya **BİLMİYORUM** ise 35. ve 36. soruları cevaplayınız)

34. 30. SORUYA CEVABINIZ EVET İSE İşletmeniz XBRL formatındaki mali raporu nasıl yayımladı? (Tek bir seçenek işaretleyiniz)

☐ Dış kaynaklardan yardım sağlayarak yayınladı
☐ İç kaynakları kullanarak yayınladı (Tamamlanmış raporlara eklendi)
☐ İç kaynakları kullanarak yayınladı (Raporlama sistemlerinin içine eklendi)
☐ Rapor hazırlama konusunda danışmanlık hizmeti sağlandı (dış kaynak kullanımı veya iç kaynak kullanımı)
☐ (...) Diğer (Lütfen belirtiniz.....)

35. 30. SORUYA CEVABINIZ HAYIR İSE XBRL'yi kullanmama sebebiniz nedir? (Birden fazla seçeneği işaretleyebilirsiniz)

- () Yönetim tarafından onaylanmaması () İstek yapılmasını beklemek
 () Yeterli teknik uzmanlığın olmaması () İşletmenin küçük olması
 () XBRL hakkında bilgi yetersizliği () Mevcut raporlama sisteminden memnun olunması
 () Bilmiyorum () Diğer (Lütfen belirtiniz)

36. XBRL ile ilgili bilmek istediğiniz veya bilmeniz gerektiğini düşündüğünüz bilgiler nelerdir? (Birden fazla seçeneği işaretleyebilirsiniz)

- () XBRL'nin güvenilirliğinin nasıl sağlandığı () XBRL sürecinde iç denetçinin rolü
 () XBRL'nin bilgi teknolojileri ve muhasebe açısından rolü () XBRL'nin denetimin planlanmasındaki rolü
 () XBRL'nin Kurumsal Kaynak Planlaması ile ilişkisi () XBRL ile ilgili denetim riskleri
 () İç kontrollerin anlaşılması () Finansal raporlama sürecine kattığı değer
 () Bilgi teknolojisi ile ilgili riskler ve kurulması gereken kontroller
 () XBRL'nin uygulanma süreci, avantajları, dezavantajları ve maliyetlere etkisi
 () Diğer (Lütfen belirtiniz)

37. Elektronik ticaret ve iç denetim ilişkisini belirten aşağıdaki ifadeler katılım düzeylerinizi belirtiniz.

(1= Kesinlikle Katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle Katılıyorum)	1	2	3	4	5
Elektronik ticaret iç kontrolün etkililiğine ilişkin asıl riskleri bünyesinde barındırır.					
Elektronik formlar ve elektronik ticaret kapsamındaki çevrimiçi işlemler, iç kontrolün etkililiğini doğrulamak amacıyla ticari işlem dokümanının bütünlüğünü sağlar.					
Geleneksel kağıt dokümanlardan elektronik ticarete geçiş iç kontrol zayıflıklarını artırır.					

38. Elektronik ticaretin örgütlenmesi sırasında iç denetçinin üzerine düşen görevlerin yerine getirilmesini belirten aşağıdaki ifadeler hakkında fikrinizi belirtiniz.

(1=1= Hiç yapılmaz, 2= Yapılmaz, 3= Bazen yapılır, 4=Yapılır, 5= Hep yapılır)	1	2	3	4	5
İşlemlerin değerini tespit etmeli					
Hissedar ve diğer hak sahiplerini tanımlamalı					
Değişim yönetimi sürecini gözden geçirmeli					
Onay sürecini incelemeli					
Açık anahtar sertifikalarına ilişkin politikaları değerlendirmeli					
Dijital imza prosedürlerini gözden geçirmeli					
Alıcı, tedarikçi ve sertifikalandırma yetkilisiyle yapılan hizmet düzeyi anlaşmalarını incelemeli					
Kalite güvencesi politikasını araştırmalı					
Elektronik ticaret faaliyetlerinde özel hayat ve bilgiler politikasını ve bu politikaya uyumu değerlendirmeli.					
Arızaları müdahale yeteneğini incelemeli ve değerlendirmeli.					

39. Elektronik ticaret faaliyetlerinin denetiminin temel unsurlarının yerine getirilme durumları hakkında fikrinizi belirtiniz.

(1=1= Hiç yapılmaz, 2= Yapılmaz, 3= Bazen yapılır, 4=Yapılır, 5= Hep yapılır)	1	2	3	4	5
Üst yönetimin belirlediği tarz da dahil iç kontrol yapısını değerlendirmek					
Hedef ve amaçlara ulaşabileceği konusunda makul güvence sağlamak					
Risklerin kabul edilebilir olup olmadığını tespit etmek					
Bilgi akışını anlamak					
Arayüz sorunlarını incelemek					
İş devamlılığı ve felaket sonrası toparlama planlarını değerlendirmek					

40.İç denetim yöneticisinin bir elektronik ticaret işinin yürütülmesinde ilgilenmesi gereken konular aşağıda sıralanmıştır. Bunların yerine getirilme durumları hakkında fikrinizi belirtiniz.

(1=1= Hiç yapılmaz, 2= Yapılmaz, 3= Bazen yapılır, 4=Yapılır, 5= Hep yapılır)	1	2	3	4	5
Elektronik ticaret projesi ve programı					
Elektronik ticaret sisteminin planlama, tasarım ve uygulamasının kurum stratejileriyle bütünleşmesi					
Sistemin performansı, güvenliği, güvenilirliği ve kullanıma hazırlığı					
Sistemin işlevselliği					
İdari ve hukuki koşullar					
Donanım ve yazılımın güvenilirliği					
İşlem süreçlerinin güncelliği, doğruluğu ve tamlığı					
Kontrol ortamı					
Risk değerlendirmesi					
İnternetle ilgili riskler					
Bilgi gizliliği					
Sözleşmenin denetim haklarını içermesi					

41. İnternet kullanımı ve iç denetim arasındaki ilişkiyi ortaya koyan aşağıdaki ifadelere katılım düzeyinizi belirtiniz.

(1= Kesinlikle Katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle Katılıyorum)	1	2	3	4	5
İşletmemizin finansal tabloları ve raporları internet erişim sayfamızdan yayınlanmaktadır.					
İnternet vasıtasıyla eş zamanlı veri ve bilgi alış verişi sağlanmaktadır.					
İşletmemizde internet ortamında yayınlanan finansal tabloların hazırlanması sürecinde XBRL kullanılmaktadır.					
İşletmemizde XBRL, veri transferinin eş zamanlı gerçekleşmesini sağlayarak eş zamanlı raporlama ve sürekli denetimin gerçekleşmesini sağlamaktadır.					
İşletmemizde risklere karşı iç denetim mekanizmaları oluşturulurken internet teknolojisinin yapılandırılması, yönetimi ve kontrolü gibi alanlar da tanımlanır.					
İşletmemizde iç denetçiler anormalliklerin takip edilmesi ve hataların tanımlanması süreçlerinde elektronik çalışma kağıtlarını kullanırlar.					

42. Elektronik Veri Değişimi ve iç denetim arasındaki ilişkiyi ortaya koyan aşağıdaki ifadelere katılım düzeyinizi belirtiniz.

(1= Kesinlikle Katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle Katılıyorum)	1	2	3	4	5
İşletmemiz elektronik veri değişimi yardımıyla iş ilişkilerini elektronik ortamda devam ettirir.					
Elektronik veri değişimi, iç denetçilerimizin muhasebe bilgi sisteminde denetim uygulaması yapmasına yardımcı olur.					
Elektronik veri değişimi, iç denetçilerin iç kontrol sisteminin etkinliğini ve yeterliliğini belirlemeye uygun denetim süreçlerini uygulamasını sağlar.					

43. Kurumsal Kaynak Planlaması ve iç denetim arasındaki ilişkiyi ortaya koyan aşağıdaki ifadelere katılım düzeyinizi belirtiniz

(1= Kesinlikle Katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle Katılıyorum)	1	2	3	4	5
Kurumsal kaynak planlaması işletmemizdeki izleme faaliyetlerinin verimliliğini arttırmıştır.					
İşletmemizde iç kontrol sistemi güvenliğini sağlamak için riskleri azaltmak amacıyla WebTrust, SysTrust gibi güvenlik sistemleri kullanılır.					
Kurumsal kaynak planlaması işletmemizde süreçlerin otomatikleşmesini sağlamıştır.					

44. Elektronik Veri İşleme ve iç denetim arasındaki ilişkiyi ortaya koyan aşağıdaki ifadelere katılım düzeyinizi belirtiniz

(1= Kesinlikle Katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle Katılıyorum)	1	2	3	4	5
İşletmemizde elektronik veri işleme teknolojileri sayesinde iç kontrol sistemi bilgisayarda yazılım düzeyinde bulunmaktadır.					
İşletmemizde finansal bilgiler ve denetim kanıtlarının çoğu elektronik ortamda tutulmaktadır.					
Gerçek zamanlı elektronik veri işleme sistemleri denetim tekniklerimizi yenilememize neden olmuştur.					
İşletmemizde elektronik veri işleme teknolojilerinin kullanımı hatalı işlemleri azaltmıştır.					
İşletmemizde elektronik veri işleme teknolojilerinin kullanımıyla ortaya çıkan güvenlik açıkları bilgi güvenliğini tehdit etmektedir.					

45.İç denetim birimi sürekli denetim yaklaşımını kullanıyor mu?

- () Evet (Cevabınız **EVET** ise 47.-55. arasındaki soruları cevaplayınız)
 () Hayır (Cevabınız **HAYIR** ise **sadece** 46. soruyu cevaplayınız)

46. 45. SORUYA CEVAP HAYIR İSE, neden kullanmıyor? (Birden fazla seçeneği işaretleyebilirsiniz)

- () Önem verilmiyor () Personel yetersizliği () Bütçe kısıtları () Zaman kısıtı
 () Uygulanması karmaşık bir yaklaşım () Bilgisayar sistemleri ve veri yapıları ile ilgili kısıtlar var
 () Veri güvenliği ve bütünlüğü ile ilgili sorunlar var () Veri girişine sorunlar var
 () Bilgi Teknolojileri bölümünden destek alınamaması () Diğer

47. 45. SORUYA CEVAP EVET İSE, sürekli denetim yaklaşımının kullanımındaki temel amaçlarınızı belirten ifadeleri önem sırasına göre sıralayınız.

(1= Kesinlikle Katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle Katılıyorum)	1	2	3	4	5
Uygulanan önerileri izlemek					
Finansal karakterli bilgilerin doğruluğuna ve güvenilirliğine ilişkin bir görüş oluşturmak					
Sürekli bilgi üzerinde bir dizi güvence hizmeti gerçekleştirmek					
Elektronik ortamda ortaya çıkan verilere ve denetim kanıtlarına odaklanmak					
Bilgi teknolojilerinin kullanımı sayesinde insan faktöründen kaynaklanan hataları ve zaman kayıplarını engellemek					
Kontrol zayıflıklarını belirlemek					
Riskleri gözlemlemek					
Potansiyel hile faaliyetlerini belirlemek					

48.İşletmenizin herhangi bir biriminde veya sürecinde iç kontroller üzerinde sürekli izleme gerçekleştirmek amacıyla bilgi teknolojileri kullanılıyor mu?

- () Evet () Hayır () Bilmiyorum

49. Yönetim/iş süreci sahipleri sürekli izleme kontrollerini uyguluyorlar mı?

- () Evet () Hayır () Bilmiyorum

50.“SÜREKLİ DENETİM TEKNOLOJİSİ, RİSK YÖNETİMİNDE KULLANILABİLEN TEKNOLOJİ ODAKLI SÜREKLİ DENETİM ÇÖZÜMLERİNİ YAYGINLAŞTIRMAK İÇİN OLUŞTURULMUŞTUR” bu ifadeye katılım düzeyinizi ifade ediniz.

- () Kesinlikle Katılmıyorum () Katılmıyorum () Kararsızım () Katılıyorum () Kesinlikle Katılıyorum

51. Sürekli denetimin fayda sağladığı alanlar hangileridir? (Birden fazla seçeneği işaretleyebilirsiniz)

- () Kapsamlı güvence sağlaması () Hileyi önleme ve bulma () İyi bir yönetim sağlama
 () Sürekli süreç iyileştirme () Maliyet azaltma
 () Diğer (Lütfen belirtiniz.....)

52.Sürekli denetimi desteklemek amacıyla işletmenizdeki bilgi teknolojisi kullanımının yaygınlığı ne düzeydedir? (Tek bir seçenek işaretleyiniz)

- () Kurumsal kaynak planlaması (ERP) gibi standart raporlama sistemleri kullanılır
 () Denetim ve izleme için tahsis edilmiş araçların kullanımı dikkate alınır
 () Kısıtlı olarak / pilot uygulama kapsamında denetim ve izleme araçları kullanılır
 () Geniş bir alanda denetim ve izleme araçları kullanılır
 () Yaygın değildir () Bilmiyorum () Diğer (Lütfen belirtiniz.....)

53. Bilgi teknolojileri tabanlı sürekli denetim araçlarının kullanımı konusunda iç denetim biriminizdeki farkındalık durumu nedir? (Birden fazla seçenek işaretleyebilirsiniz)

	Oracle GRC	SAP GRC	Oversight	Approva Bizrights	ACL	Idea	Diğer
Personel tarafından iyi biliniyor							
Personel tarafından az biliniyor							
Personel tarafından bilinmiyor							
Personel tarafından uygulanıyor							
Sistemler içinde otomatik olarak yer alıyor							

54. İç denetim biriminizde veri analizi ne zaman kullanılır? (Birden fazla seçenek işaretleyebilirsiniz)

() Denetim faaliyetinin yürütülmesinde () Hile bulma programlarında () Sürekli denetim yaklaşımında
() Denetim planlama sürecinde () Risk değerlendirme sürecinde () Denetim raporlarında
() Bilmiyorum () Diğer (Lütfen belirtiniz.....)

55. Veri Bulma, Veri Analizi ve Sürekli Denetim için hangi yazılımları kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)

YAZILIMLAR	Veri Bulma	Veri Analizi	Sürekli Denetim
Access			
ACL			
IDEA			
Excel			
Monarch			
Oracle			
AS/400 Query			
Crystal Reports			
People Soft			
SAP			
SAS			
Datas			
TeamMate			

56. İç denetim birimi Risk odaklı iç denetim yaklaşımını kullanıyor mu? () Evet () Hayır

57. Risk odaklı iç denetim süreci hakkında işletmenizdeki durum ile ilgili katılım düzeylerinizi belirtiniz.

(1= Kesinlikle Katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle Katılıyorum)	1	2	3	4	5
İç denetçi işletme içindeki olası risk alanlarını araştırmak durumundadır					
Risk tanımlamasında işletme bünyesinde bulunan riskler her risk seviyesine göre (düşük, orta, yüksek) değerlendirilir ve risk alanları tablosunda gösterilir					
Risk faktörleri tespit edildikten sonra bu faktörlerin toplam risk içindeki nispi önemini belirlemek gerekir.					
Belirlenen riskler derecelerine bağlı olarak sıraya konulur.					
Risklerle ilgili sonuçlar yönetim kuruluna, denetim komitesine ve diğer ilgililere iletilir.					

58. Kontrol öz değerlendirme yaklaşımı işletmenizde uygulanıyor mu?

() Evet () Hayır (Cevabınız HAYIR ise sadece 59. soruyu cevaplayınız)

59. 58. SORUYA CEVABINIZ HAYIR İSE kontrol öz değerlendirme yaklaşımının işletmenizde uygulanmama nedeni nedir? (Size uygun olan seçenekleri işaretleyiniz)

() Uygulama yönteminin bilinmemesi () İşletme yönetiminin bu uygulamaya sıcak bakmaması
() Yaklaşımın karmaşık olması () Diğer (Lütfen belirtiniz.....)

60. 58. SORUYA CEVABINIZ EVET İSE hangi kontrol öz değerlendirme yaklaşımını uyguluyorsunuz?

() Grup Çalışması () Anket () Yönetici Analizleri () Diğer

61. 60. SORUYA CEVABINIZ GRUP ÇALIŞMASI İSE grup çalışmasının hangi türünü uyguluyorsunuz?

() Amaca dayalı () Riske dayalı () Kontrole dayalı () Sürece dayalı

62. 58. SORUYA CEVABINIZ EVET İSE Kontrol öz değerlendirmesinin kullanıma nedenlerini hakkında katılım düzeylerinizi belirtiniz.

(1= Kesinlikle Katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle Katılıyorum)	1	2	3	4	5
Denetimin kapsamını genişletmek					
Yasalara uyum sağlamak					
Bir iş sürecinin yeniden yapılanma sürecini izlemek					
Amaçların başarılmasını sağlamak					
Katılımcıların öğrenme sürecini geliştirmek					
Etkin bir iç kontrol ve risk yönetimi için her düzeyde sorumlulukların yerine getirilmesi konusunda yönetime yardımcı olmak					
Planlama stratejilerini desteklemek					

63. İç denetim faaliyetinde kullanılan araç ve tekniklerin kullanım derecelerini belirtiniz

(1= Hiç Kullanılmıyor/Hiç kullanılmayacak, 2= Kullanılmıyor/Kullanılmayacak, 3= Kısmen kullanılıyor/Kısmen kullanılacak, 4= Kullanılıyor/Kullanılacak, 5= Çok kullanılıyor/Çok kullanılacak)	Şimdi					Gelecekte				
	1	2	3	4	5	1	2	3	4	5
Sürekli denetim teknikleri										
Veri inceleme-Veri analizi										
Veri madenciliği										
Kontrol özdeğerlendirme										
Risk odaklı iç denetim planı										
Bilgisayar Destekli Denetim Teknikleri										
Denetim uzman sistemleri (otomatik risk analizi, sistem yazılımı, kontrol hedefleri yazılımı)										
Genelleştirilmiş denetim yazılımı										
Analitik inceleme prosedürleri										
Kıyaslama (Benchmarking)										
İstatistiksel örnekleme										
Uygulama yazılımı izleme ve eşleme										
Süreç modelleme										
Bütünlük test tekniği										
Veri testi tekniği										
Paralel simülasyon tekniği										
Elektronik çalışma kağıtları										
Akış şeması yazılımları										
Balance Score Card (Balans Skor Kartı)										

64. Güvence hizmetleri ile ilgili aşağıdaki ifadelere ilişkin katılım düzeylerinizi belirtiniz.

(1= Kesinlikle Katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle Katılıyorum)	1	2	3	4	5
İç denetim işletmede kurumsal yönetim sisteminin yeterliliğini ve etkinliğini değerlendirerek yönetime güvence verir.					
İç denetim yöneticisi kararlaştırılan konularda sağlanan ilerlemenin düzenli olarak izlenmesi amacıyla yönetim ve denetim komitesi ile düzenli toplantılar yapar.					
İç denetim birimlerince bütünlüğü, doğruluğu ve tarafsızlığı denetlenip, doğrulanmış bilgi karar vericiler tarafından güvenilir bilgi olarak kabul edilir.					
İç denetim, kontrol sistemlerinin (operasyonel kontrol, finansal kontrol) etkinliğini ölçüp değerlendirerek yönetime objektif güvence sağlar.					
İç denetim, işletmede kullanılan bilgi teknolojilerinin güvenliğini ve raporlama imkanlarını içeren muhasebe bilgi sisteminin etkinliğini değerlendirir.					

65.İç denetim birimi olarak hangi güvence hizmetlerini sağlıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz)

- () Onaylama () Finansal tablo denetimi () İç kontrolün etkinliğini sağlama
 () Finansal tabloların gözden geçirilmesi () WebTrust Hizmetleri () SysTrust Hizmetleri
 () Yatırımlara ilişkin kontroller ve risklerin değerlendirilmesi
 () Dijital bilgilerin biriktirilmesi, dağıtılması ve saklanması () Hile ve yolsuzluk ile ilgili risk değerlendirmesi
 () Ticari politika ve prosedür arasındaki uyum () Kalite sertifikasyonları () Çevre denetimi
 () Diğer (Lütfen belirtiniz).....

66.Güvence sağlamada kullanılan yöntemler nelerdir? (Tek bir seçenek işaretleyiniz)

- () Çoğunlukla periyodik manuel kontroller/standart raporlar
 () Düzenli yapılan manuel ve otomatik kontrollerin karışımı
 () Gerçek zamanlı manuel ve otomatik kontrollerin karışımı
 () Çoğunlukla gerçek zamanlı otomatik kontroller () Bilmiyorum () Diğer

67. Danışmanlık hizmetleri ile ilgili aşağıdaki ifadelere ilişkin katılım düzeylerinizi belirtiniz

(1= Kesinlikle Katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle Katılıyorum)	1	2	3	4	5
İç denetçi, danışmanlık görevinin iç denetim faaliyetiyle ilgili temel görev planına uygunluğunu göz önünde bulundurur.					
İç denetçiler risk odaklı bir görev planı uyguladıklarından işletmenin ihtiyaç duyduğu denetim kapsamını belirler.					
İç denetçiler görev planının izin verdiği ölçüde danışmanlık hizmetini yerine getirmelidirler					
Danışmanlık hizmetleri, iç denetçiler tarafından sunulan ve denetlenenin işletme amaçlarına ulaşmasını sağlayacak tavsiyeleri içerir					

68.İç denetim birimi olarak hangi alanlarda danışmanlık hizmeti sağlıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz)

- () Risk yönetimi () Elektronik ticaret () Sistem güvenliği () Performans ölçümü
 () Diğer (Lütfen belirtiniz).....

69.İç denetçilerin bilgi teknolojileri üzerindeki kontrolleri incelerken kullanacağı iç kontrol sistemleri ile ilgili olarak aşağıdaki ifadeleri cevaplayınız.

	Evet	Hayır
İşletme yedeklenmiş dosyaları koruyor mu?		
Dosyalara erişim sınırlandırılmış mı?		
Kullanılan bir arşivleme sistemi var mı?		
Donanım arıza ve kayıplarına karşı alınmış önlem var mı?		
Acil durumlar için yedek sistem bulunduruluyor mu?		
Veritabanına girmek için şifre var mı?		
Bu şifreler düzenli olarak değiştiriliyor mu?		
Kullanıcılar belirlenerek ayrı ayrı şifre verilmiş mi?		
Virüs ve çeşitli saldırılara karşı önlem alınmış mı?		
Veritabanına girebilen eski işletme çalışanları var mı?		

70.İşletmeniz Risk yönetimi uygulanıyor mu? () Evet () Hayır

71.Risk yönetimi bileşenleri hakkında işletmenizdeki durum ile ilgili katılım düzeylerinizi belirtiniz.

(1= Kesinlikle Katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle Katılıyorum)	1	2	3	4	5
Kontrol ortamı, risklerin kurumda çalışan kişiler tarafından nasıl görüntülenmesi ve yönlendirilmesi gerektiğine dair bir temel oluşturur.					
Yönetim risk stratejisini göz önünde bulundurarak hedefleri belirler.					
Belirsizliklerin risk mi fırsat mı olduğu konusunda çalışmalar yapılır					
Riskler tanımlandıktan sonra bunların işletme üzerindeki olası etkileri ve meydana gelme olasılıkları değerlendirir.					
Belirlenen risklerin kurumun risk kapasitesi ve risk toleransı içinde olup olmadığı belirlenir.					
Riske verilecek karşılıkların etkili bir biçimde yerine getirilmesi ve devam eden risklerin risk kapasitesi sınırları içinde yönetilmesi için politika ve prosedürler oluşturulur.					
Kişilerin sorumluluklarını yerine getirmesi için ilgili bilgi belli bir biçimde ve belli zaman aralıkları ile tanımlanır ve iletilir.					
Risk yönetiminin uygulanması izlenir ve etkinliğini arttırmak için gerektiğinde ayarlamalar yapılır.					

72.Kurumsal yönetim anlayışı kapsamında işletmenizde iç denetimin rolü hakkında katılım düzeylerinizi belirtiniz.

(1= Kesinlikle Katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle Katılıyorum)	1	2	3	4	5
İç denetim, kurumsal yönetim sisteminin bütünleştirici bir parçasıdır.					
İç denetim, kontrol sistemlerinin (operasyonel kontrol, finansal kontrol) etkinliğini ölçüp değerlendirerek yönetime objektif güvence sağlar.					
İç denetim, işletme bilgi teknolojisi sisteminin güvenliğini ve raporlama imkanlarını içeren muhasebe bilgi sisteminin etkinliğini değerlendirir.					
İç denetim, profesyonel yöneticilere yetki devrinde güvence sağlar.					
İç denetim faaliyeti; zamanı ve emeğini, kurum çapında düzgün risk yönetimi süreçlerinin kurulmasına ve uygulanmasına katkıda bulunan danışmanlık faaliyetlerine harcar.					
İç denetim, risk değerlendirme sürecinin etkin bir şekilde çalıştığı konusunda yönetim kuruluna ve yönetime objektif güvence sağlar.					
Kurumsal yönetim anlayışının işletmede oluşması değerinin artırılması ve kalitesinin sürdürülebilmesi için iç denetimin kurumsal yönetim anlayışına işlevsellik kazandırır.					

73.Aşağıdaki ifadelerde iç denetimin tanımında yer alan ve iç denetimin önemini vurgulayan ifadeler yer almaktadır. İşletmeniz açısından aşağıdaki her bir ifade hakkında katılım düzeyinizi belirtiniz.

(1= Kesinlikle Katılmıyorum, 2= Katılmıyorum, 3= Kararsızım, 4= Katılıyorum, 5= Kesinlikle Katılıyorum)	1	2	3	4	5
İç denetim faaliyetimiz, bağımsız objektif güvence ve danışmanlık faaliyetidir.					
İç denetim faaliyetimiz, işletmeye değer katar.					
İç denetim faaliyetimiz, risk yönetiminin etkinliğini değerlendirmede sistematik bir yaklaşım getirir.					
İç denetim faaliyetimiz, iç kontrollerin etkinliğini değerlendirmede sistematik bir yaklaşım getirir.					
İç denetim faaliyetimiz, kurumsal yönetim süreçlerinin etkinliğini değerlendirmede sistematik bir yaklaşım getirir.					
İç denetim faaliyetimiz, proaktif olarak önemli finansal konuları, riskleri ve iç kontrolleri inceler.					
İç denetim faaliyetimiz, yönetime güvenilir bilgi sağlayan kurumsal yönetim süreçlerinin ayrılmaz bir parçasıdır.					
İç denetim faaliyetimizin kurumsal yönetim süreçlerine değer katmasının bir yolu denetim komitesine doğrudan erişebiliyor olmasıdır.					
İç denetim faaliyetimiz, işletme içinde etkin çalışabilecek bir konuma sahiptir.					
Bağımsızlık ve objektiflik, iç denetim faaliyetimizin katma değer sağlaması için temel faktörlerdir.					

**DEĞERLİ VAKTİNİZİ AYIRARAK
ANKETİMİZİ CEVAPLANDIRDIĞINIZ İÇİN
ÇOK TEŞEKKÜR EDERİZ.**

Araştırma sonuçlarının tarafınıza gönderilmesini istiyor musunuz? () Evet () Hayır

Cevabınız "**EVET**" ise lütfen araştırma sonuçlarının size iletebileceği bir e-mail adresi belirtiniz.

e-mail adresi:.....

Ek-3. 01.04.2011-30.06.2011 Döneminde İMKB-100 Endekste İşlem Gören Tüm Şirketler

1. ADANA ÇİMENTO SANAYİİ T.A.Ş.
2. ADVANSA SASA POLYESTER SANAYİİ A.Ş.
3. AFYON ÇİMENTO SANAYİİ T.A.Ş.
4. AK ENERJİ ELEKTRİK ÜRETİM A.Ş.
5. AKBANK T.A.Ş.
6. AKSA AKRİLİK KİMYA SANAYİİ A.Ş.
7. AKSA ENERJİ ÜRETİM A.Ş.
8. AKSİGORTA A.Ş.
9. ALARKO HOLDİNG A.Ş.
10. ANADOLU EFES BİRACILIK VE MALT SANAYİİ A.Ş.
11. ANADOLU ANONİM TÜRK SİGORTA ŞİRKETİ
12. ANEL ELEKTRİK PROJE TAAHHÜT VE TİCARET A.Ş.
13. ARÇELİK A.Ş.
14. ASELSAN ELEKTRONİK SANAYİ VE TİCARET A.Ş.
15. ASYA KATILIM BANKASI A.Ş.
16. AYGAZ A.Ş.
17. BAGFAŞ BANDIRMA GÜBRE FABRİKALARI A.Ş.
18. BANVİT BANDIRMA VİTAMİNLİ YEM SANAYİİ A.Ş.
19. BEŞİKTAŞ FUTBOL YATIRIMLARI SANAYİ VE TİCARET A.Ş.
20. BİM BİRLEŞİK MAĞAZALAR A.Ş.
21. BOYNER BÜYÜK MAĞAZACILIK A.S.
22. BRİSA BRIDGESTONE SABANCI LASTİK SAN. VE TİC. A.Ş.
23. DEVA HOLDİNG A.Ş.
24. DO & CO RESTAURANTS & CATERING AG
25. DOĞAN ŞİRKETLER GRUBU HOLDİNG A.Ş.
26. DOĞAN YAYIN HOLDİNG A.Ş.
27. DOĞUS OTOMOTİV SERVİS VE TİCARET A.Ş.
28. EİS ECZACIBAŞI İLAÇ, SİNAİ VE FİNANSAL YATIRIMLAR SANAYİ VE TİCARET A.Ş.
29. ECZACIBASI YATIRIM HOLDİNG ORTAKLIĞI A.Ş.
30. EGE GÜBRE SANAYİİ A.Ş.
31. EGE SERAMİK SANAYİ VE TİCARET A.Ş.
32. ENKA İNŞAAT VE SANAYİ A.Ş.
33. EREĞLİ DEMİR VE ÇELİK FABRİKALARI T.A.Ş.
34. FENERBAHÇE SPOR TİF HİZMETLER SANAYİ VE TİCARET A.Ş.
35. FORD OTOMOTİV SANAYİ A.Ş.
36. GALATASARAY SPOR TİF SİNAİ VE TİCARİ YATIRIMLAR A.Ş.
37. GARANTİ BANKASI A.Ş.
38. GLOBAL YATIRIM HOLDİNG A.Ş.
39. GOLDAS KUYUMCULUK SANAYİ İTHALAT İHRACAT A.Ş.
40. GOODYEAR LASTİKLERİ T.A.Ş.
41. GÖLTAS GÖLLER BÖLGESİ ÇİMENTO SAN.VE TİC.A.Ş.
42. GSD HOLDİNG A.Ş.
43. GÜBRE FABRİKALARI T.A.Ş.
44. HÜRRİYET GAZETECİLİK VE MATBAACILIK A.Ş.

45. IŞIKLAR YATIRIM HOLDİNG A.Ş.
46. İHLAS EV ALETLERİ İMALAT SANAYİ VE TİCARET A.Ş.
47. İHLAS GAZETECİLİK A.Ş.
48. İHLAS HOLDİNG A.Ş.
49. İHLAS YAYIN HOLDİNG A.Ş.
50. İPEK MATBAACILIK SAN. TİC. A.Ş.
51. T.İŞ BANKASI A.Ş.
52. İS FİNANSAL KİRALAMA A.Ş.
53. İTTİFAK HOLDİNG A.Ş.
54. İZMİR DEMİR ÇELİK SANAYİ A.Ş.
55. KARDEMİR KARABÜK DEMİR ÇELİK SANAYİ VE TİCARET A.Ş.
56. KARSAN OTOMOTİV SANAYİİ VE TİCARET A.Ş.
57. KARTONSAN KARTON SANAYİ VE TİCARET A.Ş.
58. KOÇ HOLDİNG A.Ş.
59. KONYA ÇİMENTO SANAYİİ A.Ş.
60. KOZA ALTIN İŞLETMELERİ A.Ş.
61. KOZA ANADOLU METAL MADENCİLİK İŞLETMELERİ A.Ş.
62. MARMARİS MARTI OTEL İŞLETMELERİ A.Ş.
63. METRO TİCARİ VE MALİ YATIRIMLAR HOLDİNG A.Ş.
64. MİGROS TÜRK T.A.Ş.
65. MONDİ TİRE KUTSAN KAĞIT VE AMBALAJ SANAYİ A.Ş.
66. NET HOLDİNG A.Ş.
67. NET TURİZM TİCARET VE SANAYİ A.Ş.
68. NORTEL NETWORKS NETAŞ TELEKOMÜNİKASYON A.Ş.
69. PARK ELEKTRİK MADENCİLİK SANAYİ VE TİCARET A.Ş.
70. PETKİM PETROKİMYA HOLDİNG A.Ş.
71. PETROL OFİSİ A.Ş.
72. SABANCI HOLDİNG A.Ş.
73. ŞEKERBANK T.A.Ş.
74. T. ŞİŞE VE CAM FABRİKALARI A.Ş.
75. TÜRKİYE HALK BANKASI A.Ş.
76. TÜRK EKONOMİ BANKASI A.Ş.
77. TÜRKİYE SİNAİ KALKINMA BANKASI A.Ş.
78. TAV HAVALİMANLARI HOLDİNG A.Ş.
79. TEK-ART TURİZM ZİGANA A.Ş.
80. TEK-FEN HOLDİNG A.Ş.
81. TEKSTİL BANKASI A.Ş.
82. TESCO KİPA KİTLE PAZARLAMA TİCARET VE GIDA SANAYİ A.Ş.
83. TOFAŞ TÜRK OTOMOBİL FABRİKASI A.Ş.
84. TRABZONSPOR SPOR TİF YATIRIM VE FUTBOL İŞLETMECİLİĞİ TİCARET A.Ş.
85. TRAKYA CAM SANAYİİ A.Ş.
86. TURKCELL İLETİŞİM HİZMETLERİ A.Ş.
87. TÜPRAŞ-TÜRKİYE PETROL RAFİNERİLERİ A.Ş.
88. TÜRK HAVA YOLLARI A.O.
89. TÜRK TELEKOMÜNİKASYON A.Ş.
90. TÜRK TRAKTÖR VE ZİRAAT MAKİNALARI A.Ş.
91. ÜLKER GIDA SANAYİ VE TİCARET A.S.

92. TÜRKİYE VAKIFLAR BANKASI T.A.O.
93. VESTEL ELEKTRONİK SANAYİ VE TİCARET A.Ş.
94. YAPI VE KREDİ BANKASI A.Ş.
95. ZORLU ENERJİ ELEKTRİK ÜRETİM A.Ş.
96. EMLAK KONUT GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş.
97. İŞ GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş.
98. RHEA GİRİŞİM SERMAYESİ YATIRIM ORTAKLIĞI A.Ş.
99. SİNPAŞ GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş.
100. TORUNLAR GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş.

Ek-4. Araştırma Sorularının Testinde Kullanılan İstatistiksel Analizler İle İlgili Bilgiler

Bu kısımda araştırma sorularının testinde kullanılacak istatistiksel analizler ve kavramlarla ilgili bilgi verilecektir.

Güvenilirlik Analizi

Güvenilirlik, ölçmede temel ve basit olarak tutarlılık anlamına gelir. Güvenilir bir test veya ölçek benzeri şartlarda uygulandığında benzeri sonuçlar verir. Bir test veya ölçek ne kadar güvenilir ise ondan elde edilen veriler de o derece güvenilirdir. Bir ölçeğin güvenilirliğini ölçmede çeşitli yaklaşımlar kullanılabilir (Altunışık, Çoşkun, Bayraktaroğlu ve Yıldırım, 2004: 113).

Güvenilirlik analizi ölçmede kullanılan testlerin, anketlerin yada ölçeklerin özelliklerini ve güvenilirliklerini değerlendirmek üzere geliştirilmiş bir yöntemdir. Güvenilirlik analizi ile toplam puanların söz konusu olduğu Likert tipi ölçeklerin güvenilirliğini belirleyen katsayılar hesaplanır ve ölçekte yer alan sorular arasındaki ilişkiler hakkında bilgi elde edilir (Kalaycı, 2008: 403).

Testlerin güvenilirliğini analiz etmek amacıyla, güvenilirlik katsayıları hesaplanmaktadır. Güvenilirlik katsayılarından sıklıkla kullanılan “*Cronbach Alfa*” katsayısıdır. Cronbach Alfa katsayısı 0 ile 1 arasında bir değerdir. Bu katsayının negatif çıkması güvenilirlik modelinin bozulmasına neden olur. Alfa katsayısına bağlı olarak ölçeğin güvenilirliği aşağıdaki gibi yorumlanır (Kalaycı, 2008: 405):

- $0,00 \leq \alpha < 0,40$ ise ölçek güvenilir değildir.
- $0,40 \leq \alpha < 0,60$ ise ölçeğin güvenilirliği düşüktür.
- $0,60 \leq \alpha < 0,80$ ise ölçek oldukça güvenilirdir.
- $0,80 \leq \alpha < 1,00$ ise ölçek yüksek derecede güvenilirdir.

Anlamlılık Seviyesi (α)

Seçilen anlamlılık seviyesi örneklem dağılımındaki kabul ve red bölgelerinin belirlenmesini sağlar. Sağlık bilimleri, mühendislik, sosyal bilimler gibi alanlarda genellikle kullanılan anlamlılık seviyesi 0,05 veya 0,01’dir. Anlamlılık Seviyesinin amacı, örnek istatistiği ile hipotezde yer alan ana kütle parametresi arasında gözlenen

farklılıklara temel oluşturması ve farklılıkların tesadüfen mi oluştuğu yoksa istatistiksel olarak önemli mi olduğu hakkında karar verirken esas alınmasıdır (Kalaycı, 2008: 67).

Kolmogorov-Smirnov (K-S) Normallik Varsayımı Testi

Verilere uygulanacak testlerin belirlenmesi sırasında normallik varsayımı testlerinin uygulanması önemlidir. Çünkü normal dağılım gösteren verilerde parametrik testlerin kullanılması, normal dağılım göstermeyen verilerde ise parametrik olmayan (non-parametrik) testlerin kullanılması gerekir. Bu non-parametrik testler, parametrik testlerin normal dağılım göstermeyen veri gruplarında uygulanabilecek karşılıklardır.

K-S testi yardımıyla bir örneklemden toplanan verilerin normal dağılım sergileyip sergilemediğini incelemek mümkündür (Altunışık vd., 2004: 185). Kolmogorov-Smirnov Testi, örneklem sayısı 30'dan büyük veri gruplarında kullanılır. Eğer örneklem sayımız 30'dan küçük olsaydı, Shapiro Wilk testine bakmamız gerekecekti.

K-S testine göre normallik dağılımında p (sig.) değeri 0,05 'ten büyük ise normallik varsayımı kabul edilir, aksi durumda yani p (sig.) değeri 0,05'ten küçük ise normallik varsayımı reddedilir. K-S testinin sıfır (H_0) ve karşıt (H_a) hipotezi aşağıda verilmiştir:

H_0 : Verilerin dağılımı normal dağılıma uyar.

H_a : Verilerin dağılımı normal dağılıma uymaz.

İstatistikî Analizler

Çalışmada kullanılacak analizler frekans analizleri, çapraz tablolar (değişkenler arasındaki ilişkileri gösteren tablolar) ve parametrik olmayan (non-parametrik) analiz teknikleridir. Aşağıda bunlarla ilgili özet bilgilendirmeler yer almaktadır.

Frekans analizi ve çapraz tablolar

Frekans analizi verilerin özetlenmesi ve anlaşılmasında yararlı bir yoldur. Hesaplamaları oldukça açıktır. Dağılımdaki tek tek değerler, her bir değere veya her bir yanıtı ya da her bir kategoriye yanıt verenlerin kaçının düştüğüne göre sıraya dizilir. Bu noktada mutlak değerler ve / veya yüzde değerler kullanılabilir. Sonuçlar tablolar,

grafikler veya histogramlar yardımıyla görülebilir. Yanıtların frekans analizleri dağılımın şekli hakkında da bilgi verir (Punch, 2005: 110).

Nicel araştırmalarda değişkenler arasındaki ilişkiler üzerinde durulmaktadır ve bu ilişkileri göstermek için pek çok yol geliştirilmiştir. Bunlardan birisi de çapraz tablolardır. Çapraz tablolar, iki farklı değişkenin birbiriyle çapraz halde değerlendirilmesidir. Çapraz tablolar aynı zamanda herhangi bir ölçüm düzeyindeki değişkenler için de kullanılır. Çapraz tablolardaki basit hesaplamalar bize karşılaştırmalara yaparak ki-kare (ilişki testi) istatistiğini özetleme imkanı sağlar (Punch, 2005: 111-112).

Parametrik olmayan (Non-parametrik) analiz teknikleri

Parametrik olmayan analiz teknikleri parametreye, belirli bir dağılıma ve varyansa dayanmadan işlemler yapan esnek istatistiksel yöntemlerdir (Özdamar, 2004: 449).

Parametrik olmayan analiz tekniklerinde nominal, ordinal veya normal dağılım göstermeyen sayısal veriler analiz edilebilir. Küçük örneklemelerde veya verilerin parametrik analizlerin varsayımlarına uygun olmadığı durumlarda parametrik olmayan analizler kullanılır (Kalaycı, 2008: 85).

Çalışmamızın ileriki aşamalarında ele alınarak değerlendirmeler yapabileceğimiz parametrik olmayan testler şunlardır: Kruskal-Wallis H Testi ve Spearman's Rank Order Korelasyonu. Çalışmamızda bu testlerin yapılabilmesi elde ettiğimiz verilerin normal dağılım göstermemesinin bir sonucudur. Anlamlı farklılıklar ve ilişkiler elde ettiğimiz non-parametrik testler ilgili başlıklar altında sunulacaktır.

Kruskal-Wallis H Testi (K-W H Testi), One-way Varyans Analizi olarak da bilinir ve One-way Varyans analizinin parametrik olmayan test alternatifidir. Bu test, üç veya daha fazla grubun karşılaştırılmasında kullanılır (Altunışık vd., 2004: 187; Özdamar, 2004: 494). Değerler sırası hale çevrilir ve her grup için sıralı ortalamalar karşılaştırılır. Bu test gruplar arası analizdir. Anlamlılık düzeyi 0,05'in altında olduğunda gruplar arasında anlamlı farklılıkların olduğu söylenebilir (Kalaycı, 2008: 106-108).

Spearman's Rank Order Korelasyonu, Pearson's korelasyon katsayısının parametrik olmayan test alternatifidir. Değişkenler arasındaki ilişkinin derecesinin

ortaya konulmasını sağlar. Korelasyon katsayısının anlamlılık düzeyi, örneklem büyüklüğünden etkilenmektedir. Küçük bir örnekte, (örneğin $N=30$) 0,05 alfa değerinden istatistiksel anlamlılığı olmayan çok kuvvetli olmayan bir korelasyon değeri elde edilebilir. Bununla birlikte büyük örneklerde ($N=100$ gibi) çok küçük korelasyon değerleri de anlamlı olabilir. Korelasyon katsayısı aralığı olarak 0,10 ile 0,29 aralığı ilişkinin düşük, 0,30 ile 0,49 aralığı ilişkinin orta derece ve 0,50 ile 1,00 aralığı ilişkinin yüksek olduğu aralık olarak kabul edilmektedir. Pozitif değerler direk yönlü doğrusal ilişkiyi; negatif değerler ise ters yönlü bir doğrusal ilişkiyi belirtir. Negatif korelasyonda, iki değişken arasında biri artarken diğeri azalan ters orantılı bir ilişki vardır. Negatif korelasyon katsayıları şöyledir: -0,29 ile -0,10 aralığı ilişkinin düşük, -0,10 ile -0,30 aralığı orta derece ve -0,30 ile -1,00 aralığı yüksek ilişki olarak kabul edilir. (Kalaycı, 2008: 111-112).

Kaynakça

- Abdioğlu, H. (2007). İşletmelerde kurumsal yönetim anlayışı kapsamında iç denetimin rolü ve İMKB-100 örneği, Yayınlanmamış Doktora Tezi, İstanbul: Marmara Üniversitesi.
- Abdioğlu, H. (2008). İşletmelerde kurumsal yönetim anlayışı kapsamında iç denetimin rolü: İMKB – 100 şirketleri üzerine ampirik bir araştırma, *Muhasebe Bilim Dünyası Dergisi*, 4: 185-208.
- Abdolmohammadi, M.J.; Burnaby, P. ve Hass, S. (2006). A review of prior common body of knowledge (CBOK) studies in internal auditing and an overview of the global CBOK 2006, *Managerial Auditing Journal*, 21 (8): 811-821.
- Abu-Musa, A.A. (2008). Information technology and its implication for internal auditing: an emprical study of Saudi organization, *Managerial Auditing Journal*, 23 (5): 438-465.
- Ağca, A. (2006). Sürekli denetim: denetimde bir devrim mi yoksa bir hayal mi?, *Muhasebe Bilim Dünyası Dergisi*, 8 (1): 63-78.
- Ağca, A. (2007). Üniversitelerimizde verilen denetim eğitiminin teknolojiye bağlı olarak değişen denetim olgusu ve denetçi profili karşısındaki durumu, *Muhasebe ve Denetime Bakış Dergisi*, 7 (22): 41-65.
- Ahmed, H.B. (2007). Information systems development and the changing role of internal audit, (Yüksek Lisans Tezi, University of Greenwich Business School Department of Accounting and Finance), <http://ssrn.com/abstract=1324159>.
- Ak, B. (2004). İç denetimin yönetim aracı olarak kullanılması, *Süleyman Demirel Üniversitesi, İktisadi ve İdari Bilimler Fakültesi Dergisi*, 9 (2): 353-358.
- Akgül, B.A. (2002). İç denetimde yeni yaklaşımlar, *Muhasebe Bilim Dünyası Dergisi*, 4 (3): 19-29.
- Akışık, O. İç kontrol sistemi ve bağımsız denetim içindeki yeri, *Muhasebe ve Denetime Bakış Dergisi*, 4 (14): 89-101.
- Aksoy, T. (2007). *Basel II ve iç kontrol*, Ankara SMMMO Yayın No: 53, Ankara: Başak Matbaası.
- Aktaş, R. (2009). *Bütünleşik sistemler ve muhasebe etkileşimi*, (1. baskı), Ankara: Detay Yayıncılık.

- Aktaş, R. ve Başcı, E.S. (2007). Elektronik ortamda finansal raporlamada genişleyebilir finansal raporlama dilinin (XBRL) kullanılması, *Muhasebe Bilim Dünyası Dergisi*, 9 (1): 39-60.
- Allegrini, M. ve D’Onza, G. (2003). İnternal auditing and risk assessment in large Italian companies: an emprical survey, *International Journal of Auditing*, 7: 191-208.
- Alptürk, E. (2008a). *Finans, muhasebe ve vergi boyutlarında iç denetim rehberi*, Ankara: Maliye ve Hukuk Yayınları.
- Alptürk, E. (2008b). *Elektronik denetim rehberi*, (1. baskı), İstanbul: Kurtiş Matbaacılık.
- Altunışık, R., Çoşkun, R., Bayraktaroğlu, S. ve Yıldırım, E. (2004). *Sosyal bilimlerde araştırma yöntemleri: SPSS uygulamalı*, (geliştirilmiş 3. baskı), Sakarya: Sakarya Kitabevi.
- Anameriç, H. (2005). Bilgi sistemleri ve yönetimde bilgi sistemlerinin kullanımı, *Bilgi çağı, bilgi yönetimi ve bilgi sistemleri*, Ed: Çoşkun Can Altan ve İstiklal Yaşar Vural, 1. Baskı, Konya: Çizgi Kitabevi.
- Anderson, U. (2003). Assurance and consulting services, *Research opportunities in internal auditing*, Ed.: Andrew D. Bailey Jr., Audrey A. Gramling and Sridhar Ramamoorti USA: The Institute of Internal Auditors Research Foundation.
- Anıl, D. (2006). Kontrol öz değerlendirme ve işletmelerin iç kontrol yapısının tespitine yönelik bir araştırma, Yayınlanmamış Doktora Tezi İstanbul: Marmara Üniversitesi.
- Arens, A.A.; Elder, R. J. ve Beasley, M.S. (2003). Auditing and assurance services: an integrated approach, (9. edition), New Jersey: Prantice Hall.
- Arslan, I. (2008). Kurumsal risk yönetimi, Maliye Bakanlığı Strateji Geliştirme Başkanlığı, <http://www.sgb.gov.tr/destekhizmetleri/Raporlar/Maliye%20Uzmanl%C4%B1%C4%9F%C4%B1%20Ara%C5%9Ft%C4%B1rma%20Raporlar%C4%B1/I%C5%9F%C4%B1lda%20ARSLAN.pdf> (Erişim tarihi: 10.12. 2010).
- Aslan, B. (2010). Bir yönetim fonksiyonu olarak iç denetim, *Sayıştay Dergisi*, 77: 63-86.

- Ataman, Ü., Hacırüstemoğlu, R. Ve Bozkurt, N. (2001). *Muhasebe denetimi uygulamaları*, İstanbul: Alfa Yayınları.
- Ay, M. (2007). Bilişim teknolojilerinin muhasebe denetiminde kullanılması ve türkiye’de faaliyet gösteren bağımsız denetim firmalarında bilişim teknolojilerinin kullanım düzeyi üzerine bir araştırma, *Selçuk Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi*, 7 (14): 271-290.
- Bağcı, B. (2009). Bilgi teknolojileri risk yönetimine genel bakış, <http://www.denetimnet.net/Pages/bilgiteknolojileririskyonetimi.aspx> (Erişim tarihi: 15.09.2010).
- BASEL Komite (2000). Bankalarda iç denetim ve bankacılık gözetim otoritesinin iç ve dış denetçilerle ilişkisi, *Bankacılar Dergisi*, 34: 98-115.
- Başpınar, A. (2006). Kamuda iç denetim ve merkezi uyumlaştırma fonksiyonu, *Maliye Dergisi*, 151: 23-42.
- Bedard, J.C. ; Graham, L. ve Jackson, C. (2005). Information systems risk and audit planning, *International Journal of Auditing*, 9: 147-163.
- Bensghir, T. K. (1996). *Bilgi teknolojileri ve örgütsel değişim*, (1. baskı), Ankara: TODAİE Yayın No: 274.
- Biçer, A.A. (2006). İç kontrol sisteminin etkinliğini sağlamada iç denetimin rolü ve bir uygulama, Yayınlanmamış Yüksek Lisans Tezi, İstanbul: Marmara Üniversitesi.
- Bierstaker, J.L.; Burnaby, P. ve Thibodeau, J. (2001). The impact of information technology on the audit process: an assessment of the state of the art and implications for the future, *Managerial Auditing Journal*, 16 (3): 159-164.
- Bozkurt, N. (2000). Analitik inceleme prosedürleri ve iç denetim, *MÖDAV Muhasebe Bilim Dünyası Dergisi*, 3(3): 1-8.
- Bozkurt, N. (2010). *Muhasebe denetimi*, (5. baskı), İstanbul: Alfa Yayınları.
- Brody, R. G. ve Lowe, D. J. (2000). The new role of the internal auditor: implications for internal auditor objectivity, *International Journal of Auditing*, 4: 169-176.
- Can, V. ve Uyar, S. (2010). *İşletmelerde faaliyet denetimi*, (1.baskı), Ankara: Nobel Yayınları.
- Coderre, D. (2009). *Internal auditing: efficieny through automation*, New Jersey: John Wily & Sons, Inc.

- Çatıkkaş, Ö. ve Yurtsever, G. (2009). Bankacılık sektöründe bilgisayar destekli denetim, *Vergi Sorunları Dergisi*, 32 (251) : 179-192.
- Çetiner, E. ve Erol, M. (2007). Kurumsal yönetim ve kurumsal yönetimin aile şirketlerinde uygulama düzeyinin belirlenmesine yönelik ampirik bir çalışma, *Muhasebe ve Denetime Bakış Dergisi*, 6 (21): 17-33.
- Daştan, A. (2008). *Bilgi ve eğitim teknolojilerinde yaşanan gelişmelerin muhasebe eğitimine etkisi: Türkiye değerlendirmesi*, Ankara: SPK Yayın No: 209.
- Daştan, A. (2010). Kurumsal yönetim ilkeleri ve kurumsal muhasebe etkileşimi, *Bankacılar Dergisi*, 72: 3-18.
- Demir, B. (2005). Muhasebe bilgi sistemlerinde bilgi güvenliği, *Muhasebe ve Finansman Dergisi*, 26: 147-156.
- Demir, V. ve Bahadır, O. (2006). Kurumsal kaynak planlaması (ERP) sistemlerinin maliyetlere ve işletme performansına etkileri, *Muhasebe Bilim Dünyası Dergisi*, 8 (3): 57-70.
- Demirbaş, M. (2005). İç kontrol ve iç denetim faaliyetlerinin kapsamında meydana gelen değişimler, *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 4 (7): 167-188.
- Demirbaş, M. (2008). Public Company Accounting Oversight Board'a göre iç kontrol birimlerinin faaliyetlerinde yönetimin sorumlulukları ve denetçi raporları, *Muhasebe Bilim Dünyası Dergisi*, 10 (4): 37-66.
- Dinç, E. ve Varıcı, İ. (2008). Muhasebe bilgi sisteminin kurumsallaşma düzeyine etkisi: sanayi işletmeleri üzerine bir araştırma, *Afyon Kocatepe Üniversitesi İ.İ.B.F. Dergisi*, 10 (1): 67-85.
- Dinç, E. ve Abdioğlu, H. (2009). İşletmelerde kurumsal yönetim anlayışı ve muhasebe bilgi sistemi ilişkisi: İMKB-100 şirketleri üzerine ampirik bir araştırma, *Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 12 (21): 157-184.
- Elitaş, C. (2004). İç denetçinin verdiği raporların üst yönetim tarafından değerlendirilmesi, *İSMMMO Mali Çözüm Dergisi*, 69: 220-238.
- Erdem, A.O. ve Efiloğlu, Ö. (2002). Bilgi çağında elektronik ticaret, VIII. Türkiye'de *İnternet Konferansı'nda sunulan bildiri*, <http://inet-tr.org.tr/inetconf8/bildiri/71.doc>, (Erişim tarihi: 24.04.2010).

- Erdoğan, M. (1998). Sistem kavramı ve bilgi işleme; bilgisayarlarla bilgi işleme sistemleri, *Muhasebe bilgi sistemi*, Ed. Kerim Banar, Eskişehir: T.C. Anadolu Üniversitesi Yayını No: 963, Açıköğretim Fakültesi Yayını No: 532.
- Erdoğan, M. (2006). *Denetim: kavramsal ve teorik yapı*, (güncelleştirilmiş 3. baskı), Ankara: Maliye ve Hukuk Yayınları.
- Erdoğan, N. (2004). Denetimde önemlilik, risk ve kanıt kavramları ve çalışma kağıtları, *Muhasebe denetimi ve mali analiz*, Ed. Ferruh Çömlekçi, Eskişehir: T.C. Anadolu Üniversitesi Yayını No: 1585, Açıköğretim Fakültesi Yayını No: 839.
- Ergin, H.; Sevim, Ş. ve Eliuz, A. (2008). Kurumsal yönetimin ögesi olarak denetim komitesinin etkinliği ve İMKB'ye kayıtlı şirketlerde bir araştırma, *Muhasebe ve Denetime Bakış Dergisi*, 8 (25): 1-21.
- Ergin, H.; Çetinoğlu, T. ve Kurnaz, N. (2008). Risk odaklı iç denetim: türkiye'nin 500 büyük sanayi işletmesinde ampirik bir değerlendirme, *Muhasebe ve Denetime Bakış Dergisi*, 8 (26): 17-36.
- Erhan, D. U. (2009). BDDK tebliği çerçevesinde “bilgi sistemleri denetimi” kavramının irdelenmesi ve güncel gelişmeler, *Muhasebe ve Denetime Bakış Dergisi*, 8 (27): 91-110.
- Erkuş, H. (2008). *XBRL genişletilebilir işletme raporlama dili*, Ankara: Gazi Kitabevi.
- Erol, M.; Atmaca, M. ve Şahin, L. (2004). Bilişim teknolojilerindeki gelişmelerin muhasebe meslek elemanlarının (SM-SMMM-YMM) mesleki faaliyetlerine olan etkileri ve ampirik bir çalışma, *Muhasebe ve Denetime Bakış Dergisi*, 4(13): 31-44.
- Ertaş, F. Ç. ve Güven, P. (2008). Bilgi teknolojilerinin denetim sürecine etkisi, *Muhasebe ve Finansman Dergisi*, 37: 50-59.
- Fraser, I. ve Henry, W. (2007). Embedding risk management structures and approaches, *Managerial Auditing Journal*, 22 (4): 392-409.
- Garbellotto, G. ve Hannon, N. (2006). Why XBRL is a business reporting language, *Strategic Finance*, 86 (11): 57-61.
- Gegin, E. (2010). Günümüz iş dünyası için örnek bir iç denetim modeli, *İç Denetim Dergisi*, 25: 16-21.

- Gerekan, B. ve Pehlivan, A. (2009). Türkiye’deki kamu kurumlarında kurulabilecek denetim komitelerinin kamu iç denetim elemanlarının bakış açısıyla değerlendirilmesi, *Muhasebe Bilim Dünyası Dergisi*, 11 (1): 123-148.
- Griffiths, P. (2005). *Risk-based auditing*, England: Gower.
- Gökçen, H. (2007). *Yönetim bilgi sistemleri*, Ankara: Palme Yayıncılık.
- Gönen, S. (2009). İç kontrol sisteminin unsurlarından kontrol ortamının incelenmesine yönelik bir araştırma, *Muhasebe Bilim Dünyası Dergisi*, 11 (1): 189-217.
- Gönülaçar, Ş. (2007). İç denetimde hedefler ve beklentiler, (Mali Hukuk Dergisi 130. ve 131. sayılarda yayınlanmıştır),
www.kidder.org.tr/dosyalar/makaleler/icdenetim_sgonulacar.pdf (Erişim tarihi: 10.09.2010).
- Güneş, İ. (2002). Elektronik ticaretin vergilendirilmesinin uluslararası boyutu, VIII. *Türkiye’de İnternet Konferansı’nda sunulan bildiri*,
<http://inet-tr.org.tr/inetconf8/bildiri/20.doc> (Erişim tarihi: 24.04.2010).
- Gürdal, K. (2004). Yeni ekonomi kavramı ve yeni muhasebe anlayışı, *Muhasebe ve Denetim Bakış Dergisi*, 4 (13): 87-110.
- Güredin, E. (2007). *Denetim ve güvence hizmetleri*, (11. baskı), İstanbul: Arıkan Basım Yayın Dağıtım.
- Hass, S.; Abdolmohammadi, M.J. ve Burnaby, P. (2006). The americas literature review on internal auditing, *Managerial Auditing Journal*, 21 (8): 835-844.
- Hepkul, A. (2008). İnternet ve yeni bilgi teknolojisi altyapısı, *Yönetim bilgi sistemi*, Ed. Mehmet Şahin, Eskişehir: T.C. Anadolu Üniversitesi Yayını No: 1471, Açıköğretim Fakültesi Yayını No: 784.
- İç Denetim Koordinasyon Kurulu (2007). BT denetim kılavuzu,
<http://www.bumko.gov.tr/DENETIM/Genel/BelgeGoster.aspx?F6E10F8892433CFFAAF6AA849816B2EF21AE406D1C1546DE> (Erişim tarihi: 23.03.2010).
- İlter, K. (2007). Bilgi sistemleri perspektifinden kurumsal kaynak planlaması: etkileri ve değerler, *İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 6 (11): 1-20.
- Kağnıcıoğlu, H. (2008). Çağdaş bilgi sistemleri ve dijital işletmeler, *Yönetim bilgi sistemi*, Ed. Mehmet Şahin, Eskişehir: T.C. Anadolu Üniversitesi Yayını No: 1471, Açıköğretim Fakültesi Yayını No: 784.

- Kahyaoğlu, S. B. (2010). Bir güvence modeli olarak iç denetim mesleği, *KPMG Gündem: Risk Yönetimi ve Uyum Hizmetleri Özel Sayısı*, 1 (Ocak-Mart 2010): 13-16.
- Kalaycı, Ş. (2008). *SPSS uygulamalı çok değişkenli istatistik teknikleri*, Ankara: Asil Yayın Dağıtım.
- Kalite Derneği (2005). *Özdeğerlendirme yöntemleri ve uygulama rehberi*, EFQM–KALDER, İstanbul.
- Karacaer, S. ve İbrahimoglu, N. (2003). İşletme yönetiminde muhasebe bilgi sistemi, iç kontrol, verimlilik ilişkisi ve önemi, *Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 21(1): 211-228.
- Karadal, H. (2007). Bilişim teknolojilerinin yönetim sürecine etkileri üzerine bir araştırma, *Selçuk Üniversitesi İktisadi ve İdari Bilimler Fakültesi Sosyal ve Ekonomik Araştırmalar Dergisi*, Emin Kayar Özel Sayısı 9 (7): 211-226.
- Karagül, A.A. (2005). Bilgi yönetimi, kurumsal kaynak planlaması ve muhasebe bilgi sistemi ilişkisi çerçevesinde muhasebe eğitimi, *XXVI. Türkiye Muhasebe Eğitimi Sempozyumu Bildiri Kitabı*, ss.59-87.
- Kepekçi, C. (1982). *İşletmelerde iç kontrol sisteminin etkinliğini sağlamada iç denetimin rolü*, Eskişehir: Eskişehir İktisadi ve Ticari İlimler Akademisi Yayınları No: 251/171.
- Kishalı, Y. ve Pehlivanlı D. (2006). Risk odaklı iç denetim ve İMKB uygulaması, *Muhasebe ve Finansman Dergisi*, 30: 75-87.
- Korkmaz, U. (2007). Kamuda iç denetim-I, *Bütçe Dünyası Dergisi*, 2 (25): 4-15.
- Kurnaz, N. (2007). Kurumsal yönetim ekseninde risk odaklı iç denetim: Türkiye'nin 500 büyük sanayi işletmesinde risk odaklı iç denetim uygulama analizi, *Yayınlanmamış Doktora Tezi*, Kütahya: Dumlupınar Üniversitesi.
- Kurnaz, N. ve Çetinoğlu, T. (2010). *İç denetim: güncel yaklaşımlar*, (1 baskı), Kocaeli: Umuttepe Yayınları.
- Liang, D., Lin, F. ve Wu, S. (2001). Electronically auditing EDP systems with the support of emerging information technologies, *International Journal of Accounting Information Systems*, 2: 130-147.
- Majdalawieh, M. ve Zaghloul, I. (2009). Paradigm shift in information systems auditing, *Managerial Auditing Journal*, 24 (4): 352-367.

- McCollum, T. ve Salierno, D. (2003). Choosing the right tools, *Internal Auditor*, 60 (4): 32-43.
- Memiş, M.Ü. (2006). İç denetimin yönetim fonksiyonlarının yerine getirilmesindeki rolü: türkiye’de büyük işletmeler üzerinde bir saha araştırması, Yayınlanmamış Doktora Tezi, Adana: Çukurova Üniversitesi.
- Memiş, M.Ü. (2007). Türkiye’deki iç denetim profilinin belirlenmesine ilişkin bir araştırma, *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 16 (1): 461-478.
- Memiş, M.Ü. (2008). Etkin ve başarılı bir iç denetim için gerekli koşullar, *İSMMM Mali Çözüm Dergisi*, 85: 75-91.
- Mock, T.J. ve Turner, J.L. (2005). Auditor identification of fraud risk factors and their impact on audit programs, *International Journal of Auditing*, 9 (1): 59-77.
- Moeller, R. ve Witt, H.N. (1999). *Brink’s modern internal auditing*, USA: John Willey & Sons Inc.
- Moeller, R. (2004). *Sarbanes Oxley and the new auditing rules*, New Jersey: John Wiley & Sons, Inc.
- Murthy, U.S. ve Groomer, S.M. (2004). A continuous auditing web services model for XML-based accounting systems, *International Journal of Accounting Information Systems*, 5: 139-163.
- Nakilcioğlu, İ. H. (2002). İtranetlerin çağdaş bilişim teknolojileri içindeki yeri ve kurumsal yapı üzerindeki etkileri, *VIII. Türkiye’de İnternet Konferansı’nda sunulan bildiri*, <http://inet-tr.org.tr/inetconf8/bildiri/114.doc> (Erişim tarihi: 24.04.2010).
- Nastase, P. ve Nastase, F. (2007). İnternet denetim teknolojilerinin balkan ülkelerinde kullanılması, *Muhasebe ve Finansman Dergisi*, 34: 41-51.
- Oktay, E.; Balkanlı, A.O. ve Salepçioğlu, A. (2004). Bilgi toplumunda yeni ekonomi ve e-dönüşüm stratejileri, 3. *Ulusal Bilgi, Ekonomi ve Yönetim Kongresi*, Eskişehir, ss. 155-166
- Öğüt, A. (2003). *Bilgi çağında yönetim*, 2. Baskı, Ankara: Nobel Yayın Dağıtım.
- Ömürbek, V. (2003). Kurumsal kaynak planlamasında muhasebe bilgi sisteminin rolü: gıda sektöründe uygulama, Yayınlanmamış Doktora Tezi, Isparta: T.C. Süleyman Demirel Üniversitesi.

- Ömürbek, N. ve Altın, F. G. (2008). Sigortacılık sektöründe bilgi teknolojileri uygulamasına ilişkin bir araştırma, *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 13 (3): 105-127.
- Özbay, S. ve Akyazı, S. (2004). *Elektronik ticaret (e-ticaret)*, (1. baskı), Ankara: Detay Yayıncılık.
- Özdamar, K. (2004). *Paket programlar ile istatistiksel veri analizi-1*, (genişletilmiş 5. baskı), Eskişehir: Kaan Kitabevi.
- Özer, A. (2008). Risk odaklı iç denetim ve bir uygulama, Yayınlanmamış Yüksek Lisans Tezi, İstanbul: Marmara Üniversitesi.
- Özeren, B. (2000). *İç denetim, standartları ve mesleğin yeni açılımları*, Sayıştay Araştırma/İnceleme/Çeviri Dizisi: 8, Ankara.
- Özkan, Y. (2008). 5018 sayılı kamu mali yönetimi ve kontrol kanunu kapsamında iç denetimin değerlendirilmesi ve öneriler, Yayınlanmamış Doktora Tezi, İstanbul: Marmara Üniversitesi.
- Özoğlu, B; Mercan, C. ve Çakıroğlu, S. (2010). Bir güvence ve danışmanlık hizmeti: iç denetim, (1. baskı), İstanbul Büyükşehir Belediyesi İç Denetim Birimi Başkanlığı Yayınları No: 1, İstanbul: Ayhan Matbaası.
- Parlakkaya, R. (2005). Elektronik ticaret ve muhasebe uygulamalarına etkileri, *Selçuk Üniversitesi Karaman İktisadi ve İdari Bilimler Fakültesi Dergisi*, 2 (5): 168-175.
- Pathak, J. ve Lind, M. (2006), Empirical assessment of effective e-commerce audit judgment, <http://ssrn.com/abstract=977851> (Erişim tarihi: 09.09.2010).
- Pehlivanlı, M. (2010). *Modern iç denetim: güncel iç denetim uygulamaları*, 1. Baskı, İstanbul: Beta Yayınları.
- Pekdemir, R. ve Önal, M.M. (1999). Bilgi teknolojisindeki gelişmelerin muhasebe mesleğine etkileri, *İ.Ü. İşletme Fakültesi İşletme İktisadi Enstitüsü Dergisi: Yönetim*, 10 (34): 7-14.
- Pekdemir, R. ve Selvi, Y. (2002). Teknolojik gelişmelerin denetimde yarattığı yeni fırsatlar, 17. Türkiye Muhasebe Kongresi Bildiriler Kitabı (10-12 Ekim 2002), Ankara: TÜRMOB Yayınları.
- Punch, K.F. (2005). *Sosyal araştırmalara giriş: nicel ve nitel yaklaşımlar*, (Çev. D. Bayrak, H.B. Arslan ve Z. Akyüz), Ankara: Siyasal Kitabevi.

- Rao, V., Cerpa N. ve Jamieson, R. (2001). A comparison of online electronic commerce assurance service providers in Australia, *14th Bled Electronic Commerce Conference Bled*, Slovenia, 25-26 June, ss. 520-537.
- Rezaee, Z.; Elam, R. ve Sharbatoghlie, A. (2001). Continuous auditing: the audit of the future, *Managerial Auditing Journal*, 16 (3): 150-158.
- Sawyer, L. B.; Dittenhofer, M.A. ve Scheiner, J.H. (2005). *Sawyer's internal auditing: the practice of modern internal auditing*, 5th Ed., USA: Institution of Internal Auditing.
- Saygılı, A.T. (2005). Bilgisayar teknolojisi ve muhasebe denetimi, *Mevzuat Dergisi*, 8 (91), <http://www.mevzuatdergisi.com/2005/07a/03.htm> (Erişim tarihi: 02.12.2010).
- Saygılı, A.T. (2007). Hedef maliyetleme ve diğer stratejik yönetim araçları, *E-Akademi: Hukuk, Ekonomi ve Siyasal Bilimler Aylık İnternet Dergisi*, 60, <http://www.e-akademi.org/makaleler/atsaygili-2.htm> (Erişim tarihi: 14.06.2011).
- Selim, G. ve McNamee, D. (1999). Risk management and internal auditing: what are the essential building blocks for a successful paradigm change?, *International Journal of Auditing*, 3: 147-155.
- Selimoğlu, S. (2006a). Denetim olgusunun kurumsal kaynak planlaması (ERP) sistemleriyle bütünleştirilmesi, *1. Uluslararası Muhasebe Denetimi Sempozyumu ve 7.Türkiye Muhasebe Denetimi*, İSMMMO Yayın No: 58, ss. 277-294.
- Selimoğlu, S. (2006b). Sürekli denetim ve raporlama aracı olarak: ACL ve Türkiye’de ACL kullanan işletmelere yönelik bir araştırma, *Muhasebe Bilim Dünyası Dergisi*, 8 (4): 147-173.
- Selvi, Y.; Türel, A. ve Şenyiğit, B. (2006). Elektronik bilgi ortamlarında muhasebe denetimi, *1. Uluslararası Muhasebe Denetimi Sempozyumu ve 7.Türkiye Muhasebe Denetimi*, İSMMMO Yayın No: 58, ss. 301-315.
- Senft, S. ve Frederick, G. (2009). *Information technology control and audit*, 3. Ed., USA: CRC Press.
- Sevim, A. (2005). Dijital uygulamaların muhasebe eğitimi üzerine etkileri, *XXVI. Türkiye Muhasebe Eğitimi Sempozyumu Bildiri Kitabı*, Muğla, ss. 89-105.

- Sevim, A. (2008). Dijital girişimler, *Yönetim bilgi sistemi*, Ed. Mehmet Şahin, Eskişehir: T.C. Anadolu Üniversitesi Yayını No: 1471, Açıköğretim Fakültesi Yayını No: 784.
- Sevim, A. (2009). *Dijital muhasebe*, Eskişehir: T.C. Anadolu Üniversitesi Yayınları No: 1903, İktisadi ve İdari Bilimler Fakültesi Yayınları No: 208.
- Sevimli, A. (2009). Sürekli denetim: dünü anla, bugünü değerlendir, geleceği denetle, *İç Denetim Dergisi*, 24: 30-33.
- Sezal, L. (2006). Banka işletmelerinde etkin bir iç denetim ve risk yönetim sisteminde karşılaşılan sorunlar ve çözüm önerileri, Yayınlanmamış Doktora Tezi, Adana: Çukurova Üniversitesi.
- Soltani, B. (2007). *Auditing: An international approach*, FT/Prentice Hall.
- Spira, L. F. ve Page, M. (2003). Risk management: the reinvention of internal control and the changing role of internal audit, *Accounting, Auditing & Accountability Journal*, 16 (4): 640-661.
- Sürmen, Y. ve Daştan, A. (2007). “The relationship between the historical develeopment of accounting information system and its applications and information technology”, *Edirne The Balkan Countries 1.st International Conference On Accounting And Auditing*, İstanbul: Avcıol Basım, ss. 218-232.
- Şahinaslan, E. Kantürk, A. ve Şahinaslan, Ö. (2010). Bilgi teknolojileri süreçlerinin standartlara dayalı modellenmesi, *Akademik Bilişim Konferansı*, Muğla: Muğla Üniversitesi, <http://www.ab.org.tr/ab10/bildiri/75.pdf> (Erişim tarihi: 10.06.2011).
- Şirin, M. (2006). Denetimde kanıt teorisi ve gelişimi, *Sayıştay Dergisi*, 61: 23-36
- Tektüfekçi, F. (2008). İç denetimin değişen rolü: değer yaratmak, *MÖDAV Muhasebe Bilim Dünyası*, 10 (2): 79-108.
- The Institute of Internal Auditors (IIA) (2005). *Continuous auditing: Implications for assurance, monitoring, and risk assessment*, A Summary of The IIA's Global Technology Audit Guide, ACL Services Ltd.
- Türkiye İç Denetçiler Enstitüsü (2008). *Uluslararası iç denetim standartları: mesleki uygulama çerçevesi*, Türkiye İç Denetim Enstitüsü Yayınları No: 4, Deloitte: İstanbul.

- Toraman, C. (2002). Gelişen bilgi teknolojilerinin denetime olan etkisi, *İSMMMO Mali Çözüm Dergisi*, 61, <http://www.ismmmo.org.tr/htmldergikonu.asp?id=8550&did=64&dad=MALİ> ÇÖZÜM DERGİSİ Sayı:61 EKİM KASIM ARALIK 2002, (Erişim tarihi: 10. 07. 2009).
- Toraman, C. (2008). Bilişim Teknolojileri ve meslek mensuplarının eğitimi üzerindeki etkileri, *Bilgi Çağında Muhasebe Eğitimi*, Ed.: Fevzi Sürmeli, Yılmaz Benligiray ve Adnan Sevim, *XXVII. Türkiye Muhasebe Eğitimi Sempozyumu*, Eskişehir: Anadolu Üniversitesi Yayınları: 1808.
- Tuan, K. ve Memiş, M.Ü. (2007). İç denetimin yönetim fonksiyonlarının yerine getirilmesindeki rolü, *Muhasebe ve Finansman Dergisi*, 35: 87-99.
- Tuan, A.K. ve Sağlar, J. (2004). İç Denetçinin Örgüt İçindeki Yerinin Denetim Faaliyetleri Açısından Önemi, *Muhasebe ve Denetime Bakış Dergisi*, 11: 1-16.
- Türedi, H. ve Dinç, E. (1997). Bilgisayarlı muhasebe sisteminde denetim, *Yaklaşım Dergisi*, 50, <http://www.yaklasim.com/mevzuat/dergi/makaleler/199702986.htm> (Erişim tarihi 02.12.2010).
- Uyar, S. (2006a). Bilgi teknolojisindeki gelişmelerin muhasebe mesleğine etkileri, *Bilgi ekonomisi*, Ed.: Nihal Kargı, Bursa: Ekin Kitabevi.
- Uyar, S. (2006b). Risk odaklı denetim, <http://www.muhasse4betr.com/yazarlarimiz/suleyman/004/> (Erişim tarihi: 30.11.2010)
- Uyar, S. ve Ünlüsoy, E. (2007). Uluslararası eğitim standartları (IESS) ve eğitim uygulamaları açıklamaları (IEPSS) çerçevesinde bilgi teknolojileri ile muhasebe ve denetim ilişkisi, *İZSMMO Türkiye Muhasebe Standartları Sempozyumu-XI*, Antalya.
- Uyar, S. (2009). *İç kontrol ve iç denetim: 5018 sayılı kanun açısından değerlendirme*, Ankara: Gazi Kitabevi.
- Uzay, Ş. (1999). *İşletmelerde iç kontrol sistemini incelemenin bağımsız denetim karar sürecindeki yeri ve türkiye'deki denetim firmalarına yönelik bir araştırma*, Ankara: Sermaye Piyasası Kurulu Yayın No: 132.
- Uzay, Ş. (2003). İç denetimin geleceği ve yeni eğilimler, 22. *Türkiye Muhasebe Eğitim Sempozyumu*, Antalya.

- Uzun, A.K. (1999). Organizasyonlarda iç denetim fonksiyonu ve önemi, *Active Bankacılık ve Finans Dergisi*, 6: 1-4.
- Weidenmier, M.L. ve Ramamoorti, S. (2006). Research opportunities in information technology and internal auditing, *Journal of Information System*, 20 (1): 205-219.
- Whittington, O.R. ve Pany, K. (2004). Principle of auditing and other assurance services, (14. ed.) New York: McGraw Hill / Irwin.
- Yereli, A. N. (2007). Muhasebe bilgi sistemlerinin risk yönetimine yönelik bir araştırma, *Muhasebe ve Denetime Bakış Dergisi*, 7 (23), 15-31.
- Yılcı, M. (2001). Muhasebe bilgi sistemi, iç kontrol ve verimlilik üçgeni, *MÖDAV Muhasebe Bilim Dünyası Dergisi*, 3 (3): 37-50.
- Yılcı M. (2003). Denetim komitesinin iç denetimin etkinliğini sağlamadaki ve hileleri önlemedeki rolü, *Muhasebe ve Denetime Bakış Dergisi*, 3 (8): 23-33.
- Yılcı, M. (2006). *İç denetim: Türkiye'nin 500 büyük sanayii işletmesi üzerine bir araştırma*, 2. Baskı, Ankara: Nobel Yayın Dağıtım.
- Yurdağül, Ö. (2010). *Denetim, güvence ve kontrol uzmanlarının bt standartları, rehberleri, araçları ve teknikleri*, USA: ISACA.
- Yürütücü, A. (2002). E-ticaret ve bilgi toplumundaki yapılaşma süreci, *VIII. Türkiye'de İnternet Konferansı'nda sunulan bildiri*, <http://İnet-Tr.Org.Tr/İnetconf8/Bildiri/1.Doc> (Erişim tarihi: 24.04.2010).
- Zaim, H. (2005). *Bilginin artan önemi ve bilgi yönetimi*, İstanbul: İşaret Yayınları:106.
- Zakaria, Z.; Selvaraj, S.D. ve Zakaria, Z. (2006). Internal auditors: their role in the institutions of higher education in Malaysia, *Managerial Auditing Journal*, 21 (6): 892-904.
- Zhang, Y.; Zhou, J. ve Zhou, N. (2007). Audit committee quality, auditor independence, and internal control weakness, *Journal of Accounting and Public Policy*, 26: 300-327.
- _____ Benchmarking (Kıyaslama) Nedir?, <http://www.yildiz.edu.tr/~palcan/word%20dokuman/BenchmarkingSON%20HAL.doc> (14.06.2011).
- _____ Audit and assurance services, http://www.bic.ac/assets/3-1int_syllabus.pdf (01.09.2011)