

T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
MUHASEBE BİLİM DALI

DOKTORA TEZİ

**İÇ DENETİMDE BİLGİ TEKNOLOJİLERİ VE SİBER
GÜVENLİK: BORSA İSTANBUL ŞİRKETLERİNDE
BİR İNCELEME**

Nevzat GÜNGÖR
2502170237

TEZ DANIŞMANI
Prof. Dr. Fatma Lerzan KAVUT

İSTANBUL- 2021

ÖZ

İÇ DENETİMDE BİLGİ TEKNOLOJİLERİ VE SİBER GÜVENLİK: BORSA İSTANBUL ŞİRKETLERİNDE BİR İNCELEME

NEVZAT GÜNGÖR

İşletmelerin siber güvenlik faaliyetleri, işletme yönetiminin sorumluluğundadır. Siber güvenlik faaliyetleri icra edilirken işletme yönetimlerinin en büyük destekçisi şüphesiz iç denetim birimleridir.

Bu çalışmanın üç temel amacı bulunmaktadır. Çalışmanın ilk amacı Türkiye’de faaliyet gösteren halka açık işletmelerin siber güvenlik faaliyetleri seviyelerini tespit etmek ve siber güvenlik düzeylerinin işletmelerin özelliklerine göre farklılaşıp farklılaşmadığını belirlemektir. İkinci amacı ise işletmelerde üçüncü savunma hattı olarak görev yapan iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliğini belirlemek ve iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliği işletmelerin özelliklerine göre farklılaşıp farklılaşmadığını tespit etmektir. Bu çalışmanın son amacı ise işletmelerin siber güvenlik faaliyetleri seviyeleri ile iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliği arasında ilişki olup olmadığını belirlemektir.

Bu amaçla gerçekleştirilen ankete Borsa İstanbul’a kote halka açık işletmelerde faaliyet gösteren 222 iç denetçileri katılmıştır. Yapılan analiz sonucunda halka açık işletmelerin siber güvenlik faaliyetleri seviyeleri belirlenmiş ve siber güvenlik düzeylerinin işletmelerin özelliklerine göre farklılaştığı sonucuna ulaşılmıştır. Ayrıca iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliğini tespit edilmiş ve iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliği işletmelerin özelliklerine göre farklılaştığı belirlenmiştir. Son olarak işletmelerin siber güvenlik faaliyetleri seviyeleri ile iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliği arasında çok güçlü ve anlamlı bir ilişki olduğu sonucuna ulaşılmıştır.

Anahtar Kelimeler: İç Denetim, Bilgi Teknolojileri, Siber Güvenlik, Siber Güvenlik Yönetiřimi, Üçlü Savunma Hattı



ABSTRACT

INFORMATION TECHNOLOGIES AND CYBERSECURITY IN INTERNAL AUDIT: A REVIEW IN BORSA ISTANBUL COMPANIES

NEVZAT GÜNGÖR

Cybersecurity activities are under the responsibility of business management. When cybersecurity activities are carried out, the biggest supporters of business management are undoubtedly internal audit departments.

There are three main purposes of this study. The first aim of the study is to determine the levels of cybersecurity activities of public companies operating in Turkey and to determine whether the levels of cyber security differ according to the characteristics of companies. The second aim is to determine the effectiveness of the cybersecurity activities of the internal audit departments, which serve as the third line of defense in companies, and to determine whether the cyber security activities of the internal audit units differ according to the characteristics of the companies. The final aim of this study is to determine whether there is a relationship between the levels of cybersecurity activities of companies and the effectiveness of cybersecurity activities of internal audit units.

222 internal auditors operating in public companies listed on Borsa Istanbul participated in the survey conducted for this purpose. As a result of the analysis, cybersecurity activities levels of public companies were determined, and it was concluded that cyber security levels differ according to the characteristics of the companies. In addition, the effectiveness of the activities of the internal audit units regarding cybersecurity was determined and it was determined that the effectiveness of the activities of the internal audit units regarding cybersecurity differ according to the characteristics of the companies. Finally, it has been concluded that there is a very strong and significant relationship between the cybersecurity activities levels of companies and the effectiveness of the activities of internal audit units regarding cybersecurity.

Keywords: Internal Audit, Information Technologies, Cybersecurity, Cybersecurity Governance, Triple Line of Defense.



ÖNSÖZ

Günümüzde işletmeler, bilgisayarlara, ağlara, programlara, uygulamalara, sosyal medyaya ve verilere artan bağımlılıkları nedeniyle siber tehditlere karşı giderek savunmasız hale gelmektedir. Güvenlik ihlalleri, işletmeleri ve paydaşlarını finansal açıdan ve itibar açısından olumsuz etkileyebilmektedir. İşletme dışındaki kullanıcıların bilgilere erişebilirliği bilgi teknolojileri risklerini arttırmaktadır. Özellikle işletmelerin hali hazırdaki bilgi sistemlerine güvenmesi ve gelişen yeni teknolojiler göz önüne alındığında, geleneksel bilgi teknolojileri süreçleri ve uygulama kontrolleri siber güvenlik konusunda güvence sağlamak için yetersiz kalmaktadır.

İşletmeler varlıklarını korumak için; hile yolsuzluk, casusluk, sabotaj, doğal afetler vb. tehdit ve tehlikelere karşı koymanın yanı sıra virüs, casus ve kötü yazılım, bilgisayar korsanları gibi siber tehditlere karşı da tetikte olmak durumundadır. Bu siber saldırıları ve tehditleri ortadan kaldırmak siber güvenliği sağlamakla mümkündür.

Günümüzde bilgi teknolojilerinde meydana gelen gelişmelerin ardından iç denetim birimlerinin de görev alanları genişlemiştir. Söz konusu teknolojik gelişmeler işletme risklerini ve risklere karşı alınacak önlemleri tamamen değiştirmiştir. İç denetim birimi kendilerine tanınan bağımsızlık ve tarafsızlık özelliklerinin de desteğiyle; işletme süreçlerinin iyileştirilmesi, işletmeye değer kazandırma ve işletme risklerini önleme konularında önemli roller edinmiştir. İç denetim üstlenmiş olduğu bu misyonla hem yönetsel kontrol hem de diğer işletme faaliyetleri kapsamında önemli bir konum kazanmıştır ve faaliyetleri işletmenin süreçlerine doğrudan etki eder bir hal almıştır.

İç denetim birimi, üst yönetim ile yönetim kuruluna yönetişim, risk yönetimi ve iç kontroller konusunda bağımsız ve objektif güvence sağlamaktadır. Ayrıca iç denetim, işletme yönetimi ve bilgi teknolojileri birimlerince gerçekleştirilen faaliyetlerin siber güvenlik risklerini ve tehditlerini yönetme ve önleme konusunda rol almaktadır. İç denetim biriminin faaliyetleri işletmelerin siber güvenlik fonksiyonunu doğrudan etkilemektedir ve siber güvenlik süreçlerine değer katmaktadır.

Bu çalışmanın asıl amacı; siber risklere duyarlı sektörlerde faaliyet gösteren halka açık işletmelerin siber güvenlik yönetimine yaklaşımları ve siber güvenlik seviyeleri ile iç denetim faaliyetinin siber güvenlik konusundaki etkinliğini belirlemektir.

İç denetim faaliyetlerinin işletmeler için arz ettiği önem çeşitli çalışmalar ile geçmiş araştırmalarda ortaya konulmuştur. Ancak iç denetim ile siber güvenlik konularını birlikte ele alan çalışmalar çok kısıtlıdır. Bu konuda yabancı literatürde çeşitli çalışmalar bulunmaktadır. Şubat 2021 tarihi itibarıyla Türkiye’de YÖK tez merkezinde kayıtlı, “iç denetim ve siber güvenlik” konusunda yüksek lisans ve doktora tezi bulunmamaktadır. Bu açıdan bakıldığında çalışmanın iç denetim literatürüne yeni ve farklı bir bakış açısı kazandırması beklenmektedir.

Akademik kariyerimin en başından beri bana her zaman destek olan, göstermiş olduğu özen ve dikkat ile tezimin tamamlanmasında değerli katkıları bulunan kıymetli hocam ve tez danışmanım Prof. Dr. F. Lerzan Kavut’a şükran ve teşekkürlerimi sunarım. Ayrıca tez süreci boyunca değerli katkılarından dolayı Sayın Prof. Dr. İdil Kaya’ya ve Sayın Prof. Dr. Fatih Yılmaz’a çok teşekkür ederim. Ayrıca bu tez konusunun ilham kaynağı, fikir babası Dr. Graham Gal’e ve tezin araştırmasının gerçekleştirilmesine katkılarından dolayı başta Ali Kamil Uzun olmak üzere tüm TİDE ailesine teşekkürü borç bilirim.

Eğitim hayatımın en başından beri maddi ve manevi her zaman yanımda olan aileme ve benim için her zaman motivasyon kaynağı olan, bu mesleği seçmem ve bu meslekte ilerlemem konusunda beni sürekli teşvik eden, beni her alanda destekleyen çok değerli eşim Eylül GÜNGÖR’e çok teşekkür ederim.

NEVZAT GÜNGÖR

İSTANBUL, 2021

İÇİNDEKİLER

ÖZ	ii
ABSTRACT	iv
ÖNSÖZ	vi
İÇİNDEKİLER	viii
TABLolar LİSTESİ	xiv
ŞEKİLLER LİSTESİ	xvii
KISALTMALAR LİSTESİ	xviii
EKLER LİSTESİ	xx
GİRİŞ	1

BİRİNCİ BÖLÜM İÇ DENETİM FAALİYETİ

1.1. Denetim Olgusu.....	4
1.2. İç Denetimin Tanımı ve İşlevi.....	5
1.3. İç Denetimin Tarihsel Gelişimi	8
1.4. İç Denetimin Unsurları	12
1.4.1. Bağımsızlık ve Tarafsızlık.....	12
1.4.2. Danışmanlık ve Güvence Hizmeti	13
1.4.3. İşletme Faaliyetlerinin Geliştirilmesi ve Değer Katılması.....	14
1.4.4. Sistematik ve Disiplinli Bir Yaklaşım Sahip Olma.....	15
1.5. İç Denetimin Kapsamı	15
1.5.1. İç Kontrol.....	16
1.5.1.1. COSO İç Kontrol Çerçevesi	20
1.5.1.2. CoCo Çerçevesi	25
1.5.1.3. Turnbull Raporu.....	29
1.5.2. Kurumsal Yönetişim	31
1.5.3. Risk Yönetimi	37
1.6. İç Denetim Türleri.....	43
1.6.1. Finansal Denetimler	43
1.6.2. Kontrol Güvence Denetimleri.....	44

1.6.3. Mevzuata Uygunluk Denetimleri.....	45
1.6.4. Bilgi Teknolojileri Denetimi	45
1.6.5. Operasyonel Denetimler.....	47
1.6.6. Hile (Yolsuzluk) Denetimi	47
1.7. İç Denetimin Türk Mevzuatı İçindeki Yeri	48
1.7.1. 6102 Sayılı Türk Ticaret Kanunu	48
1.7.2. 5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu.....	49
1.7.3. SPK Düzenlemeleri	50
1.7.4. BDDK Düzenlemeleri	50
1.7.5. Sigorta ve Reasürans ile Emeklilik Şirketleri Mevzuatı	51
1.8. Uluslararası İç Denetim Düzenlemeleri.....	52
1.8.1. İç Denetim ile İlgili Uluslararası Kuruluşlar.....	52
1.8.1.1. İç Denetçiler Enstitüsü (IIA)	52
1.8.1.2. Avrupa İç Denetim Enstitüleri Konfederasyonu (European Confederation of Institutes of Internal Auditing -ECIIA)	53
1.8.2. İç Denetim ile İlgili Uluslararası Düzenlemeler.....	53
1.8.3. Uluslararası Mesleki Uygulama Çerçevesi-UMUÇ.....	59
1.8.3.1. Zorunlu Rehber.....	60
1.8.3.1.1. Temel Prensipler	60
1.8.3.1.2. İç Denetimin Tanımı	60
1.8.3.1.3. Etik Kurallar	61
1.8.3.1.4. Uluslararası İç Denetim Mesleki Uygulama Standartları (Standartlar)	62
1.9. İç Denetim Süreci	66
1.9.1. Denetimin Planlanması	66
1.9.1.1. Denetim Evreninin Belirlenmesi	67
1.9.1.2. Risklilik Düzeyi Değerlendirme Ölçütlerinin Tespit Edilmesi	68
1.9.1.3. Denetim Konularının Riskinin Değerlendirilmesi	68
1.9.1.4. İç Denetim Planının Oluşturulması.....	69
1.9.1.5. İç Denetim Programının Oluşturulması	71
1.9.2. Denetimin Yürütülmesi	71
1.9.2.1. Görev Planının Hazırlanması.....	72
1.9.3. Denetim Testlerinin Gerçekleştirilmesi ve Denetim Bulgularının Değerlendirilmesi	73
1.9.4. Raporlama	74
1.9.5. İç Denetim Sonuçlarının Değerlendirilmesi ve İzlenmesi	76

İKİNCİ BÖLÜM

İŞLETMELERDE BİLGİ TEKNOLOJİLERİ VE SİBER GÜVENLİK

2.1. Bilgi Teknolojileri ve Bilgi Sistemleri	77
2.1.1. Bilgi Kavramı	77
2.1.2. Bilgi Çağı.....	78
2.1.3. Bilgi Toplumu	78
2.2. Bilgi Sistemleri ve Bilgi Teknolojileri Temel Kavramları	79
2.2.1. Bilgi Sistemleri.....	79
2.2.1.1. Muhasebe Bilgi Sistemi	81
2.2.2. Bilgi Teknolojileri	83
2.2.3. Bilgi Teknolojilerinin Yarattığı Uygulamalar	83
2.2.3.1. İnternet	83
2.2.3.2. Elektronik Ticaret.....	84
2.2.3.3. Elektronik Veri Değişimi.....	85
2.2.3.4. Kurumsal Kaynak Planlaması	86
2.2.3.5. Yapay Zekâ	87
2.2.3.6. Blok Zinciri	88
2.2.3.7. Bulut Bilişim	91
2.2.3.8. Büyük Veri	92
2.2.3.9. Nesnelerin İnterneti.....	94
2.3. Bilgi Güvenliği ve Siber Güvenlik	96
2.3.1. Bilgi Güvenliği	97
2.3.2. Bilgi Güvenliği ve Siber Güvenlik İlişkisi	98
2.3.2.1. Bilgi Güvenliği ve Siber Güvenlik İlkeleri	99
2.4. Siber Güvenlik ve Siber Güvenliğe İlişkin Kavramlar	104
2.4.1. Siber Varlık ve Siber Olay	104
2.4.2. Siber Uzay/Alan/Ortam.....	105
2.4.3. Siber Terörizm.....	105
2.4.4. Siber Casusluk	106
2.4.5. Siber Suçlar.....	106
2.5. Siber Saldırıları/Tehditler	106
2.5.1. Sosyal Mühendislik.....	107
2.5.2. Zararlı Yazılımlar.....	108
2.5.3. Botnet (Zombi Ağı)	110
2.5.4. Gizli-Arka Kapılar (Back Doors)	110
2.5.5. Oltalama (Phising)	110
2.5.6. Hizmet Dışı Bırakma-(Denial-of-Service)	112
2.5.7. İstenmeyen E-Posta (Spam)	113
2.5.8. Fidyeye Yazılımlar (Ransomware)	114
2.5.9. IP Aldatması (IP Spoofing)	115
2.5.10. Fiziksel Zarar (Physical Manipulation)	116
2.5.11. İşletme İçi Tehditler	116
2.6. İşletmelerde Sınır Güvenliği Sistemleri	117

2.6.1. Güvenlik Duvarı (Firewall)	118
2.6.1.1. Bütünleşik Güvenlik Cihazı (Unified Threat Management-UTM)	118
2.6.1.2. Saldırı Önleme Sistemi (Intrusion Prevention System-IPS)	118
2.6.1.3. Saldırı Tespit Sistemleri (Intrusion Detection Systems-IDS)	119
2.6.1.4. Anti-Virüs / Anti-Malware / Anti-Spyware	119
2.6.1.5. Uygulama Kontrolü	119
2.6.1.6. Web Filtreleme Çözümleri (URL)	120
2.6.2. VPN	120
2.6.3. Veri Sızıntısı Engelleme Sistemleri (Data loss prevention-DLP)	120
2.6.4. Sayısal İmza.....	120
2.6.5. Zafiyet Analizi ve Sızma Testleri.....	121
2.6.5.1. Test Kılavuzları.....	121
2.6.5.2. Sızma Testi Türleri.....	122
2.6.5.3. Sızma Testi Aşamaları.....	123
2.7. Güncel Siber Güvenlik Vakaları ve Siber Güvenlik İstatistikleri	125

ÜÇÜNCÜ BÖLÜM

İŞLETMELERDE SİBER GÜVENLİĞİN SAĞLANMASINDA İÇ DENETİMİN ÖNEMİ

3.1. Siber Güvenliğin İşletmeler İçin Önemi	129
3.2. İşletmelerde Bilgi Teknolojileri ve Siber Güvenlik Yönetişi	133
3.2.1. Siber Güvenlik Stratejisi ve Hedefleri	136
3.2.1.1. Standartlaştırılmış İşlemler	136
3.2.1.2. Hukuki Düzenlemeler.....	137
3.2.1.3. Üst Düzey Liderlik Gözetimi.....	137
3.2.1.4. Kaynaklar	138
3.3. Bilgi Teknolojileri, Bilgi Güvenliği ve Siber Güvenlik Standartları	138
3.3.1. ISO/IEC 27000 Serisi	139
3.3.1.1. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi.....	139
3.3.1.2. ISO/IEC 27002 Bilgi Güvenliği İçin Uygulama Kodu.....	140
3.3.1.3. ISO/IEC 27003 Bilgi Güvenliği Yönetim Sistemi Uygulama Kılavuzu ..	141
3.3.1.4. ISO/IEC 27005 Bilgi Güvenliği Risk Yönetimi.....	141
3.3.1.5. ISO/IEC 27007 Bilgi Güvenliği, Siber Güvenlik ve Gizlilik Koruması-Bilgi Güvenliği Yönetim Sistemleri Denetimi	141
3.3.1.6. ISO/IEC 27032 Siber Güvenlik İçin Kılavuz	141
3.3.2. COBIT	142
3.3.3. ITIL.....	145
3.3.4. NIST Siber Güvenlik Çerçevesi	148
3.4. Siber Risklerin Analizi ve İç Denetim	150
3.5. İç Denetçilerin Siber Güvenlik Risklerini ve Kontrollerini Değerlendirmesine Yönelik Bir Yaklaşım.....	163

DÖRDÜNCÜ BÖLÜM
BORSA İSTANBUL'DA FAALİYET GÖSTEREN İŞLETMELERİN SİBER
GÜVENLİK FAALİYETLERİ SEVİYELERİNİN BELİRLENMESİ VE İÇ DENETİM
BİRİMLERİNİN SİBER GÜVENLİK FAALİYETİNE ETKİSİNİN TESPİTİNE
YÖNELİK BİR ARAŞTIRMA

4.1. Konuya İlişkin Literatür İncelemesi.....	173
4.1.1. İç Denetim ve Siber Güvenlik	173
4.1.2. Bilgi Paylaşımı ve Siber Güvenlik	179
4.1.3. Siber Güvenlik Yatırımları.....	180
4.1.4. Siber Güvenlik Faaliyetlerine İlişkin Bilgilerin Açıklanması.....	182
4.1.5. Güvenlik Tehditleri ve Güvenlik İhlalleri	184
4.2. Araştırmanın Amacı ve Önemi	186
4.3. Araştırmanın Kapsamı	188
4.4. Araştırmanın Metodolojisi	189
4.4.1. Araştırma Yöntemi ve Veri Toplama	189
4.4.2. Örneklem Seçimi.....	190
4.4.3. Araştırma Varsayımları ve Kısıtları	193
4.5. Araştırmanın Hipotezleri, Analizler, Bulgular ve Sonuçların Yorumlanması	193
4.5.1. Araştırma Anketinin Yapısı ve Anketin Güvenilirlik Analizi	194
4.5.2. Normallik Testi Sonuçları.....	195
4.5.3. Araştırmaya Katılan İç Denetçilerin ve İşletmelerin Demografik Özellikleri (Frekans-Sıklık Dağılım Tabloları)	196
4.5.4. İşletmelerin Siber Güvenlik Faaliyetleri Seviyesine İlişkin Hipotezler, Frekans Dağılımları ve Farklılık Analizleri.....	203
4.5.4.1. İşletmelerin Siber Güvenlik Faaliyetleri Seviyesine İlişkin Hipotezler ..	203
4.5.4.2. İşletmelerin Siber Güvenlik Faaliyetleri Seviyesine İlişkin Frekans Dağılımları	207
4.5.4.2.1. Siber Güvenlik Yönetişimi ve Uygulamaları-Frekans Dağılımları	208
4.5.4.2.2. Fiziksel ve Çevresel Güvenlik Tedbirleri- Frekans Dağılımları	212
4.5.4.2.3. Bilgi Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri- Frekans Dağılımları	214
4.5.4.2.4. Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tedbirleri- Frekans Dağılımları	218
4.5.4.2.5. Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi- Frekans Dağılımları	221
4.5.4.3. İşletmelerin Siber Güvenlik Faaliyetleri Seviyelerine İlişkin Kruskal-Wallis Testleri.....	223
4.5.4.3.1. Siber Güvenlik Faaliyetleri Seviyeleri- Çalışan Sayısına Göre Kruskal-Wallis Testi	223

4.5.4.3.2. Siber Güvenlik Faaliyetleri Seviyeleri- İşletmelerin Aktif Büyüklüklerine Göre Kruskal-Wallis Testi	224
4.5.4.3.3. Siber Güvenlik Faaliyetleri Seviyeleri- İşletmelerin BT Bağımlılıklarına Göre Kruskal-Wallis Testi	226
4.5.4.3.4. Siber Güvenlik Faaliyetleri Seviyeleri- Siber Saldırıların İşletme İtibarına Etkisine Göre Kruskal-Wallis Testi	228
4.5.4.3.5. Siber Güvenlik Faaliyetleri Seviyeleri- İşletmelerin Kritik Bilgilere Sahip Olmalarına Göre Kruskal-Wallis Testi	230
4.5.4.3.6. Siber Güvenlik Faaliyetleri Seviyeleri- Faaliyet Gösterilen Sektöre Göre Kruskal-Wallis Testi	232
4.5.5. İşletmelerin İç Denetim Birimlerinin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliğine İlişkin Hipotezler, Frekans Dağılımları ve Farklılık Analizleri ...	235
4.5.5.1. İç Denetim Birimlerinin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliğine İlişkin Hipotezler.....	236
4.5.5.2. İç Denetim Biriminin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliğine İlişkin Frekans Dağılımları.....	238
4.5.5.2.1. İç Denetim ve Bilgi Teknolojileri (BT) Departmanları Arasındaki İlişkinin Algısı-Frekans Dağılımları.....	239
4.5.5.2.2. İç Denetim Departmanının Siber Güvenlik Bilgi Düzeyi Algısı-Frekans Dağılımları	241
4.5.5.2.3. Siber Güvenlik Konusunda Üst Yönetimin Desteğine ilişkin İç Denetçi Algısı-Frekans Dağılımları	242
4.5.5.2.4. İç Denetim Departmanının Siber Güvenliği Gözden Geçirme Sıklığı-Frekans Dağılımları	245
4.5.5.2.5. Siber Güvenlik Vakalarına Yönelik Frekans Dağılımları	248
4.5.5.3. İç Denetim Biriminin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliğine İlişkin Kruskal-Wallis Testleri.....	250
4.5.5.3.1. İç Denetim Biriminin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliği- Çalışan Sayısına Göre Kruskal-Wallis Testi	250
4.5.5.3.2. İç Denetim Biriminin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliği- Faaliyet Gösterilen Sektöre Göre Kruskal-Wallis Testi .	253
4.5.5.3.3. İç Denetim Biriminin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliği- İşletmelerin BT Bağımlılıklarına Göre Kruskal-Wallis Testi	255
4.5.6. İşletmelerin Siber Güvenlik Faaliyetleri Seviyesi ile İç Denetim Birimlerinin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliğine İlişkin Korelasyon Analizleri	257
SONUÇ ve ÖNERİLER	261
KAYNAKÇA	267
EK	309
ÖZGEÇMİŞ	320

TABLÖLER LİSTESİ

Tablo 1.1. İç Denetimin Temel Fonksiyonları	6
Tablo 1.2. İç Denetim Fonksiyonunda Dönemsel Değişim	9
Tablo 1.3. İç Denetim Faaliyeti Etkileyen Tarihsel Gelişmeler	10
Tablo 1.4. Uluslararası İç Kontrol Modellerinin Karşılaştırılması.....	18
Tablo 1.5. Kurumsal Yönetişimin Tarihsel Gelişimi	33
Tablo 1.6. COSO Risk Yönetimi Çerçevesi Ögeleri.....	40
Tablo 1.7. İç Denetim ile İlgili Uluslararası Düzenlemeler.....	53
Tablo 1.8. Nitelik Standartları.....	63
Tablo 1.9. Performans Standartları	64
Tablo 1.10. Denetim Test Matrisi Örneği.....	73
Tablo 2.1. Ortalama Saldırısı Temaları.....	111
Tablo 3.1. İşletmelerin Bilgi Varlıkları Değerlendirmesinde Dikkate Alması Gereken Unsurlar	165
Tablo 4.1. İç Denetim ve Siber Güvenlik Literatür İncelemesi	173
Tablo 4.2. Bilgi Paylaşımı ve Siber Güvenlik Literatür İncelemesi	179
Tablo 4.3. Siber Güvenlik Yatırımları Literatür İncelemesi	181
Tablo 4.4. Siber Güvenlik Faaliyetleri Bilgilerinin Açıklanmasına Yönelik Literatür İncelemesi	183
Tablo 4.5. Güvenlik Tehditleri ve Güvenlik İhlalleri Literatür İncelemesi	184
Tablo 4.6. Örneklem Büyüklüğü Tablosu	191
Tablo 4.7. Güvenilirlik Analizi Sonuçları	194
Tablo 4.8. Normal Dağılım Sonuçları	195
Tablo 4.9. Araştırmaya Katılan İç Denetçilerin Cinsiyetlerine Göre Frekans Dağılımı	196
Tablo 4.10. Araştırmaya Katılan İç Denetçilerin Yaşlarına Göre Frekans Dağılımı	197
Tablo 4.11. Araştırmaya İç Denetçilerin Eğitim Durumlarına Göre Frekans Dağılımı	197
Tablo 4.12. Araştırmaya Katılan İç Denetçilerin Mesleki Deneyimlerine Göre Frekans Dağılımı	198
Tablo 4.13. Araştırmaya Katılan İç Denetçilerin Çalıştıkları Pozisyonlara Göre Frekans Dağılımı	198

Tablo 4.14. Araştırmaya Katılan İç Denetçilerin Sahip Oldukları Mesleki Sertifika Sayısına Göre Frekans Dağılımı	199
Tablo 4.15. Araştırmaya Katılan İç Denetçilerin Çalıştıkları İşletmelerin Sektörüne Göre Frekans Dağılımı	199
Tablo 4.16. Araştırmada Yer Alan İşletmelerin Aktif Büyüklüklerine Göre Frekans Dağılımı	200
Tablo 4.17. Araştırmada Yer Alan İşletmelerin Çalışan Sayısına Göre Frekans Dağılımı	200
Tablo 4.18. Araştırmada Yer Alan İşletmelerin Teknoloji Bağımlılıklarına Göre Frekans Dağılımı	201
Tablo 4.19. Araştırmada Yer Alan İşletmelerin Kritik Bilgilere Sahip Olmalarına Göre Frekans Dağılımı	202
Tablo 4.20. Araştırmada Yer Alan İşletmelerin İtibar Riskine Göre Frekans Dağılımı	202
Tablo 4.21. Siber Güvenlik Yönetişimi ve Uygulamaları Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri Dağılımı	208
Tablo 4.22. Fiziksel ve Çevresel Güvenlik Tedbirleri Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri	212
Tablo 4.23. Bilgi Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri	215
Tablo 4.24. Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tedbirleri Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri	218
Tablo 4.25. Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri	221
Tablo 4.26. Siber Güvenlik Faaliyetleri Seviyeleri-Çalışan Sayısına Göre Kruskal-Wallis Testi.....	223
Tablo 4.27. Siber Güvenlik Faaliyetleri Seviyeleri -Aktif Büyüklüğüne Göre Kruskal-Wallis Testi	224
Tablo 4.28. Siber Güvenlik Faaliyetleri Seviyeleri -BT Bağımlılıklarına Göre Kruskal-Wallis Testi	227
Tablo 4.29. Siber Güvenlik Faaliyetleri Seviyeleri-Siber Saldırıların İşletme İtibarına Etkisine Göre Kruskal-Wallis Testi	228
Tablo 4.30. Siber Güvenlik Faaliyetleri Seviyeleri-İşletmelerin Kritik Bilgilere Sahip Olmalarına Göre Kruskal-Wallis Testi	230

Tablo 4.31. Siber Güvenlik Faaliyetleri Seviyeleri-Faaliyet Gösterilen Sektöre Göre Kruskal-Wallis Testi	232
Tablo 4.32. İç Denetim ve Bilgi Teknolojileri (BT) Departmanları Arasındaki İlişkinin Algısı Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri.....	239
Tablo 4.33. İç Denetim Departmanının Siber Güvenlik Bilgi Düzeyi Algısı Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri	241
Tablo 4.34. Siber Güvenlik Konusunda Üst Yönetimin Desteğine İlişkin İç Denetçi Algısı Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri.....	243
Tablo 4.35. İç Denetim Departmanının Siber Güvenliği Gözden Geçirme Sıklığı Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri	245
Tablo 4.36. Cari Dönem Vaka/Veri İhlali Sayısı Frekans Dağılımı.....	248
Tablo 4.37. Cari Dönem Siber Güvenliğine İlişkin İç Denetim Bulgularının Yüzdesi Frekans Dağılımı	248
Tablo 4.38. İç Denetim Biriminin Siber Güvenlik Konusunda Aktif Olarak Rol Alması Frekans Dağılımı	249
Tablo 4.39. Siber Güvenlik Vaka Trendi Frekans Dağılımı.....	250
Tablo 4.40. Aktif Büyüklüğüne Göre Kruskal-Wallis Testi.....	251
Tablo 4.41. Faaliyet Gösterilen Sektöre Göre Kruskal-Wallis Testi	253
Tablo 4.42. BT Bağımlılığına Göre Kruskal-Wallis Testi.....	256
Tablo 4.43. İşletmelerin Siber Güvenlik Faaliyetleri Seviyesi ile İç Denetim Birimlerinin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliğine İlişkin Korelasyon Analizi	259
Tablo 4.44. İşletmelerin Siber Güvenlik Faaliyetleri Seviyesi ile İç Denetim Birimlerinin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliğinin Alt Boyutlarının Korelasyon Analizi	259

ŞEKİLLER LİSTESİ

Şekil 1.1. COSO Küpü	21
Şekil 1.2. CoCo Çerçevesini Oluşturan Bileşenler	27
Şekil 1.3. Kurumsal Risk Yönetiminin Unsurları	40
Şekil 1.4. Denetimin Planlaması Aşamaları.....	67
Şekil 1.5. İç Denetim Faaliyetinin Uygulanması Aşamaları	72
Şekil 2.1. Muhasebe Bilgi Sisteminin Öğeleri	82
Şekil 2.2. Blok Zincirinin Çalışma Prensibi	89
Şekil 2.3. Bilgi Güvenliğinin Temel Bileşenleri.....	100
Şekil 2.4. Bilgi Güvenliğinin Temel Prensipleri	101
Şekil 2.5. Dropbox Temalı Ortalama Mesajı	112
Şekil 2.6. Spam Kaynağı İlk 10 Ülke	114
Şekil 2.7. Fidye Yazılım Örneği.....	115
Şekil 2.8. İşletme İç Tehditlerden En Çok Etkilenen Veriler	117
Şekil 3.1. COBIT'in Tarihsel Gelişim Süreci	143
Şekil 3.2. COBIT 5 Çerçevesi İlkeleri	144
Şekil 3.3. ITIL'in Tarihsel Gelişim Süreci.....	146
Şekil 3.5. Üçlü Savunma Hattı	152
Şekil 4.1. Güç Analizi Sonuçları	192

KISALTMALAR LİSTESİ

ABD	: Amerika Birleşik Devletleri
ALE	: Annual Loss Expected
BDDK	: Bankacılık Düzenleme ve Denetleme Kurulu
BGYS	: Bilgi Güvenliği Yönetim Sistemi
BIS	: Bank for International Settlements
BT	: Bilgi Teknolojileri
CCTV	: Close Circuit TeleVision
CEO	: Chief Executive Officer
CIA	: Certified Internal Auditor
CICA	: Canadian Institute of Chartered of Accountants
CIO	: Chief Information Officer
CISO	: Chief Information Security Officer
COBIT	: Control Objectives for Information and Related Technology
CoCo	: The Criteria of Control
COSO	: Committee of Sponsoring Organizations
CRAMM	: Central Computer and Telecommunications Agency Risk Analysis and Management Method
CSF	: Cyber Security Framework
CTO	: Chief Technology Officer
DDOS	: Distributed Denial of Service Attack
DLP	: Data loss prevention
DoS	: Denial of Services
ECIIA	: European Confederation of Institutes of Internal Auditing
EDI	: Electronic Data Interchange
ENISA	: European Network and Information Security Agency
ERP	: Enterprise Resource Planning
FCPA	: Foreign Corrupt Practices Act
FMEA	: Failure Mode and Effects Analysis
FMECA	: Failure Mode and Effects Criticality Analysis
FRC	: The Financial Reporting Council
IDS	: Intrusion Detection Systems
IIA	: Institute of Internal Auditors
IoT	: Internet of Things
IPS	: Intrusion Prevention System
ISA	: International Standards on Auditing
ISACA	: Information Systems Audit and Control Association
ISO	: International Organization for Standardization
ISRAM	: Information Security Risk Analysis Method

ISSAF	: Information System Security Assessment Framework
ITIL	: Information Technologies Infrastructure Library
KMYKK	: Kamu Mali Yönetimi ve Kontrol Kanunu
KPI	: Key Performance Indicators
MBS	: Muhasebe Bilgi Sistemi
NIST	: National Institute of Standards and Technology
OECD	: Organisation for Economic Co-operation and Development
OSSTMM	: The Open Source Security Testing Methodology Manual
OWASP	: Open Web Application Security Project
PCAOB	: The Public Company Accounting Oversight Board
PTEST	: Penetration Testing Execution Standard
SAS	: Statement of Auditing Standards
SEC	: Security Exchange Commission
SLA	: Service-Level Agreement
SOX	: Sarbanes-Oxley Act
SPK	: Sermaye Piyasası Kurulu
TDK	: Türkiye Dil Kurumu
TİDE	: Türkiye İç Denetim Enstitüsü
TKYD	: Türkiye Kurumsal Yönetim Derneği
TTK	: Türk Ticaret Kanunu
UMUÇ	: Uluslararası Mesleki Uygulama Çerçevesi
URL	: Uniform Resource Loader
USOM	: Ulusal Siber Olaylara Müdahale Merkezi
UTM	: Unified Threat Management
VPN	: Virtual Private Network

EK LİSTESİ

Ek - 1: Anket Formu Örneği.....	309



GİRİŞ

20. yüzyılda başlayan ve günümüzde de devam eden teknolojik gelişmeler sonucunda bilgi ve iletişim teknolojileri tüm Dünya'ya yayılmıştır. Böylelikle; bilginin işlenmesinde ve depolanmasında kullanılan bilgisayar ve iletişim teknolojileri iş hayatının merkezine yerleşmiştir. Bu durum işletmelerin kurumsal yapılanmalarını, faaliyetlerini ve hatta risklerini değiştirmiş ve tamamen teknoloji odaklı bir iş dünyasının oluşumunu hızlandırmıştır.

Bilgi teknolojileri ve dijitalleşme sürecinde yaşanan gelişmelere bağlı olarak, işletmelerin bilgi kaynaklarının ve veri tabanlarının da dijitalleşmesi nedeniyle dijital veri kullanımı artmıştır. Bilgi teknolojilerinin kullanımının bu denli artması ve nerdeyse tüm faaliyetlerin dijital ortamlarda yürütülmeye başlanması, bilgi hacminin artması ve giderek bilginin en önemli rekabet aracı haline gelmesi, bilginin ve bilgiyi sağlayan kaynakların korunmasını zorunlu hale getirmiş ve bu durum bilgi güvenliği ve siber güvenlik kavramlarının hayatımıza girmesine vesile olmuştur.

Günümüz dünyasında fiziksel güvenlik kadar siber güvenlik uygulamaları da işletmeler açısından büyük önem taşımaktadır. İşletmelerde bilgi güvenliği ve siber güvenliğe dair uyumluluğun sağlanması, bilgi güvenliği ve siber güvenlik yönetim olgusunun işletmelerin odak noktası olması, çağımızın en büyük gerekliliğidir.

Teknoloji ve dijitalleşmeye bağlı olarak; iş süreçlerinde, işletme faaliyetlerinde ve kontrol ortamlarında, varlıkların her türlü zarar ve saldırıya maruz kalma risklerine karşı alınacak tedbirlerde, uygulamalarda ve yeniden yapılanma sürecinde iç denetçilere de önemli görevler düşmektedir.

İç denetim; işletmelerde hem kontrol (güvence) hem de danışmanlık mekanizması olarak; işletmenin iş süreçlerinin amaçlara, politikalara ve çeşitli yasal düzenlemelere uyumuna yönelik usulsüzlükleri ve sistemin zayıflıklarını tespit etme ve iyileştirmeye yönelik faaliyetlerde bulunmaktadır.

IIA tarafından “Etkili Risk Yönetimi ve Kontrolünde Üçlü Savunma Hattı” ve “Siber Güvenlik Riskinin Değerlendirilmesinde Üçlü Savunma Hattının Roller” konulu kılavuzda siber risklerin analizinde üçlü savunma hattının ve özellikle de iç denetçilerin rolleri

açıklanmıştır. İşletmelerde üçüncü savunma hattı olarak iç denetim faaliyeti, birinci (işletme yönetimi) ve ikinci (bilgi teknolojileri departmanı) savunma hattıyla koordinasyonlu bir biçimde hareket ederek özellikle siber güvenlik kapsamında önemli bir rol oynamaktadır.

Çalışmanın birinci bölümünde, denetim olgusu, iç denetimin tanımı, işlevi ve iç denetimin kapsamı açıklanmıştır. Ayrıca çalışmada, kurumsal yönetim, risk yönetimi ve iç kontrol kavramları ile iç denetim faaliyetinin ilişkisine yer verilmiştir. İç denetim türleri olan; finansal denetim, uygunluk denetimi, faaliyet denetimi, bilgi teknolojileri denetimi ve hile denetimi kavramları açıklanmıştır. Bu bölümde, iç denetim ile ilgili ulusal ve uluslararası düzenlemeler, standartlar ve kuruluşlar aktarılmıştır. İç denetim süreci tüm aşamalarıyla anlatılmıştır.

Bilgi teknolojileri ve bunlara bağlı olarak ortaya çıkan uygulamalara çalışmanın ikinci bölümünde yer verilmiştir. Çalışmada ayrıca bilgi güvenliği ve siber güvenliğe ilişkin genel kavramlar ve unsurlar açıklanmıştır. Siber uzay, siber olay, siber tehditler ve işletmelerde sınır güvenliği sistemleri ve bunlara ilişkin kavramların üzerinde durulmuştur. Siber güvenlikle ilgili olaylar ve bu olayların sonuçlarının yer aldığı güncel istatistiki bilgiler ile konunun ülkeler ve işletmeler için arz ettiği öneme dikkat çekilmiştir.

Üçüncü bölümde, işletmelerde siber güvenlik yönetimi ve siber güvenlik yönetimine ilişkin kabul görmüş uluslararası standartlar açıklanmıştır. İşletmelerde siber tehditlerin önlenmesi ve minimize edilmesi konusunda işletme yönetimi, bilgi teknolojileri (BT) çalışanları ve iç denetçilere düşen roller ve görevler anlatılmıştır. IIA tarafından siber güvenlik konularında yayımlanan çerçeveler dikkate alınarak iç denetçilerin siber güvenlik risklerini ve kontrollerini değerlendirmesi konusu açıklanmaya çalışılmıştır.

Çalışmanın dördüncü bölümünde yapılan literatür taramasında siber güvenlik ve iç denetim konularında yapılan çalışmalar sınıflandırılarak açıklanmıştır. Bu bölümde, araştırmanın önemi, örneklem seçimi ve verilerin toplanması süreci ile araştırmanın varsayımları ve kısıtları belirtilmiştir. Araştırmanın amacı, hipotezler, araştırmanın yöntemi, anketin güvenilirlik analizi ve frekans dağılım analizleri bu bölüm içinde yer alan diğer bilgilerdir. Çalışmada, grup farklılığı sınamaları ile hipotezler test edilmiştir. Son

olarak araştırmanın bulguları yorumlanmış, araştırma sonuçlarına ve ileride yapılabilecek çalışmalar için önerilere yer verilmiştir.



BİRİNCİ BÖLÜM

İÇ DENETİM FAALİYETİ

1.1. Denetim Olgusu

Denetim olgusu ya da denetleme faaliyeti toplumsal perspektifte değerlendirildiğinde, insanların gerçekleştirdiği eylemlerin, önceden belirlenmiş kurullara uygun olup olmadığını tespit etmek için yapılan bir değerlendirme olarak karşımıza çıkmaktadır. İnsanların faaliyet gösterdiği her alanda açıklanan bilgilerin ve iddiaların doğru ve güvenilir olup olmadığını belirlemek için bağımsız kişi veya kişilerce ayrıca bir inceleme yapılması önem arz eden bir konudur.

İş dünyası odağında düşündüğümüzde; tarih boyunca finansal konularda alınan kararların güvenilir olmayan bilgilere dayanması sonucu ortaya çıkan büyük zararlar (muhasabe skandalları), denetim mesleğinin ve denetim ilke ve tekniklerinin finansal işlemler üzerine yoğunlaşmasına sebebiyet vermiştir.

Ancak zaman içerisinde işletmelerin faaliyet alanlarının genişlemesi ve kurumsal bir kimlik kazanmaları, paydaşların şeffaflık ve hesap verilebilirlik konularında taleplerinin artması sonucu ortaya çıkan “güven” ihtiyacı denetime olan ilgiyi arttırmıştır. Ayrıca hızlı teknolojik gelişmeler sonucu küresel ekonominin gelişmesi ve iş dünyasının teknolojik gelişmelere hızla ayak uydurması, işletmelerin alışlagelmiş risklerinin hızla değişmesine ve sürekli olarak evrilmesine yol açmıştır. Bu durum finansal denetim dışında birçok denetim türünün de ortaya çıkmasına yol açmıştır.

Literatürde denetim türleri açıklanırken denetim faaliyeti; amaç, yapılış zamanı ve denetçi statüsüne (bağlı bulunduğu kurum) göre üçe ayırarak incelenmektedir.

Denetim amaçlarına göre üçe ayrılmaktadır (Güredin 2014):

- Finansal tablolar denetimi,
- Uygunluk denetimi,
- Faaliyet denetimidir.

Yapılış zamanına göre denetim türleri üçe ayrılmaktadır. Bunlar (Kurnaz & Çetinoğlu, 2010):

- Yıl sonu denetimi,
- Ara dönem denetimi,
- Özel denetimdir.

Denetçinin statüsü yönünden denetim türleri üçe ayrılmaktadır. Bunlar (Güredin, 2014):

- Bağımsız denetim,
- Kamu denetimi
- İç denetim olarak sınıflandırılmaktadır.

1.2. İç Denetimin Tanımı ve İşlevi

Bağımsız denetimin tarihi çok eski olmasına rağmen Dünya’da iç denetimin önem kazanması II. Dünya Savaşı sonrası gerçekleşmiştir. Savaş sonrası küresel ekonominin kalkınmasına paralel olarak işletmelerin giderek büyümesi, gelişmesi ve yönetsel ve operasyonel süreçlerin karmaşıklaşması nedeniyle işletmeleri yönetmek zorlaşmış ve bu nedenlerle işletme sahipleri işletme yönetimini profesyonellere devretmeye başlamıştır. İç denetim de hızla bu gelişime ayak uydurmuştur. 1941 yılında ABD’de İç Denetçiler Enstitüsü (Institute of Internal Auditors-IIA) bir meslek örgütü olarak faaliyetlerine başlamıştır. İç denetim alanında faaliyet gösteren ilk kurum olan IIA, 1947 yılında yaptığı ilk tanımda iç denetimi, yönetime hizmet etmek ve işletme fonksiyonlarının bağımsız değerlendirilmesi faaliyeti şeklinde tanımlamıştır (Guy ve ark.,1996).

Meslek örgütü 2003 yılında ise iç denetimin tanımını; işletmenin faaliyetlerini geliştirme ve faaliyetlerine katkıda bulunma amacı güden bağımsız ve tarafsız, güvence ve danışmanlık faaliyeti olarak güncellemiştir (IIA, 2020).

IIA tarafından yapılan tanımlamalara ek olarak iç denetim; işletmelerde kurumsal yönetim, iç kontrol ve risk yönetimi süreçlerinin etkinliğinin değerlendirilmesi ve geliştirilmesi için sistematik ve disiplinli bir yaklaşım oluşturulmasına yardımcı faaliyetler bütünü olarak da açıklanmaktadır (Hass ve ark., 2006: 836).

Bugüne kadar yapılan iç denetim tanımlarından hareketle iç denetim faaliyetinin fonksiyonları Tablo 1.1’de özetlenmiştir:

Tablo 1.1. İç Denetimin Temel Fonksiyonları

Güvence Verme	➤ İşletme politikalarının etkinliği ve verimliliği hakkında tüm işletme paydaşları için doğru ve güncel bilgi sağlamak. ➤ İşletme süreçlerinin, yasal yükümlülükleri ile uyumlu olmasını sağlamak.
Değerlendirme	➤ Kontrollerin değerlendirilmesi ve etkinliği hakkında tavsiyelerde bulunmak. ➤ Etik, uygunluk, risk, verimlilik gibi konularda önerilerde bulunmak.
Gözetim	➤ Kontrollerin değerlendirilmesi ve etkinliğinin gözetimini yapmak. ➤ İşletmeye etik, uygunluk, risk, verimlilik konularında yapılan önerilerin uygulanabilirliğinin gözetimini yapmak.
Danışmanlık	➤ Etik, uygunluk, risk, verimlilik konularında önerilerde bulunarak bu uygulamalarla ilgili danışmanlık yapmak.

Kaynak: Deloitte, 2012.

Özetle iç denetim faaliyeti;

- İşletmenin finansal ve finansal olmayan bilgilerinin doğruluk ve güvenilirliği,
- Yasal düzenlemelerin ve belirlenen önceden belirlenen işletme politikalarının ve prosedürlerinin izlenip izlenmediği,
- İşletmenin karşılaşılabilecek muhtemel risklerinin tespiti, fırsata dönüştürülmesi ya da olası olumsuz sonuçların en aza indirilmesi,
- İşletmenin belirlediği amaçlara ulaşip ulaşmadığı,
- İşletmenin sahip olduğu varlıkları etkin ve verimli bir şekilde kullanıp kullanmadığı,

konularının tespiti, işletme yönetiminin ve çalışanlarının görev ve sorumluluklarını etkin bir şekilde ifa etmelerini desteklemek amacıyla tüm faaliyetlerin ve kontrollerin, objektif ve sistematik bir şekilde incelenmesi ve onaylanmasıdır (Akarkarasu, 2000: 19).

İşletme nezdinde sürdürülen iç denetim faaliyetlerine duyulan gereksinim şu nedenlere bağlanmaktadır (Kurnaz & Çetinoğlu, 2010):

“Günümüzde ticaretin küresel seviyeye ulaşması işletmelerin de ölçeklerinin büyümesine yol açmıştır. Karmaşık hale gelen ticari hayat ve büyüyen işletmelerde sahip-yönetici konumunda olan işletme sahiplerinin yönetim fonksiyonlarında yetersiz kalmaları sonucu yerlerini büyük ölçüde profesyonel yöneticilere devretmişlerdir. İşletme sahipleri ve yöneticiler arasındaki bu ilişki vekâlet akdine benzetilmektedir (vekalet teorisi-agency theory). Profesyonel yöneticiler, görevleri karşılığında uzun vadede daha fazla ücret alma/gelir elde etme temel güdüsüyle hareket edebilen ve bu yüzden çoğu zaman işletme sahipleri ile çatışabilecek kişisel amaç ve hedefleri ön plana alabilecek potansiyele sahiptirler. Bu nedenlerle, işletme sahipleri yöneticilere emanet ettikleri kaynakların etkin ve verimli olarak kullanımı hususunda endişe duymaktadırlar. İşletme sahiplerinin yöneticilerin görevlerinin yerine getirip getirmediikleri hususlarında yeterli değerlendirmeleri yapacak zamanları ya da teknik ve metodolojik yetenekleri yoktur. Bu kapsamda bir vekil olarak görev yapan yöneticinin söz konusu ilişkiden doğan borçlarını yerine getirmesi sırasında ortaya çıkabilecek düzensizlikler hakkındaki işletme sahibinin şüphelerini ortadan kaldıracak en önemli kontrollerden biri, yapılacak olan iç denetimlerdir. Bağımsız ve nesnel bir biçimde gerçekleştirilen ve tatmin edici sonuçlar veren iç denetimler, yöneticilerin taşıdıkları sorumlulukları yerine getirdikleri hususunda işletme sahiplerini daha kolay ikna etmelerini sağlamaktadır. Bu kapsamda iç denetçiler finansal ve finansal olmayan işlem ve olayları konu alan denetimler ile işletme sahibi ve yöneticiler arasındaki potansiyel çıkar çatışmasını önler.

Ayrıca, her işletmede, yöneticiler sahip oldukları yetki ve sorumluluklarının bir kısmını kendilerine bağlı olarak çalışan kişilere devretmektedirler. Bu bağlamda, iç denetçiler de yöneticilerin devrettikleri çeşitli görevleri vekâleten yürütme konumunda olan kilit personellerdir. Üst yönetimde ve çeşitli kademelerde görev yapan yöneticilerin; işletme çalışanlarının faaliyetlerinin etkinlik ve verimliliğini ve işletmenin hedeflerine

ulaşıp ulaşılmadığını takip etmeleri gereklidir. İç denetçiler, mesleki yetkinlikleriyle bilgi toplama, sorunları tanımlama ve analiz etme konularında yöneticilere güvence hizmeti vermekte ve danışmanlık yapmaktadırlar. İç denetçiler temel olarak üst düzey yöneticiler de dâhil olmak üzere her kademedeki yöneticilerin görevlerini yerine getirmekteki performanslarını yönetim kurulu adına incelemektedirler.

Modern bir iç denetçi yönetime yardımcı olacak nitelikte eğitim ve deneyime sahiptir ve işletmedeki hata ve hileleri açığa çıkarmak yanında, ileride benzer sorunlarla karşılaşılması için yöneticilere danışmanlık ve eğitim hizmeti de vermektedir. Ancak iç denetçilerin belirtilen nitelikte bir faaliyet yerine getirebilmeleri için planlama, organizasyon, yönetim ve kontrol konularında bilgi sahibi olmaları ve olayları profesyonel bir yönetici gözüyle değerlendirebilmeleri gerekmektedir.

Profesyonel olarak yürütülen denetimler sonucunda tespit edilen eksikliklerin düzeltilmesi sonucunda işletmeler maddi açıdan da büyük tasarruflar sağlamak ve kazançlar elde etmektedir. Maddi kayıpların ortaya çıkarılması ve düzeltilmesi bazen iç denetim biriminin yıllık maliyetini karşılayacak nitelikte dahi olabilmektedir.”

1.3. İç Denetimin Tarihsel Gelişimi

İç denetimin tarihi çok eskilere dayanmaktadır. İlk iç denetim faaliyetleri on üçüncü yüzyılda İtalya’da ticari merkezlerde yapılan muhasebe kayıtlarının kontrol edilmesi ile başlamıştır. ABD’de ilk iç denetçiler demiryolu işletmelerinde çalışmıştır. Avrupa ülkelerinde denetim faaliyetleri ilk olarak 1900’lü yıllarda ele alınmaya başlanmıştır. Birleşik Devletlerde 1933 ve 1934 yıllarında menkul kıymetlere ilişkin yapılan düzenlemeler sonrası iç denetime olan ihtiyaç artmıştır ve işletmeler iç denetim birimlerini kurmaya başlamışlardır. (Sawyer ve ark., 2003:4).

Denetim faaliyetinin genel olarak bir meslek olarak ortaya çıkışı yazının icadına kadar dayanmaktayken, iç denetimin meslek olarak kabul görmesi 19.yüzyılın başlarını bulmuştur (Sabuncu, 2018: 782). İç denetimin ilk ortaya çıkışı fiziki işletme varlıklarının korunmasını sağlamak için sayım ve gözlem yapmak şeklindedir (Adiloğlu, 2010). 1940’lı

yıllara gelindiğinde; işletmelerin zamanla büyümesi, kayıtların ve belgelerin giderek artması; denetimde mutlak güvence verilmesini olanaksız hale getirmiştir. Böylelikle denetimde örnekleme yöntemi kullanılmaya ve makul güvence verilmeye başlanmıştır. Bu durum güvenilir iç kontrol ortamının önemini oldukça arttırmıştır. İç kontrol ortamının öneminin artmasına paralel iç denetim faaliyeti, iç kontrol odaklı denetime dönüşmüştür (Kızılboğa & Şahin, 2013).

İşletmelerin yapısal açıdan değişimiyle birlikte iç denetim uygulamaları da köklü değişimler geçirmeye devam etmiştir. İç denetim fonksiyonunun tarihsel gelişimi ve değişimi Tablo 1.2.'de özetlenmiştir.

Tablo 1.2. İç Denetim Fonksiyonunda Dönemsel Değişim

Dönem	İç Denetimden Beklenen Faydalar	İç Denetimin Kapsamı
1950'ler	İşletme varlıklarının zarardan korunması	Muhasebe kayıtlarının kontrolü
1960'lar	İşletme verilerinin güvenilirliğinin denetlenmesi	Finansal denetimler ve uygunluk denetimlerinin yapılması
1970'ler	Uygunluk denetiminin yapılması	İşletme faaliyetlerine ilişkin finansal denetimlerin ve uygunluk denetimlerinin yapılması
1980'ler	İşletme faaliyetlerinin etkinliğinin denetlenmesi	Tüm işletme faaliyetlerin etkinliğinin denetlenmesi
1990'lar	İşletmenin hedeflerine ulaşması	İşletmenin iç kontrol sisteminin ve risk yönetiminin denetlenmesi
Günümüz	İşletmeye değer katma	Tüm süreçlerin denetimi

Kaynak: Memiş, 2008

1950'lerde iç denetim mali denetimleri odak noktası haline getirmiş ve mali nitelikteki işlemlerin doğruluğu değerlendirilmiştir 1960'larda ise iç denetim işletmelerin sahip olduğu veri ve bilgilerin güvenilirliğini tespit etmekteydi. Finansal denetimler ve uygunluk denetimleri iç denetçiler tarafından gerçekleştirilmeye başlanmıştı (Memiş, 2008: 77).

70'lerde ve 80'lerde iç denetim faaliyetinin kapsamı daha da genişlemiştir. Amerika'da çıkarılan 1977 tarihli ABD Rüşvetin Önlenmesi ve Yabancı Ülkelerde Yolsuzluk Uygulamaları Kanunu (Foreign Corrupt Practices Act-FCPA) sonrası pek çok şirket iç denetim kadrolarını oluşturmuş ya da mevcut birimlerin ölçü ve kalitelerini arttırmışlardır. (Kurnaz & Çetinoğlu, 2010). Bu yıllarda işletmelerin faaliyetlerinin etkinliği üzerinde yoğunlaşmış, uygunluk denetiminin yapılması ve işletme faaliyetlerinin etkinliğinin denetlenmesi iç denetimin odak noktası haline gelmiştir (Memiş, 2006: 83).

İç denetim faaliyeti 90'lı yıllarda işletmenin amaçlarına ulaşılması için gerekli bir fonksiyon olarak görülmeye başlanmıştır. Böylelikle iç denetim sadece geçmişe bağlı kalmayan, bugünü ve geleceği de dikkate alarak işletme yönetimine rehberlik eden ve işletmenin kısa orta ve uzun vadeli hedeflerine ulaşmasına yardımcı olan bir işletme fonksiyonu haline gelmiştir (Adiloğlu, 2010).

Milenyuma kadar yaşanan süreçte, iç denetimin kapsamı giderek genişlemiş ve iç denetim işletmeye artı değer katma amacını güden bir yapı halini almıştır (Uyar, 2009: 55; Dittenhofer ve ark, 2010: 83). İç denetim mesleğinin tarihsel gelişimi Tablo 1.3'te özetlenmiştir:

Tablo 1.3. İç Denetim Faaliyetini Etkileyen Tarihsel Gelişmeler

Tarih	Faaliyet
1933	Amerika Birleşik Devletleri Menkul Kıymetler ve Borsa Komisyonu (Security Exchange Commission- SEC)'nin kurulması.
1941	IIA'nın kurulması

1947	IIA tarafından "İç Denetçiler İçin Sorumluluk Beyanı" (Statement of Responsibilities of the Internal Auditors) nın yayımlanması.
1968	IIA etik kurallarının onaylanması.
1974	İlk sertifikalı iç denetçi sınavı yapılması.
1977	ABD Rüşvetin Önlenmesi ve Yabancı Ülkelerde Yolsuzluk Uygulamaları Kanunu'nun çıkarılması
1978	IIA İç Denetim Mesleki Uygulamaları İçin Mesleki Standartlar dokümanının ilk kez yayımlanması.
1985	COSO (Committee of Sponsoring Organizations)'nun faaliyetlerine başlaması.
1989	IIA'nın İç Denetim Standartları'nı yayımlanması.
1991	SAS (Statement of Auditing Standards) no: 65 " Denetçilerin Mali Tabloların Denetiminde İç Denetim Fonksiyonunun Değerlendirilmesi" (The Auditors Consideration of the Internal Audit Function in an Audit of Financial Statement) nin yayımlanması.
1992	COSO'nun "İç Kontrol Çerçevesini" yayımlanması.
1995	Kanada'da Kanada Yeminli Mali Müşavirler Enstitüsü (Canadian Institute of Chartered Accountants-CICA) tarafından " Kanada İç Kontrol Modelinin (Canadian Institute of Chartered Accountants' Criteria of Control Framework-CoCo) yayımlanması.
1999	İngiltere'de Finansal Raporlama Konseyi (The Financial Reporting Council-FRC) tarafından Turnbull Raporunun yayımlanması.
2002	Amerika'da Sarbanes-Oxley Yasası'nın yürürlüğe girmesi
2006	COSO'nun Kurumsal Risk Yönetimi Çerçevesini yayımlanması

2009	IIA'nın Uluslararası İç Denetim Mesleki Uygulama Çerçevesini uygulamaya koyması
2013	COSO'nun "İç Kontrol Çerçevesi"nin güncellenmesi
2013	IIA tarafından "Etkili Risk Yönetimi ve Kontrolünde Üç Savunma Hattı" adlı dokümanın yayımlanması.
2017	COSO'nun "Kurumsal Risk Yönetimi Çerçevesi"nin güncellenmesi

Kaynak: Mollaoğulları, 2018.

1.4. İç Denetimin Unsurları

IIA' nın tanımına göre iç denetim; işletme faaliyetlerinin geliştirilmesi ve değer katılması amacını taşımakta olan bağımsızlığı ve tarafsızlığı ile ön plana çıkan bir güvence danışmanlık etkinliğidir (Cömert, 2008: 24). İç denetim faaliyetinin asli görevi işletmelere güvence ve danışmanlık hizmeti sunmaktır. İç denetim işletmelerin faaliyetlerinin geliştirilmesine yardımcı olmakta ve işletmeye pozitif değer katmaktadır. Bağımsız ve tarafsız olarak yürütülen iç denetim faaliyetleri sistematik ve disiplinli çalışmalar bütünüdür (Keskin, 2006). Bu tanım ışığında iç denetimin unsurları aşağıdaki başlıklar halinde verilmiştir:

- Bağımsızlık ve tarafsızlık,
- Danışmanlık ve güvence hizmeti,
- İşletme faaliyetlerinin geliştirilmesi ve değer katılması,
- Sistematik ve disiplinli bir yaklaşıma sahip olma.

1.4.1. Bağımsızlık ve Tarafsızlık

İç denetim faaliyetinin özünde tarafsızlık yer almaktadır. Tarafsızlık; iç denetçilerin çalışmaları esnasında ön yargı ve çıkar çatışmasından uzak duracak şekilde davranmaları anlamına gelmektedir. İç denetim faaliyeti her aşamasında (kapsamın belirlenmesi, denetimin yürütülmesi ve raporlama) her türlü müdahale ile baskıdan uzak

olmalıdır. Buna paralel olarak iç denetçiler de tarafsız ve önyargısız bir şekilde davranmalı ve çıkar çatışmalarından kaçınmalıdır. İç denetim faaliyeti öznel değerlendirmelerden etkilenmemelidir. Denetim sürecinde ve sonuçların değerlendirilmesinde mevcut olanların temel alınması, iç denetim faaliyetlerini gerçekleştiren iç denetçilerin değerlendirmelerde tarafsızlıkla ve dürüst bir şekilde karar vermesi, üst yönetimle denetleme sonuçlarıyla ilgilenen kişilerin kurumun genel durumuyla alakalı en sağlıklı bilgiye sahip olması bakımından önem taşımaktadır (Korkmaz, 2007: 5).

Bağımsızlığın sağlanması için iç denetim biriminin doğrudan işletmenin yönetim kademesine rapor verecek biçimde kurgulanması gerekmektedir. Üst yönetim aksi yönde düşünse bile iç denetçiler, riskli gördüğü her alanı denetleme hususunda bağımsız faaliyet gösterebilmelidir. Üst yönetimden bağımsız ve özgür biçimde faaliyet gösteremeyen iç denetçilerin faaliyetlerinin güvenilirliği şüphe arz edecektir. Bu nedenle, iç denetçilere yönetim karşısında özgürlük tanınması ve faaliyetlerini gerçekleştirirken engellenmemesi gerekmektedir (Özeren, 2000; Güler, 2010).

1.4.2. Danışmanlık ve Güvence Hizmeti

İç denetim faaliyeti güvence ve danışmanlık fonksiyonlarından meydana gelmektedir. İç denetimin güvence fonksiyonu; iç denetçilerin operasyonları sonucunda elde ettiği verileri nesnel bir şekilde değerlendirmesi ve bağımsız bir denetim görüşü oluşturmasını kapsamaktadır (Aslan, 2010: 67-68).

İç denetim, işletmenin amaçlarını, faaliyetlerini ve kaynaklarını etkileyen risk öğeleriyle ilgili kontrolleri ve süreçleri inceleyerek bunlara dair güvence vermektedir. Ancak bu güvence hiçbir zaman %100'lük bir garanti olamaz. IIA'nın tanımında iç denetimin "tam güvence" değil, ancak "makul ölçüde güvence" sağlayabileceği belirtilmiştir. İç denetimin vermiş olduğu güvence hizmeti ile; işletmenin ortaya çıkması muhtemel riskleri belirlenecek ve bu risklerin herhangi bir zarara yol açmadan minimize edilmesi mümkün olabilecektir. Finansal riskler ve faaliyetlere ilişkin risklerin tespit edilip işletme yönetimine raporlanması işletmeler açısından hayati önem taşımaktadır (Pickett, 2005: 119).

Danışmanlık fonksiyonu ise; iç denetçilerin işletme faaliyetlerine değer katmak amacıyla üst yönetime tavsiyelerde bulunmasıdır (Burton ve ark., 2012: 151-152). İç kontrol sisteminin geliştirilmesine ve iyileştirilmesine yardımcı olma ve işletme yönetimine iç kontrol sistemi hakkında önerilerde bulunma iç denetimin danışmanlık hizmetleri kapsamına girmektedir (Akyel, 2010).

Danışmanlık fonksiyonu, iç denetimin işletme faaliyetlerine artı değer kattığı faaliyetlerin başında gelmektedir. Danışmanlık hizmeti genel olarak güvence hizmetinin bir sonucu olarak ortaya çıkmakla birlikte, güvence hizmetleri de bazı durumlarda danışmanlık faaliyetleri sonucu ortaya çıkabilmektedir (IIA, 2013). İç denetçiler, denetim faaliyeti sonucu ortaya çıkan bulgularla işletme yöneticilerine, işletmenin amaçlarına ve hedeflerine uygun olarak hareket edildiği ve kaynakların etkin verimli ve ekonomik bir biçimde kullanılıp kullanılmadığı hakkında rapor vermektedir. Ayrıca faaliyetlerinin mevzuat ve yasalara uygunluğu, işletmenin kaynaklarının korunması, mevcut iç kontrollerin yeterliliği, işletmede üretilen bilginin güvenilirliği vb. konularda güvence ve danışmanlık hizmeti vermektedir (Adiloğlu, 2010: 10).

1.4.3. İşletme Faaliyetlerinin Geliştirilmesi ve Değer Katılması

Bağımsız ve tarafsız bir faaliyet olan iç denetim; işletme faaliyetlerinin etkinliğini değerlendirmesine ek olarak, işletmenin risk yönetimi, iç kontrol ve kurumsal yönetim süreçlerinin de etkinliğini değerlendirip ve bu faaliyetlerin geliştirilmesine yardımcı olmaktadır.

Geçmişte iç denetim, işlemlere ve hataları tespit etmeye yönelik bir yaklaşıma sahipken, günümüzde süreçlere odaklanmaktadır. Günümüzde iç denetim uygulamaları, faaliyetlerin etkinliğinin artırılmasına yönelik bir anlayış benimsemektedir (Uğurlu, 2019: 23).

İç denetim faaliyetinin işletmeye değer katma fonksiyonu, paydaşların ve diğer çıkar gruplarının beklentileri sonucu ortaya çıkmaktadır. Bu paydaşları ve çıkar gruplarını devlet, işletme yönetimi, denetim komitesi, bağımsız denetçiler, çalışanlar, müşteriler ve tedarikçiler oluşturmaktadır. İşletme yönetimi, genel olarak faaliyetlerinin etkinliğinin artması ile ilgilenmektedir. Bağımsız denetçiler ise iç denetimin, işletmenin finansal

yapısıyla ilgili görev yüklerini azaltan bir iç kontrol aracı görevini üstlenip üstlenmediğiyle ilgilenmektedirler (Anderson, 2003). İşletmelerin iç denetim faaliyetlerinin güvenilir olması bağımsız denetçilerin denetim çalışmalarını nitelik, süre ve kapsam açısından etkilemektedir. (Munro & Steward, 2010: 371-372) İşletmelerin ürün ve hizmetlerinden faydalanan müşterileri, devlet ve diğer paydaşları ise iç denetimin işletme bilgilerinin doğru ve güvenilir olduğuna dair bir makul güvence sağlamasını beklemektedir (Esen, 2019).

Aslında iç denetim faaliyetinin en önemli gayesi, işletmenin faaliyetlerini ve süreçlerini göz önünde bulundurarak işletmeye amaç ve hedeflerine ulaşması için katkı sağlamaktadır. İç denetçiler, işletmelerin stratejik amaçları ve geleceğe yönelik hedefleri hakkında yeterli bilgiye sahip olmalı ve işletmelerin gereksinimleri doğrultusunda çalışmalarını sürdürmelidir. Ayrıca işletmeye danışmanlık yapma amacıyla, hazırladığı raporlarda iyileştirici ve geliştirici tavsiyeler yer almalıdır. (Chapman & Anderson, 2003, 4).

1.4.4. Sistematik ve Disiplinli Bir Yaklaşım Sahip Olma

İç denetim, iç denetim standartlarının yayımlanması ile sistematik bir faaliyet haline gelmiştir. İç denetçilere yönelik düzenlemeler, mesleki uygulama çerçeveleri ve etik kurallar, iç denetimin uluslararası seviyede kabul görmüş düzenlemelere sahip disiplinli bir meslek olduğunu göstermektedir (Uğurlu, 2019: 28). İç denetim faaliyeti sürekli, disiplinli ve sistematik bir yaklaşıma sahip olduğundan işletmede etkin bir risk yönetiminin kurulmasına yardım etmektedir. Bu süreçte iç denetçilere, yöneticilere ve işletme çalışanlarına düşen birçok sorumluluk bulunmaktadır. Bu görevler Uluslararası İç Denetim Standartları kanalıyla detaylı olarak açıklanmıştır. İç denetçiler, iç denetim faaliyetlerini, İç Denetim Mesleki Uygulama Çerçevesi ışığında sistematik ve disiplinli şekilde yürütmekle yükümlüdürler (Adiloğlu, 2010, 10).

1.5. İç Denetimin Kapsamı

Günümüzde gerçekleşen teknolojik gelişmeler ve iş dünyasındaki rekabet, iç denetimin fonksiyonunu ve kapsamını değiştirerek, iç denetimi işletmelerin amaçlarına

ulaşmasında kilit unsurlardan birisi haline getirmiştir. İç denetim faaliyeti, işletme faaliyetlerini tamamen kapsamaktadır. İç denetimin amacı, işletmelerin faaliyet ve işlemlerinin, üst yönetimden farklı ve tarafsız bir gözle değerlendirilmesini sağlamaktır (Adiloğlu, 2010).

İşletmelerde, iç kontrol, kurumsal yönetim ve risk yönetimi süreçlerinin kurulması, yönetilmesi ve denetlenmesi üst yönetimin görevidir. İç denetim, üst yönetime işletme faaliyetlerinin etkinliği ve verimliliği hakkında bilgi vermekte ve süreçlerin geliştirilmesi için gerekli tavsiyelerde bulunmaktadır. Böylelikle iç denetim işletmeye değer katmaktadır (IIA, 2009).

İç denetim, işletme faaliyetlerin kontrolü, kurumsal yönetim ve risk yönetimi süreçleri ile ilgili objektif ve bağımsız bir güvence ve danışmanlık hizmeti vererek, işletmelerde hesap verebilirliğin gelişimine katkı sağlamaktadır. (Uzun, 2009)

IIA yayınladığı uluslararası iç denetim mesleki uygulama standartlarında (UMUÇ) iç denetimin, iç kontrol, kurumsal yönetim ve risk yönetimi süreçlerinin geliştirilmesine katkıda bulunacağını vurgulamıştır. 2100–İşin Niteliği standardında iç denetimin kapsamını; *“İç denetim faaliyeti sistematik ve disiplinli bir yaklaşımla, yönetim, risk yönetimi ve kontrol süreçlerini değerlendirmek ve bu süreçlerin iyileştirilmesine katkıda bulunmak zorundadır.”* şeklinde tanımlamıştır (IIA, 2013).

Bu kapsamda çalışmada iç denetim ile ilgili faaliyet alanları temel olarak iç kontrol, kurumsal yönetim ve risk yönetimi ana başlıkları altında incelenecektir.

1.5.1. İç Kontrol

İç kontrol, işletmenin sahip olduğu varlıkların her türlü zarardan ve tehlikeden korunmasını, işletme faaliyetlerin etkinliğinin ve verimliliğinin artırılmasını, muhasebe bilgilerinin güvenilirliğinin ve doğruluğunun güvence altına alınmasını, önceden belirlenmiş yönetim politika ve prosedürlerinin doğru ve düzgün biçimde uygulanmasını sağlamak amacıyla gerçekleştirilen tüm önlem ve yöntemleri içermektedir (Güredin, 2014).

İşletmelerin zaman içerisinde büyümesi ve artan iş hacmi, operasyonların ve faaliyetlerin giderek karmaşık hale gelmesine neden olmuştur. Bu durum işletme sahiplerinin ve/veya yöneticilerinin işletmeleri doğrudan kontrol etmesini imkânsız hale getirmiştir. Olumsuz gibi görünen bu durumun çözümü ancak etkin bir iç kontrol sisteminin faaliyete geçmesi ile mümkündür (Aksoy, 2007: 215). İç kontrol sisteminin etkinliğinin sağlanması, işletmelerin hedeflerine ulaşmasını kolaylaştırmaktadır. Etkin bir iç kontrol yapısı oluşturulmasındaki temel amaçlar; “işletmenin varlıklarının korunması” “işletmenin raporlarının güvenilirliğinin sağlanması”, “işletmenin hedeflerine verimli ve etkin şekilde ulaşılmasının sağlanması” ve “kanunlara ve işletme yöneticilerinin belirlediği kurallara uyumun sağlanması” olarak özetlenebilmektedir (Türedi, 2000).

Finansal bilgilerin güvenilirliğini, işletme varlıklarının korunmasını, faaliyetlerin mevzuata uygun, etkin ve verimli bir şekilde gerçekleştirilmesini sağlayan iç kontrol sistemi işletmeler için oldukça önemlidir (Dabbağoğlu, 2007: 160-161). Etkin bir iç kontrol sisteminin temel amaçları aşağıdaki gibidir (Kepekçi, 2004: 71; Yereli & Özdoğan, 2009: 60):

- İşletme varlıklarının korunması.
- Finansal bilgilerin doğruluğunun ve güvenilirliğinin sağlanması.
- İşletme faaliyetlerinin etkin ve verimli bir şekilde gerçekleştirilmesinin sağlanması.
- Faaliyetlerin ve operasyonların önceden belirlenmiş işletme politikalarına ve yasal mevzuata uygunluğunun sağlanması.
- İşletme yönetimi tarafından belirlenmiş amaç ve hedeflere ulaşılmasının sağlanması.

İşletme faaliyetleri büyüyüp karmaşılaştıkça ve işlem sayıları arttıkça, işletme yönetiminin; varlıkların korunması, hataların ortadan kaldırılması ve politikaların değerlendirilmesi gibi amaçları gerçekleştirmek için zamanında ve güvenilir veriler elde etmesi zorunluluk haline gelmiştir (Kızılboğa & Özşahin, 2013: 223). Tüm bunlara ek olarak işletmeler açısından günümüzde, paydaşlara ve diğer çıkar gruplarına sürekli olarak bilgi verme bir gereklilik haline gelmiştir. Bu nedenle işletmelere ait finansal ve finansal olmayan veri ve bilgiler ekonomik ve etkin biçimde üretilmeli, saklanmalı ve ilgililerle paylaşılmalıdır. Finansal bilgileri üreten muhasebe bilgi sisteminin, muhasebe

verilerinin güvenilirliğini sağlamak için etkin bir biçimde çalışan iç kontrol sistemine ihtiyacı vardır. Günümüzde özellikle muhasebe işlemlerinin gerçekleştirilmesinde bilgisayarların kullanılması, iç kontrolün önemini daha da artırmıştır (Kalkınoğlu, 2003: 75).

İşletmelerin iç kontrol yapısının yeterliliğini ve etkinliğini değerlendirmeleri için geliştirilmiş çeşitli modeller bulunmaktadır. Bu modeller arasında en yaygın olarak kullanılanı COSO çerçevesidir. COSO işletmelerin, iç kontrol kavramını oluşturan temel yapılara, değerlere ve süreçlere, eskiden olduğu gibi dar kapsamlı finansal odaklanmanın çok ötesinde, geniş kapsamlı bir odaklanmaya olanak tanıyan güçlü bir araçtır ve uluslararası düzeyde en çok kabul gören iç kontrol çerçevesidir (Bakkal & Kasımoğlu, 2012). Ancak işletmelerin iç kontrol sistemlerinin etkinliğini değerlendirmek amacıyla COSO dışında da birçok model kullanılmaktadır. Kanada CoCo, İngiltere Turnbull modellerini kullanırken, Uluslararası Standartlar Örgütü (International Organization for Standardization-ISO) de iç kontrol ile ilgili kullanılmak üzere birçok standart yayımlamıştır. Aşağıdaki bölümlerde, COSO, CoCo ve Turnbull iç kontrol modellerinin karşılaştırılmasına (Tablo 1.4) ve modellerle ilgili açıklamalara yer verilmiştir.

Tablo 1.4. Uluslararası İç Kontrol Modellerinin Karşılaştırılması

İçerik	COSO	CoCo	Turnbull
Odaklandığı Konular	İç kontrol, iç kontrolün öğeleri ve boyutları	Davranışsal unsurlar	Yönetim kurulunun iç kontrol sürecindeki sorumlulukları
Bileşenleri	5 temel bileşen ve 17 ilke	4 temel bileşen ve 20 ilke	5 temel bileşen
Bileşenlerin İçeriği	Kontrol ortamı, risk değerlendirme, kontrol faaliyetleri,	Hedefler, sorumluluk,	Kontrol ortamı ve faaliyetleri, risk değerlendirme, bilgi

	bilgi ve iletişim ile izleme.	yetkinlik, izleme ve öğrenme.	ve iletişim ile izleme.
Yayımlanma tarihleri	1992 (En son 2013 yılında güncellendi)	1995	1999 (En son 2015 yılında güncellendi)
Yayımlayan Organizasyonlar	IIA, AICPA, ABD Muhasebeciler Birliği, Yönetim Muhasebecileri Enstitüsü ve Finans Yöneticileri Derneği	Kanada Yeminli Mali Müşavirler Enstitüsü (Canadian Institute of Chartered Accountants-CICA)	Birleşik Krallık Finansal Raporlama Konseyi
Uygulamaya yönelik rehber	İşletmelerde iç kontrol sisteminin kurulması, yürütülmesi ve etkinliğinin değerlendirilmesi konularında yol göstermektedir.	Uygulamaya yönelik sınırlı bilgi vermektedir. İç kontrol sisteminin bileşenlerini teorik olarak açıklamaktadır.	Uygulamaya yönelik örnek olay ve modeller yer almaktadır. Daha çok iç kontrol sisteminin kurulması ve yönetilmesi ile ilgili görev sorumlulukların belirlenmesine odaklanmıştır.
Bilgi Sistemleri Kontrollerine Yer Vermesi	Konuyu ilişkin içerik yer almamaktadır.	Konuyu ilişkin içerik yer almamaktadır.	Konuyu ilişkin içerik yer almamaktadır.

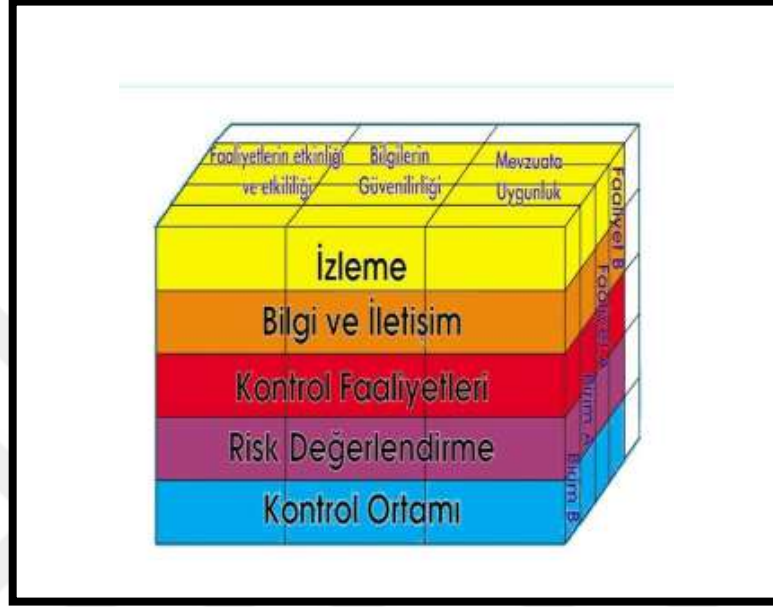
Kaynak: Türedi ve ark., 2015, 115

1.5.1.1. COSO İç Kontrol Çerçevesi

1985 yılında iç denetim ve iç kontrol uygulamalarını yönlendiren ve temel amacı finansal raporlamayı daha kaliteli hale getirmek olan COSO faaliyetlerine başlamıştır. COSO; IIA, ABD Yeminli Serbest Muhasebeciler Enstitüsü (American Institute of Certified Public Accountants-AICPA), Amerikan Muhasebe Derneği (American Accounting Association -AAA), Yönetim Muhasebecileri Enstitüsü (Institute of Management Accountants-IMA) ve Finans Yöneticileri Derneği (Financial Executives International-FEI) ,nin verdikleri desteklerle kurulmuş ve uluslararası olarak da kabul görmüş bir örgüttür. Kuruluş, 1992 yılında iç kontrol çerçevesini ve 2004 yılında da kurumsal risk yönetimi çerçevesini yayınlamıştır. 2013 yılında iç kontrol çerçevesi ve 2017 yılında da kurumsal risk yönetimi çerçevesi güncellenmiştir. (COSO, 2020).

COSO iç kontrol çerçevesi, barındırdığı içeriğin daha zengin olması ve işletmeler için uygulamada yol gösterici olması nedeniyle diğer çerçevelerden ayrılmaktadır. COSO, strateji, faaliyet, raporlama ve uyumla ilgili kısa, orta ve uzun vadeli hedefleri içeren sürecin nasıl planlanması gerektiğini ortaya koyan bir çerçevedir. COSO iç kontrol çerçevesinde 5 temel bileşen ve bileşenleri oluşturan 17 ilke bulunmaktadır. Temel bileşenler; kontrol ortamı, risk değerlendirme, kontrol faaliyetleri, bilgi ve iletişim ve izlemedir. COSO'nun 2013 yılında güncellenen İç Kontrol Çerçevesinde sunulan bu temel bileşenler ve bileşenleri destekleyen ilkeler aşağıda açıklanmıştır:

Şekil 1.1. COSO Küpü



Kaynak: Moeller, 2014

a. Kontrol Ortamı:

COSO, 2013'de yayınladığı iç kontrol çerçevesinde kontrol ortamını işletme genelinde iç kontrolün yürütülmesine dayanak oluşturan standartlar, süreçler ve yapılar kümesi olarak tanımlamıştır (COSO, 2013). Kontrol ortamı, işletmelerin sahip olduğu risklerin işletme çalışanları tarafından tespit edilmesi ve risklerle ilgili süreçlerin yönlendirilmesine bir temel oluşturmaktadır. Kontrol ortamı; ortaya çıkan/çıkması beklenen riskler ve bu risklerin yönetimi, risk iştahı, risk kapasitesi, ahlaki değerler, dürüstlük ve faaliyet gösterilen çevre gibi unsurları içermektedir. İç kontrol çerçevesinin diğer tüm bileşenlerini kapsayan iç kontrol ortamı kurumun çalışma ortamını ifade ederken, aynı zamanda iç kontrol unsurlarının temelini oluşturmaktadır. Bu kavram; tutum, davranış, farkındalık, yeterlilik, örgütsel yapı, dış etkenler, yetki ve sorumluluğun paylaştırılması ve üslup gibi kavramları bünyesinde barındırmakta ve gücünün çoğunu üst yönetim kadrosunun oluşturduğu tutumlardan almaktadır (Alpman, 2007: 2; Gönen, 2009: 195). Görevlerin dağılımı ve yönetim biçimi, tanımlanmış rol ve sorumluluklar ve kıymet hareketlerinin yetkilendirilmesi gibi işletme yönetimiyle alakalı kavramlar da yine

kontrol ortamı içinde yer almaktadır. Kontrol ortamı, iç kontrol faaliyetlerinin başarısını ve iç kontrolün diğer bileşenlerini doğrudan etkilemektedir (Keskin, 2009).

COSO'nun 2013 çerçevesinde sunulan kontrol ortamı bileşeninin temelini oluşturan ilkeler şunlardır (Mollaoğulları, 2018):

- Dürüstlük ve ahlaki ilkelere bağlılık,
- Yönetim kurulunun bağımsız bir biçimde iç kontrol sistemini izlemesi,
- Organizasyon yapısı, raporlama ilişkileri, yetki ve sorumlulukların belirlenmesi,
- Uzmanlaşmanın sağlanması,
- Hesap verebilirliğin güçlendirilmesi.

b) Risk Değerleme:

Risk Değerleme, işletmelerin amaçlarına ulaşmasını engelleyen önemli riskleri analiz ve tespit etme, bu riskleri minimize edecek prosedürleri tasarlama sürecidir (Ceyhan & Apan, 2014: 182). Risk değerlendirme yapılmasının temel amacı; işletmelerin mevcut koşullarını, fırsatlarını, risklerini belirlemek ve değerlendirmektir. Ayrıca bir diğer amaç; gelecekte meydana gelmesi muhtemel risklerle başa çıkabilmek amacıyla iç kontrolde sürekli değişiklik ve iyileştirme yapmaktır. Riskleri tamamen ortadan kaldırmak veya yok etmek mümkün olamayacağı için iç kontrol sisteminin temel amacı, bu risklerin iyi yönetilmesi ve kontrol altında tutulmasını sağlamaktır. Risklerin zamanında ve doğru şekilde tespit edilmesi için iç kontrol faaliyetinin risk esaslı olarak yürütülmesi gerekmektedir. Çünkü iç kontrol sürecinin başarıya ulaşması ancak işletmelere ait risk faktörlerinin işletme üzerinde nasıl ve ne derece etki yaratacağının tespiti ile mümkündür. Dolayısıyla, işletmelerin kuvvetli ya da zayıf taraflarının tespit edilmesi için analizlerin yapılması, riskli alanlarının belirlenmesi ve kontrol faaliyetlerinin bu alanlarda yoğunlaştırılması gerekmektedir. Risk tespit edilip tanımlandıktan sonra işletme üzerindeki muhtemel etkileri ile gerçekleşme ihtimallerinin değerlendirilmesi gerekmektedir. (Ceyhan & Apan, 2014: 183).

Risk deęerlendirmesi, deęiřen kořulların sũrekli takibinin saęlanmasını ve bu doęrultuda i kontrol faaliyetlerin de deęiřen řartlara dinamik bir řekilde ayak uydurmasını ifade etmektedir. (İbiř ve atıkkař, 2012: 102). COSO'nun 2013 erevesinde ortaya koyulan risk deęerlendirme bileřenini oluřturan ilkeler řunlardır (COSO, 2013):

- Kuruluřun hedeflerinin aık ve net bir řekilde belirlenmesi,
- Risklerin tespiti, tanımlanması ve analiz edilmesi,
- Suiistimal risklerinin deęerlendirilmesi,
- nemli deęiřikliklerin kurumu etkileme ihtimallerinin deęerlendirilmesi.

c) Kontrol Faaliyetleri

Kontrol faaliyetleri, olası risklere karřı alınacak nlemlerin etkili bir biimde uygulanması, mevcut risklerin risk kapasitesi ierisinde tutulması ve iřletmelerin yasalara ve dięer dũzenlemelere uyumunun sũrekli hale gelmesi iin belirlenen politikalar ve prosedũrleri ifade etmektedir (Tũredi & Koban, 2016: 160). Bu politika ve prosedũrler, iřletme ynetiminin direktiflerinin yerine getirilmesini saęlamak iin belirlenmektedir. İřletme genelinde, her kademedede ve bũtũn faaliyetlerde geerlidirler. Kontrol faaliyetleri, ynetimin hedeflerin geekleřtirilmesine ynelik riskleri azaltma, ynergelerinin yerine getirilmesini saęlamaya yardımcı olan politikalar ve prosedũrler aracılıęıyla oluřturulan eylemlerdir. Kontrol faaliyetleri, iřletmenin tũm seviyelerinde, iř sũrelerinde eřitli ařamalarda ve teknoloji ortamında geekleřtirilmektedir. (COSO, 2013). Kontrol faaliyetleri aynı zamanda, iřletme ũst ynetiminin i kontrol sistemini yapısal hale getirme abaları ve kendi hedeflerine ulařmak iin ortaya koyduęu nlemlerin tamamıdır. (Kaval, 2005: 127).

COSO yayınladıęı i kontrol erevesinde (2013), kontrol faaliyetlerine iliřkin ilkeleri ařaęıdaki řekilde belirlemiřtir (COSO, 2013):

- Kontrol faaliyetlerinin belirlenmesi ve geliřtirilmesi
- Teknoloji ũzerindeki genel kontrollerin ortaya koyulması ve geliřtirilmesi
- Kontrol faaliyetlerine iliřkin politika ve prosedũrlerin oluřturulması.

d) Bilgi ve İletişim:

İşletmelerin gereksinim duyduğu bilgileri elde etmesini ve bunların ilgili birimlere zamanda aktarılmasını sağlayan sistemler etkin bir iç kontrol sisteminin en temel ögelerindendir. İşletmelerin hedeflerine ulaşılması için iç kontrol sorumluluklarının yerine getirilmesi son derece önemlidir. İç kontrol biriminin de sorumluluklarını yerine getirebilmesi için bilgi gereklidir. İşletme yönetimi, iç kontrolün diğer bileşenlerinin işleyişini desteklemek için hem iç hem de dış kaynaklardan ilgili kaliteli bilgileri almakta veya üretmekte daha sonra bunları kullanmaktadır. İletişim ise, gerekli bilgilerin sağlanması, paylaşılması ve elde edilmesi amacıyla gerçekleştirilen sürekli, yinelenen bir süreçtir (COSO, 2013). Elde edilen bilgilerin ilgili kişilere ulaşmasını sağlayacak yatay, dikey ve çapraz iletişim kanallarının işler olması gerekmektedir. Bilgi ve iletişim bileşeni var olan bilgilerin diğer dört bileşene aktarımını ve koordinasyonunu sağlayarak iç kontrol sisteminin etkin çalışmasını sağlamaktadır. Etkin bir bilgi-iletişim sistemi her türlü bilginin kaydedilmesini, sınıflandırılmasını ve raporlanmasını kapsayan yöntemleri içermek zorundadır (Gökçen, 2019: 156).

COSO'nun 2013 çerçevesinde sunulan bilgi ve iletişim bileşeninin temelini oluşturan ilkeler şunlardır:

- Faaliyetlerle alakalı kaliteli bilginin temin edilmesi ve kullanılması,
- Hedefler, sorumluluklar vb. bilgilerin işletme çalışanlarıyla paylaşılması,
- İşletme dışı paydaşlar ile iletişim kurulması.

e) İzleme:

İzleme işletmelerin hedeflerine ulaşması için gerekli olan iç kontrol sisteminin istenilen şekilde işleyip işlemediğini, yeni koşullara uyum sağlayıp sağlamadığını belirlemek ve sistemdeki zayıf, aksayan yönlerin tespit edilerek iç kontrol sisteminin

sürekli olarak etkin bir şekilde işlemlerini sağlamak amacıyla yürütülen süreç olarak tanımlanmaktadır (Korga & Aslanoğlu, 2020: 100).

İzleme bileşeni sayesinde iç kontrol ortamı ve işletme faaliyetleri ile ilgili yapılan sürekli değerlendirmeler, işletmenin farklı seviyelerinde iş süreçlerine zamanında bilgi sağlamaktadır. Değerlendirmeler sonucunda elde edilen bulgular, iç kontrol ile ilgili olarak belirlenen kriterlere göre değerlendirilmekte ve eksikler yönetim ve yönetim kurullarına uygun şekilde iletilmektedir (COSO, 2013). Bu kapsamda izleme faaliyetlerine ilişkin ilkeler aşağıdaki gibidir;

- Sürekli ve periyodik olarak özel değerlendirmeler yapılması,
- Eksikliklerin değerlendirilmesi ve ilgili taraflara iletilmesi.

İç kontrol izleme unsuruyla beraber performansın belirli bir zaman aralığındaki kalitesi değerlendirilmekte ve denetim ya da diğer incelemelerin ortaya çıkan sonuçlarının hızlı bir şekilde çözüme kavuşturulması güvence altına alınmaktadır. Bu bağlamda izleme unsuru iç kontrol performansının sürekli veya belirli zaman aralıklarında izlenmesi olarak da tanımlanabilmektedir. Büyük ölçekli işletmelerde holdinglerde ve finans kuruluşlarında izleme fonksiyonu genellikle iç denetim birimlerince ve denetim komiteleri tarafından gerçekleştirilmektedir (Uzay, 2009: 102).

1.5.1.2. CoCo Çerçevesi

CICA tarafından geliştirilmiş uluslararası bir standarttır. CICA kontrol anlayışlarını aşağıdaki şekilde açıklamaktadır (Pickett, 2011: 109):

“Kontrol çok geniş kapsamı olan bir kavramdır. Kontrol, işletmelerin amaçlarına ulaşmasına yardımcı olan çalışanları destekleyen kaynaklar, sistemler, süreçler, kültürel yapı ve görevler gibi öğeleri içerir. Kontrolün etkinliği sadece her bir öğenin ayrı ayrı ele alınması ile değerlendirilemez. Bir işletmedeki kontrol öğeleri ve ölçütleri birbiriyle ilişkilidir. Kontrol bileşenleri birbirlerinden ayrı olarak tasarlanamaz veya değerlendirilemez. Kontrol risklerin tanımlanmasını ve azaltılmasını kapsamalıdır. Bu riskler sadece belirli bir hedefe ulaşmayla ilgili bilinen riskleri değil, aynı zamanda kuruluşun uygulanabilirliği ve başarısı için iki temel riski içerir:

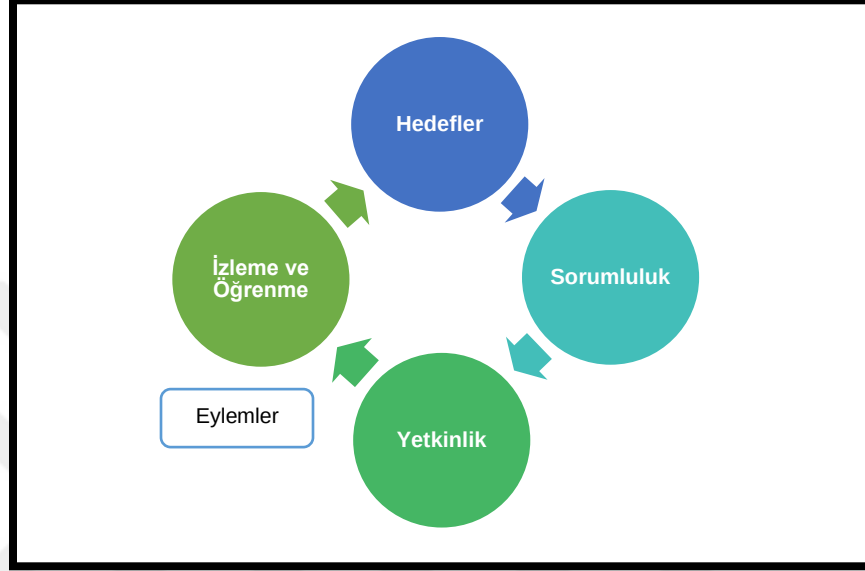
- *İşletmelerin fırsatları belirleme ve kullanma kapasitesini sürdürmemesi.*
- *İşletmelerin beklenmedik risklere ve fırsatlara uyum sağlayamaması ve kesin bilgilerin yokluğunda eksik ve yanlış bilgilere dayanarak karar vermesi.”*

Çerçeveye göre işletmelerde iç kontrolün etkinliğini değerlendirme sorumluluğu yönetim kuruluna aittir. Bu değerlendirme ilkeleri aşağıdaki gibidir (Pickett, 2011: 109):

- Değerlendirme, işletmelerin önemli hedeflerine ve bu hedeflerle ilgili risklerin yönetimine odaklanmalıdır.
- Değerlendirme, işletmeyi bir bütün olarak ele almalıdır.
- Değerlendirme sürecinin sorumluluğu yönetim kurulu başkanına (Chief Executive Officer-CEO) aittir.
- Değerlendirme, işletmenin her bölümünden çalışanların bakış açısını içeren kapsamlı ve güvenilir bir süreçtir.
- Değerlendirme, CICA kontrol çerçevesinin kriterlerine dayanmalıdır.
- Değerlendirme uygun beceri, bilgi, nitelik ve bakış açısına sahip kişilerce yapılmalıdır.
- Değerlendirme sonuçları yönetim kuruluna raporlanmalıdır.
- Değerlendirme süreci gözden geçirilerek gerekli iyileştirmeler tespit edilmelidir.

CoCo çerçevesini oluşturan bileşenler Şekil 1.2.'de sunulmuştur:

Şekil 1.2. CoCo Çerçevesini Oluşturan Bileşenler



Kaynak: Pickett, 2011

Hedefler: Çerçeveye göre işletme hedeflerinin açıkça tanımlanması gerekmektedir. Bu tanımlamada işletme stratejileri, misyon, vizyon, riskler, fırsatlar, politikalar, planlama ve performans göstergeleri yer almalıdır. Bu doğrultuda (Türedi ve ark., 2011: 97);

- İşletme hedeflerini paydaşları ile paylaşmalıdır.
- Önemli iç ve dış risk faktörleri belirlenmeli ve bunlara yönelik önlemler alınmalıdır.
- İşletmenin hedeflerine ulaşmasını sağlayan ve risklerin önlenmesini destekleyen ilkeler hazırlanmalı ve bu ilkeler çalışanlar ile paylaşılmalıdır.
- İşletmenin hedeflerine ulaşmasını sağlamak için planlama yapılmalıdır.
- Planlama süreci, stratejik hedefler ve performans ölçütlerini içermelidir.

Sorumluluk: Çerçevenin bu bölümünde, kontrol faaliyetleri ile işletme hedeflerinin eş güdümlü bir şekilde nasıl yürütüleceği, kurumsal yönetim ilkeleri ve iç kontrol yapısının etkileşimi ve çalışanların bu yapıyı benimsemesinin önemi belirtilmektedir. Bu bileşen, iç kontrol ortamı içerisinde var olan insan faktörünün etkisini ve önem derecesini anlatmaktadır. Buna göre (Türedi ve ark., 2015: 97);

- Etik kodlar tüm işletmeye uygulanmalı ve işletme çalışanları konu hakkında bilgilendirilmelidir,
- İnsan kaynakları prensipleri ve uygulamaları işletmenin hedefleri ve ahlaki değerleri ile uyum içerisinde olmalıdır,
- Hesap verebilirlik, yetkilendirme, görev ve sorumluluk dağılımı, net ve anlaşılır şekilde, işletme hedeflerine uygun bir biçimde tasarlanmalıdır,
- İşletmede çalışanlar için bir güven ortamı oluşturulmalıdır.

Yetkinlik: Bu bölümde iç kontrol ortamının yeterli ve etkin bir şekilde işlerliğini sürdürebilmesi için çalışanların yetkinliklerinin geliştirilmesi gerektiğinin altı çizilmektedir. Yetkinlik, çalışanların sadece iyi performans göstermekle kalmayıp aynı zamanda riskleri değerlendirebilmek ve kontrollerin bu risklerle başa çıkmasını kolaylaştırmak için doğru becerilere, deneyime ve tutumlara sahip olmasını sağlamaktır. Çünkü açık bir hedefin olduğu ve herkesin iyi kontroller tasarlamaya ve yürütmeye hazır olduğu işletmelerde bazı uzmanlıkların geliştirilmesine ihtiyaç vardır (Pickett, 2011: 109). Bu amaçla (Türedi ve ark., 2015);

- Çalışanlar, kontrol modelinin gerekliliklerini anlamak ve yerine getirmek için gerekli kaynaklarla donatılmalıdır.
- İletişim süreci, işletmenin stratejik hedeflerinin gerçekleştirilmesine destek vermelidir.
- İşletme bölümlerinin karar alma süreçleri ve faaliyetleri koordineli şekilde gerçekleştirilmelidir.
- Kontrol faaliyetleri; işletmenin hedefleri, riskleri ve iç kontrol sistemi ile ilgili diğer öğeler ve bunların birbirleri ile olan ilişkileri göz önüne alınarak tasarlanmalıdır.

Eylemler: Bu aşama, kontrol edilen aktivitelerin gerçekleştirilmesini içermektedir. Çerçeveye göre; çalışanlar harekete geçmeden önce, açık bir amaca, sorun ve fırsatlarla başa çıkma yeteneğine sahip olmalıdır. Bu ön koşullardan sonra gelen her eylemin başarılı bir sonuca ulaşma şansı daha yüksektir. (Türedi ve ark., 2015)

İzleme ve Öğrenme: İlgili bölümde iç kontrol ortamının yaşayan ve gelişmeye devam eden bir yapıda olması gerektiği aktarılmıştır. İzleme ve öğrenme bileşenin ilkeleri aşağıdaki gibidir (Türedi ve ark., 2015):

- İşletmenin faaliyetlerinin ve kontrol ortamının etkinliğini hakkında değerlendirme yapabilmek için işletmenin iç ve dış çevresi izlenmelidir.
- İşletme performansı, işletmenin stratejik amaçlarında yer alan ve planlama sürecinde belirlenen başarı kriterleri kullanılarak ölçülmelidir.
- İşletmenin iç kontrol ortamının altyapısı düzenli olarak denetlenmelidir,
- Kontrol ortamında yapılan değişiklikler sistematik bir şekilde takip edilmelidir.
- İşletmenin iç kontrol ortamının etkinliği değerlendirip çıktılar çalışanlar ile paylaşmalıdır.

1.5.1.3. Turnbull Raporu

1999 yılında Birleşik Krallık 'ta Finansal Raporlama Konseyi tarafından yayımlanmıştır. Raporun tam adı “İç Kontrol, Birleştirilmiş Kurallar Üzerine Yönetim Kurulu Üyeleri İçin Rehber (Internal Control: Guidance for Directors on the Combined Code)”dır. Birleşik Krallıkta borsaya kote işletmelerin kurumsal yönetim uygulamalarına ve mevzuatına bağlılığını ve uyumunu arttırmayı amaçlayan rapor kurumsal yönetim ve risk yönetimi süreçlerinde iç denetimin rolünü vurgulamaktadır.

2015 yılında tarihinde rapor güncellenmiştir. Güncellenen rapor “giriş”, “etkin bir iç kontrol yapısı yönetme”, “iç kontrol ortamının etkinliğinin değerlendirilmesi”, “iç kontrole ilişkin yönetim kurulu açıklamaları” ve “ek bölüm” olmak üzere 5 kısımdan oluşmaktadır (The Financial Reporting Council, 2015: 2).

Raporda iç kontrol ve risk yönetimi süreçlerinin önemi aşağıdaki gibi açıklanmıştır (The Financial Reporting Council, 2015: 3):

- İşletme risklerinin kontrol altında tutulması etkin bir iç kontrol yapısı ile mümkündür.

- İç kontrol işletme varlıklarının korunmasını, finansal raporlama süreçlerinin güvenilir şekilde yürütülmesini, faaliyetlerini etkin ve verimli bir şekilde gerçekleştirilmesini ve kanunlar ile düzelmelere uyum sağlanmasını kolaylaştırmaktadır.
- Etkin bir muhasebe sistemi ve finansal kontroller iç kontrolün önemli bir ögesidir. Bu ögeler, işletme varlıklarının kötüye kullanılması ve hileli finansal raporlamanın tespit edilmesine ve engellenmesinde önemli rol oynamaktadır.
- İşletmeler çoğunlukla dinamik bir iç kontrol ortamına sahip olduğundan, amaçları ve operasyonel süreçleri de sürekli bir değişim içerisinde. Bu durum işletmelerin risklerinin de değişkenlik göstermesine yol açmaktadır. İşletmelerin iç kontrol yapısı değişen riskleri tespit edebilecek bir yapıya sahip olmalıdır. Finansal başarı kontrollü bir şekilde risk almayı gerektirdiğinden iç kontrol riskleri yok etmek yerine riskleri kontrol altında tutmak için çalışmalıdır.

Raporda etkin bir iç kontrol ortamının ögeleri aşağıdaki gibi sıralanmıştır (The Financial Reporting Council, 2015: 7):

- İşletmelerin faaliyetlerini sorunsuz ve verimli bir biçimde sürdürebilmesi için en uygun politikalar ile yönetmeliklerin belirlenmesi, görevlerin dağılımının doğru şekilde yapılması etkin bir iç kontrol ortamının en önemli gerekliliklerindendir.
- İç kontroller işletme faaliyetlerini ve amaçlarını sektöre uğratması muhtemel her risk unsuruna cevap verebilecek şekilde tasarlanmalıdır.
- İşletme yönetimine ve dış paydaşlarına yapılan raporlamanın kapsamı, zamanlılığı ve güvenilirliği iç kontrol yapısının etkinliğine bağlıdır.
- İç kontrol örgüt kültürünün özelliklerini yansıtmalıdır.
- Üretilen bilginin paylaşımı, işletme içi sürekli iletişim ve gözlem faaliyetleri etkin bir iç kontrol ortamının en önemli unsurlarındandır.
- İşletmede karşılaşılan sorunların, kontrol ortamındaki zayıflıkların ve bunlara yapılan müdahalelerin üst yönetime zamanında raporlanmasını sağlayan politika ve yönetmelikler yürürlükte olmalıdır.

Rapora göre; iç kontrolün etkinliğinin değerlendirilmesi, yönetim kurulunun görevidir. İşletme yönetimi yıllık faaliyet raporunda iç kontrole ilişkin açıklama ve

bildirimleri yayımlamak zorundadır. Yönetim kurulu, hazırlanan iç kontrol raporlarını değerlendirmeli ve yıllık faaliyet raporu yayımlanmadan iç kontrolün etkinliğini belirlemek amacıyla kapsamlı bir gözden geçirme çalışması yapmalıdır (Türedi ve ark., 2015).

Buna göre, yönetim kurulunun iç kontrolü değerlendirirken dikkat etmesi gereken hususlar ise aşağıdaki gibidir (The Financial Reporting Council, 2015):

- İşletme için tehdit oluşturacak risklerin tespiti, değerlendirme süreci ve yönetimi.
- Mevcut iç kontrollerin risklerin önlenmesi veya minimize edilmesinde ne derecede etkin olduğu,
- Karşılaşılan sorunların, kontrol ortamındaki zayıflıkların raporlanma sürecinin etkinliği.
- İç kontrol ortamındaki zafiyetlere ve sorunların önlenmesine yönelik önlemlerin alınıp alınmadığı.
- İç kontrol raporlarında yer alan tespitler, kapsamlı bir inceleme ve değerlendirme gerektiriyorsa, gereğinin yapılması.

Ayrıca yönetim kurulu iç kontrol raporlarını gözden geçirirken aşağıda yer alan başlıkları dikkate almalıdır (Türedi ve ark., 2015):

- Bir önceki dönemde gerçekleştirilen gözden geçirmeden sonra risklerin ne ölçüde değiştiğinin tespiti.
- İşletmenin değişen risklerine ne ölçüde cevap verildiği.
- Değerlendirme sürecinin içeriği ve kapsamı ile mevcut olması durumunda iç denetim biriminin de değerlendirilmesi.
- Risklerin işletmenin faaliyet çıktılarına olan etkilerinin analizi.

1.5.2. Kurumsal Yönetişim

Kurumsal yönetim kavramı İngilizcedeki “corporate governance” teriminin Türkçe tercümesidir. Kurumsal yönetim kavramının dünyada kabul gören tek bir tanımı bulunmamaktadır. Kurumsal yönetim nerede ne zaman ne amaçla ve kimler tarafından

kullanıldığına veya buna ilişkin ilkelerin hangi kuruluş ve örgüt tarafından yayımlandığına bağlı olarak farklı şekillerde tanımlanabilmektedir.

Kurumsal yönetim ilkelerinin dünya genelinde yaygın bir şekilde uygulanması yönünde çalışmalar yapan “İktisadi İş birliği ve Kalkınma Örgütü” (Organisation for Economic Co-operation and Development-OECD) tarafından yayımlanan ilkelerde; *“Kurumsal yönetim; bir şirketin yönetimi, yönetim kurulu, hissedarları ve diğer paydaşlar arasındaki bir dizi ilişkiyi kapsar. Kurumsal yönetim aynı zamanda şirketin hedeflerinin belirlendiği bir yapıyı ortaya koymakta ve bu hedeflere nasıl ulaşılabileceğinin ve performansın nasıl denetleneceğinin yollarını çizmektedir.”* (OECD, 2004).

Ülgen ve Mirze’ye (2004) göre kurumsal yönetim; *“işletmenin stratejik yönetimi ile görevli ve sorumlu üst yönetimin, görevlerini ve sorumluluklarını yerine getirirken, işletme üzerinde kendilerini belirli sebeplerle “hak sahibi” gören pay sahipleri, çalışanları, tedarikçileri müşterileri ve diğer toplumsal kurumlarla olan ilişkilerini kapsar.”*

Türkiye Kurumsal Yönetim Derneği (TKYD) ve Deloitte (2006) kurumsal yönetimi; *“şirket yönetiminde, iş süreçlerinde, pay ve menfaat sahipleri ile ilişkilerde eşitlik, şeffaflık, hesap verilebilirlik ve sorumluluk yaklaşımı ile şirket faaliyetlerinin etkinlik ve verimliliği, raporlama güvenilirliği, yasal düzenlemelere uygunluk, pay ve menfaat sahiplerinin hak ve çıkarlarının korunması için güvence sağlayan yaklaşım ve ilkeler”* olarak tanımlamıştır.

IIA Uluslararası İç Denetim Standartları, iç denetim terimler sözlüğünde kurumsal yönetim; *“Yönetim kurulu tarafından, kurumun amaçlarına ulaşmaya yönelik olarak, kurumun faaliyetlerinin raporlanması, yönlendirilmesi, yönetilmesi ve izlenmesi gayesiyle uygulanan yapı ve süreçlerin bir birleşimidir.”* şeklinde açıklanmıştır (TİDE, 2011).

Üst yönetim tarafından işletmenin hedeflerine ulaşması için oluşturulan örgütsel yapı, yönetim kademeleri arasındaki yetki ve sorumluluk dağılımı, işletmenin sahip olduğu varlıklar, raporlama ilişkileri, insan kaynağı, üretim, satış, işletme içi düzenlemeler, işletmenin içinde bulunduğu ekonomik ve yasal çevre kurumsal yönetimin birer unsurudur (Paşaoğlu ve ark., 2013).

Kurumsal yönetim yaklaşımı ve bu yaklaşıma öncülük eden unsurların oluşmasına zemin hazırlayan olay ve gelişmelerin başlangıcı 17.yy'a kadar dayanmaktadır. Ancak iç denetim faaliyetinin de önemli bileşenlerinden biri olan modern kurumsal yönetim anlayışının netlik kazanması ve yaygınlaşması 1990'lı yılların başında gerçekleşmeye başlamıştır. Tablo 1.5.'te kurumsal yönetişimin gelişimine etki eden tarihsel olaylar özet olarak sunulmuştur:

Tablo 1.5. Kurumsal Yönetişimin Tarihsel Gelişimi

Tarih	Faaliyet
1600'ler	İngiltere ve Hollanda'da faaliyet gösteren Doğu Hindistan (East India) şirketinin sahiplik ile kontrolü ayıran bir çeşit yönetim kurulu yapısını oluşturması
1776	Adam Smith'in "Ulusların Refahı (The Wealth of Nations)" adlı kitabında işletmelerin kontrol edilmesindeki zafiyetlere dikkat çekmesi
1844	İngiltere'de anonim şirket kanununun çıkarılması
1933-34	ABD'de SEC'e (Security Exchange Commission) denetim yetkisi veren kanunların yürürlüğe girmesi
1968	Avrupa Birliği'nin ilk kez şirketler hukuku direktifini kabul etmesi
1987	COSO tarafından hileli finansal raporlama ile denetim komitesinin rol ve sorumlulukları konularında öneriler getiren ve iç kontrol için bir çerçeve geliştiren raporun yayımlanması
1992	İngiltere'de Cadbury Komitesi tarafından ilk kurumsal yönetim kodunun yayımlanması

1993	İngiltere’de şirketlere “uygula ya da uygulayamıyorsan açıkla” (comply or explain) yaklaşımı çerçevesinde kurumsal yönetim uygulamalarını açıklama zorunluluğu getirilmesi
1994	Güney Afrika’da King Raporu’nun yayımlanması
1995	Fransa’da Vienot Raporu’nun yayımlanması
1996	Hollanda’da Peters Raporu’nun yayımlanması
1997-98	Asya Krizi
1999	OECD Kurumsal Yönetişim İlkelerinin yayımlanması
2001-02	Enron ve WorldCom Skandalları
2002	Sarbanes-Oxley kanununun çıkarılması
2003	İngiltere’de Higgs Raporu’nun yayımlanması
2004	OECD Kurumsal Yönetişim İlkelerinin güncellenmesi
2008	Global Finansal Kriz ve sonrasında Lehmann Brothers’ın iflası

Kaynak: Alp ve Kılıç, 2014: 47-48

Tablo 1.5.’de de özetlendiği üzere; özellikle 90’lı yılların sonunda önemli uluslararası örgütler ile kuruluşlar ve bilhassa ülkeler kurumsal yönetim ile alakalı raporlar, kodlar ve ilkeler yayımlamıştır. Böylelikle kurumsal yönetim uygulamaları, iç kontrol ve risk yönetimi uygulamaları ile işletmelerin faaliyetlerini sürdürebilme kabiliyetlerini doğrudan etkiler hale gelmiştir.

Kurumsal yönetim ilkeleri, ülkeden ülkeye veya piyasadan piyasaya değişiklik gösterse de tüm dünyada kabul gören kurumsal yönetişimin temel prensipleri “şeffaflık”, “adillik veya eşitlik”, “hesap verebilirlik” ve “sorumluluktur (SPK, 2011, Pamukçu 2011: 136):

- a) **Şeffaflık:** kurumsal yönetişimin dayandığı şeffaflık (transparency) ilkesi, işletme ile ilgili her türlü finansal ve finansal olmayan bilgilerin işletmenin ortaklarına ve diğer tüm paydaşlarına doğru, tamam, eksiksiz, anlaşılabilir, zamanında düşük maliyetle ve erişimi kolay bir şekilde sunulmasını gerektirmektedir (Kavut, 2010:12). Eğer bir bilgi herhangi bir paydaşın aldığı kararı etkiliyorsa önemli bir bilgidir ve açıklanması gerekmektedir. İşletmelerin faaliyet sonuçları, denetimden geçmiş finansal tablo ve raporları, şirketin hedef ve beklentileri, ortaklık yapısı, yönetim kurulu ve üst yönetimi ve bunların aldığı prim, ikramiyeler ve ücretler, ilişkili taraflarla yapılan işlemler, öngörülebilir risk unsurları, işletmeye ait süreç ve politikalar, karşı karşıya olduğu davalar vb. finansal ve finansal olmayan bilgiler bu kapsama girmektedir (Alp & Kılıç, 2014: 59). Ayrıca bu bilgilerin doğru ve objektif bir biçimde sunulması, denetimden geçmiş olması paydaşların kolaylıkla erişebileceği bir platformda paylaşılması önemlidir. Paydaşların bilgileri analiz etmesi ve yorumlamalarına imkân tanınması ve bilgilerin karşılaştırılabilir bir formatta sunulması da şeffaflık ilkesinin gereğidir (Alp & Kılıç, 2014: 60).
- b) **Adillik veya Eşitlik:** (fairness) anlam olarak, aynı niteliktekilere veya aynı şartlarda olanlara aynı şekilde muamele edilmesi demektir (Kavut, 2010: 13). Kurumsal yönetişim açısından adillik ilkesi dört önemli ögeden oluşmaktadır. İlk olarak işletmeler bu ilke gereği tüm paydaşlarına adil davranmalı ve bunlar arasında ayrımcılık yapmamalıdır. Ayrıca aynı paydaş sınıfı içerisinde yer alan kişi ve kuruluşlara eşit yaklaşılmalıdır. Üçüncü olarak içeriden bilgi sahibi olanların fırsat eşitliğini bozacak şekilde ticaret yapmalarına izin verilmemelidir. Son olarak, adillik ilkesi, bir olayda veya işlemde yönetim kurulu ve işletmenin üst yöneticilerinin şirkete çıkar çatışması durumunu, yönetim kuruluna önceden beyan etmelerini zorunlu kılmaktadır (Alp & Kılıç, 2014, 60).
- c) **Hesap verebilirlik:** (accountability) bir konuda yetki kullanan, karar alan, işlem yapan ya da faaliyette bulunan kişilerin veya organların kullandıkları yetki, aldıkları karar, yaptıkları işlemler, yürüttükleri faaliyetler nedeniyle sorumlu tutulması ve kendisinden açıklama istenmesidir (Kavut, 2010: 12). Hesap verenler, gözetimi ve denetimi altında oldukları kişi ve organlara, kullandıkları yetkilerin, aldıkları kararların, yaptıkları işlemlerin ve yürüttükleri faaliyetlerin gerek şekil ve gerekse içerik bakımından mevcut düzenlemelere, belirlenmiş

amaç ve prosedürlere, etik kurallara ve işin gereğine uygun olduğunu ispat etmekle yükümlülerdir. Hesap verilebilirlik ilkesinin uygulanmasında; işletmede her düzeyde yetki, görev ve sorumlulukların açık ve net bir şekilde tanımlanması, hesap verme yükümlülüğünün verilen yetki ile orantılı olması, güçlü ve etkin iç kontrol yapısı ile iç denetim ve bağımsız denetim mekanizmalarının varlığı önem taşımaktadır. (Alp & Kılıç, 2014: 61).

d) Sorumluluk: (responsibility) ilkesi; özetle işletmelerin kanunlara ve toplumsal değer ve düzenlemelere uyum gösterecek şekilde faaliyet göstermesini ifade etmektedir (Kavut, 2010: 13). Kurumsal sosyal sorumluluk (corporate social responsibility) olarak da isimlendirilen bu ilke, işletmelerin faaliyetlerini sürdürürken yasal düzenlemelere ve hatta bu düzenlemelerde ötesinde topluma saygılı ve duyarlı davranması gerekliliğini savunmaktadır (TKYD & Deloitte, 2006: 5). Faaliyetleri yürütürken toplumun istek ve ihtiyaçlarını dikkate almak ve çevreye duyarlı olmak, işletmelerin varlığını sürdürmesine ve toplum nezdinde bilinirliğini ve güveni arttırarak değerinin yükselmesine neden olacaktır.

Yukarıda kısaca açıklanan bu unsurlar kapsamında kurumsal yönetimin amaçları şu şekilde sıralanabilmektedir (Küçüksözen & Küçükkocaoğlu, 2005: 83):

- Paydaş haklarının kuvvetlendirilmesi,
- Muhasebe standartlarının geliştirilerek finansal raporlamada şeffaflığın sağlanması,
- Yönetim kurulu bağımsızlığının sağlanması,
- Rekabetin teşvik edilerek haksız kazancın önüne geçilmesi,
- Kurallara uymamaktan kaynaklı ortaya çıkan cezaların uygulanabilirliğinin artırılması.

Doğru kurumsal yönetim uygulamaları işletmelere ve işletme ile ilişkili tüm çıkar gruplarına bir takım önemli faydalar sağlamaktadır. Örneğin; kurumsal yönetim ilkelerine uyum, sermaye maliyetlerinde azalma, finansmana erişim kolaylığı, sermaye piyasalarıyla daha fazla etkileşim ve kaliteli finansal raporlama uygulamalarını beraberinde getirmektedir. Ayrıca, aile içi çıkar çatışmalarının önüne geçen iyi kurumsal

yönetişim uygulamaları, üst yönetimin de keyfi uygulamalarının önüne geçerek işletmeye yetenekli insan kaynağı kazandırmanın yanı sıra, etkin bir iç kontrol yapısının oluşturulmasını sağlayarak işletmeye itibar ve katma değer de kazandırmaktadır (Sözüer ve ark., 2012).

Kurumsal yönetim ile iç denetim yakın etkileşim halindedir. Bunun yanı sıra kurumsal yönetim iç kontrol sistemiyle, kurumsal risk yönetimiyle, bağımsız denetimle, yönetim kuruluyla ve yönetim kurulunun komiteleriyle de yakın iletişim ve etkileşim halindedir. Günümüzde küreselleşmenin etkisi ve teknolojik ilerlemelerin sonucu iş dünyasının ve işletmelerin yapılarının karmaşık hale gelmesi, bir takım yönetsel sorunları beraberinde getirmiş ve kontrol faaliyetlerinin zorunluluk haline gelmesine sebebiyet vermiştir. Bu durum kontrol faaliyetlerini yürütecek uzman kişilerin varlığını gerekli kılmıştır. İşletmelerde söz konusu faaliyetleri gerçekleştirecek yegâne kişiler şüphesiz iç denetçilerdir (Baykara, 2014).

İç denetimin görevini objektif ve bağımsız bir biçimde ifa edebilmesi için, işletme yönetiminin ve ortakların etki ve baskısından korunması gerekmektedir. Bu durum işletmede bağımsız ve etkin bir biçimde faaliyetlerini sürdüren yönetim kurulu bulunması ile, bir başka ifadeyle; kurumsal yönetim ilkelerinin hakkıyla uygulandığı bir organizasyon yapısı ile mümkündür. IIA standartlarına göre bir iç denetim biriminin tam bağımsız olabilmesi için doğrudan yönetim kuruluna bağlı olması gerekmektedir. Dolayısıyla iç denetim ve kurumsal yönetim arasında sıkı bir bağlantı bulunmaktadır (Özdoğan, 2014).

1.5.3. Risk Yönetimi

IIA Uluslararası İç Denetim Standartları risk kavramını *“Risk, amaçlara ulaşılması üzerinde etkili olacak bir olayın meydana gelme ihtimalidir. Risk, söz konusu etki ve olasılık cinsinden hesaplanır.”* şeklinde tanımlamıştır. Tanıma göre risk, işletmelerin hedeflerine ulaşmasına etki edecek bir durumun ortaya çıkma olasılığıdır (IIA, 2008).

IIA’ ya göre risk yönetimi ise; işletmenin hedeflerine ulaşabilmesi için gerekli güvenceyi sağlamak ve gerçekleşmesi muhtemel olayları belirleyerek, bu olayların

gerçekleşmesi durumunda bu olaylara ilişkin değerlendirmeler yapma, süreci yönetme ve kontrol etme şeklinde tanımlamıştır (TİDE, 2008).

Risk yönetimi, işletmelerin iç ya da dış çevre ögelerinden kaynaklı risklere karşı direncini artırmak amacıyla gerçekleştirilen ve temel amacı işletmeler açısından risk-getiri oranını makul seviyelere getirmek olan bir raporlama ve denetim faaliyetidir (Alptürk, 2008: 265 – 266).

Risk yönetimi kavramı ilk olarak 1960'lı yıllarda sigortacılık sektöründe kullanılmaya başlanmıştır (Dionne, 2013). 1970'lerde mali risklerin yönetilebilmesi amacıyla türev mali araçlar ortaya çıkmış, 1973- 1979 yılları arasında körfez petrol krizi esnasında risk oranlama ve değerlendirme alanında danışmanlık hizmeti verilmeye başlanmıştır. Sonraki on yılda işletmeler için politik riskler önemli hale gelmiştir. Finans sektöründe faaliyet gösteren işletmeler öngörülemeyen riskleri azaltmak ve yönetebilmek için içsel risk yönetimi modelleri oluşturmaya başlamışlardır. Doksanlardan günümüze kadar geçen zamanda risk yönetimi işletmeler için önem verilen bir mesele haline gelmiştir. Bu süreçte işletmeler için detaylı bir risk yönetim kapsamının belirlenmesi, iç denetimin risk yönetim uygulamalarıyla entegre hale gelmesi gerçekleşmiştir. Ayrıca, risk farkındalığının işletme kültürüne yerleşmesi, risk yönetiminde üst yönetimin sorumluluğunun artırılması ve işletmelerde risk yönetim biriminin kurulması gibi önemli ilerlemeler yaşanmıştır (Beyhan, 2018: 20).

Son yıllarda işletmeler, farklı risk türlerini tespit ve analiz etmeye ve söz konusu riskleri yönetmeye başlamışlardır. İşletmeler hedeflerini gerçekleştirebilme amacıyla, içinde bulundukları piyasa ve rekabet koşullarını dikkate alan kısa, orta ve uzun vadeli stratejiler geliştirmekte ve bu stratejilerle de risk yönetimi faaliyetlerini yoğunlaştıracakları alanları belirleyip aynı zamanda risk yönetimine bir yol haritası çıkarmaktadırlar (Yücel ve ark., 2007).

Risk yönetimi, işletmenin sahip olması muhtemel risklerin tespiti ve değerlendirilmesiyle başlamaktadır. Riskin tespiti ve yapılan analizlerden sonra işletme yönetimi, tespit edilen risklerin kabul edilebilir düzeyde olup olmadığına karar vermektedir. Kabul edilemeyecek düzeyde bir risk tespit edilirse üst yönetim bu durumda

alınacak önlemleri belirlemektedir. Riski önlemek ve olası zararı asgari düzeye indirmek için atılacak en önemli adım etkin bir iç kontrol sisteminin kurulmasıdır (Özoğlu ve ark., 2010: 152)

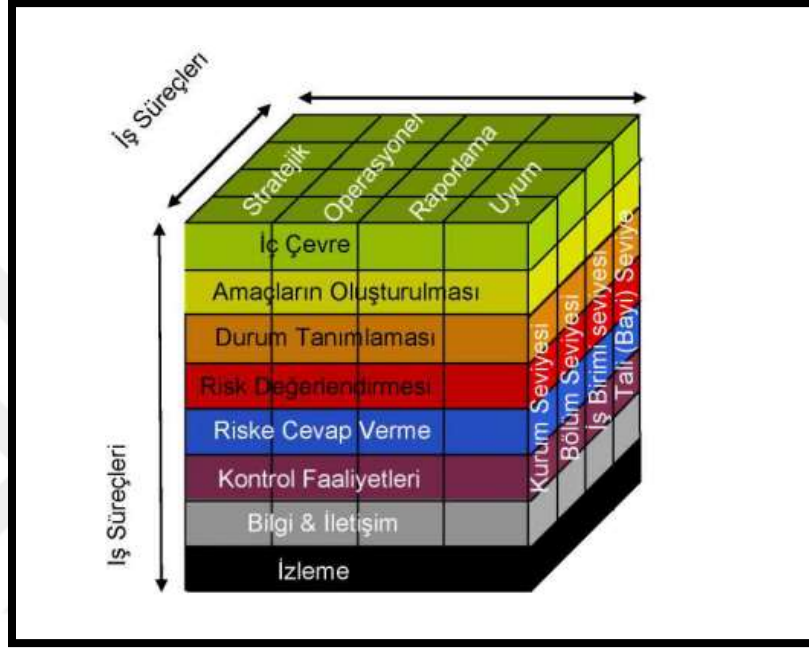
Risk yönetiminin altyapısı oluşturulduktan ve işletmeye adaptasyonu gerçekleştirildikten sonra sistemin işleyişi aşamasına geçilmektedir. Bu aşamaya işletmenin maruz kalması beklenen risklerin tanımlanması ile başlanmaktadır. Tanımlanan risklerin analizi ölçümü gerçekleştirilmektedir. Bu ölçüm ile risklerin şiddetleri ve işletmenin bu risklere ne kadar maruz kalacağı anlaşılmaktadır. Risklerin ölçüm değerleri ve işletmenin maruz kalma seviyesi göz önünde bulundurularak riskler önem derecesine göre sıralanmakta ve böylelikle işletme için en önemli risklerin hangileri olduğu ortaya çıkmaktadır. Öncelikli riskler belirlendikten sonra, bunlar için alınacak önlemlere karar verilerek kararlaştırılan karşılıklar uygulamaya koyulmaktadır. Tüm bu süreç bir yandan izlenmekte, eş zamanlı olarak ortaya çıkan aksaklıklar ortadan kaldırılmakta ve sürekli olarak sistem iyileştirilmektedir (İşgüden, 2012).

İşletmenin belirlediği misyon ve vizyon çerçevesinde; işletme üst yönetimi, işletmenin hedeflerini belirlemekte ve uygulanacak stratejiler şekillendirilmektedir. Aynı zamanda belirlenen bu stratejik planlar; amaç ve hedeflerin etkin ve verimli bir şekilde uygulanması için işletme çalışanları ile paylaşılmaktadır (Tapera, 2014).

Risk yönetimi işletme amaçlarının başarıya ulaşmasına odaklanmıştır ve bu amaçlar dört başlıkta incelenmektedir (İşgüden, 2012):

1. **Stratejik hedefler:** İşletme misyonu ile ilgili üst seviye hedeflerdir.
2. **Operasyonel hedefler:** İşletme varlıklarının etkin ve verimli kullanılmasıdır.
3. **Raporlama hedefleri:** Raporların dürüst ve güvenilir olarak hazırlanmasıdır.
4. **Uygunluk hedefleri:** Yürürlükteki kanun, tüzük ve yönetmelik vb. düzenlemelere uyum sağlanmasıdır.

Şekil 1.3. Kurumsal Risk Yönetiminin Unsurları



Kaynak: T.C. Hazine ve Maliye Bakanlığı, 2019.

COSO, işletmelerin yukarıda anlatılan amaçlara ulaşabilmesi için sekiz öge belirlemiştir. Bu ögeler Tablo 1.6.'da özetlenmiştir.

Tablo 1.6. COSO Risk Yönetimi Çerçevesi Öğeleri

Kontrol Ortamı (İç Çevre):	Kontrol ortamı, risklerin işletme çalışanları tarafından nasıl algılanacağı ve ilgili sürecin nasıl yönlendirileceğine dair temel oluşturmaktadır. Kontrol ortamı işletmeyle alakalı risk yönetimi felsefesi, risk kapasitesi, dürüstlük, etik değerler ve faaliyet gösterilen çevre gibi öğeleri içermektedir. Yetki dağılımı, yönetim biçimi, tanımlanmış rol ve sorumluluklar gibi yönetimle ilgili unsurlar da yine kontrol ortamı içinde yer almaktadır.
Amaçların oluşturulması:	İşletme yönetiminin risk stratejisini göz önünde bulundurarak hedefleri belirlemesi sürecidir. Böylelikle işletmenin risk

	kapasitesi biçimlendirilmekte ve risk toleransı risk kapasitesi ile uyumlu hale getirilmektedir.
Risk (Durum) Tanımlaması:	Risk tanımlama belirsiz durumların risk veya fırsat olup olmadığı konusunda ayırım yapmaya imkân tanımaktadır. Bu aşamada en çok kullanılan yöntemler; grup çalışması (çalıştay), görüşme, anket ve beyin fırtınasıdır. Risklerin sınıflandırılması bu aşamada gerçekleştirilmektedir. Riskler; stratejik riskler, operasyonel riskler, finansal riskler, itibar riski, bilgi teknolojileri riski, düzenleme riski ve bireysel riskler olarak sınıflandırılmaktadır.
Risk Değerlendirilmesi:	Risklerin tanımlanmasından sonra bu risklerin işletme üzerindeki muhtemel etkilerinin ve meydana gelme ihtimallerinin belirlenmesi gerekmektedir. Risk değerlemesinin üç temel ilkesi bulunmaktadır. Bunlar; her bir risk için hem etki hem de olma ihtimallerinin açık bir şekilde göz önünde bulundurulması, risk değerlendirmesinin tesislerin izlenerek ve risk öncelikleri tanımlanarak kaydedilmesi ve risklerin yapısal risk ve artık risk tabanında değerlendirilmesidir.
Riske Cevap Verme:	Riskler değerlendirmesi sonrasında, bu risklerin işletmenin risk kapasitesi ve risk toleransı içindeki yerinin belirlenmesi gerekmektedir. Riske verilecek karşılığın boyutu riskin işletmenin üstlenmeye hazır olduğu seviye sınırı içinde olup olmamasına göre değişmektedir. Riskin yapısı ve seviyesine göre verilecek karşılıklar; kabul etme, kaçınma, azaltma veya paylaşma, şeklinde sınıflandırılmaktadır.
Kontrol Faaliyetleri:	Risklere cevap olarak verilecek karşılıkların belirlenmesinden sonra, riskleri minimum seviyeye indirecek metotlar geliştirme aşamasına geçilmektedir. Kontrol faaliyetleri, risklere verilecek karşılıkların etkili bir biçimde uygulanması, mevcut risklerin risk

	kapasitesi sınırları içinde yönetilmesi ve işletmenin yasa ve yönetmeliklere uyum sağlanmasına yardımcı olmak için uygulamaya konan politika ve prosedürlerdir.
Bilgi İletişim:	Çalışanların sorumluluklarını ifa edebilmesi için ilgili bilginin belirli bir şekilde ve belirli zaman aralıkları ile tanımlanması ve iletilmesidir.
İzleme:	İşletmenin gelişimi ölçmek amacıyla risk yönetiminin uygulamasının izlenmesi ve etkinliği arttırmak için ihtiyaç durumunda çeşitli ayarlamalar yapılmasıdır.

Kaynak: COSO, 2017.

IIA tarafından yayımlanan Uluslararası İç Denetim Standartlarına göre risk temelli planının iç denetim birimi tarafından yapılması zorunludur. İç denetim birimi, üst yönetimin belirlediği risk düzeylerini de içeren risk yönetim çerçevesini dikkate almalıdır. Yönetim herhangi bir risk sınırları belirtmediyse iç denetim birimi, üst yönetimle müzakere ettikten sonra kendi belirlediği risk değerlemesini yapabilmektedir. UMUÇ Nitelik Standartlarına göre iç denetim birimi, iç denetim faaliyetinin planlanmasının ve iç denetim faaliyetlerinin kaynak gereksinimlerinin gözden geçirilmesi ve onayı için üst yönetime, denetim komitesine ve yönetim kuruluna bildirim yapmakla yükümlüdür (IIA, 2009).

İç denetçi işletme faaliyetlerine değer katmayı amaçladığından, denetim planlamasını yaparken işletmenin birincil risklerini tespit edip faaliyetlerini bu alanlarda yoğunlaştırmalıdır. Bu iç denetim yaklaşımı “risk odaklı iç denetim” olarak adlandırılmaktadır. Sonuç olarak, işletmenin hâlihazırda başarılı bir risk yönetimi altyapısının bulunması, iç denetim için sağlıklı bir plan yapılmasına zemin hazırlamaktadır. Risk yönetimi faaliyetinin yeterli olmadığı işletmelerde iç denetim birimi, bu faaliyeti geliştirmekle sorumludur (Özdoğan, 2014).

İç denetim birimi risklerin tespiti, değerlendirilmesi ve yönetimi konularında işletme yönetimine güvence vermelidir. İç denetçiler, risk yönetim sürecinin işletmeden işletmeye

değişebileceğini bilmelidir. Bundan dolayı işletmelerin büyüklüğü, yapısı, çevresi ve örgüt kültürü, işletme hedefleri ile yönetim biçimi gibi konularda tecrübe ve bilgi sahibi olmalıdır (Coderre, 2009: 9). Tüm bunlara ek olarak iç denetim faaliyeti, işletme genelinde işlerliği olan risk yönetim süreçlerinin kurulması ve uygulanması için danışmanlık faaliyetlerinde de bulunmalıdır (Özoğlu ve ark., 2010: 154).

İşletmenin risk yönetimi sürecine dâhil olan kişilerin ve departmanların faaliyetler ve sorumluluklar yerine getirilirken entegre şekilde faaliyet göstermesi önem arz etmektedir. Bu sorumlulukların ve faaliyetlerin, işletmelerin stratejik planlarında, denetim komitesi ve yönetim kurulu tarafından belirlenen yönetmeliklerde, genelgelerinde, faaliyet prosedürlerinde ve diğer yönetsel belgelerde açık bir şekilde ifade edilmesi gerekmektedir (TİDE, 2008).

İç denetim biriminin risk yönetimi sürecinde alacağı rolü tespit etme, işletme yönetiminin ve denetim komitesinin görevidir. İşletme yönetiminin iç denetim biriminin rolü konusundaki görüşü de kurum kültürü, iç denetim personelinin tecrübe ve yeteneği, faaliyet gösterilen ülkenin yerel şartları ve gelenekleri gibi faktörler göz önünde bulundurularak belirlenmektedir (TİDE, 2008).

1.6. İç Denetim Türleri

İç denetimin çalışma evreni işletmenin bütün faaliyetlerini kapsamaktadır. Bunun sonucu olarak farklı iç denetim türleri ortaya çıkmıştır. Uygulamada iç denetim türleri genel olarak finansal denetimler, kontrol güvence denetimleri, mevzuata uygunluk denetimleri, bilgi teknolojileri denetimi, operasyonel denetimler ve hile(yolsuzluk) denetimleri şeklinde sınıflandırılmaktadır.

1.6.1. Finansal Denetimler

Finansal denetimler, faaliyetlerin finansal tablolara doğru aktarılıp aktarılmadığı, finansal tabloların güvenilirliği, muhasebe süreçlerindeki kontrollerin yeterliliği ve etkinliği,

yönetmelik muhasebe kapsamında hazırlanan bilgi ve raporların doğruluğu ve yeterliliğini kapsayan denetimlerdir (PCAOB, 2007).

Paydaşlar ve çıkar grupları işletme ile alakalı karar alırken çoğunlukla finansal tablolardan yararlanmaktadır. Bu nedenle finansal tabloların hata ve hileden arınmış ve eksiksiz olması, genel kabul görmüş muhasebe ilkelerinden sapmaması ve mevzuatlara uygun olarak hazırlanması önem arz etmektedir (Yörüker, 2004).

Finansal denetimde; gerçekleşen finansal olaylar sonucu ortaya çıkan ve işletme yönetiminin iddiaları doğrultusunda hazırlanmış tablolar ile bunları açıklayan dipnotlar denetlenmektedir. Bahsi geçen finansal tabloların ve dipnotların muhasebe standartlarına ve mevzuata uygunluğu, tablolarda yer alan finansal kalemlerinin değerlemesi için kullanılan yöntemlerin geçerliliği, dipnotlar ve açıklamaların doğru ve eksiksiz şekilde raporlanması finansal denetime tabidir. Bağımsız denetçilerden farklı olarak iç denetçiler finansal tabloların doğruluğu hakkında görüş beyan edilebileceği gibi işletme tarafından belirlenmiş yönergelerle uyum, işletmenin yıllık bütçe hedefleriyle mevcut durumu karşılaştırma, işletmenin mali durumunun (gelir-gider) verimlilik ve etkinliği, daha önce yönetim tarafından belirlenmiş olan hedeflere uygunluk gibi konular da görüş bildirebilmektedir. (Badara, 2012: 58).

1.6.2. Kontrol Güvence Denetimleri

Kontrol güvence denetimleri; operasyonel, finansal ve/veya mevzuata uygunluk alanlarına ilişkin önemli kontrol faaliyetlerinin dizaynı ve işlerliğine yönelik sunulan güvence hizmetleridir. İç kontrol sisteminin ve faaliyetlerinin denetimidir (Collier ve ark., 2006).

Kontrol güvence denetimleri ile denetlenen işletmenin faaliyetleri ve iç kontrol sistemi organizasyona katkı sağlayan bir yaklaşımla analiz edilmektedir. Yine bu denetim sayesinde kalitenin ve uygunluğun araştırılması, işletme kaynaklarının ve hâlihazırda uygulamada olan yöntemlerin yeterliliği ölçülmektedir. Özetle; kontrol güvence

denetimlerinin temel amacı, uygulanan kontrol faaliyetlerinin etkinliği ve verimliliğini ölçme gayesiyle iç kontrol sisteminin detaylı olarak incelenmesidir (İşgüden, 2012: 64).

1.6.3. Mevzuata Uygunluk Denetimleri

Mevzuata uygunluk denetimleri; işletme faaliyetlerinin işletmenin uyması gereken iç ve dış mevzuata uygunluğunun denetimidir. (Gantz, 2014). Dış mevzuat; kamu otoriteleri, yasa düzenleme ve denetleme yetkisi olan kurumlar ile bunların dışındaki sektör veya ürün bazında düzenleme ve denetleme yetkisine sahip kurumlar tarafından yapılan düzenlemelerdir. İç mevzuat ise; işletme üst yönetimi tarafından işletme faaliyetlerine yönelik olarak çıkarılan her çeşit yönetmelik, tebliğ, politikalar, stratejiler, prosedürler ve etik kurallar şeklinde tanımlanmaktadır (Mantar, 2013).

Mevzuata uygunluk denetimlerinde amaç; işletme yönetimi veya kamu yetkilileri tarafından belirlenen kanun, politika ve yönerge vb. düzenlemelere işletmenin ne derece uyduğunu tespit etmektir. İç denetçiler işletmelerde bu denetimi gerçekleştirirken; kamu kuruluşlarında ise kamu denetçileri bu denetimleri gerçekleştirmektedir (Bozkurt, 2012).

Günümüz dünyasında kanunların, toplumsal düzenlemelerin, iş dünyası ile ilgili finansal veya finansal olmayan standartların ve raporlama zorunluluklarının, mesleki çerçevelerin giderek ayrıntılı hale gelmesi ve sürekli olarak gelişmesi, işletmeleri bu düzenlemelere uyum konusunda ihtiyatlı davranmaya itmiştir. Küresel ekonomide sayıları giderek artan çok uluslu işletmeler; birden fazla ülkenin mevzuat ve düzenlemelerine adapte olmak durumunda kalmışlardır. Özellikle bu işletmeler, marka değerini korumak ve saygınlıklarını sürdürebilmek için bu düzenlemelere %100 uyumu hedeflemektelerdir. Bu nedenle, uygunluk denetimleri işletmelerin iç denetim birimi açısından her zaman önem arz etmeye devam edecektir. (Koban, 2019).

1.6.4. Bilgi Teknolojileri Denetimi

Bilgi teknolojileri (BT) denetimi; işletmenin tüm teknolojik alt yapısının, donanım, yazılım, güvenlik ve bilgi erişimi konularının belirli prensipler doğrultusunda ve bir kurumsal bilgi teknolojileri yönetimi bakış açısıyla sistemli bir şekilde denetlenmesidir (Koç ve ark., 2019)

Özellikle bilgisayar kullanımının iş dünyasında yaygınlık kazanmasına paralel olarak BT denetimi de ön plana çıkmıştır. BT denetimi, işletmelerin iç kontrol sisteminin kritik bir bileşenini teşkil eden BT kontrollerinin etkin, yeterli ve uyumlu olup olmadığını belirlemektedir (Bellino ve ark., 2007).

BT denetimi, finansal ve finansal olmayan bilgilerini elektronik ortamda üreten ve saklayan işletmeler için yasal zorunluluktan ziyade kurumsal sürdürülebilirliklerinin güvencesi açısından kritik önemi olan bir meseledir. Örneğin; yazılım ve donanımları, bilgi sistemi süreçlerini, finansal veri üretiminde bilgi sistemlerini çoğunlukla kullanan bankacılık sektöründe BT denetimi yasal bir zorunluluk haline gelmiştir (Deloitte, 2020).

Bilgi teknolojileri denetimlerinin yapılmasındaki asıl amaç, bilgisayar ve diğer bilgi sistemleri için hâlihazırda kullanılan kontrolleri, politikaları ve süreçleri inceleyerek ve bu süreçleri iyileştirecek ek kontrolleri belirlemektir. Böylelikle olası riskli vakalar karşısında olası kayıpları en aza indirmek mümkün olacaktır (Kurnaz & Çetinoğlu, 2010: 244).

İşletmelerin muhasebe ile ilgili işlemlerinin bilgi sistemleri kullanılarak oluşturulması kaydedilmesi ve saklanması bilgi teknolojileri denetimini ve bu denetimin iç denetim içindeki ağırlığını ve önemini artırmaktadır. Bu denetimler, finansal denetim ile kontrol ve güvence denetimlerine destek olacak şekilde yürütülebilmekte veya finansalların ya da iç kontrol ortamının risklerini değerlendirmek amacıyla da gerçekleştirilebilmektedir (Adiloğlu, 2010: 22).

BT denetimi konusunda Türkiye ve dünyada kullanılan farklı standartlar ve en iyi uygulamalar mevcuttur. COBIT, ISO 27001 ve ITIL başta olmak üzere, işletmelerin uyguladığı mevzuat, faaliyet gösterdiği sektör, bilgi teknolojilerinin işletme süreçleri içerisindeki önemi göz önünde bulundurularak farklı standartlara göre BT kontrollerinin kurulması ve denetimi mümkündür (Deloitte, 2020).

BT denetimi ile alakalı kanunlar ile diğer mevzuat, standart ve çerçeveler gözden geçirildiğinde bilgi sistemlerinin entegre bir denetim süreci kapsamında değerlendirildiği görülmektedir. Bu yönde, iş süreçlerinde bu teknolojileri yoğun olarak kullanan sektörler ve işletmeler için BT denetimlerinin iç denetim ve bağımsız denetim çalışmalarında bir

zorunluluk haline getirilmesi ve BT denetimi ile alakalı kiři ve kurumların yetkilendirilerek gözetiminin gerçekleştirilmesi önem arz etmektedir (KPMG, 2017: 30).

1.6.5. Operasyonel Denetimler

Operasyonel denetimler, varlıkların korunması, operasyonların etkinlik ve verimlilięi, kârlılık hedeflerinin gerçekleştirilmesine yönelik güvence hizmeti sunulmasıdır (Sawyer ve ark., 2003). Operasyonel denetimler faaliyet denetimi veya performans denetimi olarak da isimlendirilmektedir (Arens ve ark., 2017).

Operasyonel denetimler, işletmelerin temel faaliyetlerinin, finansal kontrollerinin ve bilgi teknolojilerinin tüm boyutlarıyla bağımsız yaklaşımla incelenmesi amacını taşımaktadır. Bu denetim, işletme faaliyetlerinin daha önceden belirlenen amaçlara ne ölçüde ulaşılabilğini tespit etme amacı gütmektedir. Ayrıca işletmelerin iç kontrol sisteminin yeterli, etkin ve verimli olup olmadığı, finansal bilgilerinin güvenilirlik düzeyi, kanunlara ve diğer düzenlemelere uyumu değerlendirmektedir (Kavcı, 2016).

Faaliyet denetimi sonucunda yönetime, ilgili bölüm faaliyetlerinin iyileştirilmesi konusunda önerilerde bulunmaktadır (Güredin, 2014:17). Operasyonel denetimlerin en büyük zorluğu; faaliyetlerin etkinliğini ve verimliliğini nesnel bir şekilde tespit etmek zorunda olmasıdır. (Reider, 1994). Bu denetim faaliyetine esas olacak standartlar için kesin belirlenmiş kriterler mevcut değildir. Denetçiler genellikle kriter olarak bütçe verileri, başarı ölçütleri, rasyoları ve sektör ortalamalarını kullanmaktadırlar (Selimoğlu, 1999: 194).

1.6.6. Hile (Yolsuzluk) Denetimi:

Hile veya suiistimal, sahtekârlık, yolsuzluk, usulsüzlük gibi görevi ve güveni kötüye kullanma olarak adlandırılabilir hukuka aykırı fiillerdir. Hile; para, mal veya hizmet sağlama, hizmeti gerçekleştirme ya da ödemedi kaçınma, kişisel olarak veya iş ile ilgili bir fayda edinmek gibi amaçlarla çeşitli taraflar ve kuruluşlar tarafından gerçekleştirilebilmektedir (TİDE, 2011).

Hileli işlemlerin tespit edilmesi ve hilenin önlenme amacıyla yapılan çalışmalar, hile denetiminin temel konularını oluşturmaktadır. Hile; varlıkların kötüye kullanılması, hileli finansal raporlama ile yolsuzluk ve etik olmayan davranış olarak 3 kategoride sınıflandırılmaktadır (Koban, 2019: 22).

Hile denetimi, iç denetçilerin doğrudan sorumluluk alanına girmemektedir. İç denetim biriminde hile denetimi alanında uzmanlaşmış iç denetçilerin var olması halinde, hileyle ilgili güvence hizmeti verilebilmektedir. Ancak, denetçiler, kontrol ortamının yeterliliğini ve etkinliğini inceleyerek hilenin önlenmesi konusunda hizmet vermelidirler. Örneğin, iç denetçiler, işletmenin varlıklarının çalınması ve kayıt dışı bırakılmasına yönelik girişimleri engelleyebilmek adına caydırıcı denetimler ve yapay zekâ, veri madenciliği, blok zinciri benzeri teknolojik sistemlerden yararlanmalıdırlar (TİDE, 2011).

1.7. İç Denetimin Türk Mevzuatı İçindeki Yeri

Türkiye’ de iç denetim; 6102 sayılı Türk Ticaret Kanunu, 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu, Sermaye Piyasası Kurulu ve Bankacılık Düzenleme ve Denetleme Kurulu (BDDK) düzenlemeleri, Sigorta ve Reasürans ile Emeklilik Şirketleri mevzuatı ve birçok kanun ve düzenlemede kendine yer bulmuştur. Bu kapsamda Türk mevzuatında iç denetimin gelişimi ve kapsamı açıklanmaya çalışılmıştır.

1.7.1. 6102 Sayılı Türk Ticaret Kanunu

6102 sayılı Türk Ticaret Kanunu’nda iç denetime ilişkin doğrudan açık ve doğrudan bir hüküme yer verilmemiştir. 366. madde ve 375. madde iç denetime ilişkin ifadelere yer verilmiştir. Ancak bu ifadeler tavsiye şeklindedir ve işletmeler için herhangi bir zorunluluk getirilmemiştir.

TTK 366 (2)’de *“Yönetim kurulu, işlerin gidişini izlemek, kendisine sunulacak konularda rapor hazırlamak, kararlarını uygulatmak veya iç denetim amacıyla içlerinde yönetim kurulu üyelerinin de bulunabileceği komiteler ve komisyonlar kurabilir.”* ifadesi yer almaktadır.

TTK' nın 375. maddesinin 1. fıkrasının c bendinde aktarıldığı üzere “*Muhasebe, finans denetimi ve şirketin yönetiminin gerektirdiği ölçüde, finansal plânlama için gerekli düzenin kurulması*” işletmenin yönetim kurulunun yetki ve sorumluluğundadır. Bu madde de yer alan “finans denetimi” ibaresi ile iç denetimin kastedildiği kanunun gerekçesinde açıklanmıştır. Gerekçenin devamında; işletmelerin büyüklükleri fark etmeksizin, muhasebe biriminden tamamen bağımsız bir iç denetim birimine gereksinim duyacağı belirtilmiştir.

Türk Ticaret Kanunu, iç denetim ile ilgili düzenlemeleri içermesine rağmen ifadeler tavsiyenin ötesine geçmemekte ve genel olarak kesinlik içermemektedir. Bu nedenle işletmelerin uluslararası standartlarda ve etkin bir iç denetim sistemi kurabilmeleri için konu ile ilgili ek düzenlemelere ihtiyaç duymaları kaçınılmazdır.

1.7.2. 5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu

Ülkemizde kamu mali yönetimiyle ilgili ilk yasal düzenleme, 1927 yılında yürürlüğe giren, Muhasebe-i Umumiye Kanunu’dur (Ergen, 2016). Küçük değişikliklerle yaklaşık seksen sene uygulanan kanun, 2000’lerin başında kamu kurum ve kuruluşlarının ihtiyaç ve beklentilerini karşılamakta yetersiz kalmaya başlamıştır. AB uyum süreci kapsamında; 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu (KMYKK) 24.12.2003 tarihli ve 25326 sayılı Resmî Gazete ’de yayınlanmış ve 1 Ocak 2006 tarihinde yürürlüğe girmiştir (Gösterici, 2006). Kanunun yürürlüğe girmesiyle kamuda iç denetim anlayışı köklü değişikliklere uğramıştır. Kanunun 63. maddesi iç denetimi; “*İç denetim, kamu idaresinin çalışmalarına değer katmak ve geliştirmek için kaynakların ekonomiklik, etkililik ve verimlilik esaslarına göre yönetilip yönetilmediğini değerlendirmek ve rehberlik yapmak amacıyla yapılan bağımsız, nesnel güvence sağlama ve danışmanlık faaliyetidir*” şeklinde tanımlamıştır.

KMYKK 64. maddede “iç denetçilerin görevleri”, 65. maddede “İç denetçinin nitelikleri ve atanması” konuları düzenlenmiştir. Kanunun 66 ve 67. maddelerinde ise İç Denetim Koordinasyon Kurulu’ nun görevleri açıklanmıştır.

1.7.3. SPK Düzenlemeleri

6362 sayılı Sermaye Piyasası Kanunu kapsamında Sermaye Piyasası Kurulunun hesap, işlem ve faaliyetlerinin iç denetimi hakkında usul ve esasların belirlenmesi amacıyla 31/1/2014 tarihinde Sermaye Piyasası Kurulu İç Denetim Usul ve Esasları Hakkında Yönetmelik yayımlanmıştır. Dört bölümden oluşan yönetmelikte; iç denetimin amacı, iç denetim başkanının görev ve yetkileri, iç denetçilerin görevleri, yetkileri ve sorumlulukları ile iç denetimin esasları yer almaktadır.

Yönetmelikte iç denetim; *“Kurul çalışmalarına değer katmak ve geliştirmek için kaynakların ekonomiklik, etkinlik, etkililik ve verimlilik esaslarına göre yönetilip yönetilmediğini değerlendirmek ve rehberlik yapmak amacıyla yapılan bağımsız, nesnel güvence sağlama ve danışmanlık faaliyeti”* şeklinde tanımlanmıştır. Ayrıca yönetmelik iç denetim birimini kurulun risk yönetimi süreçlerinde ve diğer yönetsel süreçlerin idaresinde ve geliştirilmesinde kurula yardımcı olmak ve tavsiyelerde bulunmak üzere kurulan danışma birimi olarak bahsetmektedir. Yönetmelikte iç denetim başkanı ve denetçilerin yetki ve sorumlulukları detaylı bir biçimde açıklanmıştır.

SPK iç denetim ile ilgili olarak ayrıca, Aracı Kurumlarda Uygulanacak İç Denetim Sistemine İlişkin Tebliğ'i çıkarmıştır. Aracı kurumların iç denetim faaliyetine ilişkin esasları ve usulleri belirlemek amacı ile yayımlanan tebliğ, diğer işletmeler açısından da iç denetim alanında önemli bir rehber olma özelliği taşımaktadır (Yılancı, 2015: 24).

1.7.4. BDDK Düzenlemeleri

01 Kasım 2005 tarihi itibarı ile yürürlüğe giren “5411 sayılı Bankacılık Kanunu” beraberinde iç denetim faaliyetine yönelik birçok düzenleme getirmiştir. Kanunun İç Sistemler başlığında yer alan ikinci bölümün 29-32. maddeleri bankaların oluşturması gereken iç sistemler hakkında çeşitli hükümler içermektedir.

29.Madde, *“Bankalar, maruz kaldıkları risklerin izlenmesi, kontrolünün sağlanması amacıyla faaliyetlerinin kapsamı ve yapısıyla uyumlu ve değişen koşullara uygun, tüm şube ve konsolidasyona tâbi ortaklıklarında yeterli ve etkin bir iç kontrol, risk yönetimi ve iç denetim sistemi kurmak ve işletmekle yükümlüdürler. İç kontrol, risk yönetimi ve iç*

denetim sistemlerinin kuruluşu, işleyişi, yeterliliği, oluşturulacak birimler, icra edilecek faaliyetler, üst yönetimin görev ve sorumlulukları ile Kuruma yapılacak raporlamalara ilişkin usûl ve esaslar Kurulca belirlenir.” ibaresini içermektedir.

Kanun'un 32. maddesinde yer alan hüküm ise *“Bankalar bütün birim, şube ve konsolidasyona tâbi ortaklıklarını kapsayan bir iç denetim sistemi kurmak zorundadır. Bu çerçevede, faaliyetlerin mevzuata, ana sözleşmeye, iç düzenlemelere ve bankacılık ilkelerine uygunluğu, banka müfettişleri tarafından denetlenir. İç denetim faaliyetleri, tarafsız ve bağımsız bir şekilde, gerekli meslekî özen gösterilerek, yeterli sayıda müfettiş tarafından yerine getirilir. Ana ortaklık niteliğindeki bankanın iç denetiminde görev alanlar konsolidasyona tabi ortaklıklarda iç denetim görevini ifa edebilir. İç denetimle görevli birimce veya yetkili müfettişlerce Bankacılık Kanunu’nun 29 uncu maddesinin ikinci fıkrası kapsamında düzenlenecek iç denetim raporunun, en az üçer aylık dönemler itibarıyla ve denetim komitesi aracılığıyla yönetim kuruluna tevdi zorunludur.”* şeklindedir.

BDDK 2006 yılında ise yukarıda bahsedilen düzenlemelerle alakalı olarak *“İç Sistemler Yönetmeliğini* çıkarmıştır. Yönetmeliğin ilk maddesinde de amaç ve kapsam *“Bankaların kuracakları iç kontrol, iç denetim ve risk yönetim sistemlerine ve bunların işleyişine ilişkin usul ve esasları düzenlemek”* olarak belirlenmiştir.

Özetle, BDDK yaptığı düzenlemelerle bankalarda; iç denetimi bankaların tüm birimlerini, şubelerini ve konsolide ortaklıklarını kapsayacak şekilde zorunlu hale getirmiştir. Ayrıca iç denetim faaliyetinin amacı, kapsamı, bağımsızlık ve tarafsızlığı, mesleki özen kavramları üzerinde durulmuş, müfettişlerin görevlendirilmesi ve iç denetim raporları gibi konularda düzenlemeler gerçekleştirilmiştir (Ceran, 2009: 170).

1.7.5. Sigorta ve Reasürans ile Emeklilik Şirketleri Mevzuatı

2007 yılında yürürlüğe giren 5684 Sayılı Sigortacılık Kanunu 4. maddesi 8. fıkrasında yer alan hüküm ile sigortacılık sektöründe iç denetim sistemi kurulması zorunlu hale gelmiştir. Aynı madde çerçevesinde sigorta şirketlerine iç denetim hizmetini dışarıdan alabilme hakkı da tanınmıştır.

2008 yılında ise sigortacılık kanununda zorunlu hale getirilen iç denetim sisteminin esaslarını düzenleyen Sigorta ve Reasürans ile Emeklilik Şirketlerinin İç Sistemlerine İlişkin Yönetmelik” yürürlüğe girmiştir. Yayımlanan yönetmelik; iç denetim sisteminin amaç ve kapsamını, iç denetçilerin sahip olmaları gereken özellikleri ve yetkilerini, iç denetim süreçlerini, iç denetimin planlanması aşamasını ve raporlama aşamasını detaylı bir biçimde açıklamıştır.

Bu düzenlemelere ek olarak; Hazine Müsteşarlığı Sigortacılık Genel Müdürlüğü tarafından oluşturulan ve 2004 yılında yayımlanan genelge ile sigorta şirketlerinde iç denetimi birimi oluşturulması ve sorumlu müdür ile bu birimde görev yapacak iç denetçilerin görevlendirilmesi zorunlu hale getirilmiştir (Oksay & Acar, 2007).

1.8. Uluslararası İç Denetim Düzenlemeleri

Dünyada iç denetim faaliyeti ve mesleği ile ilgili birçok yasal düzenleme yürürlüğe girmiş ve standartlar yayımlanmıştır. Yapılan düzenlemelerden bazıları doğrudan iç denetimi ilgilendirirken, bazıları da dolaylı olarak iç denetimle ilişkilidirler. Çalışmanın bu bölümünde dünyada iç denetimle ilgili faaliyet gösteren kuruluşlar ve öne çıkan bazı düzenlemelere yer verilecektir.

1.8.1. İç Denetim ile İlgili Uluslararası Kuruluşlar

Günümüzde iç denetim alanının mevcut durumunu ve gelişmeleri takip etmek, gelişmelere katkıda bulunmak ve iç denetim mesleğinin uluslararası düzeyde itibarını ve tanınırlığını artırmak amacını güden birçok mesleki örgüt ve organizasyon bulunmaktadır. Bu kuruluş ve organizasyonlar aşağıda açıklanmıştır:

1.8.1.1. İç Denetçiler Enstitüsü (IIA)

Uluslararası bir mesleki örgüt olan IIA, 1941 yılında Amerika Birleşik Devletleri’nde kurulmuştur. IIA, dünyada iç denetim mesleğini temsil eden ilk kuruluş olmasının yanı sıra halen iç denetim alanında en çok kabul gören kuruluş konumundadır. IIA üyelerini iç denetim, risk yönetimi, yönetim, iç kontrol ve bilgi teknolojileri denetimi konularında

uzman kişiler oluşturmaktadır. Kuruluşun, mesleki uygulama çerçevesi (Bölüm 1.8.3.'de detaylı olarak açıklanacaktır), iç denetim standartları ve etik ilkelerin yayımlanması konularında mesleğe önemli katkıları bulunmaktadır. Aynı zamanda "Sertifikalı İç Denetçi" (Certified Internal Auditor, CIA) eğitimleri ve sınavları yaparak mesleki sertifikasyon sağlamaktadır. 2020 yılı mart ayı itibarıyla IIA'nın dünya çapında 161.000 sertifikalı denetçisi ve 200.000'den fazla üyesi bulunmaktadır (IIA, 2019).

1.8.1.2. Avrupa İç Denetim Enstitüleri Konfederasyonu (European Confederation of Institutes of Internal Auditing -ECIIA)

1980 yılında faaliyetlerine başlayan ECIIA 2001 yılından bu yana kâr amacı gütmeyen bir kuruluş olarak Brüksel'de faaliyet göstermektedir. Organizasyon aralarında Türkiye'nin de yer aldığı 34 ülkenin iç denetim enstitüsünden oluşmaktadır. ECIIA üyeleri, IIA'nın de önemli bir parçası olup, iç denetim faaliyetlerinin IIA'nın etik ilkelerine ve uluslararası standartlar kapsamında yürütülmesini desteklemektedirler. ECIIA' nın öncelikli amacı, Avrupa'da iç denetim mesleğini geliştirmektir (ECIIA, 2020).

1.8.2. İç Denetim ile İlgili Uluslararası Düzenlemeler

İç denetim alanında tüm dünya tarafından kabul görmüş birçok hukuki düzenleme mevcuttur. İç denetim ile alakalı önemli uluslararası yasal düzenlemeler Tablo 1.7'de sunulmuştur:

Tablo 1.7. İç Denetim ile İlgili Uluslararası Düzenlemeler

Basel Düzenlemeleri
Cadbury Raporu
COBIT (Control Objectives for Information and Related Technology),
CoCo Kanada İç Kontrol Modeli (Canadian Institute of Chartered Accountants' Criteria of Control Framework)

COSO (The Committee of Sponsoring Organizations of the Treadway Commission- Internal Control– Integrated Framework)
Denetim Standartları Tebliği (Statement of Auditing Standards- SAS)
ISO İç Kontrol Modeli (International Organization for Standardization)
Sarbanes-Oxley Yasası
Uluslararası Denetim Standartları (International Standards on Auditing-ISA)
Turnbull Raporu
Yolsuzluk ve Rüşveti Önleme Kanunu (Foreign Corrupt Practices Act)

Kaynak: Türedi ve ark., 2015

Basel Düzenlemeleri:

Uluslararası Takas Bankası (Bank for International Settlements-BIS), Almanya, Belçika, Fransa, İngiltere, İtalya, Japonya, Amerika Birleşik Devletleri ve İsviçre arasında hükümetler arası bir anlaşma ile 1930 yılında İsviçre'nin Basel şehrinde kurulmuştur. Amacı bankaların uluslararası standartlarda çalışmalarını sağlamak Basel Komitesi olarak da adlandırılan Bankacılık Düzenleme ve Denetleme Komitesi ise 1974 yılında oluşturulmuştur. Komite üye ülkelerin merkez bankaları ve bankacılık alanında tecrübe sahibi denetçilerin katılımı ile oluşturulmuştur (BIS, 2020).

Basel Komitesi 2001 yılında "Bankalarda İç Denetim ve Murakıbin Denetçilerle İlişkisi" (Internal audit in banks and the supervisor's relationship with auditors) adlı dokümanı yayımlamıştır (BIS, 2001). Bu dokümanda iç denetimin kapsamı;

- Bankaların iç kontrol sisteminin etkin ve yeterli olup olmadığının incelenmesi ve değerlendirilmesi,
- Risk yönetimi faaliyetlerinin yeterliliğinin ve etkinliğinin incelenmesi,
- Yönetmelik ve finansal bilgi sistemlerinin gözden geçirilmesi

- Kurulmuş olan muhasebe bilgi sistemi ve hazırlanan finansal tabloların doğru ve güvenilir olup olmadığının tespit edilmesinden oluşmaktadır.

Dokümanda bahsedilen iç denetimin ilkeleri aşağıdaki gibidir:

- Bankaların iç denetim departmanları, bankanın diğer birimlerinden bağımsız olarak yönetim kurulu ya da denetim komitesine raporlama yapmalıdır.
- İç denetçiler objektif olmalı ve menfaat çatışmalarından uzak durmalıdır.
- İç denetim birimi çalışanlarının tümü yeterli mesleki yeterlilik ve tecrübeye sahip olmalıdır.
- İç denetim kapsamına bankanın her faaliyeti ve her departmanı dâhil olmalıdır.
- İç denetçilerin iç denetim ilkelerine uymasını sağlamaktan sorumlu yetkili iç denetim birimi yöneticisidir.

Cadbury Raporu:

1992 yılında Birleşik Krallık 'ta Sir Adrian Cadbury 'nın başkanlığını yaptığı komite tarafından hazırlanan ve "Cadbury Raporu" olarak da adlandırılan "Kurumsal Yönetimin Finansal Boyutu: Cadbury Komitesi Raporu (The Cadbury Committee Report: Financial Aspects of Corporate Governance) ile özellikle kurumsal yönetim alanında farkındalık ve tartışmalar ve çalışmalar ivme kazanmıştır. Komitenin temel amacı; finansal raporlama ve denetim faaliyetlerinin güvenilirliğinin güçlendirilmesi kurumsal yönetim anlayışının işletmelere yerleştirilmesidir. Yayımlanan raporda; yönetim kurulu ve yöneticilerin sorumlulukları tanımlanmış ve hissedar hakları ve sorumlulukları ile denetçilerin görevleri açıklanmıştır (Cengiz, 2013: 413).

Rapora göre; iç denetim birimlerinin amacı, işletmenin faaliyetlerini ve özellikle de iç kontrol ortamının gözetimini yapmaktır. Ayrıca iç denetçiler, işletme faaliyetlerinin etkinliği ve verimliliğini arttırmak amacıyla faaliyet göstermelidirler. İç denetim birimi, yönetim kurulu veya denetim komitesine bağlı olarak çalışarak suiistimal şüphesi olan vak'aların takibini yapmalıdır (Adiloğlu, 2010).

Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri (Control Objectives for Information and Related Technology-COBIT):

COBIT, Bilgi ve İlgili Teknoloji için Kontrol Hedefleri anlamına gelmektedir. Bilgi Sistemleri Denetim ve Kontrol Derneği (Information Systems Audit and Control Association-ISACA) tarafından BT yönetişimi ve yönetimi için oluşturulan bir çerçevedir. Yöneticiler için destekleyici bir araç olarak tasarlanmıştır ve teknik sorunlar, iş riskleri ve kontrol gereksinimleri arasındaki önemli boşluğun kapatılmasına izin verir. COBIT, herhangi bir sektördeki herhangi bir kuruluşa uygulanabilen, tamamen tanınan bir kılavuzdur. Genel olarak COBIT, bir organizasyondaki bilgi sistemlerinin kalitesini, kontrolünü ve güvenilirliğini sağlamaktadır KPMG, 2017). Çalışmanın 3.3.2. bölümünde COBIT ile ilgili detaylı bilgi verilecektir.

İç denetimle ilgili uluslararası düzenlemelerden *COSO Modeli*: çalışmanın 1.5.1.1. bölümünde ve *CoCo Modeli* çalışmanın 1.5.1.2. bölümünde, detaylı olarak açıklanmıştır.

Denetim Standartları Tebliği (Statement of Auditing Standards – SAS):

ABD’de AICPA tarafından 1947 yılında, “Genel Kabul Görmüş Denetim Standartları” olarak yayımlanan bu standartlar, 1972 yılı itibari ile, Denetim Standartları Komitesi (Auditing Standards of Board) tarafından revize edilmiş ve denetim standartları tebliği (statement of auditing standards –SAS) adıyla tekrar yayımlanmıştır. Tarihi finansal tablo denetimi esnasında denetçilere rehberlik eden bu standartlar; “Genel Standartlar, Çalışma Alanı Standartları ve Raporlama Standartları” olmak üzere 3 bölümden oluşmaktadır. “Genel Kabul Görmüş Denetim Standartları” kapsamında, 65 numaralı standart (SAS no: 65) ile iç denetçilerin finansal denetimleri gerçekleştirirken dikkat etmesi gereken hususlar ve bağımsız denetçiler ile ilişkileri hükme bağlanmıştır (Arens & Loebbecke, 2000).

ISO İç Kontrol ve Risk Yönetimi Standartları (ISO Internal Control and Risk Management Standards):

Günümüzde kredi kartının boyutlarından demiryolu köprüleri inşa etme standartlarına kadar çok birçok ürün ve faaliyeti içine alan ve geniş bir yelpazeyi kapsayan yaklaşık 20.000 ISO standardı bulunmaktadır.

Etkin bir iç kontrol yapısı oluşturmak için önemli olan ISO standartları iki başlıkta incelebilmektedir. Bunlar kurumsal risk yönetimi standartları ve kurumsal iç kontrol süreçlerinin oluşturulması için genel standartlardır. Ürün kalitesi süreçlerini kapsayan ISO standartları hariç, bunların çoğu “çok Avrupalı” olarak görülmüş ve geçmişte birçok ABD’li şirket yöneticisi tarafından göz ardı edilmiştir. Ancak günümüz iş dünyasında, tüm kurumsal yöneticiler ISO standartlarının önemini ve iç kontrol süreçlerine katkılarının farkına varmışlardır. (Moeller, 2014: 259). Bu standartlar;

- ISO 9000 Kalite Sistem Standartları serisi
- ISO 27000 Bilgi Güvenliği Yönetim Standartları serisi

Çalışmanın ilerleyen bölümünde bu standartlar detaylı bir biçimde incelenecektir.

Sarbanes-Oxley Kanunu:

ABD’de Enron ve Worldcom skandalları sonrası borsada işlem gören işletmelerin finansal tabloları ve açıklamalarına karşı güvensizliğin artması üzerine "Halka Açık Şirketler Muhasebe Reformu ve Yatırımcıyı Koruma Kanunu" diğer adıyla Sarbanes-Oxley Kanunu 30 Temmuz 2002’de yürürlüğe girmiştir. Adını hazırlanmasına öncülük eden senatör Paul Sarbanes ve Milletvekili Michael Oxley’den alan kanun halka açık işletmeler ve denetim firmalarının faaliyetlerine büyük reformlar getirmiştir. İşletmelerin finansal raporlama sürecindeki kontrollerin iyileştirilmesini ve işletmelere etkin kurumsal yönetim yapısının kurulmasını destekleyen kanun ABD’de halka açık işletmelerin tamamını kapsamaktadır (Ertikin, 2017).

Kanunun 404 no’lu bölümü uyarınca; işletme üst yönetimi finansal raporlama süreci için yeterli iç kontrollerin oluşturulmasından, uygulanmasından ve kontrollerin etkinliğinin değerlendirilmesinden sorumludur. Ayrıca kanun iç denetçilere belirtilen görevler yerine getirilirken işletme yönetimine yardımcı olma sorumluluğu yüklemiştir. (SEC, 2002).

Bölüm 404, tüm Sarbanes-Oxley Kanunu bölümlerinin uyumluluk açısından uygulanması için en karmaşık, en tartışmalı ve en maliyetli olanıdır.

Bölüm uyarınca işletme yönetimi iç kontrol sisteminin etkinliğinin değerlendirildiği bir iç kontrol raporu yayımlamak zorundadır. Ayrıca bu raporda iç kontrolün eksiklikleri de rapor edilmelidir. Ayrıca, çalışanların ya da işletme yönetiminin yapmış olduğu hileler hakkında, bağımsız denetçiler ile denetim komitesine bilgi verilmelidir. Bu bağlamda, iç denetim birimi, iç kontrolün etkinliğinin sağlanması, hilelerin tespiti ve varlıkların korunması konularında yönetime yardımcı olmaktadır (SEC, 2002).

Uluslararası Denetim Standartları (International Standards on Auditing-ISA):

Uluslararası Denetim ve Güvence Standartları Kurulu (The International Auditing and Assurance Standards Board- IAASB), denetim mesleğine olan kamu güvenini güçlendirmek amacıyla denetim, güvence ve kalite kontrol konularında uluslararası denetim standartları yayımlamaktadır.

610 no'lu Uluslararası Denetim Standardı, iç denetçiler ve iç denetim çalışmaları ile ilgili açıklamalara yer vermektedir. Standartta yer alan; iç denetimin kapsam ve amaçları, iç denetim ile bağımsız denetçi arasındaki ilişki, iç denetimin anlaşılması ve ilk değerlendirme, iş birliğinin zamanlaması ve koordinasyon, iç denetim çalışmalarının değerlendirilmesi ve test edilmesi başlıkları adı altında ise konunun detayları açıklanmaktadır (Akpınar, 2010: 177).

Bu standardın asıl amacı, iç denetim çalışmalarının kullanılması bağlamında bağımsız denetçilere rehberlik etmektir (IAASB, 2013).

Turnbull Raporu: Çalışmanın 1.4.1. bölümünde detaylı olarak açıklanmıştır.

Yolsuzluk ve Rüşveti Önleme Kanunu (Foreign Corrupt Practices Act-FCPA):

Enron ve WorldCom gibi şirket skandallarından yaklaşık 30 yıl öncesinde ABD benzer skandallar ile karşı karşıya kalmıştır. 1974-1977 dönemi Amerika Birleşik Devletleri'nde sosyal ve politik kargaşalar meydana gelmiş, 2000'lerin başındaki şirket skandalları sonrası yürürlüğe giren Sarbanes-Oxley gibi bu yolsuzluk ve rüşvet olayları sonrası 1977 yılında da FCPA yürürlüğe girmiştir.

FCPA, özellikle rüşvet ve yolsuzluk konularında hükümler içermektedir. Ayrıca işletmelerin finansal olayları ayrıntılı, eksiksiz ve doğru bir biçimde aktaran muhasebe kayıt düzeni oluşturmaları ve iç muhasebe kontrollerini uygulamaya geçirmeleri yönünde direktifler yer almaktadır. (Moeller, 2014: 7). Kanunda, yasalara aykırı veya kayıt dışı ödemeleri muhasebe sisteminin ya da iç kontrollerin tespit edebilmesi için işletmelerin düzenli çalışan ve güvenilir bir iç kontrol yapısına sahip olmaları gerektiğini vurgulamaktadır. Kanuna göre bu durumun sağlanması işletmelerde iç denetim departmanının varlığı ile mümkündür (Ercan, 2008: 29). Bu düzenleme ile birçok işletme iç denetim departmanı kurmuş ya da hali hazırdaki kadrolarını genişletmiştir (Cangemi & Singleton, 2002: 30)

1.8.3. Uluslararası Mesleki Uygulama Çerçevesi- UMUÇ

IIA, uluslararası mesleki uygulama çerçevesi-UMUÇ (International Professional Practices Framework-IPPF), iç denetim standartları ve etik ilkeleri yayımlayarak iç denetim mesleğinin standardizasyonu için önemli adımlar atmıştır.

İç denetim faaliyeti, yapısı, faaliyet konusu, hedefleri, sektörü, uymak zorunda olduğu mevzuatı, kültürel yapısı birbirinden farklı birçok kurum ve kuruluşta içeriden ve/veya dışarıdan kişilerce gerçekleştirilmektedir. Bu farklılıklar, iç denetim uygulamalarının işletmeden işletmeye farklılık göstermesine neden olmaktadır (IIA, 2017). Tüm bu farklılıklara rağmen UMUÇ' ta yer alan standartlara uyum, iç denetim uygulamalarının hayata geçirilmesinde önem teşkil etmektedir.

UMUÇ' un amaçları (TİDE, 2020);

- IIA'nın global anlamda iç denetim mesleğinin standartlarını belirleyici pozisyonunu desteklemek ve resmi bir mesleki rehber oluşturmaktır.
- Gelecekte gerçekleşmesi muhtemel ilerlemeler fırsat tanımak ve bununla birlikte güncel iç denetim uygulamalarını da kapsayacak şekilde tüm dünyadaki meslek mensupları ve paydaşlara, iç denetim pazarının büyümesi konusunda yardımcı olmaktır.

UMUÇ' ta iki farklı rehber yer almaktadır. Bunlar “Zorunlu Rehber” ve “Kuvvetle Tavsiye Edilen Rehber”dir. Zorunlu rehberde temel prensipler, iç denetimin tanımı, etik kuralları ve standartlar yer alırken; kuvvetle tavsiye edilen rehberde pozisyon raporları, uygulama önerileri ve uygulama rehberlerine yer verilmiştir.

1.8.3.1. Zorunlu Rehber

Zorunlu rehberin açıkladığı ilkelere uyum sağlamak iç denetim mesleğinin uygulaması için zorunlu ve önemlidir. Zorunlu rehber, kamu görüşleri de göz önünde bulundurularak geliştirilmiştir. Zorunlu rehber dört bölümden oluşmaktadır.

1.8.3.1.1. Temel Prensipler

Temel prensipler, bütüncül bir bakış açısı ile değerlendirildiğinde, bu ilkelerin iç denetimin etkinliğine atıf yaptığı anlaşılmaktadır. Bir işletmede etkin bir iç denetimden bahsedebilmek için tüm prensipler uyumlu hızlı ve etkin bir biçimde işlemelidir. İç denetçinin sahip olması gereken prensipler aşağıda sunulmuştur. Buna göre iç denetçi (IIA, 2017):

- Dürüst ve erdemli şekilde görevini yapar.
- Alanında yetkindir ve gerekli mesleki özeni gösterir.
- Hiçbir etki altında kalmadan bağımsız ve objektif şekilde çalışmalarını yürütür.
- İşletmenin strateji, hedef ve riskleriyle uyumlu şekilde faaliyet gösterir.
- İşletmede uygun şekilde konumlandırılmıştır ve yeterince kaynağı vardır.
- Sürekli gelişim gösterme amacındadır.
- İletişim kanallarını etkin bir biçimde kullanır.
- Risk-tabanlı güvence sağlar .
- Proaktif, anlayışlı ve gelecek odaklı bir kişiliğe sahiptir.
- Örgütsel gelişimi destekler.

1.8.3.1.2. İç Denetimin Tanımı

Zorunlu rehberde iç denetimin tanımı “İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık

faaliyetidir. İç denetim, kurumun risk yönetim, kontrol ve yönetim süreçlerinin etkililiğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur.” şeklinde yapılmıştır (IIA, 2017).

1.8.3.1.3. Etik Kurallar

Etik Kurallar, iç denetim sürecinde yer alan kişi ve kurumların davranışlarını düzenleyen ilke ve beklentileri belirtmektedir. Bu kurallar; kesin ve açık faaliyetlerin yerine asgari davranış ve beklentileri içermektedir. Amacı, iç denetim mesleğinin etik kültürünün gelişimini sağlamaktır. İç denetçilerden aşağıdaki ilkeleri uygulamaları ve desteklemeleri beklenmektedir (IIA, 2017).

Dürüstlük

İç denetçilerin dürüstlüğü güven tesis eder ve bu durumda denetçilerin kararlarına güvenilmesi için temel oluşturur (IIA, 2017).

Objektiflik

İç denetçiler, inceledikleri faaliyet ve süreçler hakkında bilgi toplarken, değerlendirme yaparken ve raporlarken en üst düzeyde mesleki tarafsızlık sergilerler. İç denetçiler, iletim durumların dengeli bir değerlendirmesini yapar ve çıkarım yaparken şahsi menfaatlerini ve 3. tarafların menfaatini gözetmez (IIA, 2017).

Gizlilik

İç denetçiler, aldıkları bilginin değerine ve sahipliğine saygı duyarlar ve yasal veya mesleki bir zorunluluk olmadıkça bilgileri uygun yetki olmadan ifşa etmezler (IIA, 2017).

Yetkinlik

İç denetçiler, iç denetim hizmetlerinin yürütülmesinde ihtiyaç duyulan bilgi, beceri ve deneyimi ortaya koymak için çaba sarfa ederler (IIA, 2017).

1.8.3.1.4. Uluslararası İç Denetim Mesleki Uygulama Standartları (Standartlar)

Standartlar, ilke odaklıdır ve iç denetimin uygulanmasına dair bir çerçeve belirlemektedirler. Standartların zorunlu gereklilikleri aşağıdaki gibidir:

- İç denetimin mesleki uygulanması ve uygulamanın etkinliğinin değerlendirilmesine dair temel gereklilikler.
- Kullanılan terim ve kavramları açıklayan yorum metinleri (Yorumlar).

Standartları doğru şekilde anlamak ve uygulamak için hem standartları ifade eden cümlelerin hem de yorumların dikkate alınması gerekir. Standartlarda, Terimler Sözlüğünde özel anlamları açıklanan terimler kullanılmaktadır (IIA, 2017).

Standartların amaçları (IIA, 2017):

1. İç denetim uygulamasının sahip olduğu temel ilkeleri tanımlamak,
2. Katma değerli iç denetim faaliyetlerini teşvik etmeye ve uygulamaya yönelik bir çerçeve sağlamak,
3. İç denetim performansının değerlendirilmesine uygun bir altyapı oluşturmak,
4. Gelişmiş kurumsal süreç ve faaliyetleri teşvik etmek,

şeklinde belirlenmiştir.

Standartlar; Nitelik ve Performans Standartları olmak üzere 2 kısma ayrılmıştır (IIA, 2017):

Nitelik Standartları; iç denetim faaliyetini gerçekleştiren kuruluşların, birimlerin ve denetçilerin özelliklerini belirleyen standartlardır.

Nitelik standartları; iç denetim faaliyetinin amaç, yetki ve sorumluluklarının bir yönetmelikle tanımlanması, bağımsızlık ve tarafsızlık, mesleki yeterlilik, mesleki özen ve dikkat, sürekli mesleki gelişim, kalite güvence ve geliştirme programından oluşmaktadır (Karcioğlu & Yanık, 2010).

Standartlar 4 ana bölümden ve 14 alt başlıktan oluşmaktadır. Tablo 1.8’de standartlar başlıklar halinde listelenmiştir:

Tablo 1.8. Nitelik Standartları

Nitelik Standartları
1000 – Amaç, Yetki ve Sorumluluklar 1010 – Zorunlu Rehberin İç Denetim Yönetmeliğinde Tanınması
1100 – Bağımsızlık ve Objektiflik 1110 – Kurum İç Bağımsızlık 1111 – Yönetim Kurulu ile Doğrudan Etkileşim 1120 – Bireysel Objektiflik 1130 – Bağımsızlık veya Objektifliğin Bozulması
1200 – Yeterlilik ve Azamî Meslekî Özen ve Dikkat 1210 – Yeterlilik 1220 – Azamî Meslekî Özen ve Dikkat 1230 – Sürekli Meslekî Gelişim
1300 – Kalite Güvence ve Geliştirme Programı 1310 – Kalite Güvence ve Geliştirme Programının Gereklilikleri 1311 – İç Değerlendirmeler 1312 – Dış Değerlendirmeler 1320 – Kalite Güvence ve Geliştirme Programı Hakkında Raporlama 1321 – “Uluslararası İç Denetim Meslekî Uygulama Standartlarına Uygundur” İbaresinin Kullanılması

Kaynak: IIA, 2017.

Performans standartları; iç denetimin sürecini açıklamakta ve iç denetim faaliyetinin performansını değerlendirmek için kullanılan kalite ölçütlerini belirlemektedir.

“Performans standartları; iç denetim faaliyetinin yönetimi, işin niteliği, görev planlaması, görevin yapılması, sonuçların raporlanması, gelişmelerin izlenmesi, bakiye riskin yönetimce üstlenilmesini içermektedir. Söz konusu standartlar uygulama önerileri ile desteklenerek iç denetçilere çalışmalarında kılavuzluk sağlanmaktadır” (Karcıoğlu & Yanık, 2010).

Standartlar 7 ana bölümden ve 25 alt başlıktan oluşmaktadır. Performans standartlarının başlıkları Tablo 1.9’da sunulmuştur:

Tablo 1.9. Performans Standartları

Performans Standartları
2000 – İç Denetim Faaliyetinin Yönetimi 2010 – Planlama 2020 – Bildirim ve Onay 2030 – Kaynak Yönetimi 2040 – Politika ve Prosedürler 2050 – Eşgüdüm (Koordinasyon) ve İtimat 2060 – Üst Yönetim ve Yönetim Kuruluna Raporlamalar 2070 – Dış Hizmet Sağlayıcı ve Kurumsal Sorumluluk
2100 – İşin Niteliği 2110 – Yönetişim/Kurumsal Yönetim

2120 – Risk Yönetimi
2130 – Kontrol
2200 – Görev Planlaması
2201 – Planlamada Dikkate Alınması Gerekenler
2210 – Görev Amaçları
2220 – Görev Kapsamı
2230 – Görev Kaynaklarının Tahsisi
2300 – Görevin Yapılması
2310 – Bilgilerin Tespiti ve Tanımlanması
2320 – Analiz ve Değerlendirme
2330 – Bilgilerin Kayıtlı Hâle Getirilmesi
2340 – Görevin Gözetim ve Kontrolü
2400 – Sonuçların Raporlanması
2410 – Raporlama Kıstasları
2420 – Raporlamaların Kalitesi
2421 – Hata ve Eksiklikler
2430 – “Uluslararası İç Denetim Mesleki Uygulama Standartları’na Uygun Olarak Yapılmıştır” İbaresinin Kullanılması
2431 – Görevlendirmelerde Aykırılıkların Açıklanması
2440 – Sonuçların Dağıtımı
2450 – Genel Görüşler
2500 – İlerlemenin Gözlenmesi

Kaynak: IIA,2017.

1.9. İç Denetim Süreci

Uluslararası iç denetim standartları uyarınca iç denetim sistemi işletmelerin faaliyetlerine katma değer katacak bir yaklaşımla tasarlanmalıdır. İç denetim birimi işletmenin stratejik amaçlarını dikkate alarak risk temelli bir planlama yapmalı, iç denetim sürecini dizayn etmeli ve faaliyetlerin işlerliğini titizlikle sağlamalıdır. Ayrıca, iç denetim çalışmasının sonuçlarını yönetime kısa ve öz bir şekilde raporlamalıdır. İç denetim sürecinin adımları aşağıda sunulmuştur (Reider, 1994 :20; Kangermann ve ark., 2008: 92)

- Denetimin Planlanması
- Denetimin Yürütülmesi
- Raporlama

1.9.1. Denetimin Planlanması

İşletmelerin iç kontrol sisteminin ve risk yönetimi süreçlerinin etkin bir biçimde yönetilmesi sorumluluğu üst yönetime aittir. İç denetim birimleri ise bu süreçlerin yürütülmesi esnasında yönetime yardımcı olmakla görevlidir. Günümüz iş dünyasında; işletmelerin hedeflerine ve risk esasına dayalı olarak planlama yapılmakta ve denetim çalışmaları risk odaklı olarak yürütülmektedir (Çarıkçı & Yıldırım, 2020). İşletmelerin sahip olması muhtemel risklerinin tespit edilmesi, tanımlanması ve değerlendirilmesi ile riskli alanlar belirlenmekte, iç denetim planı ve programı bu kapsamda hazırlanmaktadır. İç denetim faaliyeti, hazırlanan bu plan ve programa uygun olarak yürütülmektedir (İç Denetim Koordinasyon Kurulu, 2013). Denetimin planlanması aşaması Şekil 1.4'te sunulmuştur (Adiloğlu, 2010):

Şekil 1.4. İç Denetimin Planlanması Aşamaları



1.9.1.1. Denetim Evreninin Belirlenmesi

Denetim evreni, denetlenebilecek alanların tamamını ifade etmektedir. Genel ilke, denetim evreni kapsamına işletmenin tüm faaliyetlerinin dahil edilmesidir (Pickett, 2005: 188-189). Denetim evreni gerçekleştirilebilecek bütün denetimlerin bir listesidir ve hangi işlemlerin faaliyetlerin ve alanların denetleneceğine ışık tutmaktadır. İşlem süreçleri, birim, bölüm, bölgesel ve yerel organizasyonlardaki ana ve alt fonksiyonlar, dışarıdan temin edilen hizmetler, özel projeler, geleceğe yönelik planlar, gibi konulardan oluşmaktadır (Özbek, 2012). Başka bir deyişle denetim evreni; tüm faaliyet veya fonksiyonların toplamından oluşmaktadır.

Denetimin esnekliğini sağlamak ve görevleri yönetilebilir ve takip edilebilir bir şekilde sınırlandırmak için denetim evreni alanlara bölünebilmektedir. Denetim evrenin; birimler, faaliyetler, süreçler, projeler ya da bunlardan birkaç tanesinin topluca değerlendirilmek üzere faaliyetlerin bölümlere ayrılmasıyla denetim alanları belirlenmektedir (Moeller, 2005).

Denetim evrenine dahil edilecek faaliyet ve alanlar belirli durumlarda sınırlandırılabilir. Bu durumlar aşağıdaki gibidir (İç Denetim Koordinasyon Kurulu, 2013):

- İşletme hedeflerinin gerçekleştirilmesinde önemli bir katkısının olup olmadığı,
- İşletme faaliyetlerini etkileyecek büyüklükte olup olmadığı,
- Denetlenmesi sonucu oluşacak maliyetin getirisinden büyük olması.

1.9.1.2. Risklilik Düzeyi Değerlendirme Ölçütlerinin Tespit Edilmesi

Denetim konularının hangisinin öncelikli olarak denetleneceğine karar verilmesi için tüm denetim konularının ortak risk kategorilerine (ölçütleri) göre risklilik seviyelerinin değerlendirilmesi gerekmektedir (Griffiths, 2005). En sık şekilde kullanılan risk düzeyi değerlendirme ölçütleri aşağıda sunulmuştur (Anderson ve ark., 2017):

- Maddi Tutar
- Hırsızlık veya Usulsüzlük Olasılığı
- Faaliyetlerdeki Karmaşıklık veya Sıklık
- Yasal Sorumluluk Riski
- İtibar Kaybı Olasılığı
- Üst Düzey Yönetimin İlgisi
- Sürecin Manuel (elle) veya Teknoloji Ağırlıklı Gerçekleştirilmesi
- Değişim/Reorganizasyon
- Plan/Bütçelerden Sapmalar
- Kontrol Ortamı
- Önceki Denetim Sonuçları
- Son Denetimden Bu Yana Geçen Süre

1.9.1.3. Denetim Konularının Riskinin Değerlendirilmesi

Denetim alanlarına ilişkin risk ölçütleri belirlendikten sonra, alanların söz konusu risk ölçütleri karşısındaki durumu değerlendirilerek risk düzeyleri belirlenmektedir. Bu değerlendirme yapılırken iki farklı yöntem kullanılabilmektedir (Celayir, 2011: 170-171):

- **Kümülatif yöntem:** Bu yöntem uyarınca; risk ölçütlerine işletme faaliyetlerine etki ve önemi dikkate alınarak bir ağırlık verilmektedir. Ayrıca risk ölçütlerine risk seviyesini gösteren 1-5 arası bir değer verilmektedir. (En düşük seviye 1 ve en

yüksek seviye 5). Sonrasında, değerler ağırlıklar ile çarpılmakta her bir ölçüt için risk puanı hesaplanmaktadır. En son aşamada ölçütlerin risk puanları toplanarak ilgili alanının risk düzeyi belirlenmektedir.

- **Göreceli yöntem:** Bu yöntemle göre, her risk ölçütü için sahip olduğu risklerinin işletme faaliyetlerini etkileme olasılığı dikkate alınarak 1-5 arası etki değeri atanmaktadır. (En düşük seviye 1 ve en yüksek seviye 5). Her risk ölçütü ile ilgili riskin gerçekleşme ihtimali değerlendirilerek 1- 5 arası bir olasılık değeri verilmektedir (En düşük seviye 1 ve en yüksek seviye 5). Daha sonra, belirlenen olasılık değeri ile etki değerinin çapılması ile ölçütlere ait risk puanı hesaplanmaktadır. Son aşamada risk puanları toplanmakta ve denetim alanının risk düzeyi belirlenmektedir.

Risk değerlendirmesinin son aşaması, her bir denetim alanının risklerinin karşılaştırılarak denetim alanlarının sıralanmasıdır. Bu aşamada denetlenebilir alanlar, risk ölçütleri temel alınarak derecelendirilmektedir. Derecelendirme sonuçlarına göre, denetim alanları olabildiğince basit bir ölçek ile ifade edilmektedir. Örnek derecelendirme ölçeği aşağıdaki gibidir (Anderson ve ark., 2017):

1. Riski yüksek alan
2. Orta riskli alan
3. Riski düşük alan

1.9.1.4. İç Denetim Planının Oluşturulması

İç denetim planı; iç denetim faaliyetinin etkin, ekonomik ve verimli bir biçimde gerçekleştirilmesini sağlamak için denetimin kapsamı, alanı ve konuları, gereksinim duyulan insan kaynağı ve diğer kaynaklarla eğitim faaliyetleri de dahil olacak şekilde hazırlanmaktadır (Pickett, 2005).

İç denetim planı, işletme faaliyetlerinin ve işletmenin olası risklerinin kapsamlı olarak incelenmesi ve analiz edilmesi sonucu hazırlanmaktadır. İç denetim yöneticisi;

planı oluştururken işletmenin tüm faaliyetleri ve birimleri için işletme yönetiminin oluşturduğu *risk yönetim çerçevesini* dikkate almaktadır. Ancak işletmede mevcut risk yönetim çerçevesinin olmaması durumunda iç denetçi risk değerlendirmesini kendisi yapmaktadır (Pehlivanlı, 2008).

İç denetim planı hazırlanırken öncelikle iç denetimin hedefleri belirlenmektedir. Bu hedefler (Sabuncu, 2017):

- Yönetmel süreçlerin dizayn ve işleyişinin işletmenin hedeflerine uygunluğunun incelenmesi,
- Risk yönetim sisteminin, karşılaşılabilecek risklerin tanımlanması, ölçülmesi ve giderilmesi için yeterli olup olmadığının değerlendirilmesi,
- Finansal ve operasyonel tüm süreçlerde iç kontrol uygulamalarının etkin ve verimli olup olmadığının değerlendirilmesidir.

Uluslararası standartlar uyarınca, iç denetim faaliyetlerine ilişkin planın, yılda en az bir kez gerçekleştirilen risk değerlendirmesini temel alması gerekmektedir. Planlama yapılırken, işletme yönetiminin sürece ve plana ilişkin görüşlerinin alınması önem arz etmektedir (İç Denetim Koordinasyon Kurulu, 2013).

"Denetim planı uygulamada genellikle yıllık ve üç aylık dönemler itibariyle tasarlanmaktadır. Yıllık plan bir yıl boyunca tamamlanacak denetim faaliyetlerini ve bu faaliyetlerin hangi çeyrekte yer alacağını göstermektedir. Üç aylık planların ise yıllık planlara göre ortaya çıkabilecek riskleri belirleme olasılığı daha fazladır. İyi bir denetim planı aşağıdaki özelliklere sahip olmalıdır" (Celayir, 2011):

- *Pay sahiplerinin güvenini yükseltmeli,*
- *Denetim bütçesinin etkin kullanıldığını göstermeli,*
- *İşletmenin itibarını arttırmalı,*
- *İşletme değerini, kültürünü ve amaçlarını yansıtmalı,*
- *Denetçinin çalışma şevkini yükseltmeli,*
- *İşletmeye önemli etkileri olan denetim hizmetlerinin verilmesini sağlamalıdır.*

1.9.1.5. İç Denetim Programının Oluşturulması

İç denetim programı; yüksek risk içeren alan ve konulara öncelik verilecek biçimde denetiminin maliyeti de göz önünde bulundurularak hazırlanmaktadır. Program; hazırlanma sürecinde yöneticilerin ve gerekli durumlarda çalışanların da görüşleri alınarak, iç denetim planı ile uyumlu bir biçimde ve yıllık olarak hazırlanmaktadır. Yüksek riskli birimler ve faaliyetler, kurumsal yeniden yapılandırma projeleri, organizasyonda ve insan kaynaklarında önemli değişiklikler ve benzeri durumlar denetim programında önceliklendirilmektedir (Griffiths, 2005). Denetim programında yer alması gereken maddeler aşağıda sunulmuştur (Kepekçi, 1982).

- Denetimin amaç ve kapsamına karar verilmesi,
- Denetimi gerçekleştirilecek faaliyetlere ilişkin temel bilgilerin edinilmesi,
- Denetimi kaynaklarının belirlenmesi,
- Denetimi gerçekleştirilecek faaliyetler ve kontroller hakkında bilgilerin edinilmesi,
- Denetlenecek alanlara ve faaliyetlere ilişkin ön incelemenin gerçekleştirilmesi,
- Ön inceleme sonrası, kontrol amaçları, kontrol önlemleri ve yordamların incelenmesi,
- Denetlenecek alan ve kanıt toplama yaklaşımı hakkında gerekli açıklamaların yapılması,
- Denetim çıktılarının nasıl, ne zaman ve kime iletileceğinin belirlenmesi.

1.9.2. Denetimin Yürütülmesi

İç denetim faaliyetinin planlama aşamasından iç denetim faaliyetinin uygulama süreci başlamaktadır. Uygulama süreci sonunda denetim görüşüne ulaşabilmek amacıyla denetimin yürütülmesi için denetim planından hareketle bireysel denetim planları oluşturulmaktadır (Griffiths, 2005). İç denetim faaliyetinin uygulanması aşaması Şekil 1.5.'te sunulmuştur.

Şekil 1.5. İç Denetim Faaliyetinin Uygulanması Aşamaları



Kaynak: Griffiths, 2005

1.9.2.1. Görev Planının Hazırlanması

İç denetim faaliyetini gerçekleştirmek için; denetimin kapsamını, amacını, zamanını ve bütçesini dikkate alan, yıllık iç denetim planı dâhilinde ve denetimin başlangıç-bitiş tarihini içeren bir görev planı hazırlanmaktadır (Vallabhaneni, 2005, 4). Görev planı hazırlanması aşamaları aşağıda sunulmuştur (İç Denetim Koordinasyon Kurulu, 2013):

- Denetime ilişkin görevlendirme ve bilgilendirmelerin yapılması
- Denetimin hedef ve kapsamının belirlenmesi
- Başlangıç incelemeleri ve ilgili sürecin anlaşılması
- Denetim açılış toplantısı
- Risk kontrol matrisinin hazırlanması
- Denetim testlerinin belirlenmesi
- Denetim çalışma programının hazırlanması ve onaya sunulması
- Denetim için gerekli kaynaklarının tahsis edilmesi

1.9.3. Denetim Testlerinin Gerçekleştirilmesi ve Denetim Bulgularının Değerlendirilmesi

Bu aşamada, görev planında belirlenen denetim testleri gerçekleştirilmektedir. Denetim testleri ve denetimin kapsamında yer alan diğer konular ile alakalı kontrollerin etkinliği ve verimliliği süreç, kayıt ve belgeler yardımıyla incelenmektedir. Bu incelemeler yazılı hale getirilmeli, araştırma ve gözlemlerle desteklenmelidir. Gözlem ve araştırmalar sonucu elde edilen bulgular çalışma kağıtlarına geçirilmelidir. (Pickett, 2005)

Test seviyeleri, denetim evreni sonuçları ile paralel olacak şekilde belirlenmektedir. Bunun ardından her denetim alanında uygulanacak testler ve prosedürler belirlenmektedir. Başlıca test ve prosedürler (Güredin, 2014):

- Mülakat veya görüşme,
- Gözlem,
- Gözden geçirme,
- Belge ve kayıtların karşılaştırılması – kayıt sisteminin yeniden izlenmesi,
- Analitik inceleme prosedürleri,
- Örneklem yöntemi uygulamasıdır.

Testlerin denetim alanlarına uygulanması ve beklentiler ile sonuçların mukayese edilmesinden sonra test sonuçları ortaya çıkmaktadır. Test sonuçları denetim test matrisine işlenmekte ve matris çalışma kâğıtları içerisinde yer almaktadır (Pehlivanlı, 2008, 117).

Tablo 1.10. Denetim Test Matrisi Örneği

Riskli Alanlar	Test Yaklaşımı	Test Sonuçları	Sonuç

Kaynak: Sobel, 2005

Denetim alışmasının yrtlmesi denetim bulgularının belirlenmesi ile sona ermektedir. Bulguların destekleyici kanıtlar ile alışma kâğıtları ierisinde bulunması gerekmektedir. Elde edilen bulguların iřletme ynetimi birlikte incelenmesi nemlidir. Ynetim ile yapılan bu inceleme gerekleřmesi muhtemel hatalı yorumlamaların nne geecek ve sonuların son řeklinin ortaya ıkmasını saėlayacaktır (Pehlivanlı, 2008).

İ denetiler denetim srecinde elde ettiėi bulguları nem derecesine gre sınıflandırmalı ve bulgu formuna iřlemelidir. Bu formda, tespitler, nedenler, olası riskler ve etkileri, kriterler ve nerilere yer verilmelidir. Bulgu formu: (İ Denetim Koordinasyon Kurulu, 2013).

- Tespitler kısmı, “yanlıř veya sapma nedir” sorusunu yanıtlamalıdır.
- Nedenler kısmı, yanlıř veya sapmanın nedenini ortaya koymalıdır.
- Riskler ve etkileri kısmı, yanlıř veya sapma sonucunda iřletmenin karřı karřıya olduėu riskleri ve bu risklerin muhtemel etkilerini gstermelidir.
- Kriterler kısmı, ilgili mevzuat, standart ve iyi uygulamalar erevesinde olması gerekeni aıklamalıdır.
- neriler kısmı, olması gereken duruma ulařma yolunu belirlemelidir.
- Daha sonra bulgular nem derecesine gre sınıflandırılmalı ve bulgular denetlenen birimle paylařılmalıdır.

1.9.4. Raporlama

İ denetim birimi, denetim faaliyetini st ynetim adına gerekleřtirmektedir (Sawyer ve ark., 2003 :687). Uluslararası standartlar uyarınca, i denetim biriminin yneticisi, i denetim alışmasının amacını, denetilerin yetkilerini, grevlerini, sorumluluklarını ve performanslarını ieren raporları, dnemsel olarak st ynetime sunmak durumundadır (IIA, 2017).

Denetim raporu i denetim ynetmeliėi, raporlama beklentileri ve raporla ilgilenenlerin ihtiyaları kurum kltrnden etkilenmektedir (Sobel, 2005). Bu raporlar, nemli risk gstergeleri, kontrollerin problemlerini, kurumsal ynetiřim sorunlarını ve ayrıca st ynetimin ihtiya duyduėu diėer meseleleri ierebilmektedir (IIA, 2017).

Özetle; denetim raporu, gerçekleşen denetim çalışmalarının amaç, kapsam ve sonucunu özetlemektedir. İyi bir şekilde hazırlanmış rapor, iç denetim faaliyetinin etkisini temsil edecek önemli bir araç olarak görülmektedir. Bu bağlamda iç denetim raporunun üç ana amacı bulunmaktadır (Eşkazan, 2004).

- **Bilgilendirme:** Bulgu ve sonuçları açıklama
- **İkna:** Denetim bulgularının etkinliği ve geçerliliğini ispat
- **Sonuçlar Elde Etme:** Üst yönetimi faaliyetlerin geliştirilmesi ve iyileştirilmesine yönlendirme

Denetim sonuçlarının raporlanması, taslak iç denetim raporu ve kesinleşmiş iç denetim raporunun hazırlanması olarak iki aşamada gerçekleşmektedir. İlk olarak; denetçilerle denetlenen birimler arasında denetim bulguları üzerinde yapılan görüşmeler göz önünde bulundurularak taslak bir iç denetim raporu hazırlanmaktadır. (Pickett, 2005). Denetçiler, taslak raporu belirli bir süre içerisinde cevaplanmak şartı ile ilgili birimlere göndermektedir. Birim yöneticileri, gerekli durumlarda çalışanların ve ilgililerin görüşlerini alarak rapora ilişkin cevaplarını denetçilere geri göndermektedir (Adiloğlu, 2010).

İç denetim birimi, denetlenen birimlerden aldığı geri dönüşler ile bunlara ait değerlendirmelerini içeren kesinleşmiş raporu üst yöneticiye sunmaktadır. 2400 numaralı “Sonuçların Raporlanması” performans standardına göre nihai rapor; denetim sonuçlarını, denetçilerin önerilerini, çalışmanın amaçlarını, kapsamını ve denetçi görüşünü içermelidir (IIA, 2017).

Kesinleşmiş iç denetim raporunun taşınması gereken özellikler aşağıdaki gibidir (Adiloğlu, 2010, 94):

- Doğru
- Tam (Eksiksiz)
- Zamanında
- Objektif (Dürüst, Tarafsız)
- Açık ve Anlaşılır
- Özlü

- Yapıcı

Rapor formatı ve içeriği işletmeye veya göreve göre farklılaşmakla birlikte iç denetim, raporlarında bulunması gereken asgari başlıklar aşağıda sunulmuştur (Adiloğlu, 2010: 95):

- Rapor Tarihi
- Gönderildiği kişi
- Amaç,
- Kapsam
- Tespit ve Öneriler
- Sonuç ve Görüşler
- Raporu Düzenleyen

1.9.5. İç Denetim Sonuçlarının Değerlendirilmesi ve İzlenmesi

İç Denetim standartları iç denetçilerin, denetim sonucunu yayımlamadan önce sonuç ve tavsiyelerini işletme yönetiminden sorumlu kişilerle değerlendirmelerini zorunlu kılmıştır (IIA, 2017). İç denetim birimi, raporda belirlenen denetim bulgularından hareketle doğru işlem ve yordamların gerçekleştirildiğini takip etmek amacıyla denetim sonuçlarını izlemelidir (Adiloğlu, 2010: 99).

İKİNCİ BÖLÜM

İŞLETMELERDE BİLGİ TEKNOLOJİLERİ VE SİBER GÜVENLİK

2.1. Bilgi Teknolojileri ve Bilgi Sistemleri

2.1.1. Bilgi Kavramı

Bilgi kelimesi Latince 'deki 'informatio' kökünden türetilmiştir ve şekillendirme, bilgi ya da haber verme anlamlarına gelmektedir (Balay, 2004: 66).

Türk Dil Kurumu ise bilgiyi "kurallardan yararlanarak kişinin veriye yönelttiği anlam" olarak tanımlamakta ve "*insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf*" şeklinde açıklamaktadır (TDK, 2020).

Aristo'ya göre bilgi; amaçlanan şey veya aranan hakikattir. Sokrates bilgiyi amaca yönelik, temel prensipleri olmayan deneyim veya çiraklık olarak tanımlamıştır. (Drucker, 1994). Farabi 'ye göre ise bilgi, "*varlığı ve devamlılığı insanın yapıp etmelerine bağlı olmayan varlıkların mevcudiyetiyle ilgili olarak akılda kesin hükmün hâsıl olmasıdır.*" (Farabi, 1986).

Osmanlı döneminde bilimsel olarak üretilen bilgi için "ilm" kelimesi kullanılmıştır. İlm kelimesi "*okumakla veya görmek ve dinlemekle veya ihsan-ı Hak'la elde edilen malumat.*" şeklinde tanımlanmaktadır (Luggat, 2020).

Günümüz Türkçe' sinde işlenmiş veri bilgi olarak adlandırılmaktadır. Veriyi bilgiden ayıran en önemli özelliği verinin tek başına bir anlam ifade etmek zorunda olmamasıdır. Veriler bir araya gelerek bilgiyi oluşturmaktadır. İngilizce karşılığı data olan veri, Latince datum kelimesinden (çoğul şekli "data") gelmektedir. Dilimizde de "*olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi*" anlamında, veri kelimesi kullanılmaktadır. Bilgi teknolojisi bağlamında ise veri; bir konu ile alakalı, birbiriyle bağlantısı henüz kurulmamış bilinenler ya da kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanmaktadır (Canbek & Sağıroğlu, 2006: 166).

2.1.2. Bilgi Çağı

İnsanlık tarihi meydana gelen gelişim ve değişimler dikkate alınarak çağlara ayrılmıştır. İnsanlığın ilkel dönemleri, tarıma ve yerleşik yaşama geçiş; buharlı makinelerin icadı ile başlayan sanayi çağı bu durumun başlıca örneklerdir. Bilgi çağı ise; bilgi ve iletişim teknolojilerinin uygarlığı sosyal, ekonomik ve bilimsel olarak yönlendirdiği ve ağ toplumunun ortaya çıktığı dönem olarak adlandırılmaktadır. 1950'lerin sonuna doğru, üretim sektörü başta olmak üzere, ulaştırma, inşaat ve enerji sektörlerindeki gelişmelerin ileriye taşıdığı sanayi toplumunun gelecekte nasıl şekilleneceği üzerine tartışmalar başlamıştır (Webster, 2001: 30). İlk olarak bu dönem "Sanayi Sonrası Çağ" olarak adlandırılmaktayken bilgisayarların icadı ve 80'li yıllarda internet kullanımının yaygınlaşmaya başlaması, 1995 yılında tamamen serbest bırakılmasıyla bu dönem "Bilgi Çağı (Information Age) olarak adlandırılmaya başlanmıştır. "Bilgi Çağı" kavramı günümüzde, doksanlardan bugüne kadar geçen zamanı anlatmak için kullanılmaktadır.

Teknolojik gelişmelerin sonucu olarak, bilgi ve iletişim altyapısı geniş coğrafyalara yayılmıştır. Mobil teknolojiler sayesinde verilere ve bilgilere erişim zaman ve mekâna bağlı olmaktan kurtulmuştur. Bu durum kişilerin, kuruluşların ve toplumların ilişki ve etkileşimlerinin önemli bir kısmını bilgisayar ve diğer iletişim ağları ile yürütmelerini sağlamıştır. Bilgi çağında insanlar ve işletmeler hayatta kalmak ve faaliyetlerini sürdürmek için veri ve bilgiye ihtiyaç duymaktadır.

2.1.3. Bilgi Toplumu

Bilgiye duyulan ihtiyacın sonucunda bilgi toplumu kavramı ortaya çıkmıştır. Bilgi teknolojisinin hızla gelişmesi sonucu başta ABD, Japonya ve Batı Avrupa ülkeleri olmak üzere sanayi toplumu bilgi toplumuna evrilmiştir (Törenli, 2003).

Bilgi toplumunda temel üretim faktörü bilgidir. Bilgi toplumunda konvansiyonel ağır sanayi anlayışı yerini bilgi teknolojilerine bırakmaktadır (Çelik, 1998: 54). Bu yüzden; bilginin işlenmesinde ve depolanmasında kullanılan bilgisayar ve iletişim teknolojileri çok büyük öneme sahiptir. (Tonta, 1999). Bilgi toplumunda bilgisayarlar ve elektronik araçlarla yürütülen faaliyetler, elektronik haberleşme, reklam, eğitim, sigortacılık,

danışmanlık araştırma-geliştirme faaliyetleri başlıca önemli sektörleri oluşturmaktadır (Aktan & Vural, 2016).

Bilgi toplumu; bilgi ve teknoloji odaklı bir dünya yaratmıştır. Buna bağlı olarak iş dünyasının da iş yapış şekilleri ve değer yargıları tamamen değişmiştir. Bilgi toplumundaki bu değişimler ve bilgi toplumunun genel özellikleri aşağıda sunulmuştur (Selvi, 2011):

- Sanayi toplumunun kullandığı insan gücü ve makineler bilgi toplumu ile yerini dijital teknolojilere bırakmıştır
- Haberleşme bilgisayar ve internetin yaygınlaşması ile daha kolay ve hızlı bir şekilde gerçekleşmeye başlamıştır
- Bilgiye hızlı erişim sağlamak amacıyla bilgi ağları, veri tabanları ve bulut bilişim benzeri platformlar oluşturulmuştur
- Eğitim süreklilik kazanmıştır.

2.2. Bilgi Sistemleri ve Bilgi Teknolojileri Temel Kavramları

Abaküsün kullanılması ile başlayan, 1642 yılında Blaise Pascal'ın ilk mekanik hesap makinesini icat etmesinden günümüze gelişmeye ve değişmeye devam eden bilgi teknolojileri hayatımızın her alanında yerini almıştır. Özellikle bilgisayarların icadı ve internetin yaygınlaşması ile bilgiye ulaşmanın hızlı ve güvenilir yolu haline gelen teknoloji, işletmeler ve kişiler açısından hayatta kalma, büyüme ve gelişmede önemli bir faktör haline gelmiştir. Çalışmanın bu bölümünde bilgi teknolojileri ve bilgi sistemlerine ait temel kavramlar açıklanmıştır.

2.2.1. Bilgi Sistemleri

Bilgi teknolojileri ile bilgi sistemleri kavramları karıştırılmakta veya birbirlerinin yerine kullanılmaktadır. BT kavramı, bilgi üretme amacıyla bilgi sistemlerinin kullandığı donanımlar ve yazılımlara verilen isimdir. Bilgi sistemleri, kullanıcıların amacına uygun bilgiyi üretmek için verileri toplayan, depolayan ve yöneten bilgisayar tabanlı ve manuel

olarak kontrol edilebilen unsurlardan oluşan sistemlerdir (Gelinas, Dull & Wheeler, 2012: 14).

İşletmelerde bilgi akışı bir başka ifade ile verilerin işlenip doğru ve güvenilir bilgilere dönüştürülmesi, edinilen bu bilgilerin depolanması ve ilgili birimler ya da kişiler ile paylaşılması bilgi sistemleri vasıtasıyla gerçekleşmektedir. *“Bilgi sistemleri; kişilerin ve toplumun faydalanacağı belirli amaçları sağlamak için, verileri uygulayıcılar açısından anlamlı bilgilere dönüştüren, insan gücü, programlar ve yönetsel süreçlerden oluşan bir takımdır.”* (Bengshir, 1996).

Bilgi sistemleri yarattıkları bilgi akışı ile işletmelerin faaliyetlerinin planlanması ve kontrol edilmesinde ve karar verme süreçlerinde yöneticilerin işlerini kolaylaştırmaktadır. Ancak bilgilerin geçerliliği ve güvenilirliği bu süreçleri doğrudan etkilemektedir. Bilgi sistemlerinde meydana gelen aksaklıklar veya zayıflıklar sistemin yarattığı bilgilerin doğruluğunu ve kalitesini olumsuz etkilemektedir. Bu durum işletmeler açısından büyük bir yönetim ve risk unsuru haline gelmektedir.

Bilgi sistemleri dışarıdan sağlanan bilginin yönetilmesini sağlamaktadır. Bu sisteme göre birbirleriyle bağlantı içinde olan unsurlar çevreden alınan girdiyi işlemekte ve bu girdileri kişilerin veya organizasyonların amaçladığı çıktılara dönüştürmektedir. Bilgi sistemlerinin amaçları aşağıda belirtilmektedir (Tekbaş, 2019: 46):

- Güvenilir bilgiyi gereken yere zamanında teslim etmek
- İşletme içerisinde mevcut olan yahut ortaya çıkması olası riskli durumlarla ilgili karışıklığı ortadan kaldırmak ya da en alt seviyeye indirmek
- Yöneticilerin karar alırken kullanacakları bilgiyi sağlamak
- İşletmelerin en etkili şekilde faaliyetlerini sürdürmesi, üretilen mal ve hizmetlerin kalitesinin artırılması amacıyla önemli bilgileri ortaya koymak
- Gereken bilgiyi zamanında uygun formatlarda ve yerde sunmak.

Bilgi sistemleri; işlem destek sistemleri ve yönetim destek sistemleri olmak üzere ikiye ayrılmaktadır (Tekbaş, 2019: 47):

I. İşlem Destek Sistemleri: İşletme faaliyetlerinden üretilen ya da işletme faaliyetlerinde kullanılan verileri işlemek için kullanılan sistemlerdir. İşlem destek sistemleri 3 gruba ayrılmaktadır:

- Faaliyet İşleme Sistemleri
- Süreç Kontrol Sistemleri
- Kurumsal İş Birliği Sistemleri

II. Yönetim Destek Sistemleri: Üst yönetime bilgi sağlayan ve yöneticilerin etkin ve doğru karar vermelerine yardımcı olan sistemlerdir. Yönetim destek sistemleri de kendi içerisinde 3 gruba ayrılmaktadır:

- Yönetim Bilgi Sistemleri
- Karar Destek Sistemleri
- Üst Düzey Bilgi Sistemleri

Günümüzde işletmeler muhasebe de dâhil tüm süreçlerini bilgi sistemleri yardımıyla gerçekleştirmektedir. Muhasebe ve finansal raporlama süreçlerinde bilgi sistemlerinin kullanılması finansal verilerin incelenmesini saklanması aktarılmasını doğrudan etkilemekte ve işletmelerin iç kontrol ortamının yapısını değiştirmektedir.

2.2.1.1. Muhasebe Bilgi Sistemi

Muhasebe bilgi sistemi (MBS), işletmelerin bilgi sistemlerine entegre alt bir sistemdir. Finansal ve diğer verilerden bilgi elde edilmesi amacıyla donanım ekipman ve insan gibi kaynakların bir araya gelmiş şekline muhasebe bilgi sistemi denir. (Bodnar & Hopwood, 2013: 1). Yöneticilerin artan bilgi gereksinimlerini karşılamak için yönetim bilgi sistemi içerisinde yer alan MBS, giderek önemi artan bir faaliyete dönüşmüştür (Türel, 2018: 6). MBS' nin öğeleri Şekil 2.1.'de sunulmuştur:

Şekil 2.1. Muhasebe Bilgi Sisteminin Öğeleri



Kaynak: Gelinas ve ark., 2015

Şekilden anlaşılacağı üzere, MBS gerçekleşen finansal olaylar ile ilgili verileri işletme içi ve dışı kaynaklardan toplamakta, işlemekte ve depolamaktadır. Buna ek olarak, karar verme süreçleri sonunda iç ve dış paydaşlara finansal ve finansal olmayan bilgileri içeren raporlar hazırlamaktadır (Türel, 2018: 7).

MBS defter vekaleminden oluşan manuel bir sistem olabileceği gibi, en son bilgi teknolojilerinin kullanıldığı karmaşık bir sistem de olabilmektedir. İşletme sürekliliğinin sağlanması için satışlar, alımlar, ödemeler ve tahsilatlar gibi işlemler ile ilgili verilerin doğru şekilde kaydedilmesi, işlenmesi ve saklanması gerekmektedir. MBS işletmenin bilgi sisteminin temelini oluşturmakta ve 6 unsurdan meydana gelmektedir (Türel, 2018: 8):

1. Sistemi kullanan insan
2. Verilerin toplanması saklanması ve işlenmesi amacıyla kullanılan yöntem ve talimatlar
3. İşletme ve işletme faaliyetleri ile alakalı veriler
4. Verilerin işlenmesi için kullanılan yazılımlar

5. MBS' de kullanılan bilgisayarlar, ağ iletişim cihazları ve diğer aygıtlardan oluşan bilgi sistemi altyapısı
6. MBS' de depolanan verileri koruyan iç kontroller ve güvenlik tedbirleri.

İyi tasarlanmış bir MBS sayesinde işletme faaliyetlerinin verimli ve etkin şekilde sürdürülmesi sağlanmaktadır. Ayrıca mamul ve hizmetlerin kalitesi artırılabilenekte, iç kontrol yapısı ve verilen kararların isabet derecesi geliştirilebilmektedir (Türel, 2018: 9).

2.2.1.2. Bilgi Teknolojileri

Bilgi teknolojileri, işletmelerin faaliyetlerini sürdürmek için kullandıkları bilgisayar destekli sistemlerin tümü ve bunlarla ilişkili diğer teknolojileri ifade etmektedir (Laudon & Laudon, 2006: 4). Bilgi teknolojileri, bilgi üretme amacıyla işletmelerin bilgi sistemlerine dâhil olan donanımların ve yazılımların hepsini kapsamaktadır (Bourgeois & Bourgeois, 2014).

2.2.2. Bilgi Teknolojilerinin Yarattığı Uygulamalar

Bilgi teknolojileri verilerin kaydedilmesi, saklanması, işlenerek bilgiye dönüştürülmesi ve bu bilgilerin ilgili çıkar gruplarına aktarılması süreçlerine olanak sağlamakta ve bu süreçleri kısaltıp kolaylaştırmaktadır. Bilginin hızlı ve ekonomik bir biçimde tüm dünya ile paylaşılması ve karşılıklı etkileşimin giderek artması nedeniyle işletmeler de faaliyetlerini tamamen ya da büyük çoğunlukla elektronik ortam üzerinden gerçekleştirmeye başlamışlardır. Kişiler ve kuruluşlar tarafından yoğun şekilde tercih edilen bilgi teknolojileri sürekli bir gelişim içerisinde ve günümüzde hem sosyal hayatın hem de iş dünyasının önemli bir parçası haline gelmiştir. Çalışmanın bu bölümünde işletmeler açısından bilgi teknolojilerinin yarattığı uygulamalar ele alınmaktadır.

2.2.2.1. İnternet

İnternet dünyadaki tüm bilgisayar sistemlerinin birbirine bağlanması ile oluşturulmuş elektronik iletişim ağına verilen isimdir (Merriam-Webster, 2020). İnternet, bir IP-Bilişim Protokolü kullanarak oluşturulmuş birbirine bağlı bilgisayar iletişim ağlarının bütünü tanımlanabilmektedir (Erol, Atmaca & Şahin, 2004: 33). İnternet çok sayıda

(akademik, ticari, devlet ve serbest) bilgisayar ağıının katılımıyla oluşturulmuştur. Bu ağlar dünya genelini kapsamakta ve tüm faaliyetlerin gerçekleştirilmesi için kullanılan bir bilgi işlem merkezi alanı oluşturmaktadır (Sevim, 2009: 32).

İnternet; en yoğun şekilde kullanılan, güncelliğini koruyan ve diğer teknolojilerin ortaya çıkmasını sağlayan bilgi teknolojisidir. İnternet, dünyanın farklı yerlerindeki kişiler, işletmeler ve toplumlar arasında kurulan elektronik bir etkileşim, paylaşma ve dayanışma ortamı olarak kullanılmaktadır (Öğüt, 2003: 47).

2.2.2.2. Elektronik Ticaret

Doksanlı yıllarda hayatımıza giren elektronik ticaret (e-ticaret) günümüzde hemen her mal ve hizmetin sunulduğu büyük bir sanal pazar haline gelmiştir.

E-ticaret kavramı, her türlü ürünün ve hizmetin, iletişim ve bilgisayar teknolojisi kullanılarak alım ve satımını sağlayan süreçler şeklinde tanımlanmaktadır Kısacası e-ticaret, ödeme işlemlerinin internet üzerinden yapıldığı alış ve satış süreçleridir (Zengin, 2018: 5).

Elektronik ticaret, 7 gün 24 saat hizmet veren çevrimiçi mağaza, hızlı ve esnek yapısı ile geleneksel ticaretten farklılaşmaktadır. Bu alan bilgi teknolojilerinin de gelişmesine paralel büyüme gösteren alanların başında gelmektedir (Elibol & Kesici, 2004).

Elektronik Ticaret, kullanan veya kullanmak isteyen işletmeler için aşağıdaki faydaları sağlamaktadır (Gökmen 2019: 63):

- Yer ve mekân kavramı olmadan bir ticaret ortamının yaratılmasına olanak vermektedir.
- Yeni bir reklam aracı ve satış kanalıdır.
- Ürünlerin satışlarının gerçekleştirilmesini kolaylaştırmaktadır.
- İşletme giderlerinin minimize edilmesini sağlamaktadır.
- Değişimlere uyum hızlı bir şekilde sağlamaktadır.
- Tüketici ile ilişkiler birebir yürütülmektedir.

- Karşılıklı pazarlama fırsatı bulundurmaktadır.
- Stokların maliyetlerini azaltmak adına fırsat yaratmaktadır.

Yukarıda sayılan avantajların yanında e-ticaret faaliyetlerinde karşılaşılabilecek güvenlik sorunları bulunmaktadır. Bunlar (Karaçay, 2011):

- Bilgi varlıklarının kesintiye uğraması
- Bilgi varlıklarının yok edilmesi veya hasara uğraması riski
- Kullanıcı bilgilerinin değiştirilmesi
- Ağ ve bilgi kaynaklarını çalınması
- Sunulan hizmetin, iletilen ya da alınan bilgilerin inkâr edilmesi

2.2.2.3. Elektronik Veri Değişimi

En eski elektronik iletişim sistemlerinden birisi olan elektronik veri değişimi (Electronic Data Interchange-EDI) çalışanların iş yükünün ve kâğıt tüketiminin azaltılması amacıyla kullanılmaya başlanmıştır. İşletmeler tarafından müşterilere bilgi aktarma, sipariş bilgileri sunma, tedarikçilere sipariş verme veya elektronik para transferinde kullanılmaktadır (IBM, 2020).

EDI, işletme içi belge ve bilgilerin diğer firmaların bilgisayar sistemlerine iletilmesine izin veren bir çeşit organizasyonlar arası elektronik iletişim sistemidir (Lee, Lee & Kang, 2005).

Günümüzde tedarik zincirinde işletmeler arası veri değişimi ve entegrasyon uygulamaları için EDI kullanımına karar verilmesi gereken bir durum olmaktan çıkmış, uygulanması gereken bir iş gereksinimi haline gelmiştir. EDI tedarik zinciri içindeki işletmelere birtakım avantajlar sağlamaktadır. Elektronik veri değişiminin firmalara sağladığı faydalardan bazıları şu şekilde sıralanmaktadır (Ayvaz, 2006):

- İş süreçlerinde daha az hata yapılmasını sağlamaktadır.
- İş dokümanlarının daha hızlı iletilmesini sağlamaktadır.
- Envanter seviyesini düşürmektedir.
- İşletmelere maliyet tasarrufu sağlamaktadır.

- Kullanıcılara son derece güvenli bir ortam sunmaktadır.
- Operasyonların geliştirilmesini sağlamaktadır.
- Müşteri hizmetlerinin geliştirilmesini sağlamaktadır.
- Ticari ortaklarla ilişkilerin geliştirilmesini sağlamaktadır.

2.2.2.4. Kurumsal Kaynak Planlaması

Kurumsal kaynak planlaması (Enterprise Resource Planning-ERP), işletmelerin hedefleri doğrultusunda müşterilerinin taleplerini karşılamak amacıyla farklı coğrafi bölgelerde bulunan tedarik, üretim ve dağıtım imkânlarının etkili ve verimli olarak planlanması, koordine edilmesi ve denetimine imkân sağlayan bir sistemdir. (Kurnaz & Kestane, 2019: 146).

ERP, işletmelerin tüm tedarik zincirindeki süreci optimize etmek için tasarlanan entegre yazılım uygulamalarıdır ve genel amaçlı, geniş bir kapsamlı yönetim bilişim sistemi olarak görülmektedir. ERP işletmelerin tüm faaliyet alanlarında veri ve takibin müşteri ve tedarikçilerle paylaşıldığı entegre bir sistemdir. Bu sistem özellikle faaliyetleri ve işlemleri fazla büyük ölçekli firmalarda bilginin sistemler üzerinde dağılmasını ortadan kaldırmaktadır (Çağlıyan, 2012).

ERP kaynak planlama aşaması dışında veri depolama, iletişim, bilgi tasnifi ve kurumsallaşma gibi faaliyetlerin sistematik şekilde sürdürülmesini sağlamaktadır. Ayrıca uluslararası firmalarda meydana gelen sorunlara çözüm bularak firmalara büyük avantaj sağlamaktadır. ERP sisteminin işletmelere sağladığı faydalar aşağıda sunulmuştur (Deloitte, 2015):

- İşletmede çalışan personel sayısının azalması
- Satın alma giderlerinin azalması
- Gelirlerin artması
- İletişim ve lojistik giderlerinin azalması
- Verimliliğin artması
- Stokların azalması
- Sipariş yönetiminin gelişmesi

- Parasal döngülerin kolaylıkla kapanması
- Ödeme yönetiminin gelişmesi
- Sistem bakım ve onarım giderlerinin azalması

2.2.2.5. Yapay Zekâ

“Yapay zekâ, insanın düşünme yapısını anlamak ve bunun benzerini ortaya çıkaracak bilgisayar işlemlerini geliştirmeye çalışmak olarak tanımlanmaktadır. Yani programlanmış bir bilgisayarın düşünme girişimidir. Daha geniş bir tanıma göre ise, yapay zekâ, bilgi edinme, algılama, görme, düşünme ve karar verme gibi insan zekâsına özgü kapasitelerle donatılmış bilgisayarlara verilen isimdir” (Bozüyük ve ark., 2005).

Günümüzde farklı sektörlerde faaliyet gösteren işletmelerde yapay zekâ yaygın şekilde kullanılmaktadır. Sürücüsüz araç geliştirmeleri, çevrimiçi arama motorlarının hedefe yönelik arama sonuçları sunmaları, yüz tanıma teknolojisi, sosyal medyada haber akışlarının filtrelenmesi, medya şirketlerinin kullanıcılarına kitap veya etkinlik önerisinde bulunması, perakendecilerin alışveriş yapanlar için kişileştirilmiş çevrimiçi alışveriş deneyimleri sunmaları bu faaliyetlerin başlıca örneklerindendir. Lojistik firmalarının teslimatlar için en iyi güzergâhları seçmeleri, hükümetlerin salgınları önceden tahmin etmeleri, pazarlama uzmanlarının müşterilerine gerçek zamanlı son derece kişiselleştirilmiş içerikler sunmaları, sanal yardımcıların tüketicilerle etkileşim kurmak için ses-kontrollü doğal bir dil kullanmaları da yapay zekânın kullanım alanlarındandır. Yapay zekânın kullanımı ses tanıma ve anlama, insan gözünü algılama, doğal dil üretimi gibi alanlarda ciddi anlamda başarıya ulaşmaktadır. Bunlara ek olarak; kayıp modelleme, kredi analizi, değerlendirme işlemleri, işlem prosesleme gibi yıllardır yapılmakta olan sıradan günlük işler ve diğer pek çok iş de yapay zekâyla iyileştirilmektedir (TİDE, 2017).

Yapay zekâ uygulamalarının işletmeler açısından yarattığı fırsatlar aşağıdaki gibidir (TİDE, 2017):

- Veri işleme döngüsünü kısaltma
- Kusursuz ve hatasız tekrarlanabilen makine hareketleriyle insan hareketlerini ikame ederek hataları azaltma

- Uzun süren faaliyetleri, zamandan tasarruf eden (süreç otomasyonu) faaliyetlerle destekleyerek işçilik süresinden ve maliyetinden tasarruf etme
- Tehlikeli durumlarda insanların yerine, robot veya dronların görev yapmasını sağlama
- Yapay zekâ projeleri aracılığıyla işletme gelirlerini arttırabilme ve yönetebilme işletmenin pazar payını arttırabilme

Yapay zekâ uygulamalarının iş dünyası açısından meydana getirdiği riskler aşağıdaki gibidir (Siberbülten, 2019):

- Finansal riskler
- Marka veya itibar riskleri
- Güvenlik, sağlık ve çevre riskleri
- Hasta güvenliği riskleri (Sağlık sektörü)

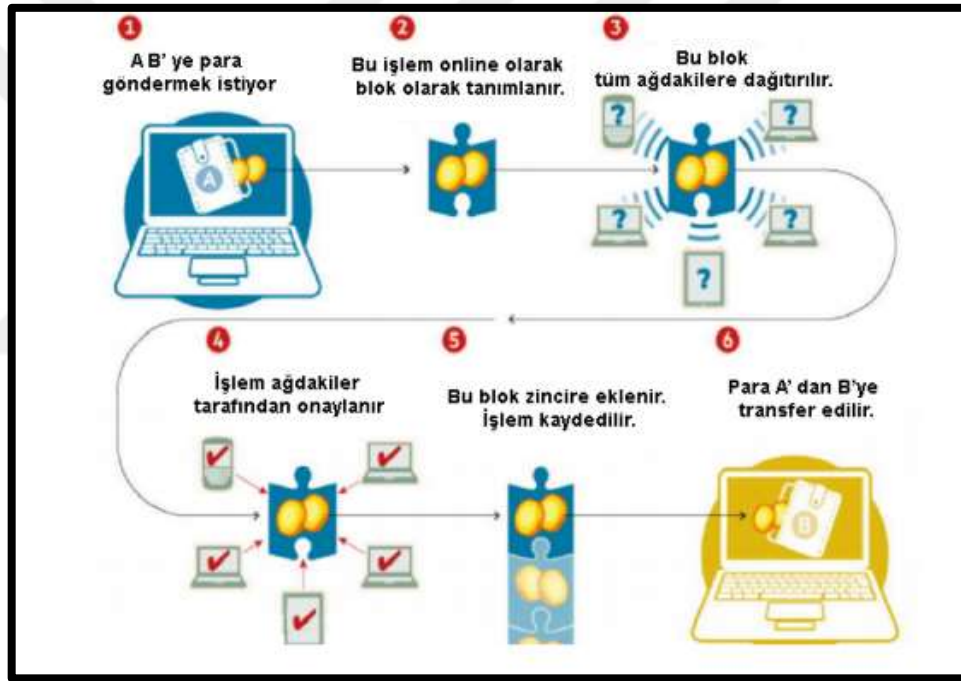
2.2.2.6. Blok Zinciri

Blok zinciri ya da uluslararası kabul gören adıyla Blockchain, içeriği ve kayıtları manipüle edilemeyen ve silinemeyen büyük defter (ledger) olarak tanımlanmaktadır (Byström, 2016: 3). Literatürde dağıtık hesap defteri (distributed ledger) olarak da adlandırılan olan blok zinciri teknolojisi en az iki tarafın kendi aralarında mutabakata vararak hataları minimize edip hatta sıfıra indirip, işlemi farklı veri tabanları üzerinde kaydederek değiştirilememesini garanti altına aldıkları bir veri saklama yaklaşımı olma özelliği taşımaktadır (Deloitte, 2018).

Blok zincirin en önemli özelliği sistemin düzenleyicisinin veya regüle eden bir üst otoritenin bulunmamasıdır. Bu özellik aracı kurum/kuruluşlara olan ihtiyacı ortadan kaldırmaktadır. Örneğin; hisse senedi alım/satım işlemleri için aracı kurumlara ve düzenleyici otoritelere ihtiyaç duyulmaktadır. Blok zinciri teknolojisi, bu tarz işlemleri gerçekleştiren isteyen tarafların herhangi bir aracı ya da düzenleyici kuruluşa ihtiyaç duymaksızın işlemlerini hızlı şekilde gerçekleştirebilmelerini sağlayan altyapıdır (Özdoğan & Karğın, 2018: 162).

Blok zinciri temelde değer içeren verilerin -para, kimlik, değerli kâğıtlar gibi- güvenli ve emin şekilde depolanması ve yönetilmesi için tasarlanmış bir teknolojidir (Durbilmez & Türkmen, 2019: 31). Şekil 2.2'de Blok zincirinin çalışma prensibi sunulmuştur:

Şekil 2.2. Blok Zincirinin Çalışma Prensibi



Kaynak: (Avunduk & Aşan, 2019)

Blockchain teknolojisi, Şekil 2.2.'de sınırlı veya belirlenmemiş sayıdaki tarafların ağındaki birçok katılımcının, yeni işlemleri girişi, yeni işlem bloklarını doğrulaması ve bunların (önceden onaylanmış işlemlerin) işlem bloklarını zincire eklemesi şeklinde çalışmaktadır (Durbilmez & Türkmen, 2019: 32).

Blok zincirinin başlıca kullanım alanları aşağıda özetlenmiştir (Durbilmez & Türkmen, 2019: 34):

- Para birimi
- E-ticaret

- Kamusal kayıtlar
- Uluslararası ödemeler
- Sözleşmeler, kontratlar
- Kredilendirme
- Mikro finans
- Fikri mülkiyet
- Tedarik zinciri
- Hisse senedi, türev araçlar
- Askeri emir komuta zinciri
- Dijital kimlik
- Fiziksel varlık kilitleri

Blok zinciri teknolojisinin yukarıda belirtilen alanlar dışında hem iş dünyası hem de kamu kurum kuruluşları tarafından kullanımı gün geçtikçe artmaktadır. Blok zinciri teknolojilerinin faydaları aşağıda sunulmuştur (Blasea, 2017):

- İzlenebilirlik, şeffaflık ve veri kaybını önleme
- Otomasyon
- Erişim/Ulaşılabilirlik:
- Güvenlik
- Hızlı Ödeme
- Maliyet ve Zaman Tasarrufu

Sağladığı avantaj ve faydaların yanında blok zinciri teknolojisinin birtakım dezavantajları da bulunmaktadır. Bu dezavantajlar aşağıda sunulmuştur (Tanrıverdi, Uysal & Üstündağ, 2019: 205):

- Kullanılan bilgisayarlar çok pahalıdır ve çok enerji harcamaktadır.
- Blok zinciri geleneksel veri tabanları ile performans bakımından kıyaslandığında yetersiz kalmaktadır.
- Ağdaki her bir düğümün tüm verilerin bir kopyasını saklayabilmesi ve içeriğine erişebilmesi, kullanıcıların mahremiyetine zarar verebilmektedir.

- Akıllı sözleşmeler oluşturulduktan sonra blok zincirinde herkesin erişimine açık halde saklanmaktadır. Bu da sistemi kötü niyetli saldırılara karşı savunmasız bırakabilmektedir.

2.2.2.7. Bulut Bilişim

Bulut bilişim; donanım, sistem yazılımı ve uygulamaların internet üzerinden bir hizmet olarak dağıtılması anlamına gelmektedir. Bu sistemde hesaplamalar ve veri işleme, herhangi bir yerde bulunan “Bulut” ortamında yürütülmekte, bazı veri merkezleri üçüncü taraflar tarafından yönetilmektedir. Hizmet sağlayıcıları tarafından belli bir ücret karşılığında ya da kullanıcının hizmeti kullandığı kadar ücretlendirmesi şeklinde nihai kullanıcıya ulaştırmaktadır (Koruyan & Bingöl, 2015: 369).

Amerika Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology -NIST) bulut bilişimi: *“Bulut bilişim, minimum yönetim çabası veya servis sağlayıcı etkileşimiyle hızlı bir şekilde elde edilebilen ve serbest bırakılabilen, ayarlanabilir bilgi işlem kaynaklarının (ağlar, sunucular, depolama, uygulamalar ve hizmetler) paylaşıldığı bir havuza talep modeli üzerinden kolay ağ erişimi sağlayan bir modeldir. Bu model erişilebilirliği desteklemekte ve beş temel unsuru, üç hizmet sunumunu ve dört yerleştirme modelini kapsamaktadır.”* şeklinde tanımlamıştır (Mell & Grance, 2015).

Günümüzde ABD, Avrupa Birliği Ülkeleri, Japonya, Güney Kore, Türkiye gibi ülkeler bulut bilişime büyük yatırımlar yapmaktadırlar. Microsoft, Google, Apple, Amazon ve IBM vb. şirketler kişilere ve işletmelere ürün ve hizmet sunmaktadır. (BTK, 2020)

Bulut bilişim, özellikle günümüz iş dünyasında yer alan kurum ve kuruluşlar için önemli avantajlar sağlamaktadır. Bulut bilişimin en öne çıkan avantajı maliyet bakımından büyük bir tasarruf sağlamasıdır. İşletme maliyetlerini düşürmesine ek olarak kullanışlı olması, sınırsız depolama olanağı sağlaması bulut bilişimin kullanımını arttırmaktadır. Bulut bilişimin sağladığı faydalar aşağıda özetlenmiştir (Albayrak, 2015: 56-57):

- Donanım maliyetini düşürmesi
- Yüksek performans

- Yazılım maliyetlerini düşürmesi
- Anında güncelleme
- Limitsiz depolama kapasitesi
- Gelişmiş dosya formatı uyumu
- Grup çalışmasına yatkınlık

Yukarıda sayılan faydaların dışında bu teknolojinin veri mülkiyeti konusunda, internet kullanma zorunluluğu, güvenlik açıkları ve bağlantıya göre yavaş çalışması gibi dezavantajları da bulunmaktadır. Bulut bilişimin dezavantajları aşağıda özetlenmiştir (Albayrak, 2015: 58):

- İnternet bağlantısı gereksinimi
- Düşük internet hızında yaşanan problemler
- Uygulamaların yavaş çalışması
- Güvenlik açıkları
- Sürekli devam eden güncellemeler
- Deneyimsiz bulut operatörleri

2.2.2.8. Büyük Veri

Büyük veri (Big data), işletme içinde ve dışında; geleneksel ve dijital kaynaklardan edinilen, inceleme ve analiz için bekleyen veri koleksiyonuna verilen isimdir (Ward & Barker, 2013). Büyük veri, bilimsel alanda ve finans, sağlık, eğitim gibi farklı sektörde ürün ve hizmet sağlayan işletmeler tarafından kullanılmakta ve her geçen gün gelişme gösteren teknolojik araçlar ve bu araçların veri üretim şekillerine bağlantılı olarak değişmektedir (Reeder-Hayes ve ark., 2017).

Büyük veri, işletmelerde kullanılan geleneksel programların verileri kaydetme, saklama, yönetme ve işleme kapasitelerinin çok daha ötesindeki veri kümelerini ifade etmekte kullanılan bir kavramdır. Geleneksel yöntemler devasa büyüklükteki verilerin işlenmesi konusunda yetersiz kalmış ve bu noktada büyük veri analizleri ortaya çıkmıştır. Büyük verinin analizi beraberinde yeni teknolojileri ortaya çıkarmıştır. Kısacası büyük

veri, yalnız bilgi elde edilen verinin türünü değil, onu depolamak ve dönüştürmek için kullanılan teknolojiyi de kapsamaktadır (Cackett, 2013: 14).

Büyük veri analitiği günümüzde birçok sektörde etkin olarak kullanılmaktadır. Bu sektörlerden bazıları aşağıda sunulmuştur (Morabito, 2015):

- Bilişim Sektörü
- Bankacılık Sektörü
- İletişim, Medya ve Eğlence Sektörleri
- Perakendecilik Sektörü
- Sağlık Sektörü
- Eğitim Sektörü
- Kamu Sektörü

Büyük veri analitiğini etkin ve verimli bir şekilde kullanan işletmeler birçok fayda ve avantaj sağlamaktadır. Bu faydalar aşağıda özetlenmiştir (Morabito, 2015):

- Verimlilik, yaratıcılık ve üretkenliği artırması
- Daha düşük maliyetle daha kaliteli analiz yapılmasına imkân vermesi
- İşletme içi bilgi paylaşımının daha etkin ve verimli hale getirmesi
- İleri düzey analizlerle değer ortaya çıkarma ihtimali yüksek olan durumların test edilmesi ve oluşturulmasına imkan tanınması.

İşletmelere sağladığı faydaların yanında uygulamada hala birtakım riskler ve zorluklar bulunmaktadır. Bu zorluklar aşağıda özetlenmiştir (Altunuşık, 2015):

- Teknik zorluklar
- Verilerin analizi
- Etkin insan kaynağı problemi
- Verilerin telif hakları
- Veri tabanı hakları
- Kişisel mahremiyet sorunu
- Gizlilik

- Yasal düzenlemeler

2.2.2.9. Nesnelerin İnterneti

Nesnelerin interneti (Internet of Things-IoT), nesnelerin veya cihazların birbirleriyle ya da daha büyük sistemlerle bağlantılı olduğu bir iletişim ağıdır. Diğer bir başka ifadeyle nesnelerin interneti, cihazların (bilgisayarlar ve telefonlar dışında kalan) internete bağlanmasını ifade etmektedir (Thibaud ve ark., 2018: 79). Örneğin; arabalar, buzdolabı, bulaşık makinesi vb. ev aletleri ve hatta kalp monitörleri nesnelerin interneti ile internete bağlanabilmektedir. IoT teknolojisi ile milyonlarca nesnenin de birbirine bağlanması mümkündür. IoT üç temel unsurdan oluşmaktadır (Doyduk & Tiftik, 2017: 133):

1. Nesneler – Demirbaş veya teçhizat
2. Nesnelerin bağlantısını sağlayan ağlar
3. Nesnelerin yarattığı veriyi işleyip kullanan bilgisayar sistemleri

Dünyada 2018 itibari ile internete bağlı 22 milyar yaklaşık milyar cihaz bulunmaktadır. Artan kullanım alanı ve talep düşünüldüğünde 2025 yılında uygulamayı kullanan ve ağı dâhil olan cihaz sayısının 39 milyarı 2030 yılında ise 50 milyarı bulması beklenmektedir (Statista, 2020).

Nesnelerin interneti teknolojisinin başlıca kullanım alanları aşağıda özetlenmiştir (Silverio-Fernández ve ark., 2018: 6):

- Akıllı Çevre: Binalarda sismik titreşimlerin izlenmesi, şehirlerde kirlilik ve radyasyon seviyelerinin izlenmesi, trafik yönetimi, afete müdahale, atık yönetimi, tedarik zincir yönetimi vb.
- Akıllı Binalar: Ev otomasyonu endüstrisi, IoT uygulamalarının iyi bir örneğidir. Örneğin bu teknoloji sayesinde kullanıcılar, evine bağlı olan su tankındaki su kullanımını tespit edebilmekte telefonuyla komut vererek evini serin tutmak için klimayı uzaktan açabilmekte, tüm elektronik cihazları ve elektrikli cihazları akıllı telefonla uzaktan çalıştırabilmektedir. Ayrıca bunlara ek olarak oda sıcaklığı, toz seviyesi, gürültü seviyesi, hatta oksijen seviyesinin ölçümü yapılabilmekte ve kaydedilmektedir.

- Sektörel Uygulamalar: Endüstriyel otomasyon ise IoT ile birlikte hızla gelişmektedir. Örnek olarak; akıllı şebekeler ile enerji tüketimi takibi ve yönetimi sağlanmaktadır. Tedarik Zinciri ekranları ile tedarik zinciri boyunca depolama koşulları izlenmekte ve ürün takibi yapılmaktadır. Gıda sektöründe özellikle kırmızı et kesme işleme ve kurutma süreçlerinde ozon seviyelerinin izlenmesi IoT ile etkin şekilde gerçekleştirilmeye başlanmıştır. Tarım sektöründe kullanılan sensörler ile su ihtiyacı olan bölgeler belirlenmekte ve su kaynaklarının israfı önlenmektedir. Sağlık sektöründe ise hastanelerdeki veya evlerindeki hastaların durumlarının izlenmesi IoT teknolojisi ile mümkün olmaktadır.
- Güvenlik ve Acil Durumlar: IoT teknolojisi ile İnternet bağlantısı kullanılarak dünyanın herhangi bir yerinden izlenebilen ve yönlendirilen Kapalı Devre Televizyon (Close Circuit TeleVision-CCTV) kameralar ile 7/24 gözetim yapılabilmektedir. IoT ayrıca veri merkezlerinde, depolarda veya hassas bina zeminlerinde meydana gelen arızaları tespiti, nükleer santrallerin çevresindeki radyasyon seviyelerinin ölçümü, kimyasal ürünlerin üretimini yapan fabrikaların ve madenlerin içindeki gaz seviyelerinin ve kaçaklarının tespiti vb. faaliyetlerinde kullanılmaktadır.
- Lojistik ve Taşımacılık: Depo veya liman gibi büyük yüzeylerde münferit eşyaların aranması, depolama uyumsuzluk tespiti, filo takibi vb. lojistik sektöründe yer alan IoT uygulamalarından bazılarıdır. IoT ile toplu taşıma sistemini takip edilmesi, trafik ve yaya yoğunluklarının belirlenmesi, trafik kazalarının ve hasarların tespiti, seyahat rotasının optimizasyonu ve benzeri daha birçok uygulama gerçekleştirilmektedir.

Bu sektörler dışında; sosyal medya, otomotiv, havacılık, inşaat, tekstil ve sağlık gibi farklı sektörlerde bulunan pek çok firma kendi nesnelerin interneti uygulamalarını geliştirerek piyasada avantaj elde etmeye çalışmaktadır (Ranger, 2020). IoT teknolojinin işletmelere sağladığı faydalar aşağıdaki gibidir (Doyduk & Tiftik, 2017):

- Maliyetleri minimize etmesi
- Faaliyetlerin etkinliğini ve verimliliğini arttırması
- Rekabet avantajı sağlaması

- Anlık müşteri analizi ile fiyatlandırma kararlarını isabetli şekilde gerçekleştirmesi
- Tedarik zinciri yönetiminde depolama, yük taşıma işlevleri hızlı, güvenilir ve kolay yapılabilir hale getirmesi
- Uzaktan algılama, fiziksel dünyayı denetleyebilme imkânı sunması

Sağladığı faydalarla birlikte nesnelerin interneti teknolojisi uygulamada teknik ve sosyal anlamda çeşitli risklere ve zorluklara sahiptir. Bu zorlukları 3 başlıkta toplamak mümkündür (Doyduk & Tiftik, 2017):

- **Bilgi Güvenliği:** IoT teknolojisine entegre nesnelerin kriptolama veya şifrelemeye uygun olmaması nedeniyle bilgi güvenliğine riski ortaya çıkmaktadır.
- **Gizliliğin Korunması:** IoT teknolojisine entegre nesnelerin gizlilik politikaları ile donanmış olmaları gereklidir. Aksi takdirde veri sahiplerinin onayı olmadan verilerin kullanılması mümkün olmaktadır.
- **Yasal Yükümlülükler:** IoT incelenmesi ve üzerinde çalışılması gereken yeni yasal yükümlülükler ortaya çıkarmıştır.

2.3. Bilgi Güvenliği ve Siber Güvenlik

Bilgi teknolojilerinin son yıllarda giderek gelişmesi ve işletmeler tarafından yaygın olarak kullanılması birçok avantaj ve faydayı beraberinde getirmiştir. Aynı zamanda çalışmada daha önce de bahsedildiği gibi bu gelişmeler birçok risk unsurunu barındırmaktadır. Bu unsurların en başında şüphesiz bilgi güvenliği ve dijitalleşmenin de etkisi ile bilgi güvenliği ve siber güvenlik riskleri gelmektedir.

Günümüzde, siber güvenlik kavramı ve bilgi güvenliği kavramı çokça karıştırılmakta ve birbirlerinin yerine kullanılmaktadır. Bilgi güvenliği kavramından kastedilen dijital bilgi ve analog bilginin güvenliği iken, siber güvenlik kavramı dijital bilgilerin ve bilgileri sağlayan kanalların ve altyapı sistemlerinin güvenliğine odaklanmaktadır. Ancak günümüzde bilgi teknolojilerinin iş hayatına girmesi ve bilginin çoğunlukla dijitalleşmesinin etkisi ile bu iki kavram iç içe geçmiş durumdadır. Çalışmanın bu bölümünde bilgi güvenliği ve siber güvenlik konuları açıklanacaktır.

2.3.1. Bilgi Güvenliđi

21. yüzyılda bilgi teknolojilerinin her alanda kullanılması ve vazgeçilmez bir hale gelmesi, özellikle nerdeyse tüm faaliyetlerin dijital ortamlarda yürütölmeye başlanması, bilgi hacminin artması ve bilginin en önemli rekabet aracı olması bilginin ve bilgiyi sağlayan kaynakların korunmasını zorunlu hale getirmiştir.

Bireyler ve işletmeler bilginin ve bilgi teknolojilerinin güvenliđini nasıl sağlayacakları üzerine birçok çalışma yapmaktadırlar. Bilgi güvenliđinin amacı, güvenlik olaylarının olası etkisini minimize ederek, iş sürekliliđini sağlamak ve hasarı en aza indirmektir. (Von Solms, 1998). Bilgi güvenliđi, aşağıda vurgulandıđı gibi çeşitli şekillerde tanımlanmaktadır:

Bilgi güvenliđi bilgi varlıklarının risk faktörlerinden korunması anlamına gelmektedir. Bilginin deđiştirilmeden, dođru amaçla kullanılmasını ve istenmeyen kişilerin eline geçmesini engellemek olarak tanımlanmaktadır (Canberk & Sağırođlu, 2006: 165).

Amerikan Ulusal Güvenlik Sistemleri Komitesi, bilgi güvenliđini; bilginin ve bilgiyi kullanan, depolayan ve ileten sistemler ve donanım dâhil kritik unsurların korunması olarak tanımlamaktadır. Komiteye göre bilgi güvenliđi; bilgisayar güvenliđi, veri güvenliđi ve ađ güvenliđi unsurlarını da içermelidir (Whitman & Mattord, 2017: 11).

ISO / IEC 27002 standardında bilgi güvenliđi; bilginin gizliliđinin, bütönlüđünün ve kullanılabilirliđinin korunması olarak tanımlanmaktadır (ISO / IEC 27002, 2005:1). Standarda göre bilgi çeşitli şekillerde karşımıza çıkmaktadır. Buna göre bilgi; kâğıt üzerine basılabilmekte veya yazılabilmekte, elektronik olarak saklanabilmekte, posta veya elektronik yollarla iletilebilmekte, filmlerde gösterilebilmekte, konuşmada aktarılabilmektedir (ISO / IEC 27002, 2005: 1).

Bilgi güvenliđi bir ürün veya teknoloji deđil, bir süreçtir (Mitnick ve Simon, 2002: 4). İşletmelerde bilgi güvenliđi sürecinin tasarlanması, kurulması devam ettirilmesi ve yönetilmesi üst yönetimin desteđiyle iç denetim departmanı ve bilgi teknolojileri çalışanlarının katkısıyla gerçekleştirilmektedir.

Yukarıdaki tanımlar hakkında dikkat çekilmesi gereken bir diğer önemli husus ise, bilgi güvenliğinin, güvenli bilgilerin sahip olması gereken özellikler açısından tanımlanmasıdır. Bunlar genellikle bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini içermektedir. Ancak zaman içerisinde; gelişen bilgi teknolojilerinin güvenliğinin de sağlanması gerektiğinden, güvenli bilginin sahip olması gereken özellikler de değişime uğramıştır. Söz konusu özellikler çalışmanın ilerleyen bölümlerinde açıklanacaktır.

2.3.2. Bilgi Güvenliği ve Siber Güvenlik İlişkisi

Güvenlik kavramı, varlıkların çeşitli zafiyetlere, tehditlere, risk unsurlarına ve bunların yarattığı zararlara karşı korunması ile ilgilidir. Güvenlik süreçleri de zafiyetlerin yol açtığı riski azaltmaya yardımcı olan güvenlik kontrollerinin (karşı önlemler olarak da adlandırılmaktadır) seçimi ve uygulanması ile ilgilenmektedir (ISO / IEC 27002, 2005).

Bilgi güvenliği, fiziksel olarak tutulan ve sanal ortamda bulunan bilgilerin, yetki olmaksızın kullanılmasının, tahrip edilmesinin veya değiştirilmesinin engellenmesidir. Siber güvenlik ise, bilgisayarların, verinin ve ağların olası saldırılardan, yetkisiz erişimlerden veya tahriplerden korunmasıdır. Her iki terimin ortak değerlendirilmesi gerekirse (Baykara, Daş & Karadoğan, 2013; Çek 2017):

- Her iki disiplin de verilerin fiziksel bütünlüğünün korunmasını gerektirmektedir.
- Bilgi güvenliği yaklaşımına göre, işletmelere ait verilerin kanunlara aykırı erişimlerden uzak tutulması gerekmektedir. Siber güvenlik açısından da sanal ortamlarda yer alan veriye kanunlara aykırı erişimin engellenebilmesi temel problemdir. Siber güvenlik, siber uzayı yetkisiz sayısal erişimlerden korurken, bilgi güvenliği bilgi varlıklarının yetkisiz erişimlerden korumaktadır.
- Siber güvenlik, siber uzayda var olan tehditlere karşı koruma sağlarken, bilgi güvenliği, bilgiye karşı olan tüm tehditlerle ilgilenmektedir.

Teknolojinin gelişmesine paralel olarak siber tehditlerin giderek artması ve siber saldırıların yaygınlaşması işletmelerin varlıklarını yetkisiz erişime karşı korumak zorunda bırakmıştır. Bu durum sadece özel sektörde faaliyet gösteren işletmelerle sınırlı değildir; kamu kurumları bu siber saldırılara karşı eşit derecede savunmasızdır. Günlük olarak çok hassas verilerle uğraşan işletmeler (Finans, Sağlık, Enerji, Telekomünikasyon sektörü

vb.) altyapılarını korumak için gelişmiş güvenlik sistemlerine yatırım yapmaktadır. Bu yatırımlar siber güvenlik ve bilgi güvenliğini işletmelerin yeni odak noktası haline getirmiştir (Güngör, 2015).

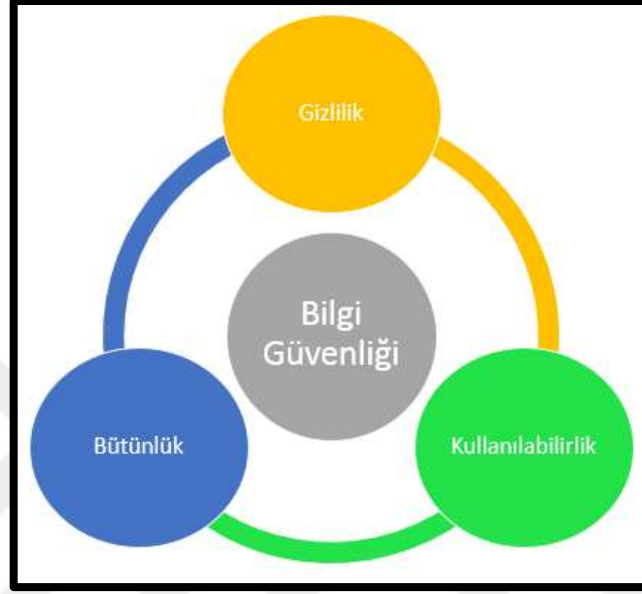
Özetle; siber güvenlik ağları, bilgisayarları ve verileri yetkisiz elektronik erişimden korumakla ilgilenirken; bilgi güvenliği, bilginin fiziksel veya dijital biçimde olup olmadığına bakılmaksızın bilgi varlıklarını korumakla ilgilenmektedir.

Bilgi teknolojileri kullanımının artması ve hayatımızın her alanına entegre olması, bilgi güvenliğine dair problemleri de beraberinde getirmiştir. Bu dijitalleşme sürecinde işletmelerin bilgi kaynaklarının ve veri tabanlarının da dijitalleşmesi nedeniyle analog bilgi kullanımı azalmış ve bu durum bilgi güvenliği ve siber güvenlik kavramlarının iç içe geçmesine sebebiyet vermiştir. Her ne kadar bilgi güvenliği kavramı ve siber güvenlik kavramları birbirlerinin yerine kullanılsa da bu unsurların farklılıkları ve kesişen özellikleri mevcuttur. Her iki unsorda işletmeler açısından eşit derecede öneme sahiptir. Bu nedenle teknoloji ve güvenlik tehditlerini anlamak yöneticiler, iç denetçiler siber güvenlik ve bilgi güvenliği profesyonelleri için gereklidir.

2.3.2.1. Bilgi Güvenliği ve Siber Güvenlik İlkeleri

ISO'nun bilgi güvenliği tanımında bahsi geçen bilgi güvenliğinde C.I.A (Confidentiality, Integrity, Availability) üçgeni olarak da bilinen ilkeler BT sektörünün genel kabul görmüş ilkeleri haline gelmiştir.

Şekil 2.3. Bilgi Güvenliğinin Temel Bileşenleri



Kaynak: (Whitman & Mattord, 2017: 11).

Şekil 2.3.'te yer alan gizlilik, bütünlük, kullanılabilirlik geçmişten günümüze bilgi güvenliği modeli olarak kullanılmıştır (Whitman & Mattord, 2017: 11). Bu modelde yer alan unsurlar önemini bugün de korumaktadır ancak C.I.A. modeli artık sürekli gelişen ve değişen teknoloji ve iş dünyasına hitap etmede yetersiz kalmaktadır. Günümüzde, gizlilik, bütünlük ve bilginin kullanılabilirliğine yönelik tehditler, kazara veya kasıtlı hasar, imha, hırsızlık, insan veya insan dışı tehditlerden kaynaklanan diğer kötüye kullanımlarla birlikte giderek karmaşık bir hal almaya başlamıştır. Bu sürekli gelişen tehditler dizisi, mevcut bilgi güvenliği ortamının karmaşılaşan yapısına yönelik daha gelişmiş modellerin ortaya çıkmasını sağlamıştır. Yıllar içerisinde bilgi güvenliği önemini korurken aynı zamanda bilgi teknolojilerinin gelişimine paralel siber güvenlik de önem kazanmış ve bu durum C.I.A modelinin evrilmesini sağlamıştır (Solms & Van Niekerk, 2013: 98). Günümüzde kabul gören bilgi güvenliği ve siber güvenliğin temel prensipleri Şekil 2.4'te sunulmuştur.

Şekil 2.4. Bilgi Güvenliği ve Siber Güvenliğin Temel Prensipleri



Kaynak: (Cherdantseva, & Hilton, 2013: 4)

Gizlilik (Confidentiality): Gizlilik, bilgilerin yetkisiz kişilerden korunması olarak tanımlanmaktadır (Knorr & Rohrig, 2001). Gizlilik, bilgiye sadece yetkilendirilmiş kullanıcıların erişmesi anlamına gelmektedir. Yetkisiz kişiler veya sistemler bilgileri görüntülediğinde, gizliliği ihlal edilmiş sayılmaktadır. Bilgilerin gizliliğini korumak için alınabilecek önlemlerden bazıları aşağıda sunulmuştur (Whitman & Mattord, 2017: 11):

- Bilgi sınıflandırması
- Güvenli belge depolama
- Genel güvenlik politikalarının uygulanması
- Bilginin güvenliğinden sorumlu kişilerin ve kullanıcıların eğitimi

Gizliliğin sağlanması ile işletmelerin önemli bilgilerinin ifşa edilmemesi ve önemli evrakların yetkisiz kişilerce ele geçirilmemesi sağlanmakta, böylelikle işletmenin itibarı ve geleceği korunmaktadır.

Bütünlük (Integrity): Bütünlük, hatalı işlemlerle (kasıt olmaksızın) veya kötü niyetle bilginin değiştirilmemesi ya da zarar görmemesi olarak tanımlanmaktadır. (Knorr & Rohrig, 2001: 76) Bilgiler tam, eksiksiz ve bozulmamış ise zaman bütünlük korunmuş kabul edilmektedir. Bilginin bütünlüğü, yolsuzluk, hasar, tahribat veya orijinal durumunun değişmesine neden olacak herhangi bir etkene maruz kaldığında tehdit altına girmektedir (Whitman & Mattord, 2017: 17).

Bütünlüğün bozulması, bilginin saklanması veya aktarılması aşamalarında meydana gelmektedir. Bilgisayar korsanları (hacker) bu amaçla birçok bilgisayar virüsü ve solucanı tasarlanmaktadır. Bütünlük hacker saldırısı dışında beklenmedik donanım arızası ve düşük voltaj seviyesine sahip bir devrede veri iletimi gibi sebeplerle de bozulabilmektedir (Whitman & Mattord, 2017: 17). Bunun dışında çalışanlar da bilgi bütünlüğü için tehdit unsuru olarak karşımıza çıkmaktadır. Çalışanlar bazen yanlışlıkla dosyaları silmekte, yanlış veriler girmekte veya yanlış dosyaları düzenlemektedir. Dosya bozulması ise bu konuda meydana gelen başka bir sorundur. Bilgi aktarılırken, saklanırken veya virüsler tarafından dosya bozulması oluşabilmektedir (Steichen, 2012).

Bütünlüğü sağlamak birçok önlem alınmaktadır. Bu önlemlerden bazıları aşağıdaki gibidir (Penber-Bey, 2012: 12):

- Veri doğrulama ve sağlama kontrolleri (Data verification and validation checks),
- Hesaba Dayalı Adresleme (Hashing),
- Veri ve bilgileri yedekleme (performing and maintaining backups).

Erişilebilirlik (Availability): Erişilebilirlik ilkesinin temel amacı, bilgi sistemlerine içeriden ya da dışarıdan yapılan saldırıların engellenerek kullanıcıların ulaşmaya çalıştıkları bilgilere zamanında ve güvenilir bir şekilde ulaşmalarını sağlamaktır Erişilebilirlik, yetkili kullanıcıların (kişilerin veya bilgisayar sistemlerinin) herhangi bir parazit veya engel olmadan bilgilere erişmesini mümkün kılmaktadır. Bu nedenle sistemlerde meydana gelen herhangi bir aksaklık işletmelerin operasyonel süreçlerini olumsuz etkileyebilmektedir (Yıldız, 2014: 60).

Günümüz dünyasında, bilgi kaynakları erişilebilir değilse, işletmeler açısından gelir ve müşteri kaybına uğrama riski de artmaktadır. Bu nedenle kaynakların korunması ve

erişilebilirliğin sağlanması, bilgi güvenliğinden sorumlu personel için en büyük görevlerden biri haline gelmiştir. Erişilebilirliğin sağlanması yaygın olarak kullanılan yöntemler aktif / aktif kümeleme (active/active clustering) ve aktif / pasif kümelemedir (active/passive clustering). (Sadece bir sunucunun aktif diğerlerinin pasif olduğu (sadece arıza durumunda aktif olduğu) kümelemelere Active/Passive Clustering, sunucuların aynı anda çalıştırıldığı kümelemelere Active/Active Clustering denilmektedir.) (Penber-Bey, 2012: 16).

Hesap Verilebilirlik (Accountability): Hesap verilebilirlik, sistemin kullanıcıların işlemlerini; ihtiyaç anında sorumluluk sahibinin belirlenmesi amacıyla izlemesi ve kaydını tutmasıdır (Weitzner ve ark., 2008: 83).

Dijital ortamlarda gerçekleştirilen işlemlerin ihtiyaç duyulduğunda izlenebilmesi için kayıt altına alınması gerekmektedir. Bilgi sistemleri açısından düşünüldüğünde bu işlemler e-posta gönderimi, herhangi bir sosyal medya hesabından mesaj gönderilmesi, internet sitelerine yapılan girişler vb. işlemleri kapsamaktadır. Toplanan bilgiler sayesinde sistemin bilinen saldırı türlerine maruz kalıp kalmadığının tespiti kolaylaşmaktadır (Yıldız, 2014: 60).

Özgünlük & Güvenilirlik (Authenticity & Trustworthiness): Bilgi depolandığında veya aktarıldığında, ilk yaratıldığı zamanki durumu korumakta ise özgün (orijinal) kabul edilmektedir. Ayrıca; özgünlük bir mesajın, işlemin veya başka bir bilgi değişiminin iddia ettiği kaynaktan geldiğini garanti etmektedir. Bu durumu sorgulamak ve bilgi güvenliğini sağlamak için ise kimlik doğrulaması işlemi gerçekleştirilmektedir (Cherdantseva, & Hilton, 2013).

Özgünlük ve güvenilirliğin garanti altına alınması amacıyla günümüzde kullanılan en yaygın yöntemlerden biri dijital sertifikalardır. Dijital sertifikalar, web sitesi üzerinden erişilen kullanıcıların kimliğini onaylayan dosyalardır. Dijital sertifikalar, sertifika vermek için yetkilendirilmiş kuruluşlar tarafından verilmektedir.

Denetlenebilirlik (Auditability): Denetlenebilirlik, veri tabanındaki öğelere erişen veya değiştiren kişileri takip edebilme eylemidir (Farahmand, Sharp & Enslow, 2005: 2004). Bu ilke, sistem davranışının tüm geçmişi üzerine uygulanan tüm ilgili eylemlerin tarihsel

kayıtlardan yeniden oluşturabilmesini içermektedir. Denetlenebilirlik; sistemdeki arızaların keşfedilip sebeplerinin bulunması ve bir güvenlik olayı arızasının ve sonuçlarının kapsamını belirlenmesi amacını gütmektedir (Yan ve ark.,2012: 1002).

Yetkili kullanıcıların gerçekleştirdikleri işlemler ve eylemler, işletmelerin bilgi güvenliğinin sağlanabilmesi açısından önem arz etmektedir. Birçok site, bilgi sistemlerine ve teknolojilerine sızabilen, zarar verebilen virüsler ya da solucanlar içermektedir. Bütün bunların önüne geçebilmek için kullanıcıların denetlenebilirliği önem arz etmektedir.

2.4. Siber Güvenlik ve Siber Güvenliğe İlişkin Kavramlar

Siber Güvenliğin sözlükteki karşılığı; elektronik verilerin yasadışı veya izinsiz kullanımına karşı korunma durumu veya bunu başarmak için alınan önlemlerdir (Oxford English Dictionary, 2020).

Siber güvenlik, istenen düzeyde koruma sağlamak için bilgisayarlara uygulanan güvenlik önlemleri olarak tanımlanmaktadır (Conklin ve White, 2006, 1). Ağları, bilgisayarları, programları ve verileri saldırı, hasar veya yetkisiz erişime karşı korumak için tasarlanmış teknolojiler, süreçler ve uygulamalara siber güvenlik uygulamaları denilmektedir (Kohnke ve ark., 2016: 15).

Siber güvenlik kavramı çok boyutlu bir kavramdır. Literatürde yer alan siber güvenlik ile ilgili temel kavramlar aşağıdaki bölümlerde açıklanmaktadır.

2.4.1. Siber Varlık ve Siber Olay

Bilgisayar, sunucu, ağ cihazları, nesnelerin internetine entegre cihazlar gibi bilişim unsurları ve tüm bu unsurların yazılım ve donanım bileşenleri “siber varlık” olarak tanımlanmaktadır (Bozgeyik, 2018: 26).

Siber olay; bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilgi veya herhangi bir verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya buna teşebbüs edilmesini ifade etmektedir (T.C Ulaştırma Bakanlığı, 2016: 8).

Ulaştırma Denizcilik ve Haberleşme Bakanlığı'nın bu tanımına ek olarak; bilgi ve iletişim teknolojilerinden yararlananların, bu teknolojiler sayesinde elde ettikleri menfaat ve faydanın olumsuz etkilendiği, doğal afet, elektrik kesintisi, fiber optik hatlarda oluşan arızalar veya benzer herhangi bir vaka "siber olay" olarak nitelendirilebilir (Bozgeyik, 2018: 27).

2.4.2. Siber Uzay/Alan/Ortam

Siber uzay bir bilgi ortamıdır. Sırf sanal bir ortam olmamakla birlikte yaratılan, saklanan ve paylaşılan dijital verilerden ve bu verileri saklayan bilgisayarlara ilave olarak bunların akışına izin veren sistem ve altyapılardan oluşmaktadır. Siber uzay kavramı içerisinde ağ tabanlı bilgisayarların interneti, kapalı intranet sistemler, hücresel teknolojiler, fiber optik kablolar ve uzay tabanlı iletişim bulunmaktadır. Siber alanda, sunucular, web sayfaları, hizmetler vb. araçlar karşılıklı olarak birbirlerine bağlı ve bağımlı olarak birlikte çalışmaktadırlar (Alioğlu, 2019: 4). Siber uzay dört ögeden oluşmaktadır. Bunlar (Schmit, 2016):

- Kullanıcılar;
- Paylaşılan bilgi;
- Yazılım ve protokoller;
- Fiziksel altyapıdır.

2.4.3. Siber Terörizm

Siber terörizm, terör örgütlerinin siber ortamın sunduğu kolaylıkları, uygulamaları, araçları, altyapıları, teknik ve teknolojileri, boşlukları, zararlı yazılım ve içerikleri bulup kullanarak, tuzaklar veya yeni yöntemler yardımıyla ulusları, toplumları işletmeleri ya da kişileri yönlendirme, sindirme, zarar verme, yıldırma, bezdirme ve çıkar elde etme amacıyla yaptığı faaliyetlerdir (CyberMag, 2017: 19).

2.4.4. Siber Casusluk

Siber casusluk, bir lke, iřletme ya da organizasyonun, hassas ve kritik nem dzeyine sahip siber ortamında yer alan bilgilerinin gizlice ele geirilmesi eylemidir. Bu eylem bireysel ya da kolektif olarak finansal ıkar amacıyla da gerekleřtirilebilmektedir. Ayrıca bir devletler birbirlerine zarar vermek amacıyla da siber casusluęa bařvurabilmektedir. Siber casusluk faaliyetleri siber savařların en byk nedeni olarak grlmektedir (Yayla, 2013: 196). Siber casusluk iki kategoride incelenmektedir (Alkan, 2017: 20):

- **Ekonomik Casusluk:** İřletmelerin, kurumların ve bireylerin, fikri mlkiyetini ticari ve teknik sırlarını ya da deęeri yksek bilgilerini, siber ortam ve aralarını kullanarak alma eylemidir. Bu tr hırsızlıklar, kendi bařlarına alıřan suluların yanı sıra, firmalarca (rakiplerinden bilgi alma) veya devletler tarafından desteklenmektedir.
- **Askeri Casusluk:** Bir devletin siber ortam ve aralarını kullanarak bařka bir devletin iine sızması yolu ile askeri kurum veya tesislerden bilgi sızdırmasıdır.

2.4.5. Siber Sular

Siber suların birok tr bulunmaktadır. Bunlardan ilki; elektronik haberleřme ve bilgi sistemleri zerinden iřlenen dolandırıcılık ve sahtecilik sularıdır. Dięer bir siber su tr ise yasadıřı ierięin elektronik ortam zerinden yayılmasıdır. Irkılık, nefret sylemleri ve cinsel ocuk istismarı gibi sular siber su trlerine rnektir. Son olarak; bilgi sistemleri hizmetinin aksatılması, durdurulması veya hacklenmesi de siber sular kapsamına girmektedir (Hekim & Bařıbyk, 2013).

2.5. Siber Saldırıları/Tehditler

Siber saldırı; *“siber uzayda bulunan biliřim sistemlerinin gizlilik, btnlk veya eriřilebilirlięini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kiři ve/veya biliřim sistemleri tarafından kasıtlı olarak yapılan iřlemler”* olarak tanımlanmaktadır (T.C Ulařtırma Bakanlıęı, 2016).

Siber tehditler geleneksel tehditlere göre çeşitli farklılıklar göstermektedir. Bu farklılığın oluşmasının nedeni tehditlerin önceden tahmin edilebilmesinin pek de mümkün olmamasıdır. Çünkü siber saldırılar, hızlı bir şekilde gerçekleştirilmekte ve tespit edilmesi uzun zaman almaktadır. Farklılıklardan bir diğeri ise katlanılan maliyetlerden ileri gelmektedir. Siber saldırı gerçekleştirmek için ucuz yöntemler etkili olabilmektedir. Ancak saldırıya maruz kalan taraf ise oldukça büyük maliyetlere ve zararlara katlanmak zorunda kalabilmektedir (Gürkaynak ve İren, 2011: 265). Günümüzde global ölçekte faaliyet gösteren işletmelerin tamamına yakını neredeyse her gün siber saldırılara maruz kalmaktadır (Cisco, 2020).

Cisco Yıllık Siber Güvenlik Raporuna göre, olayların toplam hacmi Ocak 2016 ile Ekim 2017 arasında dört kat artmıştır. Saldırganlar savunmasız iş sistemlerinden yararlanmaya çalıştıkça siber suçlar her yıl artmaya devam etmektedir. 2019 yılı itibariyle gerçekleşen siber saldırıların yüzde 53'ü 500.000 dolar veya daha fazla zararla sonuçlanmaktadır (Cisco, 2020).

2015' de 2 milyar olan internet kullanıcısı sayısı 2018 yılında yaklaşık 4 milyarı bulmuştur. (Dünya nüfusunun yaklaşık yarısı 7,7 milyar). Tarihsel olarak nüfus artışıyla bağlantılı olarak büyüyen sokak suçları gibi siber suçlarda insan sayısının ve dijital hedeflerin artmasına paralel benzer bir gelişim göstermektedir. 2017 yılında siber suçların küresel ekonomiye 600 milyar dolara mal olmuştur. 2018'de küresel finansal hasar, yıllık %50 artışla 1 trilyon doları aşmıştır. 2021 yılında bu rakamın 6 trilyon doları bulması beklenmektedir. (Cybercrime Magazine, 2020)

Bu veriler ışığında işletmelerin BT çalışanları ve iç denetçilerinin siber tehditleri iyi şekilde tanınması ve bilgi teknolojilerini ve sistemlerini korumak için gerekli sistemleri kurması, bilgi güvenliği yönetişimini üst yönetimin de desteğini alarak gerçekleştirmesi son derece önemlidir. Çalışmanın bu bölümünde işletmelerin maruz kaldığı siber saldırı türleri açıklanacaktır.

2.5.1. Sosyal Mühendislik

Sosyal mühendislik, insan tutum ve davranışlarındaki önyargılar üzerine kurgulanan; etkileme, zorlama, aldatıcı ilişkiler geliştirme, sorumluluğu, etik değerleri,

dürüstlüğü ya da bağlılığı azaltma amacını güden yöntemler kullanarak kişileri gizli bilgi vermeleri veya erişim sağlamaları için aldatma sürecidir (Bağcı, 2009). Siber güvenlik açısından sosyal mühendislik; bir bilgisayar korsanının bilgi sistemlerini kullanan kullanıcıları psikolojik ve sosyal numaralar ile manipüle ederek, sisteme erişmek için gerekli bilgileri elde etmesi şeklinde tanımlanmaktadır (Yavanoğlu, Sağıroğlu, & Çolak, 2012).

Sosyal mühendisler kendilerini sahte senaryolar yardımıyla kendilerini kamu görevlisi, firma yetkilisi, bir tanıdık veya tanıdığın yakını olarak tanıtmaktadırlar. Bu kişiler uygulanan psikolojik teknikler ve senaryolar yardımıyla ilk aşamada karşısındakilerin güvenini kazanmakta, yakınlık duygusu hissedilen hedef sosyal mühendisin istediklerini, yönlendirmelerini şüphe duymaksızın yapabilmektedirler (Yılmaz, 2015).

Sosyal mühendisler öncelikle hedef kullanıcı hakkında araştırma yapmakta, daha sonra kullanıcının güvenini sağlamak amacıyla hareket, davranış ve eylemlerde bulunmaktadır. Özellikle hedef hakkında kişisel bilgilerin edinilmesi ve son aşamada sosyal mühendisi ele verebilecek tüm kanıtların yok edilmesi sosyal mühendislik yaşam döngüsünün en önemli basamaklarını oluşturmaktadır. (Gündüz & Daş, 2016, 2).

Bilgisayar korsanları ve kötü yazılım geliştiricilerinin bilgi sistemlerine izinsiz erişebilmek için uzun süren çalışmalar yaptıkları düşünüldüğünde; kullanıcılara ait kişisel veri ve bilgileri bu tarz hilelerle edinmek çok daha kolay olduğundan, sosyal mühendislik çalışmaları siber saldırganların en güçlü silahlarından birisi olarak öne çıkmaktadır (Mitnick & Simon, 2003).

2.5.2. Zararlı Yazılımlar

En geniş ifade ile bilgi teknolojilerini kötü amaçlı kullanmak için sistem bilgilerine erişim sağlamaya yarayan ya da bilgi teknolojilerine ciddi zararlar veren kötü bilgisayar programlarıdır (USOM, 2014). Kötü amaçlı yazılımlar, altı kategoride incelenebilir (Ünver ve ark., 2011). Bunlar;

- Bilgisayar virüsleri,
- Solucan (Worm)

- Truva atı (Trojan),
- Klavye kaydedici yazılımlar (Key logger),
- Reklam ve tanıtım (Adware) yazılımları,
- Casus / köstebek (Spyware) yazılımlarıdır.

Bilgisayar Virüsleri; kendilerini sistemdeki dosyalardan ya da programlar biri olarak değiştiren bilgisayar kodları olarak tanımlanmaktadır. Virüslerin aktif hale gelmesi için bir kullanıcı tarafından çalıştırılmaları gerekmektedir. Genellikle bir kullanıcıdan gelen e-postanın açılması, ya da USB'nin otomatik çalıştırılması halinde virüs bulaşabilmektedir. (USOM, 2014). Bilgisayar virüsleri kendilerini gizlemeyi ve daha fazla kaynağa yaymayı amaç edinmişlerdir (Krutz & Vines, 2007: 131-135).

Solucanlar, virüsler gibi kendilerini bir bilgisayardan başka bilgisayara kopyalamak için tasarlanmış zararlı yazılımlardır (USOM, 2014). Solucanların virüslerden farkı yayılma işlemini ağ üzerinden otomatik olarak yapmalarıdır. Solucanlar, bilgi teknolojilerini hedef alarak bu teknolojilerin ulaşılabilirliğini engellemekte ve bu varlıkların kontrolünü ele geçirmektedirler (Ünver ve ark., 2011: 11).

Truva atı (Trojen), bilgisayar kullanıcılarının içeriği hakkında derinlemesine bilgisi olmadan yükledikleri zararlı yazılımlardır. Kullanıcıların uygulamaları, programları ya da dokümanları güvenilir bir kaynaktan yüklemek yerine bilmedikleri bir kaynaktan yüklenmesi durumunda truva atı yüklü bir program gelmesi muhtemeldir (USOM, 2014).

Klavye kaydedici yazılımlar, klavyedeki her hareketi ve basılan her tuşu izleyip kayıt eden ve elde edilen verileri siber saldırganlara gönderen yazılımlardır. Saldırganlar bu yazılımlar sayesinde kişisel ve önemli her türlü bilgiye (e-mail şifresi, kredi kartı numarası) erişim sağlamaktadır (Krutz & Vines, 2007: 149-151).

Casus / köstebek (Spyware) yazılımlar bilgisayarlarda casusluk yapmak için yaratılmış programlardır. Casus yazılım, kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanmaktadır. Bu casus yazılımlar, diğer kötücül yazılımlara göre özellikle internet kullanıcıları tarafından sistemlere farkında olmadan bulaştırılmaktadırlar (USOM, 2014).

2.5.3. Botnet (Zombi Ağı)

Botnet sözcüğü, "robot" ve "network" (ağ) sözcüklerinin birleşimi ile oluşmuştur. Siber güvenlik terimi olarak robotlaşmış, köleleştirilmiş, kontrolü başkasında olan bilgisayar ağı anlamına gelmektedir. Kullanıcısı farkında olmadan zararlı yazılımlar yüklenmiş, tamamen ya da kısmen bilgisayar korsanları tarafından kontrol edilen ve verilen siber saldırı komutlarını yerine getiren bilgisayarlara "zombi bilgisayar" denilmektedir. Bu bilgisayarlar, siber saldırıların merkezinde olmasına rağmen işlenen siber suça hizmet ettiğinin farkında dahi olmayan cihaz ve sistemlerdir. Botnet veya zombi bilgisayar ağı siber saldırı altyapı bileşenlerinin en önemlilerinden biridir. Botnet ağı; komuta ve kontrol sunucuları ve yüzbinlerce enfekte olmuş, uzaktan yönetilebilen bilgisayarlardan oluşmaktadır (Marinos ve ark., 2016: 26, Bozgeyik, 2019).

2.5.4. Gizli- Arka Kapılar (Back Doors)

Arka kapı herhangi bir bilgi sistemine yönelik normal kimlik doğrulama yöntemini devre dışı bırakılarak başka bir yöntemle sisteme giriş yapma ve verilere erişim imkânı sağlayan yazılımlardır (Akarslan 2015: 98).

Arka kapılar yazılım hataları nedeniyle ortaya çıkabilmektedir. Bunun dışında zararlı yazılımlar tarafından oluşturulabilir veya üreticiler tarafından bilinçli olarak hazırlanabilirler. Bu program çalıştığı zaman arka kapı isimli yazılımı yerleştiren yaratıcısına uzaktan erişim yönetimi kullanarak ve hâlihazırda mevcut olan sistem kontrollerine fark edilmeden sisteme ulaşma olanağı tanımaktadır. (Sağıroğlu, 2018)

2.5.5. Oltalama (Phising)

Oltalama, yasadışı yollarla kullanıcıların herhangi bir sistem için kullandıkları kullanıcı adı, şifre, kimlik bilgileri, kredi kartı ayrıntıları gibi bilgilerin ele geçirilmesidir. Sözcük, İngilizce password (şifre) ve fishing (balık avlamak) sözcüklerinin birleşmesiyle oluşturulmuş phishing ifadesinin Türkçe karşılığıdır. "Yemleyici" diye tanımlanan şifre avcıları, genelde e-posta gibi yollarla kişilere ulaşmakta ve onların kredi kartı gibi ayrıntılarını talep etmektedirler. Bu tip mailleri cevaplayan kullanıcıların da hesapları, şifreleri vb. özel bilgileri çalınmaktadır. (USOM, 2014)

Olta saldırısının asıl hedefi kurbanların verilerini ve bilgilerini elde etmek için, kurbanların kullandıkları cihaz veya sistemlere zararlı yazılımlar yüklemektir. Bu saldırı türünde, güvenilir görünmek için kurbanlara aşına olduğu etkinliklerden, güvenilir kurum ve kuruluşlardan, markalardan ve kendi tanıdığı kişilerden geldiği izlenimi oluşturan e-postalar, web sayfaları ve reklamlar ile algı karmaşası yaratılmakta, kullanıcının bu e-posta ve web adreslerindeki bağlantılara tıklaması sağlanmaktadır. Böylelikle yazılım kullanıcıların sistemine yüklenmekte veya dijital veriler çalınmaktadır (Marinos ve ark., 2016: 33). 2018 yılı itibariyle gerçekleştirilen ortalama saldırısı temaları Tablo 2.1.'deki gibidir (ENISA, 2018: 44):

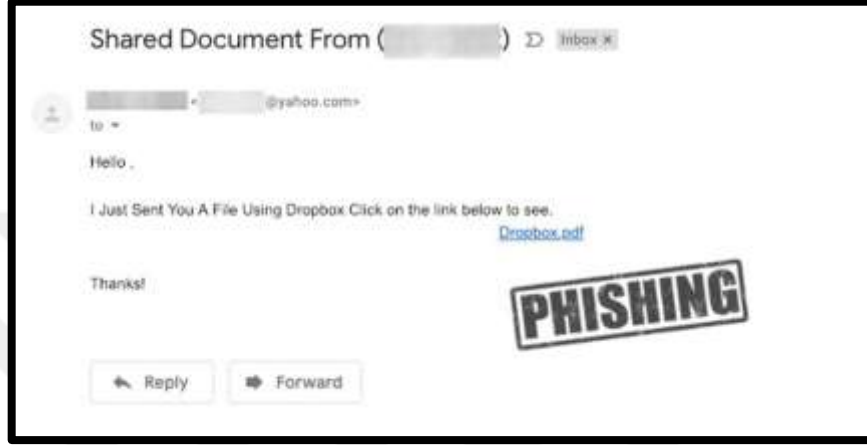
Tablo 2.1. Ortalama Saldırısı Temaları

1)	Dropbox hesabı	11)	Amazon
2)	Finansal kuruluşlar	12)	Apple hesabı
3)	E-Posta uygulamaları	13)	Microsoft Excel Online
4)	Microsoft Outlook	14)	Linkedin hesabı
5)	Office 365 hesabı	15)	Windows ayarları
6)	Adobe hesabı	16)	Posta/kargo şirketleri
7)	Google Drive	17)	MyEtherWallet
8)	DocuSign uygulaması	18)	Alibaba
9)	Netflix	19)	OneDrive
10)	PayPal	20)	Retail

Kaynak: ENISA, 2018

Oltalama mesajı örneği şekil 2.5.'de sunulmuştur:

Şekil 2.5. Dropbox Temalı Oltalama Mesajı



Kaynak: Mailguard, 2020.

2.5.6. Hizmet Dışı Bırakma- (Denial-of- Service)

Hizmet dışı bırakma saldırıları kısaca DoS (Denial of Service) olarak adlandırılmaktadır. Hizmet dışı bırakma saldırıları bir bilgi sisteminin erişilebilirliğine yönelik olarak düzenlenmekte ve sistemin hizmetini engelleme amacı gütmektedir. Bu saldırılar, bilgi hırsızlığı veya BT sistemlerine sızma amacıyla yapılmazlar. Asıl amaç BT sistemleri tarafından sunulan hizmetin geçici olarak veya tamamen engellenmesidir (Vacca, 2006: 12).

Bu saldırı çeşidinin pek çok yöntemi bulunmaktadır. Tüm yöntemlerin ortak amacı sistem ile çok sayıda sahte bağlantı kurularak, sunuculara aşırı iş yükü bindirmek ve sunucunun gerçekten bağlantı kurmaya çalışan kullanıcılara cevap veremez hale gelmesini sağlamaktır (Bozgeyik, 2019).

Dağıtık Hizmet Dışı Bırakma Saldırısı” (Distributed Denial of Service Attack- DDOS) saldırıları ise organize şekilde gerçekleştirilmektedir. Saldırılarda çok sayıda botnet bilgisayar kaynak olarak kullanılmaktadır. DDOS saldırısının amacı işletmeleri

veya organizasyonları itibar kaybına uğratarak finansal zarar vermektir. Saldırının arkasındaki kişi veya kişileri bulmak neredeyse imkânsızdır (Bozgeyik, 2019).

2.5.7. İstenmeyen E-Posta (Spam)

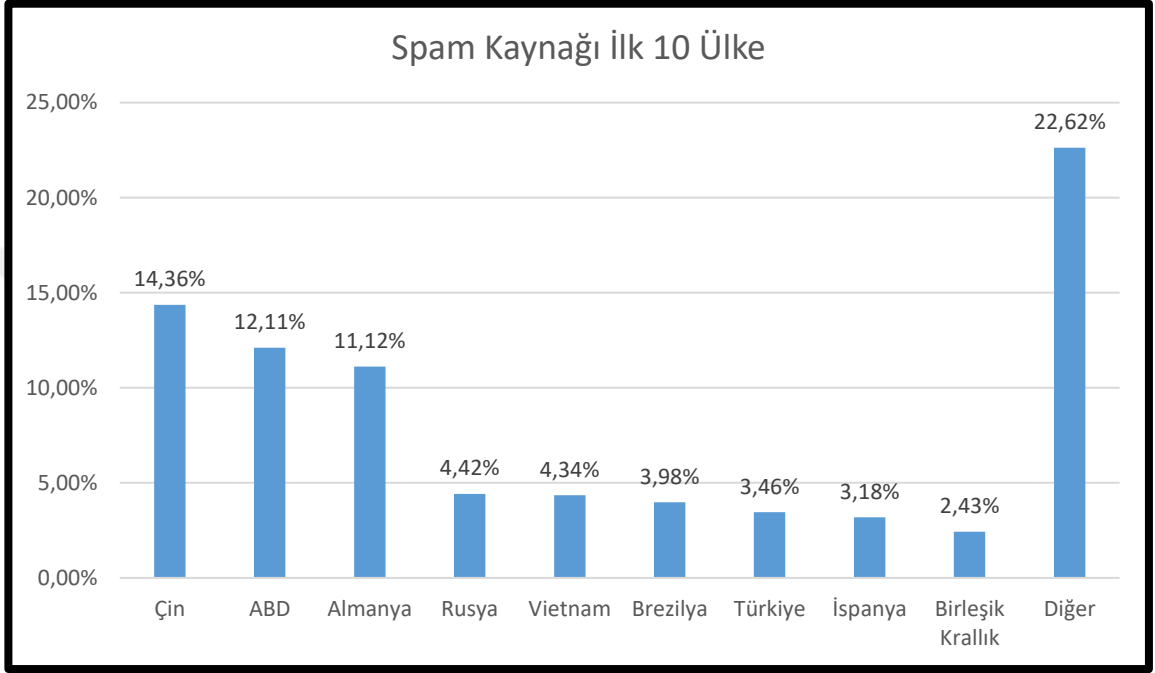
Kullanıcılar talep etmediği ve istemediği halde, zorla gönderilen mesajlar "istenmeyen e-posta (spam) olarak adlandırılmaktadır (Ünal, 2010: 159).

Spam e- postalar virüs yazılımcıları ya da bilgisayar korsanları tarafından merak ve ilgi uyandıran; eğlence, reklâm, yardım, duygu sömürüsü, bankacılık vb. içeriklerle nihai kullanıcılara gönderilmektedir. Zararlı ve gizli kod taşıyan e-postalar ile kullanıcıların adres defteri, kimlik bilgileri, internet bankacılığı bilgileri, kullanıcı girişi yapılan hesapları, mesajlaşmaları gibi özel bilgileri ele geçirilmektedir (Şahinaslan ve ark., 2010: 1). Spam e-postaların%75'i 3 kategoriden oluşmaktadır (Trustware, 2018):

- Sağlık içerikli (%26,6),
- Kötü amaçlı yazılım kaynaklı (%25,7) ve
- Çevrimiçi tanışma siteleri kaynaklı (%21,4).

Yukarıda listelenenler dışında; sahte iş teklifleri, finansal içerikli ve yetişkinlere yönelik içeriği olan e-postalar diğer spam türlerini oluşturmaktadır. Spam mailler giderek yerel bir hal almakta ve farklı dillerde yayılmaya devam etmektedir. 2017 yılında spam e-postaların %96'sı İngilizce iken 2018 yılında bu oran %6 gerileyerek %90 seviyesine düşmüştür. Spam maillerin kaynağı ülkeler Şekil 2.6.'da sunulmuştur:

Şekil 2.6. Spam Kaynağı İlk 10 Ülke



Kaynak: Kaspersky, 2018.

2.5.8. Fidyeye Yazılımları (Ransomware)

Fidyeye yazılımlar; yazılımlar, bilgi sistemi ya da dosya erişimini engelleyen ve kullanıcıları dosyalarına erişim karşılığında fidye ödemeye zorlayan zararlı yazılımlardır (Çelik & Çeliktaş, 2017).

Fidyeye yazılımlar, erişim sağladıkları sistemlerde bir ekran uyarısı şeklinde ortaya çıkarak (Şekil 2.7.), kullanıcıların dosyalarını şifrelediklerini ve erişimi kısıtladıklarını belirtmektedirler. Erişimi tekrar açmak için ise fidye talep etmektedirler.

Geçmiş yıllarda fidye yazılımlara yapılan ödemeler, geleneksel ödeme yöntemleri gerçekleşmekte ve güvenlik güçleri bu ödemeleri takip ederek suçluları kolaylıkla tespit etmekteydi. Ancak günümüzde ethereum, bitcoin vb. para birimleri ve ödeme kanalları aracılığı ile gerçekleşen ödemeler nedeniyle siber suçluların tespiti ve takibi imkânsız hale gelmiştir (Çelik ve Çeliktaş, 2017).

Fidye yazılımlar, dünyada en yaygın siber tehditlerden biri olarak görülmekte özellikle finans, sağlık ve telekomünikasyon sektöründe faaliyet gösteren işletmelere yönelik fidye yazılım saldırıları artış göstermeye devam etmektedir (Hallam-Baker, 2016: 2).

Şekil 2.7. Fidye Yazılım Örneği



Kaynak: Database, 2020.

2.5.9. IP Aldatması (IP Spoofing)

Bilgisayar bağlantıları çeşitli protokoller vasıtasıyla sağlanmaktadır. Protokoller vasıtasıyla başka bir bilgisayara bağlanıldığında bağlanan bilgisayar kimliğini diğer tarafa tanıtmaktadır. Bağlanılan bir bilgisayara gerçek IP adresinin gösterilmemesi yani asıl kimliğin gizlenmesine IP spoofing (Aldatma) denilmektedir (Arslan, 2016: 5).

IP aldatması, siber suçluların sahte veya "yanıltıcı" IP adresi kullanarak başka sistemlere yetkisiz erişim elde etmeye çalışmasıdır. Saldırganlar bunu gerçekleştirmek için yasal bir ana bilgisayarın IP adresini edinip kendi sistemlerinden gönderilen paket

başlığını değiştirerek bunları orijinal, güvenilir bilgisayardan gelmiş gibi göstermektedir (Kaspersky, 2020).

2.5.10. Fiziksel Zarar (Physical Manipulation)

Fiziksel saldırılar gerçek bir siber tehdit olmamasına rağmen, bugün işletmelerde hala BT açısından önemli bir risk unsurudur. Bilgi teknolojilerine ve cihazlara fiziksel erişim saldırganlara kötü amaçlı etkinliklerini yürütme fırsatı vermektedir. ATM sahtekârlığı ve POS cihazı saldırıları; fiziksel saldırıların en yaygın örneklerindendir (ENISA, 2018: 74.) Bu saldırılara ek olarak özellikle perakende sektöründe, kart kopyalama (Card Skimming) bir diğer fiziksel saldırı türü olarak öne çıkmaktadır. (Verizon, 2018)

Verizon'un 2018 yılında yaptığı araştırmada veri ihlallerinin %11'nin fiziksel saldırı kaynaklı olduğunu ortaya çıkarmıştır. Sağlık, kamu ve finans sektörleri, fiziksel hırsızlık veya kayıp nedeniyle veri ihlallerinin gerçekleştiği sektörlerin başında gelmektedir. Finans sektöründeki veri ihlallerinin %25'i, BT cihazlarının kaybolması veya çalınmasından ötürü gerçekleşmektedir. (Verizon, 2018)

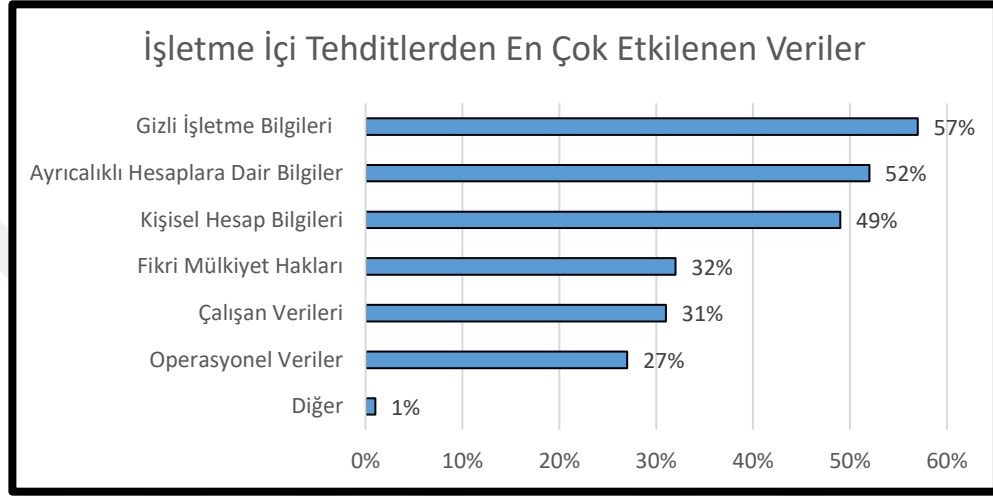
2.5.11. İşletme İçi Tehditler

Siber güvenlik açısından iç tehditler her işletme ve kuruluştaki mevcut olabilmektedir. İşletmenin bilgi sistemlerine erişim hakkı olan mevcut veya eski bir çalışanın, iş ortağının ve anlaşmalı tarafların bu erişimi kasten veya istemeden kötüye kullanabilme ihtimali her zaman bulunmaktadır (ENISA, 2018: 69). İşletme içi tehdit oluşmasındaki nedenler aşağıda sunulmuştur (Marinos ve ark., 2016: 32):

- Hassas veriler üzerine çalışanların dikkatsiz davranışları,
- Çalışanların güvenlik kural ve politikalarını uygulamak için yeterli eğitime sahip olmaması,
- İş yükünden dolayı bilgi güvenliğinin önemsenmemesi,
- Çalışanların bilgi güvenliğini ciddiye almaması,
- Bilgi güvenliği kural ve politikalarının ek iş yükü getirmesi.

İşletme içi saldırılara maruz kalan veri çeşitleri Şekil 2.8.'de sunulmuştur:

Şekil 2.8. İşletme İçi Tehditlerden En Çok Etkilenen Veriler



Kaynak: ENISA, 2019, 71.

Avrupa Ağ ve Bilgi Güvenliği Ajansının (European Network and Information Security Agency-ENISA) 2019 yılında yayımladığı raporda; işletme içi tehditlerden en çok etkilenen veri türleri; gizli işletme bilgileri, ayrıcalıklı hesaplara ilişkin bilgiler, kişisel hesap bilgileridir. Bu veri türlerini fikri mülkiyet hakları, çalışan verileri ve operasyonel veriler izlemektedir. (ENISA 2019: 71) Ortalama saldırıları, zayıf veya yeniden kullanılan şifreler, kilitsiz cihazlar, şifre paylaşım uygulamaları ve güvenli olmayan WiFi ağları işletme içi tehditleri yaratan uygulamaların başında gelmektedir (ENISA 2019: 72). Bu tehditler işletmenin iç kontrol ortamının zayıflıklarından ileri gelmektedir ve riskleri minimize etmek için BT personeli ve iç denetim birimine büyük sorumluluk düşmektedir.

2.6. İşletmelerde Sınır Güvenliği Sistemleri

Sınır güvenliği sistemleri, değişen siber tehdit karakteristiklerine, ihtiyaçlara uyum sağlayacak şekilde bilgi yönetimi, koruma, tespit /teşhis/takip, test, izleme, kayıt ve yeniden oynatma gibi özellikleri olan sistemlerdir (Adır, 2019: 41) İşletmelerde siber

varlıkların güvenliğini sağlanması sınır güvenliği sistemlerinin etkinliğine bağlıdır. Bu bölümde işletmelerde sınır güvenliği sistemleri açıklanmıştır.

2.6.1. Güvenlik Duvarı (Firewall)

Güvenlik duvarı, bilgisayar ağlarında, önceden tanımlanmış veya kurallar ve ilkelere dayanarak ağ üzerinde gelen ve giden trafiğini kontrol eden, oluşturulan filtreleme politikalarına göre veri transferine izin veren veya engelleyen yazılımsal veya donanımsal sistemlere verilen isimdir (ESET, 2020a). Bu araçlar iç ağ ile güvenilmeyen dış ağ arasında bir güvenlik duvarı oluşturmaktadır. Güvenlik duvarı; güvenilir olmayan servislerin filtrelenmesi, sisteme kontrollü erişimin sağlanması, güvenlik zafiyetleri olan servislerin ağa girmesinin ve çıkmasının önlenmesi gibi birçok önleyici işlemin yapılmasına olanak sağlamaktadır. Güvenlik duvarı teknolojileri, işletmelerin ağlarını dışarıdan saldırılara karşı korumak için sürekli gelişmektedir. Yapılarına göre donanımsal ve yazılımsal olmak üzere iki farklı güvenlik duvarı türü vardır. Yazılım tabanlı olanlar genelde istemci veya sunucu üzerindeki işletim sistemlerine kurulmaktadır. Donanım tabanlı olan güvenlik duvarı cihazları ise, özel donanımlar üzerinde çalışmaktadır (Özgü & Akbaş, 2014).

2.6.1.1. Bütünleşik Güvenlik Cihazı (Unified Threat Management –UTM)

Anti-virüs, içerik filtreleme, saldırı tespit sistemi ve spam filtreleme kullanan çoklu sistemler yerine, günümüzde daha çok tüm özellikleri barındıran UTM cihazları yaygın olarak kullanılmaktadır. Bu cihazlar çoklu tehditlere karşı daha kapsamlı güvenlik sağlayabilmektedir (Adır, 2019: 42)

2.6.1.2. Saldırı Önleme Sistemi (Intrusion Prevention System- IPS)

Saldırı önleme sistemleri (IPS), ağ trafiğini sunuculara gelmeden önce üzerlerinden geçirip inceleyen, denetleyen ve gerektiğinde saldırıları engellemeye yarayan sistemlerdir (Cannady, 1998). Saldırı önleme sistemleri, kaynak ve hedef arasındaki doğrudan iletişim yoluna yerleştirilmektedirler ve ağ trafiği üzerinde daha önce oluşturulmuş saldırı imzalarına uyan hareketleri denetlemektedirler. Saldırıları tespit ettiklerinde paketi engelleme veya TCP bağlantısını sonlandırma işlemlerini gerçekleştirmektedirler (Tekerek ve ark. 2016).

2.6.1.3. Saldırı Tespit Sistemleri (Intrusion Detection Systems- IDS)

IDS'ler, adli araç olarak geliştirilmiş yazılımsal ve donanımsal sistemlerdir. IDS, ağ trafiğini izlemekte, analiz etmekte ve istenmeyen bir paket, zafiyet veya saldırı tespit etmeleri durumunda bunları kayıt altına alarak yöneticiye bildirmektedirler. Genellikle güvenlik duvarının hemen arkasında bulunmaktadır. Saldırı tespit sistemlerinin saldırı anında yöneticiye uyarı gönderme, zararlı paketleri bırakma, trafiği engelleme, bağlantıyı yenileme gibi birçok özelliği mevcuttur. IDS teknolojilerinin bilgi toplama, kaydetme, algılama ve önleme gibi farklı yetenekleri vardır. IDS sistemlerin host tabanlı ve ağ tabanlı olmak üzere iki türü bulunmaktadır. Özetle IDS, saldırıları tespit etmek için, geliştirilmiş yazılımsal veya donanımsal güvenlik sistemleridir (Mukhopadhyay ve ark., 2011).

2.6.1.4. Anti-Virüs / Anti-Malware / Anti-Spyware

Anti-virüsler, Truva atı, tehlikeli web siteleri, fidye yazılımları gibi zararlı yazılımlara karşı koruma sağlayan yazılımlardır (ESET, 2020b).

Gelişmiş Anti-virüs mekanizmaları, ağ geçidindeki çok sayıda saldırıya karşı koruma sağlamaktadır. SMTP, POP3, IMAP, FTP ve HTTP gibi önemli protokolleri incelemektedirler. Virüslerin en çok yayıldığı e-posta, http ve ftp trafikleri anti virüs ağ geçidine yönlendirilmekte ve tarama işleminden sonra gerekli yerlere iletim yapılmaktadır. Bu sistemle dışarıdan gelecek olan virüsler engellenmektedir (Hasanefendioğlu, 2018).

Sunucu bilgisayarları üzerine kurulacak virüs koruma yazılımları ve çalışanların sistemlerini kontrol edecek yazılımlarla kurumsal anti virüs sistemi kurulmaktadır. Bu sistemlerle istem dışı e-postaları engellemek, içerdiği kelimelere ya da eklerine göre silme/arşivleme vb. işlemler yapılabilmekte ve e-posta yönetimi sağlanabilmektedir (Adır, 2019).

2.6.1.5. Uygulama Kontrolü

Uygulama kontrolü ile kullanıcıların kullanabilecekleri uygulamalar sınırlandırılmaktadır. İnternet üzerinden kullanılacak servisler veya indirilecek dosyalar kontrol edilmekte ve kullanıcı bazlı engellemeler gerçekleştirilmektedir. (Adır, 2019).

2.6.1.6. Web Filtreleme Çözümleri (URL)

URL filtreleme yöntemleri, kullanıcıların ve işletme çalışanlarının siber tehditlerden ve aynı zamanda zararlı yazılım ve oltalama saldırıları içeren sitelerden korunmasını sağlamaktadır. Bu sistemler kullanıcıların internet erişimlerinin güvenli bir şekilde yapılabilmesi için vekil sunucu görevini üstlenmekte ve sahip oldukları üstün inceleme ve tespit motorları, raporlama arabirimleri ve bildirimleri sayesinde, anlık olarak kullanıcı erişimleri denetlenebilmektedir. Bant genişliği kontrolü, uygulama kontrolü, anti virüs kontrolü, SSL sonlandırma gibi çeşitli kontroller yapılabilmektedir (Federal Communications Commissions, 2011).

2.6.2. VPN

VPN, İngilizce Virtual Private Network' ün kısaltmış şeklidir ve Türkçe olarak Sanal Özel Ağ anlamına gelmektedir. Bu ağ, yetkilendirilmiş uzak kullanıcıların yerel ağa güvenli bir şekilde bağlanmasını sağlamaktadır. Kurumlar ve işletmeler, güvenlik duvarı üzerinde uzak erişim VPN yapılandırılarak mobil kullanıcılar için güvenli erişim sağlamaktadırlar (Scarfone & Mell, 2007).

2.6.3. Veri Sızıntısı Engelleme Sistemleri (Data loss prevention-DLP)

DLP, birbirlerinin yerine de kullanılabilen “data loss” prevention ya da “data leak” prevention sözcüklerinin kısaltması olup veri sızıntısı önleme, veri kaybı önleme anlamlarına gelmektedir. Mobil çalışanlar, kurum içi yetkili kullanıcılar, hacker ve diğer dış aktörlerin kötü niyetli veya kazara sebep olduğu veri sızıntılarını önlemek için kullanılan sistemlerdir. Bu sistemler, hassas verilerin yetkisiz kullanımı, iletiminin izlenmesini ve korunmasını amaçlamaktadırlar. Ayrıca sistem belirli kurallar çerçevesinde ağ trafiğini gözetlemekte, e-posta sunucusuyla entegre çalışmakta ve kullanıcı bilgisayarında kurallar çerçevesinin dışına çıkılmamasını denetlemektedir (Adır, 2019).

2.6.4. Sayısal İmza

Sayısal İmza kavramı Türkiye’de 15.01.2004 tarihli 5070 sayılı Elektronik İmza Kanunu ile Elektronik İmza (E-İmza) olarak isimlendirilmiş ve bu adla hukuki statü kazanmıştır. Bir kullanıcı, sunucu ya da hosttan gönderilen bilgilerin kesinlikle o kuruma

veya kişiye ait olduğunu doğrulayarak, verinin başkası tarafından yollanmadığını garanti eden dijital sertifikadır (Uçmaz, 2009: 51).

2.6.5. Zafiyet Analizi ve Sızma Testleri

Zafiyet analizi, sistemler üzerindeki güvenlik açıklarının belirlenmesi için gözden geçirilme süreci olarak tanımlanmaktadır. Sızma testleri, teknik olarak saldırganların istismar etmek için yararlanabileceği zafiyetleri ve açıklıkları bulmak amacıyla “içeriden” veya “dışarıdan” detaylı bir şekilde bilgi varlıklarının analiz edilmesi ve incelenmesidir (Shrestha, 2012). Sızma testleri ile güvenlik kusurları, zafiyetler ve ihlaller tespit edilerek kurumların mevcut güvenlik durumu belirlenmektedir. Testler zayıf noktalara yönelik doğru güvenlik yatırımlarının yapılmasına imkân sağlamaktadır. Sızma testleri ile kritik sistemler üzerindeki yanlış yapılanmalar bulunmakta, IEC/ISO 27001, PCI DSS, COBIT vb. gibi bilgi güvenliği sertifikaları ve politikalarının gereksinimleri test edilmektedir (Gülmüş, 2011).

2.6.5.1. Test Kılavuzları

Sızma testi için, OSSTMM, OWASP, ISSAF, NIST ve PTES olmak üzere kabul görmüş uluslararası test kılavuzları bulunmaktadır. Bunlardan; OSSTMM (The Open Source Security Testing Methodology Manual) kılavuzu, uluslararası kabul görmüş açık kaynaklı güvenlik test metodoloji kılavuzudur. Gerçek güvenlik doğrulaması için tasarlanmış olan bu kılavuz, her denetim türüne uygulanabilir testler, etik saldırılar, güvenlik değerlendirmeleri, güvenlik açığı değerlendirilmeleri, kırmızı takım vb. gibi detaylar içermektedir (Herzog, 2020). OSSTMM, fiziksel güvenlik, kablosuz güvenlik, telekomünikasyon ve veri ağları testlerini, uyum yönetmeliği, STAR ile raporlama bölümlerini içeren bir kılavuzdur (Şahinaslan, 2013).

OWASP (Open Web Application Security Project), web uygulama açıklıkları için alınabilecek önlem ve iyileştirmeler konusunda rehberlik hizmeti veren test kılavuzudur. Uygulama güvenliği konusunda yazılım araçları ve bilgi tabanlı belgeler sunmaktadır. ISSAF (Information Systems Security Assessment Framework), OWASP gibi aktif bir topluluk değildir fakat kapsamlı sızma testi kaynağıdır. ISSAF (Information System Security Assessment Framework), kaynak kod denetimi, sosyal mühendislik, kayıt izleme ve denetim, proje yönetimi, teknik kontrol, risk değerlendirme metodolojisi, şifre güvenliği,

şifre kırma stratejileri, güvenlik duvarı, anti virüs, kablosuz güvenlik, saldırı tespit sistemi ve VPN güvenlik değerlendirme, sızma test laboratuvarı tasarımı vb. benzeri alanları kapsamaktadır (Şahinaslan, 2013).

NIST, ABD ekonomisini ve kamu refahını destekleyen bir kılavuzdur. Ulusal Standartlar ve Teknoloji Enstitüsü tarafından yayınlanan NIST SP800- 115 (Bilgi Güvenliği Test ve Değerlendirme Teknik Kılavuzu), teknik anlamda bilgi güvenliğini test ve yöntemlerini planlama, yürütme, analiz stratejileri geliştirme, gözden geçirme teknikleri, güvenlik açıklığı değerlendirmeleri gibi konularında kurumlara yardımcı olacak önemli referans kaynaklarından (Shrestha, 2012).

PTES (Penetration Testing Execution Standard), öz sözleşme, istihbarat toplama, tehdit modelleme, zafiyet analizi, istismar süreci, sömürme ve raporlama gibi 7 ana bölümden oluşan açık kaynak proje sızma testi yürütmek için hazırlanmış bir rehberdir (PTES, 2020).

2.6.5.2. Sızma Testi Türleri

Sızma testini yapmadan / yaptırmadan testin türüne karar verilmelidir. Hedef sistem hakkındaki bilginin çeşitliliğine göre sızma testleri siyah kutu, beyaz kutu ve gri kutu testleri olmak üzere üçe ayrılmaktadır (Crest, 2017).

Siyah kutu testinde testi gerçekleştirecek olan kişiler hedef sistem hakkında önceden herhangi bir bilgiye sahip değildirler. Kara kutu testine uzaktan penetrasyon testide denilmektedir. Testi gerçekleştiren kişi güvenlik açıklıklarını ortaya çıkarabilmek için saldırganların kullandığı tekniklere benzer şekilde yöntemler kullanmaktadır (Poston, 2020).

Beyaz Kutu testinde, ağ hakkında gereken bilgiler verilerek içeriden bir kişinin sistemdeki açıkları kullanması sonucunda nelerin yapılabileceği tespit edilmektedir. Teste tabi tutulacak IP aralıkları, ağ topolojisi, sunucular, servisler, sunucu üzerinde tanımlı kullanıcı adı ve parolaları vb. gibi bilgiler test yapacak kişiye verilmektedir. İç tehdit aktörlerinin (çalışan, emekli, işten ayrılmış vb.) sahip oldukları şifre, parola, ağ yapısı gibi bilgileri ile kurumu hedef alması durumunda neden olabilecekleri zararın tespit edilmesi için beyaz kutu testleri gerçekleştirilmektedir (Adır, 2019).

Gri kutu sızma testleri, beyaz kutu sızma testleri ile siyah kutu sızma testleri arasında yer alan bir sızma metodudur. Beyaz kutu ve siyah kutu test türleri birlikte kullanıldığında daha güçlü bir bakış açısı sağlamaktadır. Testi gerçekleştirenlerin kamuya açık bilgileri daha hızlı elde etmeleri için tercih edilen bir yöntemdir. Testi gerçekleştirecek olan kişi sistem hakkında bilgilendirilir fakat bu bilgi detaylı değil yüzeyseldir (Appiah, 2014).

2.6.5.3. Sızma Testi Aşamaları

Sızma testini bir standarda kavuşturmak için 2010 yılında oluşturulan PTES standardında sızma testleri yedi (7) ana aşama olarak belirlenmiştir (PTES, 2020):

1) Katılım Öncesi Etkileşim (Pre-engagement Interactions)

Teste tabi tutulacak sızma testi türü, IP aralıkları, sistemlerin tipi gibi detaylar belirlenmektedir. İşin kapsamı, testin türü, testin gerçekleştirileceği sistemlere ait IP, domain vb. gibi bilgiler, test tarihi ve saati gibi bilgilerin belirlenmesi gerekmektedir.

2) İstihbarat Toplama (Intelligence Gathering)

Hedef sistem hakkında domain, IP aralıkları, kullanıcı profilleri, domain ve subdomain alan adları, servisler, ağ yapısı gibi bilgiler için web üzerinden bilgi toplanmaktadır. Beyaz kutu testlerinde bilgi toplamaya ihtiyaç duyulmamaktadır çünkü gerekli olan tüm bilgiler güvenlik uzmanına verilmektedir. Aktif ve pasif bilgi toplama işlemleri ile hedef sistem hakkında detaylı bilgilere ulaşılmaktadır. Pasif bilgi toplama işleminde, teste tabi tutulan kurum hakkında internet üzerinde yer alan bilgilere erişilmeye çalışılmaktadır. Bu işlem gerçekleştirilirken herhangi bir sisteme veya sunucuya ulaşılmasına gerek yoktur.

Aktif bilgi toplama işleminde ise, teste tabi tutulan kuruma ait IP adresleri elde edilebilmektedir. Özel metotlar ve araçlar kullanılarak IP adresleri üzerinden çeşitli bilgi elde edilebilmektedir.

3) Tehdit Modelleme

Ağ ve sistem alt yapısındaki cihazların açık portlarının ve açık servislerinin tespit edilmesi için yapılan bilgi toplama ve tarama aşamasıdır. Bazı kaynaklarda “Ağ Haritalama” olarak ta ifade edilmektedir. VPN, firewall, IPS cihazlarının belirlenmesi, işletim sistemlerinin

belirlenmesi, versiyonlarının belirlenmesi ve ağ haritasının çıkarılması gibi işlemleri kapsamaktadır.

4) Zafiyet Analizi (Vulnerability Analysis)

Çeşitli zafiyet tarama araçları veya manuel olarak kritik sistemler üzerindeki güvenlik açıklıklarının ortaya çıkarılması aşamasıdır. Bu süreçte hedef sisteme zarar vermeyecek taramalar gerçekleştirilmektedir.

5) İstismar (Exploitation)

Penetrasyon sürecidir. Çeşitli metot ve zafiyet tarama araçları ile elde edilen güvenlik açıklıklarının istismar edilmesi sürecidir. Açıklık için uygun tarama aracı yok ise sıfırdan Exploit yazılmaktadır.

6) İstismar Sonrası (Post Exploitation)

Açıklıklar istismar edilerek sistem üzerinde bir şekilde yetkisiz erişim hakkı elde edilmektedir. Daha sonra sızılan sistem üzerinde kalıcı hale gelme ve yetki yükseltme gibi işlemler gerçekleştirilmektedir. Yetki yükseltme işlemi basit bir ifadeyle, standart bir kullanıcı hesabının root, administrator gibi tam yetkili bir kullanıcı moduna yükseltilmesi işlemidir. Bunun için çeşitli exploit denemeleri yapılmaktadır.

7) Raporlama (Reporting)

Yönetici raporu, kritik güvenlik açıklıkları ve alınması gereken tedbirler konusunda tavsiyeleri içeren dokümanlardır. Raporda, test ekibi, kontrol eden kişi, testin gerçekleştirildiği erişim noktaları, testin türü ve test işlemleri, risk seviyelerine göre tespit edilen açıklıklar ve alınması gereken önlemleri içeren bölümler yer almaktadır. Doküman şifreli bir şekilde kuruma teslim edilmektedir.

2.7. Güncel Siber Güvenlik Vakaları ve Siber Güvenlik İstatistikleri

Bu bölümde, özellikle son yıllarda gerçekleştirilmiş olan siber saldırılar ve siber güvenliğe dair istatistiki bilgiler verilecektir. Bununla amaçlanan; gerçekleşen siber saldırılara ilişkin fikir edinmek ve sızmaların nasıl ve nerden kaynaklandığı sorularına cevap aramak, gelecekte izlenecek olan siber güvenlik politikalarının oluşturulması zemin hazırlanmaktadır.

Son yıllarda meydana gelen siber güvenlik olayları sonucu ortaya çıkan istatistiki veriler ve tahminler aşağıda derlenmiştir:

1. Dünya genelinde işletmelerin %62'si 2018 yılında ortalama ve sosyal mühendislik saldırıları yaşamıştır (Cybint Solutions, 2019).
2. Dünya çapında yapılan araştırmaya göre işletme yöneticilerinin %68'i siber güvenlik risklerinin yıllar içerisinde hızlı bir şekilde arttığını düşünmektedir (Accenture, 2019).
3. Global ölçekte yapılan araştırmaya göre ortalama olarak işletmelerdeki klasörlerin sadece %5'i gerçek anlamda korunmaktadır (Varonis, 2019).
4. Dünya genelinde 2019 yılının ilk 6 ayında 4,1 milyar veri ihlali girişimi kayıtlara geçmiştir (Risk Based, 2019).
5. 2019 yılında; ihlallerin %71'i finansal sebeplerle, %25'i ise siber casusluk nedeniyle gerçekleştirilmiştir (Verizon, 2019).
6. Dünya genelinde siber güvenlik harcamalarının 2022'de 133,7 milyar dolara ulaşacağı tahmin edilmektedir (Gartner, 2018).
7. 1 Ocak 2005 – 31 Mart 2020 tarihleri arasında ABD'de faaliyet gösteren işletmeler yönelik başarıya ulaşan 11,256 siber saldırı bulunmaktadır (ID Theft Resource Center, 2020).
8. 2020 yılının sonuna kadar Dünya çapında insanlar ve makineler tarafından kullanılan tahmini şifre sayısının 300 milyarı aşacağı tahmin edilmektedir (Cybersecurity Media, 2020).
9. Dünya genelinde faaliyet gösteren kurumsal işletmelerin %83'ünün 2020 yılı sonuna kadar faaliyetlerini ve veri tabanlarını bulut bilişime entegre etmesi beklenmektedir (Forbes, 2018).

10. 2020 yılı itibariyle bilgisayar korsanları her 39 saniyede bir, günde ortalama 2.244 kez saldırı gerçekleştirmektedir (Maryland Üniversitesi, 2020).
11. 2019 yılı itibariyle bir siber saldırının tespit edilmesi ortalama olarak 206 günü bulmaktadır. Bir veri ihlalinin ortalama yaşam süresi (ihlalin başlangıcından kontrol altına alınana kadar geçen süre) 314 gündür (IBM, 2019).
12. 2013 yılında gerçekleşen ve 3 milyar Yahoo kullanıcısının hesabının ele geçirilmesi ile sonuçlanan saldırı tarihin en büyük siber saldırılarından biri olarak kabul edilmektedir (NY Times, 2017).
13. 2016 yılında gerçekleştirilen siber saldırıyla UBER firmasına ait 57 milyon müşteri ve şoföre ait bilgi çalınmıştır. İşletme, çalınan verileri silmeleri ve ihlali gizlemeleri için bilgisayar korsanlarına fidye ödemiştir. Bu durum ortaya çıkınca da firma mahkemelik olmuştur (Bloomberg, 2017).
14. 2017 yılında 147,9 milyon tüketici Equifax'a gerçekleştirilen veri ihlalinin etkilenmiştir ve saldırı işletmeye toplamda 4 milyar dolara mal olmuştur (Equifax, 2017).
15. 2018 yılında gerçekleşen veri ihlali ile MyFitnessPal uygulamasını kullanan 150 milyon kullanıcının kişisel verileri çalınmıştır (Under Armor, 2018).
16. 2019 yılı itibariyle zararlı yazılımların %94'ü e-posta aracılığı ile yayılmaktadır (Verizon, 2019).
17. 2018 yılında veri ihlallerinin %11 işletme içi kaynaklı iken 2019 yılında bu oran %34'e yükselmiştir (Verizon, 2019).
18. İşletmelerin %51'i 2018'de hizmet dışı bırakma saldırıları yaşamıştır (Cybint Solutions, 2019).
19. En az 150 ülkede 100.000 kişi ve 400.000'den fazla makine Wannacry virüsünden etkilenmiştir. Virüsün Dünya ekonomisine zararı yaklaşık 4 milyar dolardır (Technology Inquirer, 2017).
20. Nesnelerin İnterneti cihazları ayda yaklaşık olarak ortalama 5.200 saldırıya maruz kalmaktadır (Symantec, 2019).
21. Günümüzde işletmelere yapılan fidye yazılımı saldırısının ortalama maliyeti 133.000 doları bulmaktadır (SafeAtLast, 2020).

22. 2018 yılında günde ortalama 10.573 kötü amaçlı mobil uygulama engellenmiştir. Her 36 mobil cihazdan 1'inde yüksek riskli mobil uygulamalar bulunmaktadır (Symantec, 2019).
23. İşletmelerin %69' uyuym harcamalarını çok maliyetli olarak tanımlamaktadır (CSO Online, 2020).
24. Dünya genelinde yapılan araştırmaya göre; işletmelerin %53'ünde her çalışanın erişimine açık 1000'den fazla hassas bilgiler içeren dosya bulunmaktadır. İşletmelerin %22'sinde ise tüm çalışanların her dosyaya erişim hakkı bulunmaktadır (Varonis, 2020).
25. İşletmeler, AB Genel Veri Koruma Tüzüğü (General Data Protection Regulation- GDPR) uyumluluk gereksinimlerini karşılamak için ortalama 3 milyon dolar harcamışlardır (EY & IAPP, 2018).
26. Google 2019 yılında GDPR yükümlülüklerini ihlal ettiği gerekçesi ile 57 milyon dolar cezaya çarptırılmıştır (TechCrunch, 2019).
27. 2019 yılında siber saldırı kurbanı olan işletmelerin %43'ü KOBİ'lerdir. Ayrıca saldırıların %16'sı kamu kurum ve kuruluşlarına; %15'i Sağlık sektöründe ve %10'u finans sektöründe faaliyet gösteren işletmelere gerçekleştirilmiştir (Verizon, 2019).
28. 2019 yılında siber saldırılar dolayısıyla sağlık sektörünün kaybı yaklaşık 25 milyar dolar olarak tahmin edilmektedir (SafeAtLast, 2020).
29. Fidyeye yazılımları kullanılarak en fazla saldırıya uğrayan sektör sağlık sektörüdür. Saldırıların 2020'nin sonuna kadar dört katına çıkması beklenmektedir (CSO Online, 2020).
30. Finans sektöründe faaliyet gösteren her bir kurumsal işletme sadece 2018 yılında siber saldırılar için ortalama 18 milyon dolar harcamıştır (Accenture, 2019).
31. Çalınan her bir kayıt başına ortalama maliyet yaklaşık 150 dolardır. Sağlık sektöründe bu tutar kayıt başına yaklaşık 450 dolardır (IBM, 2019).
32. Siber suçlarla ilgili zararın 2021 yılında, 6 trilyon dolara ulaşacağı tahmin edilmektedir (Cybersecurity Ventures, 2018).
33. Global ölçekte yapılan araştırmaya göre işverenlerin %82'si siber güvenlik konusunda işletmelerinin yetersiz olduğunu düşünmektedir. Ayrıca işverenlerin

%61'i siber güvenlik ile alakalı işlere başvuran adayların mesleki donanım açısından yetersiz olduğunu düşünmektedir (ISSA, 2017).

34. Günümüzde siber güvenlik uzmanlarının işsizlik oranı %0'dır ve bu sayının 2021 yılında aynı kalması beklenmektedir (CSO Online, 2020).
35. 2021 yılına kadar, dünya genelinde büyük şirketlerin tamamına yakınının bir bilgi güvenliği başkanı (Chief Information Security-CISO) pozisyonuna sahip olacağı tahmin edilmektedir (Cybersecurity Ventures, 2018).

Yukarıda bahsi geçen vak'alar ve istatistiki bilgiler, işletmeler açısından bilgi güvenliği ve günümüzün dijital dünyasında siber güvenliğin ne derece önemli olduğunu kanıtlar niteliktedir. Günümüz dünyasında fiziksel güvenlik kadar siber güvenlik uygulamaları da işletmeler açısından büyük önem taşımaktadır. İşletmelerde bilgi güvenliği ve siber güvenliğe dair uyumluluğun sağlanması, bilgi güvenliği ve siber güvenlik yönetişimin işletmelerin odak noktası olması çağımızın en büyük gerekliliğidir. Ayrıca maliyeti ne olursa olsun gerekli altyapı yatırımlarının yapılması, sistemlerin kurulması, yetkin ve tecrübeli BT personellerinin çalıştırılması da bir diğer önemli noktadır. Tüm bunlara ek olarak süreç işletmelerin faaliyetlerinin, kontrol ortamının ve varlıklarının her türlü zarar ve saldırıdan korunmasını içerdiğinden iç denetçilere de bu süreçte önemli görevler düşmektedir. İşletme yönetimi, BT personeli ve iç denetim biriminin bu süreçte iş birliği içerisinde koordineli bir şekilde çalışması risk ve tehditlere karşı işletmelerin en etkili silahı olacaktır.

ÜÇÜNCÜ BÖLÜM

İŞLETMELERDE SİBER GÜVENLİĞİN SAĞLANMASINDA İÇ DENETİMİN ÖNEMİ

3.1. Siber Güvenliğin İşletmeler İçin Önemi

İşletmeler, siber güvenlik vakaları ve bu vakalar sonucu ortaya çıkan zarar ve kayıpları birçok faktörden ötürü açıklamakta güçlük çekmektedirler. Bu faktörlerin başında, rekabet, itibar ve müşteri kaybı gelmektedir (Hoffer ve Straub, 1989: 35-43; Panko, 2009, Richardson, 2011).

Ancak detaylı olarak irdelendiğinde kayıp ve zararların ekonomik boyutları kadar insani, toplumsal ulusal ve küresel boyutları da bulunmaktadır. Çalışmada açıklanan siber tehditler ve bunların yarattığı zararların boyutu düşünüldüğünde bu konunun önemi de daha iyi anlaşılacaktır.

Bireysel, kurumsal veya ulusal bilgi kaynakları günümüzde özellikle iş dünyasında en önemli unsurlar arasında görülmektedir. Bu nedenle kişilerin işletmelerin, diğer kuruluşların ve ulusların bilgi varlıklarının güvenliğinin sağlanması gerekmektedir. Bu durumun işletmeler açısından etik, hukuki insani ve ekonomik pek çok sebebi bulunmaktadır. Bilgi teknolojilerinin gelişmesine paralel bilgi varlıklarının güvenliği siber güvenlik uygulamalarını ön plana çıkarmıştır.

Bilgi toplumuna evirilen Dünya'mızda, bilgi teknolojisini faaliyetlerini devam ettirmek için kullanan işletmelerde çalışanların ve yöneticilerin; siber güvenliğe ilişkin farkındalığa sahip olmaları, konu ile ilgili önlemleri almaları ve uygulamaları bir zaruriyet olarak karşımıza çıkmaktadır. Bu durum en çok da işletmelerin varlıklarını ve faaliyetlerini itibarlarını korumak için başka bir ifade ile hayatta kalabilmeleri için gereklidir. Gerekli önem verilmediği takdirde bu durum, işletmelerin kurumsal imajlarının zedelenmesine, paydaşların özellikle de müşterilerin güveninin sarsılmasına yol açacaktır. Bunlara ek olarak, iş gücü ve zaman kaybının oluşması, işletmenin faaliyetlerini ve hali hazırda

kurulu sistemlerini eski haline getirmenin maliyetli olması, önemli verilerin, ticari sırların veya diğer bilgilerin kaybı ciddi sorunları ortaya çıkaracaktır.

Günümüzde verilerin korunması konusu hukuki açıdan da önemli sonuçlar doğurmaktadır. Yürürlükteki yasa ve yönetmeliklerin uygulanması, yasal yükümlülüklerin yerine getirilmesi işletmeler açısından önemli bir zorunluluktur.

Siber ortamda bulunan işletme bilgilerinin; gizlilik, bütünlük ve erişilebilirliğinin sağlanması, işletmelerin rekabet güçlerini, ticari imajlarını korumaları ve sürdürmeleri açısından bir gereklilik haline gelmiştir.

Günümüzde işletme varlıklarını korumak için sadece, hile yolsuzluk, casusluk, sabotaj, doğal afetler vb. tehdit ve tehlikelere karşı koymak yeterli olmamaktadır. Virüs, casus ve kötü yazılım, bilgisayar korsanları gibi siber tehditlere karşı önlem almak fiziksel önlemlerle eş değer öneme sahiptir. Bu siber saldırıları ve tehditleri ortadan kaldırmak siber güvenliği sağlamakla mümkündür.

Bilgi teknolojileri ve bu teknolojilerin yarattığı uygulamalara bağımlılık, işletmeleri güvenlik açısından daha riskli hale getirmektedir. Bilginin üretim, transfer, depolama ve erişim süreçlerinin karmaşık hale gelmesi; denetlenmesini de zorlaştırmaktadır. Ayrıca, yeni teknoloji, altyapı, kullanılan algoritma, uygulama ve hizmetlerin kapsamı sürekli değişmekte ve gelişmektedir. Bu değişimler sonucunda yeni saldırılar ve tehditler ortaya çıkmaktadır. Tüm bunların sonucu meydana gelebilecek tehdit ve tehlikeleri en aza indirmek için siber güvenliğin sağlanması gerekmektedir.

Mevcut siber varlıklarının güvenliğinin sağlanması; işletmelerin risklerinin ve kayıplarının minimuma indirilmesi, yeni teknolojilerin geliştirilmesi, yeni bilgilerin üretilmesi, fırsatların yatırımlara dönüşmesi ve sonuçta sağlıklı bir siber güvenlik ekosistemi ve ekonomisinin oluşturulması için önemlidir.

Siber uzay bünyesinde; e-ticaret, bankacılık, enerji üretimi ve dağıtımı, akıllı sistemler, mobil operatörler, haberleşme, hava trafik kontrol merkezleri, sağlık, bilgisayar ve iletişim sistemleri ve bunlar gibi birçok sektörün kritik altyapılarını, ağlarını ve sistemlerini barındırmaktadır. Bu sebeple makro düzeyde düşüldüğünde siber uzaya

yapılacak saldırıların, işletmelerin varlıklarına ve faaliyetlerine zarar vermesinin yanı sıra toplumsal, ulusal hatta günümüz dünyasında küresel ölçekte etkiler bırakması kaçınılmazdır.

Çalışmada daha önce açıklanan Yapay Zekâ, Nesnelerin İnterneti, Büyük Veri, Blok Zinciri ve Bulut Bilişim vb. uygulamaların yaygınlaşması, bu uygulamaların güçlü yanları kadar riskli yanlarının da mevcut olması, siber güvenlik ve savunmaya olan ihtiyacı daha da pekiştirmektedir.

Güvenlik faaliyetlerinin işletmelerin operasyonlarını ve varlıklarını sürdürdükleri süre zarfında süreklilik göstermesi hayati önem taşımaktadır. Bu sürekliliğin siber güvenlik açısından doğru bir şekilde devam ettirilmesi, işletmelerin bilgi teknolojileri ve iç denetim departmanları başta olmak üzere tüm çalışanları ve yöneticileri ile birlikte hareket etmeleri; gerekli farkındalığa sahip olmaları, süreçleri, sistemleri ve iç kontrol ortamını dikkatli bir şekilde izlemeleri ve gerekli adımları zamanında atılmalarına bağlıdır. Özetle, konuya ilişkin farkındalığın ve ihtiyatlılığın işletme kültüründe yer edinmesi, olaylara müdahalenin zamanında yapılması; kaynak israfını önleyeceği gibi, verimliliği ve kaliteyi arttıracak ve daha etkin ve güvenilir bir siber güvenlik sistemi tesis edilecektir.

Günümüzde işletmeler, bilgisayarlara, ağlara, programlara, uygulamalara, sosyal medyaya ve verilere artan bağımlılıkları nedeniyle siber tehditlere karşı daha savunmasız hale gelmektedir. Güvenlik ihlalleri, işletmeleri ve paydaşlarını finansal açıdan ve itibar açısından olumsuz etkileyebilmektedir. İşletme dışındaki kullanıcıların bilgilere erişebilirliği bilgi teknolojileri risklerini arttırmaktadır. Özellikle işletmelerin hali hazırda bilgi sistemlerine güvenmesi ve gelişen yeni teknolojiler göz önüne alındığında, geleneksel bilgi teknolojileri süreçleri ve uygulama kontrolleri siber güvenlik konusunda güvence sağlamak için yetersiz kalmaktadır.

Siber güvenlik, işletmelerin bilgi varlıklarını (bilgisayarlar, ağlar, programlar ve veriler) yetkisiz erişimden korumak için tasarlanmış teknolojileri, süreçleri ve uygulamaları ifade etmektedir. Siber saldırıların sıklığı ve şiddeti artarken, gelişmiş siber güvenlik risk yönetimine olan ihtiyaç giderek artmaktadır (IIA, 2016:3).

Siber güvenlik, bir işletmenin operasyonların etkinliği ve verimliliği, iç ve dış raporlamanın güvenilirliği ve geçerli yasa ve yönetmeliklere uyumla ilgili hedeflerini destekleyen sistemlerle ilgilidir. Bir işletme, bilginin bütünlüğünü, gizliliğini ve kullanılabilirliğini korumak için genellikle işletme genelinde siber güvenlik kontrolleri tasarlamakta ve uygulamaktadır (IIA, 2016:5).

Siber saldırılar, finansal dolandırıcılık, bilgi hırsızlığı veya bilginin kötüye kullanımı, aktivist nedenler, bilgisayar sistemlerini çalışmaz hale getirmek ve bir hükümetin veya işletmenin kritik altyapısını ve iş süreçlerini bozmak gibi sebeplerle gerçekleştirilmektedir. Bir işletme ile ilgili siber tehditleri anlamak için, hangi bilgilerin saldırganlar için değerli olacağını veya olası bir müdahalede işletme için bir kesintiye neden olacağını belirlemek önemlidir. Ayrıca, başkaları tarafından edinilmiş veya kamuya açıklanmışsa hangi bilgilerin işletmede finansal zarara, rekabet kaybına veya işletme itibarına zarar verebileceğini belirlemek de önemlidir. Dikkate alınacak bilgi türleri aşağıdakileri içermektedir (IIA, 2016:5):

- Finansal veriler,
- Müşteri ve çalışan verileri,
- Fikri mülkiyet,
- Tedarik zinciri,
- Ürün kalitesi ve güvenliği,
- Sözleşme şartları ve fiyatlandırma,
- Stratejik planlama.

İşletmelerin faaliyet gösterdikleri sektör, siber tehditleri belirlerken önemli bir bağlam oluşturmaktadır. Örneğin, perakendeciler müşteri verilerini korumaya ve müşteri hizmetlerinin kesintiye uğramamasını sağlamaya odaklanmaktadır. Fikri mülkiyet, araştırma ve geliştirmeye odaklanan işletmeler için önemli bir endişe kaynağı olabilmektedir. Üretim yapan işletmeler, üretim ve tedarik zinciri sistemlerinin güvenilirliği ve verimliliği ile ürünlerin kalitesi ve güvenliğine önem vermektedirler. Hizmet işletmelerinin odağı ise, sözleşmelerde ve finansal maliyetlendirme modellerinde yer alan hassas ticari bilgileri korumaktır (IIA, 2016:5).

Siber güvenlikte asıl amaç; işletmelerin bilgi varlıklarının güvenliğinin makul bir seviyede sağlanmasıdır. Bu bağlamda siber güvenliği sağlanmak için işletmelerin siber risklerinin tespiti ve yönetimi önemli bir unsurdur. Bu sebeple, risklerin tespit ve minimize edilmesi için iyi bir risk yönetimi yapılmalı, mevcut teknikler, teknolojiler, politikalar, standartlar ve çözümler uygulanarak siber güvenlik kapsamında çalışmalar yürütülmelidir. Siber güvenlikte aşağıdaki unsurlar yer almaktadır (Sağıroğlu, 2018: 44):

- İşletme genelinde siber güvenlik politikası oluşturulmalı ve uygulanmalıdır.
- Maliyetleri azaltmak adına gereği kadar koruma prensibi uygulanmalıdır.
- İyi bir siber risk analizi ve yönetimi gerçekleştirilmelidir.
- Bilgi sistemlerine belirli periyotlarla hataları, eksiklikleri, açıklıkları ve zafiyetleri gidermek amacıyla testler (sızma testleri) yapılmalıdır.
- Bilgi sistemlerini kullanan kullanıcıların erişimleri kısıtlanmalı ve denetlenmelidir.
- Siber güvenlik ile ilgili standartlar ve düzenlemeler güncel şekilde uygulanmalı ve takip edilmelidir.
- Siber tehditler ve tehlikeler güncel şekilde takip edilmeli, önlemeye yönelik çalışmalar yapılmalı ve bu amaç doğrultusunda mekanizma ve yapılar kurularak işletilmelidir.
- Güvenli bileşenleri tanımlama ve güvenlik gerektiren bileşenlerin sayıları en aza indirme temel amaç olmalıdır.
- Siber güvenlik sistemleri ile ilgilenen uzmanların kendilerini geliştirmeleri konusunda fırsat verilmelidir.

3.2. İşletmelerde Bilgi Teknolojileri ve Siber Güvenlik Yönetiřimi

Bilgi teknolojileri yönetiřimi (Information Technology Governance), bilgi teknolojileri ve sistemleri kullanan işletmelerin bu kaynaklarının kontrol sürecidir (Hunton, 2004, 2). İşletme yönetimi ve paydařlar kurumsal yönetiřimin iřleyiřinden sorumlu oldukları kadar bilgi teknolojileri ve siber güvenlik yönetiřiminden de sorumludurlar. Kurumsal yönetiřim, kurum stratejisini kurmayı ve uygulamayı saęlayan, kurumun amaçlarını verimli bir řekilde gerekleřtirmesini hedefleyen ve risklerin yönetimini

gerçekleştiren bir süreçtir. Bilgi teknolojileri yönetişimi, organizasyonun bilgi ve iletişime bağımlı olması, bilgi teknolojileri yatırımlarının, bilgi teknolojilerinin stratejik fırsatlar yaratması ve bilgi teknolojisi riskleri seviyesinden dolayı önem kazanan kurumsal yönetişimin alt dallarından biridir (Hunton, 2004: 2).

Bilgi teknolojileri, kamu ve özel sektör kuruluşlarının faaliyetlerini güvenilir, doğru, hızlı bir yürütmek için kullandıkları önemli bir kaynaktır. Ancak, işletmenin hedefleriyle uyumsuz BT kullanımı, iyi yönetilemeyen BT projeleri, yanlış BT yatırımları, siber saldırılar ve tehditler bilgi teknolojileri kaynaklı muhtemel risklerdir ve bu riskler büyük maddi ve manevi kayıplara neden olabilmektedir. Geçmişte, siber risklerin öneminin farkında olmayan işletme yöneticilerinin, bilgi teknolojilerinin ve siber güvenliğin iş süreçlerindeki öneminin farkında olmayışları, yapılacak yatırımları maliyetli bulmaları ve bunları teknik bir konu olarak algılamaları, BT departmanlarının yönetim düzeyinde güçlü destek bulamamalarına neden olmuştur. Ancak zaman içerisinde yaşanan saldırılar ve ihlaller, işletme yönetimlerinin siber saldırı, tehdit ve risklerle sık sık karşılaşmaları, bilgi teknolojileri ve siber güvenlik yönetişimine önem vermelerine sebep olmuştur (Ponemon Institute Research Report, 2013).

Bilgi Sistemleri Denetim ve Kontrol Birliği (Information Systems Audit and Control Association – ISACA) BT yönetişimini; “kurumsal yönetişimin ayrılmaz bir parçası olan ve BT kaynaklarının, kurumsal strateji ve hedefleri desteklemesini sağlayacak örgütsel yapıları, süreçleri ve liderlik unsurlarının tamamını içeren bütüncül bir anlayışı” şeklinde tanımlamaktadır. (ISACA, 2009). BT yönetişimi, geleceğe yönelik yapılacak tüm BT geliştirme süreçlerinin, ne şekilde kimler tarafından yönetileceğine dair BT stratejisinin üst yönetimin tarafından planlanması ve uygulanmasıdır (Bilgin, 2016: 32).

Stratejik BT altyapısının kurulması, çoğu işletmenin iş yapma biçiminde köklü bir değişikliklere neden olmaktadır. Bu nedenle işletmelerin BT yönetişimi sürecinin başarıya ulaşması üst yönetimin süreci iyi şekilde yönetmesine bağlıdır. Teknolojik gelişmeler kurumsal kaynakları tehdit etmeye devam ettikçe, işletme yöneticilerinin de teknik konular hakkında kendi bilgilerini geliştirmeleri gerekmektedir. Buna ek iyi bir BT yönetişimi için işletmede konusunda uzman BT ve iç denetim çalışanlarının yer alması çok önemlidir. Çünkü işletmeler bilgi teknolojisi yönetişimi amaçlarına, bilgi varlıklarını yönlendirmek ve

kontrol etmek için kullanılabilecek kapsamlı bir rasyonel prosedürler ve ilişkiler yapısı inşa ederek ulaşılabilmektedir. Bu prosedürlerin tasarlanması konusunda işletme yönetimine en çok BT ve iç denetim birimleri destek olmaktadır. Sonuç olarak BT yönetiřimi, řirketin BT kaynakları ile iř stratejisi arasında somut bir baęlantı kurmaktadır ve bunu iřletmenin amalarına deęer katacak řekilde yapmaktadır (Kohnke ve dięerleri, 2016: 29). BT yönetiřiminin amacı, bilgilerin (Kohnke ve dięerleri, 2016: 30):

- Etkili kullanımını,
- Verimli kullanımını,
- Gizlilięini,
- Bütünlüęünü,
- Uygun řekilde daęıtımını,
- Yönetmeliklere uyumunu,
- Sürekli kullanılabilirlięini saęlamaktır.

BT iletiřiminin yukarıda yer alan amaları siber güvenlięi doęrudan BT yönetiřiminin odak noktası haline getirmektedir. İřletme üst yönetimi, siber risk yönetiřimini de içeren BT yönetiřiminin güvenilirlięini ve devamlılıęını saęlamaktan doęrudan sorumludur. İyi yönetiřimin bir parası olarak, yönetim kurulu üyeleri hissedarlarını, alıřanlarını ve paydařlarını siber risklerden kaynaklanabilecek yasal sorunlara karřı korumakla yükümlüdür. Tüm bunlara ek olarak iřletme üst yönetiminin iç denetim faaliyetini; iřletmenin siber güvenlik süreçlerinin etkinlięini arttırmak veya denetlemek için bir araç olarak kullanması BT yönetiřimi ve siber güvenlik yönetiřimi süreçlerinin saęlıklı iřlemesi aısından ok önemlidir (Price, 2018).

Giderek zorlařan bir tehdit ortamında, birok iřletme siber güvenlik yönetiřiminin etkin ve verimli bir řekilde uygulanması mücadele vermektedir. Günümüzde birok iřletme, siber güvenlik yönetiřimi için ařaęıda sayılan beř temel zorlukla mücadele etmektedir (Swinton, 2019):

- Siber Güvenlik Stratejisi ve Hedefleri
- Standartlařtırılmıř İřlemler
- Hukuki Düzenlemeler

- Üst Düzey Liderlik Gözetimi
- Kaynaklar

3.2.1. Siber Güvenlik Stratejisi ve Hedefleri

İyi bir siber güvenlik yönetim programı oluşturmak için işletmenin risk yönetimi politikalarının, stratejisinin ve hedeflerinin açıkça tanımlanması gerekmektedir. İşletme yönetimi işletmenin siber güvenliğe dair strateji ve hedeflerini tanımlamadan önce mevcut risk yönetimi yaklaşımlarını değerlendirmek durumundadır. Siber güvenlik stratejisi, işletmenin genel risk yönetimi yaklaşımını sürdürmesi ve iyileştirmesi için bir yol haritası vazifesi görmektedir. Strateji ve hedefler belirlendikten sonra, işletme genelini kapsayacak bir politika düzeyi belirlenmekte ve uygulanmaktadır (Swinton, 2019). Etkili bir siber güvenlik stratejisi geliştirmenin temel bileşenleri aşağıdaki gibidir (ENISA, 2014):

- Siber güvenlik riskinin kritik iş operasyonları ile olan ilişkisinin açık şekilde tespit edilmesi,
- Organizasyon için stratejik hedefler geliştirilmesi,
- Stratejinin kapsamının tanımlanması,
- Siber güvenlik ihtiyaçlarının belirlenmesi ve hedeflerin geliştirilmesi,
- Temel performans göstergelerinin (Key Performance Indicators-KPI) oluşturulması,
- Kaynak ihtiyaçlarının belirlenmesi,
- Risk iştahının belirlenmesi,
- Sürekli izleme oluşturulması.

3.2.1.1. Standartlaştırılmış İşlemler

Tekrarlanabilir, onaylanmış, standartlaştırılmış süreçler işletmelerin faaliyetlerinin verimli, kaliteli veya tutarlı olmasını doğrudan etkilemektedir. Tutarlılık, işletme genelinde risklere ilişkin ortak bir anlayış ve yönetim yaklaşımı sağlamak için kritik öneme sahiptir. Tekrarlanabilir süreçler oluşturmak, işletmelerin genel siber güvenlik programları için kilit bir rol oynamaktadır. Kısacası, geçici ve tutarsız bir siber güvenlik yönetim programının güvenlik ihlallerinin ve saldırılarının artmasına neden olması olasıdır (Swinton, 2019).

3.2.1.2. Hukuki Düzenlemeler

Siber uzayda siber suçlar, siber saldırılar ve siber güvenlik birbiriyle sıkı sıkıya bağlı kavramlardır. Bütün siber saldırılar siber suç olmazsa bile bütün siber suçlar aynı zamanda siber saldırdır ve her ikisi de siber güvenliği tehdit eden olaylardır. Kabul görmüş ve etkin bir uluslararası mekanizmanın yokluğu nedeniyle, her ülke kendi hukuk ve kültür anlayışı ve teknolojik gelişme düzeyine kısmen cevap verebilecek birtakım düzenlemelere gitmiştir (Akyeşilmen, 2018: 86)

Bu nedenle, her ülkenin siber hukuk ve siber suçlar tanımı ve düzenlemeleri de farklıdır. Siber suçların uluslararası doğası gereği ve uluslararası iş birliğinin zayıf olması nedeniyle bu tür ulusal düzenlemeler genellikle yetersiz kalmaktadır. Küresel bir anlaşmanın yokluğu nedeniyle, siber suç türleri ve uygulanacak yaptırımlar üzerine ortak bir karar verilememiştir. Bu nedenle, her ulusal ya da bölgesel düzenlemede farklı tanımlar, kısmen farklı tür ve kategorileri görmek mümkündür (Akyeşilmen, 2018: 86). İşlemeler ulusal ve uluslararası birçok düzenlemeye uymak zorundadır. Bu durum özellikle uluslararası düzeyde iş yapan işletmelerin faaliyetlerini yavaşlatmakta ve çok sayıda düzenlemeye tabi olmaları nedeniyle siber güvenlik stratejileri ve süreçlerini karmaşık hale getirmekte, maliyetleri arttırmaktadır (European Court of Auditors, 2019)

3.2.1.3. Üst Düzey Liderlik Gözetimi

Siber güvenlik ile ilgili tehditler ve riskler işletmelerin faaliyetlerini ve departmanlarını bütünüyle etkiledikleri için, siber güvenlik programının odağı ve yönü üst yönetim tarafından sürekli olarak gözetilmelidir. Üst düzey liderlik, siber güvenlik uygulamalarını desteklemediği sürece, kuruluşun risk yönetimi çabaları büyük olasılıkla başarısız olması kaçınılmazdır. (Swinton, 2019). İşletme yönetimi tarafından belirlenen siber güvenlik politikası aşağıda yer alan unsurları içermelidir (Swinton, 2019):

- İşletmenin stratejik hedeflerine uygun olmalıdır
- İşletmenin bilgi güvenliği hedeflerini kapsamalıdır.
- Bilgi güvenliği uygulamalarının sürekli olarak iyileştirilmesi amacını taşımalıdır.

3.2.1.4. Kaynaklar

Siber güvenlik sistemlerine yapılan yatırımlar maliyetli olmaları nedeniyle birçok işletme tarafından gerçekleştirilmemektedir. Ancak olası bir siber saldırı durumunda kayıplar yatırımların maliyetlerinin çok çok üstünde gerçekleşmektedir. Bu nedenle, işletme üst yönetimi, işletmenin siber güvenlik stratejisi ve hedefleri ile orantılı olarak temel siber güvenlik yönetişimi ve uyum ihtiyaçlarını karşılamak için yeterli kaynakların mevcut olmasını sağlamalıdır. Kaynaklar, risk düzeyleri için yeterli bilgi ve bilgi sistemlerini güvence altına almak için en yüksek önceliklere tahsis edilmelidir. Kaynak kullanımı, kalifiye personel ve eğitimleri için özel finansman da içermelidir. Ek olarak, kaynaklar, performans göstergelerini yeterince ölçmek ve tekrarlanabilir süreçleri sürdürmek için yeterli araçların tedarik edilmesine izin vermelidir. (Swinton, 2019).

İşletme yönetiminin desteği, etkili BT yönetişiminin ön koşuludur. Siber güvenliği sağlamanın en doğru yolu, yaygın olarak kabul edilen en iyi standartlardan, çerçevelerden ve örnek uygulamalardan yararlanarak en iyi süreçleri ve uygulamaları geliştirmektir. (Kohnke, 2015:11)

3.3. Bilgi teknolojileri, Bilgi Güvenliği ve Siber Güvenlik Standartları

İşletmeler, belirledikleri stratejik hedeflere ulaşmak için onları destekleyen ve yönlendiren bilgi teknolojilerini kullanmaktadır. Kullanılan teknolojiler genel olarak ülkeden ülkeye, sektörden sektöre, hatta işletmeden işletmeye değişiklik göstermektedir. Dolayısı ile işletmelerin BT ve siber risk profili birbirlerinden farklıdır.

Denetim ve kontrol faaliyetleri, büyüklük, kullanılan kaynaklar ve yürütülen denetim ve kontrol yordamları bakımından farklılık gösterdiği için, bu faaliyetlerin yürütülmesinde tutarlı bir çerçeveye ihtiyaç duyulmaktadır. (Weiss ve Solomon, 2016: 74). Bu amaçla bilgi teknolojileri, bilgi güvenliği ve siber güvenlik konularında için birtakım standartlar geliştirilmiştir (Takçı ve ark., 2010: 170).

Standartlar, ürün ya da hizmetlerin kalite, güvenlik, güvenilirlik, verimlilik vb. istenilen özelliklere sahip olmasını sağlamaktadır (Tofan, 2001: 128). Bilgi teknolojileri,

bilgi güvenliği ve siber güvenlikle ilgili standart ve düzenlemeler, işletme içerisindeki bilginin yönetim şekillerini tanımlayan bir dizi belgelenmiş, üzerinde anlaşmaya varılmış politikalar, prosedürler ve süreçlerdir. Bu standartların asıl hedefi, işletmelerin riskleri ile güvenlik zafiyetlerini azaltarak işletme genelinde güveni artırmaktır. Bu amaçla çeşitli sektörler için uluslararası düzeyde kabul görmüş çok sayıda standart ve düzenleme bulunmaktadır. Bu standart ve düzenlemelerden bilgi teknolojileri ve siber güvenlikle alakalı olan ve yaygın yaygın şekilde kullanılanları ISO/IEC 27000 Serisi, COBIT, ITIL ve NIST Siber Güvenlik Çerçevesi gibi standartlar ve düzenlemelerdir (Koç ve ark., 2019: 127).

3.3.1. ISO/IEC 27000 Serisi

İşletmelerin bilgi güvenliği ve özellikle de siber güvenlik konusunda sürekliliği sağlaması için teknik altyapıların ve sistemlerin kurulmasının yanı sıra, teknik olmayan (insan faktörü, yönetsel faktörler vb.) önlemlerin alınması da gerekmektedir. İşletmelerin bilgi güvenliği ve siber güvenlik süreçlerinin devamlılığını sağlamaları için amacıyla Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmaları gerekmektedir. Bu standartlar işletmelerin iş süreçlerini ve varlıklarını fiziki risklerden ve siber güvenlik risklerinden korumaları, önleyici tedbirleri sistematik biçimde işletebilmeleri ve belgelendirilmeleri amacıyla geliştirilmiştir (Şen & Yerlikaya, 2013: 677). Standart ailesi ilk çıktığı yıllarda asıl odak noktası bilgi güvenliği iken, son yıllarda bilgi güvenliği siber güvenlik yakınsaması nedeniyle siber güvenlik konusunu da tamamıyla ilgilendiren bir hal almıştır.

ISO 27000 ailesi bilgi teknolojileri bilgi güvenliği ve siber güvenlik konularını içeren dünya çapında kabul görmüş bir çerçeve sağlamaktadır. 27000'dan başlayarak 27999 arası standartlar bilgi güvenliği standartlarına ayrılmıştır. Bu bölümde ISO 27000 standart ailesi içerisinde yer alan önemli standartlar açıklanacaktır.

3.3.1.1. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi

ISO/IEC 27001 standardı özü itibarıyla işletmelerde bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekli çerçeveyi çizmekte ve kontrol maddelerini belirlemektedir. Bu standartta ortaya konulan maddeler genel olarak hazırlanmıştır ve tür, büyüklük ve doğalarından bağımsız olarak

tüm işletmelerde uygulanabilirler. Standart, işletmelerin bilgi güvenliği konusunda yapması gerekli işlemleri teknik detaya girmeden açıklamaktadır (Gündoğan, 2016: 20).

Bilgi güvenliği yönetim sistemi teknik bir süreçten ziyade bir yönetim sürecidir. Standart, BGYS için, “Planla- Uygula- Kontrol Et- Önlem Al (PUKÖ)” yaklaşımını benimsemiştir. PUKÖ modeli aşamaları aşağıda özetlenmiştir (Şen ve Yerlikaya, 2013: 679):

Planlama: Bilgi güvenliği politikasının oluşturulması, süreçlerin, amaçların, hedeflerin ve prosedürlerin belirlenmesi gerekmektedir. Belirlenecek olan hedefler işletmelerin politika ve hedeflerine uygun olmalıdır. Döngünün periyodik uygulanması sırasında bundan sonraki evrelerde oluşabilecek risk oranlarının düşük olması için önlemlerin önceden planlanması gerekmektedir.

Uygulama: Bilgi güvenlik politikasının, süreçler, prosedürler ve denetimlerin ayrıntılarının oluşturularak işletilmesidir. Bu süreçte ortaya çıkabilecek eksiklikler tespit edilerek belge haline getirilmekte ve iyileştirme yapmak amacıyla kullanılmaktadır.

Kontrol etme: Bilgi güvenlik politikasında alınan önlemlerin ne kadar iyi olduğunun ölçülmesi, performansın değerlendirilmesi, amaçların ve hedeflerin gözden geçirilmesi bu konuda raporların oluşturulması, ilgili sonuçların rapor edilmesidir.

Önlem alma: Bilgi güvenliği yönetim sisteminin, kontrol etme aşamasında ortaya çıkan geribildirimlere dayalı olarak sistemin düzeltilmesi, geliştirilmesi için gerekli tedbirlerin alınmasıdır. İşletmelerde önceki aşamalarda fark edilen eksiklikler, güvenlik risk ve zayıflıkları bu aşamada düzeltilmektedir.

3.3.1.2. ISO/IEC 27002 Bilgi Güvenliği İçin Uygulama Kodu

ISO 27001(2005) standardından sonra hazırlanan 27000 ailesi içindeki ilk standarttır. Bu standart 14 bölümde topladığı konuları, 35 alt kategoriye ayırarak, 114 kontrol maddesiyle sunmaktadır. Bilgi güvenliği yönetimi, insan kaynakları, varlık yönetimi, erişim kontrolü, mobil cihazların güvenliği, ağ güvenliği, yasal gerekliliklere uyum, teknik yapıya uyum, bilgi transferi, iletişim güvenliği, kriptografik kontroller,

sistemin gelişimi ve korunması, fiziksel ve çevresel güvenlik, bilgi güvenliği politikaları ve destekçilerle olan ilişkileri ele alan ve öneriler sunan bir standarttır (Akay, 2014: 41).

3.3.1.3. ISO/IEC 27003 Bilgi Güvenliği Yönetim Sistemi Uygulama Kılavuzu

Bu standart 2017 yılında yayınlanmış tavsiye niteliğinde olan bir standarttır. Bilgi güvenliği yönetim sisteminin başarılı tasarım ve uygulaması için kritik hususlarını kapsamaktadır. BGYS kapsamı, politikası ve tasarımı gibi konuları açıklamaktadır. İşletme analizi, risk değerlendirme ve işleme planlarını yönetme, BGYS projesini uygulama, kabul etme ve onaylama konularını içermektedir (ISO, 2020).

3.3.1.4. ISO/IEC 27005 Bilgi Güvenliği Risk Yönetimi

2018 yılında güncellenen bu standart kapsamında ISO27001 ve ISO27002 no'lu standartlarda belirtilen bilgi güvenliği yönetim sisteminin yönetilmesi, uygulanması, kontrolleri ve etkinliğinin değerlendirmesi sırasında yapılacak ölçümler hakkında tavsiyelere yer verilmektedir. Standart ölçümlerin nasıl yapılacağı ile ilgili kılavuzluk yapmaktadır (ISO, 2020).

3.3.1.5. ISO/IEC 27007 Bilgi Güvenliği, Siber Güvenlik ve Gizlilik Koruması- Bilgi Güvenliği Yönetim Sistemleri Denetimi

2020 yılında güncellenen standart, ISO 19011 (Yönetim Sistemlerini Denetleme Yönergeleri) yer alan rehber ek olarak, bir bilgi güvenliği yönetim sistemi denetim programının yönetilmesi, denetimlerin yapılması ve denetçilerinin yeterliliği hakkında rehberlik sağlamaktadır (ISO, 2020). Bu standart, bir BGYS'nin iç veya bağımsız denetimlerini anlamak, yürütmek veya bir BGYS denetim programını yönetmek isteyenler için yayımlanmıştır.

3.3.1.6. ISO/IEC 27032 Siber Güvenlik İçin Kılavuz

Bu standart 2012 yılında yayımlanmıştır. Siber güvenliğin uygulanabilmesi için rehber niteliğinde olan bir çalışmadır. Siber güvenliğin diğer güvenlik alanları ile olan ilişkilerini ve diğer standartlarla olan bağlantılarını açıklamaktadır. Siber uzayda yer alan

paydaşlar için temel güvenlik uygulamalarını kapsamaktadır. Bu Uluslararası Standart aşağıdaki başlıkları barındırmaktadır:

- Siber güvenliğe genel bakış,
- Siber güvenlik ve diğer güvenlik türleri arasındaki ilişkinin açıklaması,
- Paydaşların tanımı ve siber güvenlikteki rollerinin tanımı,
- Yaygın siber güvenlik sorunlarına yönelik rehberlik ve paydaşların siber güvenlik sorunlarının çözümünde iş birliği yapmalarını sağlayacak bir çerçeve.

3.3.2. COBIT

“Control Objectives for Information and related Technology-COBIT Türkçe literatürde “Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri” olarak isimlendirilmiştir. COBIT BT Yönetimi için en iyi uygulamaları içeren bir rehber olarak ISACA (Information Systems Audit and Control Association-Bilgi Sistemleri Denetim ve Kontrol Birliği ve ITGI (Information Technology Governance Institute-Bilgi Teknolojileri Yönetişimi Enstitüsü) tarafından 1992 yılında geliştirilmiştir (Guldentops & Haes 2002: 25-31). COBIT; ISO standartları, ISACA ve Avrupa Birliği tarafından oluşturulan dokümanlar, COSO, AICPA tarafından yayımlanan iç kontrol ve denetim standartları göz önüne alınarak şekillendirilmiştir (ITGI, 2020).

COBIT’in temel amacı; işletme yönetimine, iç denetçilere ve BT çalışanlarına verimliliği arttırmak için kabul görmüş ölçü, gösterge, süreç ve en iyi uygulamaları sağlamaktır. COBIT sistemin kapsama alanı, işletmenin bilgi işlem teknolojisi ile birlikte tüm işletmedir ve sistem güvenilir finansal raporlamayı, faaliyet etkinliğini, mevzuata uygunluğu, bilgilerin gizliliğini sağlamayı amaçlamaktadır (Dabbaoğlu, 2009: 111).

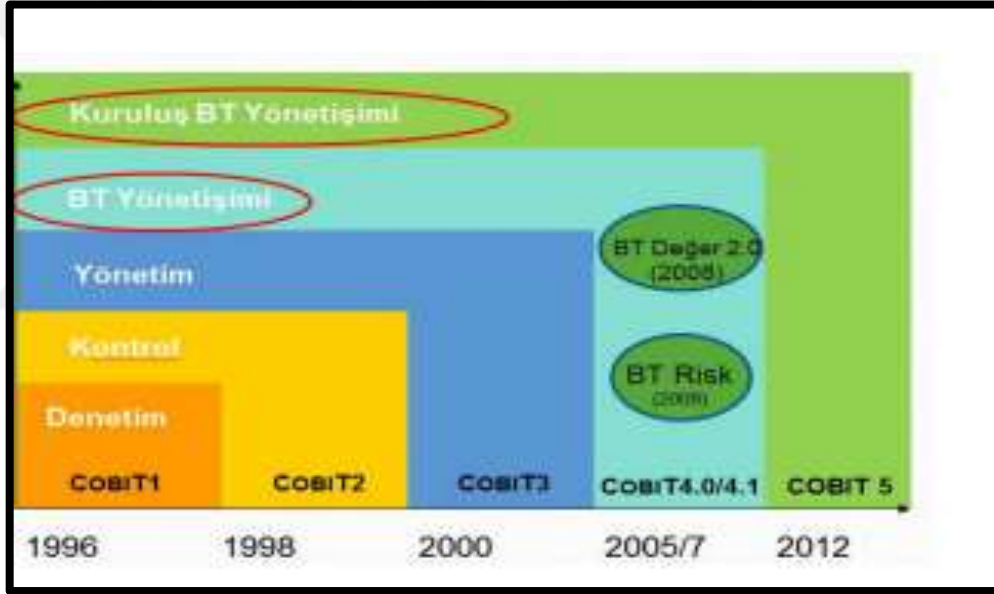
COBIT, kontrol odaklıdır, süreçler ile ilgilenmemektedir. Ayrıca kullanım açısından yalnızca çalışanlar ve denetçilerle birlikte iş süreçlerine dâhil olan herkese hitap etmektedir. COBIT çerçevesi bu özellikleri ile, bilgi sistemleri teknolojisine sağladığı kaynaklar açısından önemli bir rehberdir (Fasanghari. 2008: 516).

ISACA COBIT’in ilk sürümünü 1996 yılında yayımlamıştır. Çerçevenin amacı; işletme yöneticileri ve denetçilerinin günlük kullanımı için geçerli, güncel, uluslararası

kabul görmüş BT kontrollerini araştırma, geliştirme ve teşvik etmektir. “Yönetim Rehberi”, 1998’de yayınlanan 2. sürümüne eklenmiştir. 3. sürüm 2000 yılında yayınlanmış, 2005 yılının aralık ayında 4. basım yayınlanmıştır. Haziran 2012’de COBIT 5 yayımlanmıştır.

ISACA tarafından 1996 yılında yayınlanan COBIT’in çıkış noktası bilişim teknolojileri denetimidir. Şekil 3.1.’de gösterildiği gibi COBIT, günümüzde denetim, kontrol, yönetim ve yönetişimi kapsamaktadır.

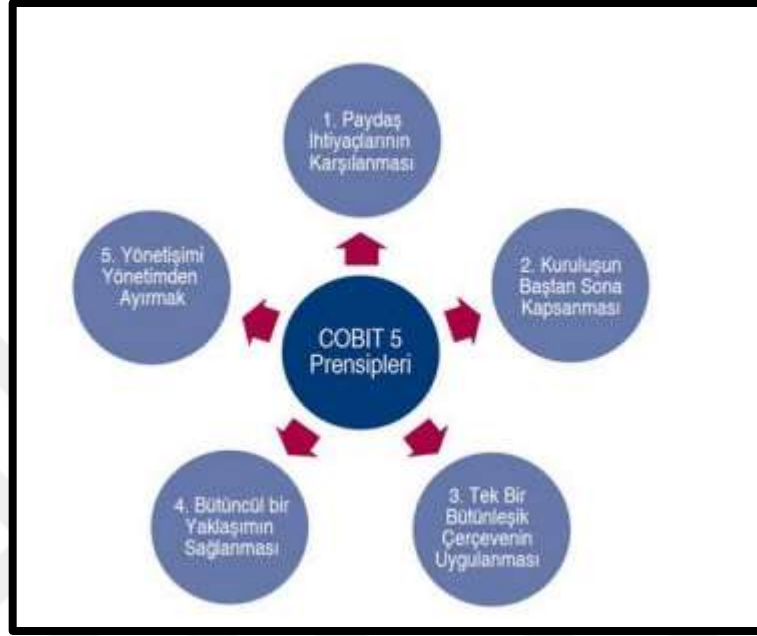
Şekil 3.1. COBIT’in Tarihsel Gelişim Süreci



Kaynak: Efe, 2016

COBIT'in tarihsel gelişimi izlendiğinde, önceleri denetim, kontrol ve daha sonra yönetim çerçevesi iken risk ve katma değer ile ilgili standartları da bünyesine alarak zamanla bir BT yönetim çerçevesi haline geldiği açıkça görülmektedir. Her versiyonunda kendini yenileyen COBIT en güncel hali olan COBIT 5 versiyonunda, sadece BT değil diğer iş süreçlerini de bünyesine alarak bütünlükçü, kapsayıcı ve uyarlayıcı bir çerçeveye evrilmiştir (Efe, 2016).

Şekil 3.2. COBIT 5 Çerçevesi İlkeleri



Kaynak: ISACA, 2012

COBIT 5 çerçevesi aşağıdaki 5 ilkedен oluşur: (ISACA, 2012)

İlke 1: Paydaş ihtiyaçlarının karşılanması

İlke 2: İşletmenin uçtan uca kapsanması

İlke 3: Entegre çerçeve uygulaması

İlke 4: Bütüncül bir yaklaşımın benimsenmesi

İlke 5: Yönetişimi yönetimden ayırma

COBIT-5 çerçeve yaklaşımını 5 temel ilke “principles” oluşturmaktadır. Bu ilkeler çerçevenin esas sütunlarını teşkil etmektedirler. Bu ilkeler üzerinde yapılacak olan yapısal kurgu ve süreç uygulamaları da gerçekleştiriciler “enablers” vasıtasıyla temellendirilebileceklerdir. BT-bağılantılı hedeflerin başarılanması, başarılı uygulama ve

birkaç gerçekleştiricinin kullanımını gerektirmektedir. Çerçeve de yer alan gerçekleştiriciler aşağıda sunulmuştur (ISACA 2012):

- İlkeler, politika ve çerçeveler,
- Süreçler,
- Organizasyonel yapılar,
- Kültür, etik ve davranışlar,
- Bilgi,
- Servis, altyapı ve uygulamalar,
- İnsan, beceri ve yetkinlikler.

COBIT 5' hedef/ ölçü ve girdi/çıktı kavramlarında detaylı ve yönlendirici bilgiler içermektedir. COBIT'te kurum, süreç ve kontrol hedefi (ya da yeni adıyla yönetim ve yönetim uygulaması) bazında hedef ve ölçülere yer verilmektedir. Bununla birlikte her bir yönetim uygulaması için girdi ve çıktılar tanımlanmış durumdadır. Ayrıca sorumluluk atama çizelgelerinin (RACI charts), iş birimlerini daha çok kapsayacak şekilde detaylandırılmış olması, sorumlulukların daha açık ve anlaşılır şekilde takip edilebilmesini sağlamaktadır (Cantürk, 2013). Ayrıca COBIT 5, ITIL, ISO 20000 ve ISO 27001 gibi çok sayıda güvenilir uygulama çerçeveleri ve standartları ile uyumludur. COBIT 5 çerçevesi her boyuttaki işletmelere aşağıdaki konularda yardımcı olmaktadır (Sibertime, 2020):

- İş kararlarını desteklemek için yüksek kaliteli bilgileri geliştirme ve sürdürme,
- İş hedeflerine ulaşmak için BT'yi etkin bir şekilde kullanma,
- Operasyonel mükemmelliğe teşvik etmek için teknolojiden faydalanma,
- BT riskinin etkili bir şekilde yönetildiğinden emin olma,
- Kuruluşların BT'deki yatırımlarının değerini anlamalarını sağlama,
- Yasalara, düzenlemelere ve sözleşme anlaşmalarına uyum sağlama.

3.3.3. ITIL

ITIL yani Information Technologies Infrastructure Library (Bilgi Teknolojisi Altyapı Kütüphanesi) kelimelerinin ilk harflerinin birleştirilmesi ile oluşturulmuştur. ITIL bilgi

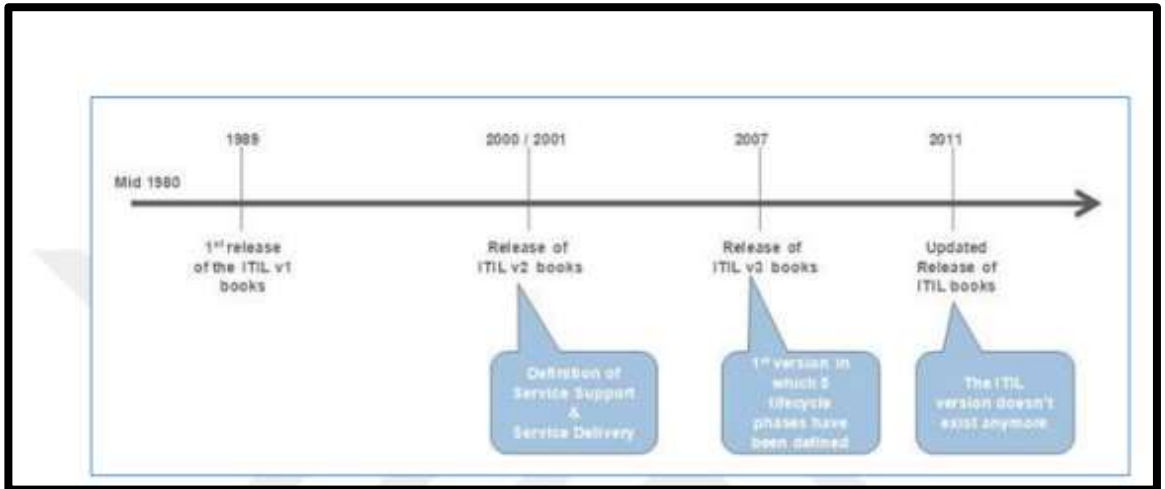
teknolojilerini bir hizmet olarak yönetmek için kullanılan bir metodolojidir (Sibertime, 2020).

ITIL, bilgi teknolojileri süreçlerini standartlaştırmayı ve herkes tarafından kabul gören ortak bir dil haline getirmeyi hedeflemektedir. ITIL, daha iyi bir BT ve siber güvenlik yönetişimi ile BT hizmetlerinin maliyetinin ve kalitesinin iyileştirilmesini amaçlamaktadır (Özbilgin, 2017).

ITIL, ücretsiz bulunabilen, hiçbir kimse tarafından kontrol edilemeyen ve sahiplenemeyen en iyi uygulamaların açık bir derlemesidir. ITIL, her tür servis yönetimi iyileştirme çalışmasında iyi bir başlangıç noktası olabilecek şekilde hizmet veren değerli bir rehberler setidir (Alpay, 2008).

ITIL metodolojisi, 1980'li yıllarda Birleşik Krallık'ta faaliyet gösteren işletmelerde bilgi teknolojileri hizmet kalitesinin artırılması amacı ile geliştirilmiş olup, günümüze kadar dört versiyon olarak gelişmiştir. İlk 1989'te olmak üzere 2001, 2007 ve 2019' da V2, V3, V4 yayımlanmıştır (Demir, 2014).

Şekil 3.3. ITIL'in Tarihsel Gelişim Süreci



Kaynak: Educare, 2019

ITIL'in en güncel versiyonu olan V4, 2019 yılında ITIL V3 çerçevesinin yükseltilmiş bir sürümü olarak yayımlanmıştır ve BT servis yönetiminin işletme gereklilikleriyle daha fazla uyumunu sağlayan gelişmiş stratejik ögeler içermektedir. Versiyon bilgi teknolojilerine uygun etkin ürün ve hizmetlerin yaratılması, sunulması ve sürekli iyileştirilmesi için baştan sona bir işletim modeli sunarak etkin bir BT Hizmet Yönetimi süreci oluşturulmasına yardımcı olmuştur. ITIL V4 ayrıca, yeni servis yönetimi zorluklarının üstesinden gelmek için organizasyonlara rehberlik etmektedir. Cloud, Agile, DevOps ve dijital dönüşüm çağında verimli çalışabilen modern teknolojinin potansiyelinden yararlanmaya yardımcı olmaktadır. ITIL, BT hizmet yönetimi için beş aşamalı hizmet döngüsüne dayanan bir çerçevedir (Sibertime, 2020):

1. Hizmet Stratejisi: Müşterileri anlamak ve BT hizmetlerini ihtiyaçlarını karşılamak için nasıl geliştirilip başarıyla yürütülmesi gerektiğini içermektedir.

2. Servis Tasarımı: Servisin verimli ve düşük maliyetli bir şekilde tasarlanmasını sağlamaktadır.

3. Servis Geçiş-Devreye Alma: Tasarlanan ve test edilen tasarımı göstermektedir.

4. Servis Operasyonu: Servisi teslim etmekte ve yönetmektedir.

5. Sürekli Hizmet İyileştirme: Hizmetin ve yönetiminde kullanılan teknolojinin ve süreçlerin iyileştirilmesi için bir mekanizma sağlamaktadır.

ITIL kullanımının amaçları genel olarak aşağıdaki gibi sıralanmaktadır (BMC, 2020);

- Maliyetlerin düşürülmesi
- Erişilebilirliğin artırılması
- Kapasitenin artırılması
- İş gücünün artırılması
- Kaynakların verimli kullanımının sağlanması
- Ölçülebilirliğin sağlanması.

ITIL, kaliteli bir BT hizmeti alınabilmesi için servis geliştirme uygulamaları, proje yönetimi tekniklerinin uygulanması, kurumun servis yönetimi kültürünü benimsemesi ve ITIL süreçlerinin doğru yorumlanarak uygulanması gerektiğini savunmaktadır. ITIL, aşağıda yer alan faydaları sağladığı için işletmeler tarafından benimsenmektedir (Akdaş, 2019: 22):

- Bilgi teknolojileri servisi ile işletmeye değer katmak
- Bilgi teknolojileri servisi için işletmenin ihtiyaçları ve iş stratejisini entegre etmek
- Ölçme, izleme ile bilgi teknolojileri servisleri ve servis sağlayıcı performansını optimize etmek
- Bilgi teknolojileri yatırımlarını ve bütçesini yönetmek
- Risk yönetimini sağlamak
- Bilgiyi yönetmek
- Etkin ve verimli hizmet sunmak için yetenekleri ve kaynakları yönetmek
- İşletme genelinde hizmet yönetimi için standart bir yaklaşım benimsenmesini sağlamak
- Kurum kültürünü değiştirerek sürekli bir başarı için çaba göstermeyi desteklemek
- Müşterileri ile etkileşim ve ilişki geliştirmek, optimize etmek ve maliyetleri düşürmek

3.3.4. NIST Siber Güvenlik Çerçevesi

Tam adı “National Institute of Standards and Technology-NIST” olan kuruluş, ülkemizdeki TSE – Türk Standartları Enstitüsü ile benzeşmektedir. 1901 yılında Amerika Birleşik Devletleri Ticaret Bakanlığı tarafından kurulmuştur. NIST çok geniş yelpazede standartlar yayımlayarak hizmetlerini sürdürmeye devam etmektedir. Hizmet alanlarından bir tanesi de Bilgi Sistemleri ve Güvenlik konularıdır (Turan, 2020). Siber güvenlik çerçevesi (Cyber Security Framework-CSF) kritik altyapıya sahip her türlü organizasyona uyum sağlayabilen siber güvenlik risk yönetim aracıdır. Uygulandığı kurumda sürdürülebilir performans sağlamayı amaçlayan CSF, siber güvenlik ekosisteminde endüstri tarafından kabul edilmiş standartları (NIST SP 800-53 Rev.4, ISO/IEC 27001:2013, COBIT 5, CIS CSC, ISA 62443-2-1:2009, ISA 62443-3-3:2013)

esas olarak versiyon 1.0 2014 yılında yayımlanmıştır (Çolak, 2020). Nisan 2018 itibariyle CSF versiyon 1.1 yürürlüğe girmiştir (Karadeniz, 2019).

CSF'nin geliştirilme amaçları aşağıda sunulmuştur (Çolak, 2020):

- Kritik altyapıya sahip tüm sektörlerde uygulanabilir güvenlik standartları ve kuralları belirlemek
- Performans ve verimliliğe dayalı esnek ve tekrarlanabilir bir yapı sağlamak
- Siber risklerin belirlenmesi, değerlendirilmesi ve yönetilmesine yardımcı olmak
- Mevcut siber riskler için iyileştirme alanları belirlemek
- Yayımlanmış standartların karşılamadığı güvenlik boşluklarını belirlemek ve bu boşluklar için eylem planları geliştirmek.

Çerçeve özetle, siber güvenlik ve temel altyapı sistemlerini korumak için daha sağlam bir yaklaşım geliştirmeye yardımcı olan beş temel işlevi içermektedir:

- Tanımla
- Koru
- Tespit Et
- Müdahale Et ve
- Geri Dön.

Böylelikle, çerçeve risklerin belirlenmesi, tehditlere karşı korunma, güvenlik olaylarına müdahale etme ve herhangi bir potansiyel olaydan geri dönüş için kapsamlı bir yol haritası sunmaktadır (Karadeniz, 2019).

NIST siber güvenlik çerçevesine göre bir siber güvenlik programının oluşturulması 7 adımda gerçekleşmektedir. Bu adımlar ve adımlarda gerçekleştirilecek işlemler aşağıda sunulmuştur (Çolak, 2020):

Adım 1: Önceliklendirme ve Kapsam

İşletme, hedeflerini ve üst düzey önceliklerini belirlemelidir. Siber güvenlik programında hangi işin ve hangi süreçlerin ele alınacağı kararlaştırılmalıdır.

Adım 2: Yönlendirme

İşletme; kapsam, yasal veya düzenleyici şartlar ve genel risk yaklaşımı ile ilgili sistemleri ve varlıkları tanımlamalıdır.

Adım 3: Mevcut Profil Oluşturma

İşletme, 'Öz' bölümündeki hangi kategori sonuçlarına şu anda ulaşıldığını gösteren mevcut profil oluşturmalıdır.

Adım 4: Risk Değerlendirmesi Yürütme

İşletme, bir siber güvenlik olayının olasılığını ve olayın organizasyon üzerindeki etkisini anlamak için operasyon ortamını analiz etmelidir.

Adım 5: Hedef Profil Oluşturma

İşletme, istenen siber güvenlik sonuçlarını tanımlayan kategorileri, kuruluş hedeflerini ve yasal uyumluluk ile ilgili gereklilikleri dikkate alarak değerlendirmeli ve Hedef Profil oluşturmalıdır.

Adım 6: Fark Belirleme, Analiz Etme ve Önceliklendirme

İşletme; Mevcut Profil ile Hedef Profil'i karşılaştırarak farkları ele almalı, Hedef Profil'e ulaşmak için farklara yönelik eylem planı hazırlamalı ve kaynakları belirlemelidir.

Adım 7: Eylem Planını Uygulama

İşletme, önceki adımda belirtilen açıkları gidermek için hangi önlemlerin alınacağını belirlemeli ve daha sonra Hedef Profil'e ulaşmak için mevcut siber güvenlik uygulamalarını ayarlamalıdır.

3.4. Siber Risklerin Analizi ve İç Denetim

İşletmeler içindeki risk ve kontrol işlevlerinin etkinliğini ve verimliliğini iyileştirmek için en iyi uygulama yaklaşımı, IIA tarafından Ocak 2013'te yayınlanan "Etkili Risk

Yönetimi ve Kontrolünde Üçlü Savunma Hattı” nda sunulmuştur. Ayrıca IIA tarafından tamamlayıcı rehber olarak 2016 yılında Küresel Teknoloji Denetimi Kılavuzu (Global Technology Audit Guide) “Siber Güvenlik Riskinin Değerlendirilmesi Üçlü Savunma Hattının Rollerı” yayımlanmıştır. Kılavuzda yer alan siber risklerin analizinde üçlü savunma hattının ve özellikle de iç denetçilerin rolleri aşağıda sunulmuştur.

İç denetim biriminin siber güvenlikteki rolünü değerlendirmenin en önemli adımı, üçlü savunma hattının uygun şekilde oluşturulduğundan ve her bir hattın etkin bir şekilde çalıştığından emin olmaktır. Ek olarak, işletmenin kabul etmeye istekli olduğu risk seviyesinin belirlenmesi (risk iştahını aşan risklerin belirlenmesi) ve ilgili süreçlerin yönetilmesi için tanımlanan rollerin ve sorumlulukların tanımlanması için bir raporlama protokolü oluşturulmalıdır (IIA, 2013).

Birinci savunma hattı, yönetim kontrollerinden oluşmaktadır. Diğer bir ifadeyle işletmenin tüm süreçlerine ilişkin risklerin ilk kontrol altına alındığı hattır. Birinci savunma hattı yönetim kontrolleri, otomasyon kontrolleri, süreç kontrolleri, manuel kontroller vb. kontrollerinin tasarlandığı kısımdır. İşletme yönetimi, verilerin, süreçlerin, risklerin ve kontrollerin sahibidir ve bunları yönetmekle yükümlüdür. Siber güvenlik açısından değerlendirildiğinde ilk savunma hattı, riskleri kontrol eden ve yöneten ve süreçleri ve kontrol eksikliklerini gidermek için düzeltici eylemler uygulayan operasyonel birimlerin yöneticilerinden meydana gelmektedir (IIA, 2013).

İkinci savunma hattı, birinci hattın oluşturduğu süreçlerin ve kontrollerin varlığını ve etkin bir şekilde çalışmasını sağlamaktan sorumlu risk, uygunluk, kontrol ve gözetim faaliyetlerini içermektedir. Bu faaliyetleri, etkili risk yönetimi sağlamaktan ve siber güvenlik alanındaki riskleri ve tehditleri izlemekten sorumlu birimler ve çalışanlar gerçekleştirmektedir (IIA, 2013).

İşletmelerde üçüncü savunma hattı olarak görev yapan iç denetim birimi, üst yönetim ile yönetim kuruluna yönetişim, risk yönetimi ve iç kontroller konusunda bağımsız ve objektif güvence sağlamaktadır. Ayrıca birinci ve ikinci savunma hatları tarafından gerçekleştirilen faaliyetlerin siber güvenlik konusunda genel etkinliğini değerlendirmekte üçüncü savunma hattının önemli görevlerinden biridir (IIA, 2013).

Şekil 3.5. Üçlü Savunma Hattı



Kaynak: IIA, 2013

Birinci Savunma Hattı Sahipleri ve Temel Faaliyetleri:

Birinci savunma hattı, risklere ve kontrollere sahip olan ve bunları yöneten ve süreç ve kontrol eksikliklerini ele almak için düzeltici eylemler uygulayan operasyon yöneticilerinden oluşmaktadır (IIA, 2016).

İşletmelerde baş teknoloji sorumlusu (Chief Technology Officer-CTO), genellikle işletmelerin mevcut teknolojileriyle ilgili bilgi ve yönlendirme sağlama ve işletmenin fikri mülkiyetini koruma sorumluluğuna sahiptir. CTO'nun sorumlulukları arasında, işletmenin rekabet avantajı, stratejik değişim ve inovasyon sağlayacak sonraki teknolojik gelişim aşamalarına hazırlanmasını sağlamak da yer almaktadır. İşletmelerde siber güvenlik kapsamında; Bilgi güvenlik yöneticileri (CISO, Chief Information Security Officer), bilgi yöneticisi (CIO, Chief Information Officer) veya BT (Bilgi Teknolojisi)'den sorumluları da görev yapabilmektedir (IIA, 2016).

Bilgi teknolojileri yöneticisi, siber suç ve ilgili siber saldırılara karşı mücadelede CEO ve diğer üst yönetim üyeleriyle iş birliği içerisinde olmalıdır. Ayrıca işletmede faaliyet

gösteren bölümler kendi teknolojilerinden sorumludur. Birim yöneticileri işletme içindeki diğer risk değerlendirme faaliyetleriyle koordineli olarak teknolojilerini ve verilerini güvence altına almak için uygun kontrolleri tasarlama ve uygulama sorumluluğunu da üstlenmektedirler (IIA, 2016).

İşletmeler yukarıda açıklanan pozisyonlara sahip olamayan bir ölçeğe ya da kurumsal yapıya sahip değillerse siber güvenlik riskine yanıt verme konusunda yetkili birimler veya BT yöneticileri gereken sorumlulukları üstlenmelidir (IIA, 2016).

Birinci savunma hattında yer alan faaliyetler aşağıdaki gibidir:

- Siber güvenlik prosedürlerinin; yönetimi, eğitimi ve testleri
- Düzenlemelerin/konfigürasyonların güvenli araçlarla sürdürülmesi, uygulamaların güncellenmesi, yamaların yapılması
- Saldırı tespit sistemini etkin kullanmak ve penetrasyon (sızma) testlerinin yürütülmesi
- Network trafik akışını yeterli seviyede yönetmek ve korumak için güvenli şekilde network yapılandırılması
- Bilgi varlıklarının, teknolojik araçların ve ilgili yazılımların envanteri
- İzleme/gözetim ile ilgili veri koruma ve kayıp önleme programlarının etkin kullanımı
- Erişim kısıtlaması
- Gerekli yerlerde verilerin şifrelenmesi
- İç ve dış taramalar ile zafiyet yönetimi uygulamaları
- Sertifikalı BT, BT riski ve bilgi güvenlik personelinin işe alımı ve devamlılığı

Siber tehditler, sistemleri/iş süreçlerini bloke etmek, operasyonlara zarar vermek veya verileri hırsızlığı için tasarlandığından; tehditler genellikle kritik verilerin depolandığı alanlarda ortaya çıkmaktadır. Bu alanlar; veri merkezleri, dahili ağlar, harici olarak barındırılan ortamlar ve iş sürekliliği platformlarıdır. Saldırı nerede meydana gelirse gelsin, saldırı sonucunda yasa ve yönetmeliklerin ihlali, para cezaları, itibar zedelenmesi ve gelir kaybı meydana gelme ihtimali oldukça yüksektir (IIA, 2016).

İşletmelerde hassas ve gizli veriler dahili ya da harici olarak sınıflandırılabilir ve depolanabilirler. Dahili veriler konusunda, çoğu işletme ilk savunma hattı olarak güvenli yapılandırmalar, güvenlik duvarları ve erişim kontrolleri gibi teknolojilere güvenmektedir. Ancak bu teknolojiler ve kontroller de zaman zaman aşılabilmektedir. Örneğin güvenlik duvarının aşırı yüklenmiş olduğu özel bir saldırıda, saldırganlar sistemlere ve verilere erişim elde edebilir ve yetkisiz işlemler gerçekleştirilebilirler (IIA, 2016).

Bu tür saldırıların güvenlik duvarına ulaşma riskini azaltmak için, birinci savunma hattı, ağların çevresinde önleyici tedbirler almalıdır. Bu durum, erişimi kısıtlamayı ve yetkisiz trafiği engellemeyi içeren zorlu bir süreçtir. Kötü amaçlı yazılımlar, organizasyonlar ve web siteleri hakkında elde edilen bilgiler ışığında bilinen güvenlik açıklarını izlemek için kontroller kurulmalıdır (IIA, 2016).

Pek çok işletme, iyi bir ağ trafiği için bir beyaz liste ve engellenen ağ trafiği için de bir kara liste oluşturmaktadır. Ancak, ağ trafiğinin dinamik yapısı nedeniyle aktif izleme ve sık güncelleme kritik önem taşımaktadır. Çünkü, eğer saldırgan sisteme erişmeyi başlarsa, sonraki saldırı için büyük olasılıkla yönetici ayrıcalıkları elde edecek ve sistemdeki izlerini kapatmayı başaracaktır (IIA, 2016).

Verilerin işletme dışında depolanması durumunda, işletmelerin hizmet sağlayıcıları ilgili riskleri uygun şekilde yönetmesi gerekmektedir. Birinci savunma hattı için kritik olan adım, aşağıda yer alan unsurları içeren güçlü sözleşmeler oluşturmaktır (IIA, 2016):

- Hizmet kuruluşu kontrol (service organization control-SOC) raporları
- Denetim hakkı hükümleri
- Hizmet seviyesi anlaşmaları (service level agreements SLA)
- Siber güvenlik inceleme görevleri

Hizmet sağlayıcısı ile anlaşma sağlandıktan ve sözleşme yerine getirildikten sonra yönetim, hizmet seviyesi anlaşmalarına uyumluluğu sağlamak için kilit ölçütleri izleyip raporlayarak hizmet sağlayıcısını denetlemelidir. Hizmet sağlayıcısı sözleşme gereksinimlerini karşılamıyorsa işletme; sorunların zamanında çözülmesini isteyebilir,

cezai yaptırım uygulayabilir ve gerekirse alternatif bir hizmet sağlayıcısına geçiş planlarını değerlendirebilir (IIA, 2016).

İşletme yönetimi ayrıca, kimlik avı e-postaları ve kötü niyetli telefon aramaları dahil olmak üzere sosyal mühendisliği içeren saldırılara karşı da dikkatli olmalıdır. Saldırganlar, bilgi ya da eyleme ihtiyaç duyan meşru bir işletme veya kişinin kimliğine bürünerek, yetkili kişileri hassas verileri paylaşmaya, sistem kimlik bilgilerini sağlamaya, sahte web sitelerine yönlendiren bağlantıları tıklamaya ve kötü amaçlı yazılım yükleyen eylemler gerçekleştirmeye ikna edebilmektedir. Kötü amaçlı yazılım yüklendikten sonra, işletmenin ağında çoğalabilmekte, sistem performansını ve kullanılabilirliğini bozabilmekte, verileri çalınmasına ve saldırıların sahtekarlık çalışmalarını ilerletmesine neden olmaktadır (IIA, 2016).

Kötü amaçlı yazılımlar, farkındalık eksikliğinden yararlanılarak geliştirilmektedir. Bu nedenle, kişilere sık sık şüpheli veya olağandışı e-postalar, benzeri görülmemiş talepler, telefon görüşmeleri veya sistem aktiviteleri için tetikte olmalarını hatırlatmak önemlidir. Eğitim ayrıca bireylerin hayali iletişimlerini tanımlarına ve bu tür olayları araştırma, yükseltme ve çözüm için hızlı bir şekilde rapor etmelerine yardımcı olacaktır. Sektördeki meslektaşlardan alınan dersler ve kazanılan istihbarat, eğitim, farkındalık ve ek önleyici tedbirlerin benimsenmesi için de kullanılabilir (IIA, 2016).

İkinci Savunma Hattı Sahipleri ve Temel Faaliyetleri

Siber güvenlik açısından ikinci savunma hattı işletmelerin BT birimleridir. BT risk yönetimi ve BT uyum işlevlerinden oluşan ikinci savunma hattı, bir işletmenin güvenlik durumunda ve program tasarımında önemli bir rol oynamaktadır. İkinci savunma hattı aşağıdakilerden sorumludur (IIA, 2016):

- Siber güvenlikle ilgili riskleri ve riskleri değerlendirmek ve bunların kuruluşun risk iştahıyla uyumlu olup olmadığını belirlemek
- Mevcut veya ortaya çıkması muhtemel riskleri, yasa ve yönetmeliklerdeki değişiklikleri izlemek
- Uygun kontrol tasarımını sağlamak için birinci savunma hattı ile iş birliği yapmak

Siber güvenlik riskleri, geleneksel risklere göre çok daha dinamikdir ve zamanında müdahale gerektirmektedir. Siber riskler ve işletmelerin bu risklere maruz kalma biçimi sürekli değişkenlik gösterdiğinden, ikinci savunma hattı, işletmenin bu risklere zamanında yanıt vermesini sağlamak ve bilgi varlıklarını güvence altına almak için yönetim ve gözetim faaliyetleri gerçekleştirmektedir. Ayrıca BT süreçlerine ilişkin politikalar ve standartlar tasarlamak da ikinci hattın temel görevlerindendir (IIA, 2016).

İkinci savunma hattı, yönetim kurulu veya yönetim organları arasında etkili bir farkındalık yaratmak ve siber güvenlik riskleri ile kontrolleri hakkında raporlamanın yeterli ve güncel olmasını sağlamak için birinci ve üçüncü savunma hatlarıyla koordineli bir biçimde çalışmalıdır. İkinci savunma hattı risk değerlendirmelerini gerçekleştirirken ve raporlarken, siber güvenliği bir öncelik olarak tutmaya devam etmelidir (IIA, 2016).

İşletmeler, kritik iş süreçlerinde satıcılardan ve tedarikçilerden yararlanmaktadır. İkinci savunma hattının, tedarikçilerin veya satıcıların hassas, sınıflandırılmış verilere doğrudan ağ bağlantıları veya diğer veri aktarım yöntemleri aracılığıyla erişimleri olabileceğinden, bu üçüncü taraf hizmet sağlayıcılarla ilişkileri siber güvenlik riski açısından değerlendirmesi gerekebilmektedir. Özellikle, teknik ve sözleşmeye dayalı kontrol hükümlerinin gözden geçirilmesi gerekmektedir. Ayrıca bu hizmet sağlayıcıların, üzerinde anlaşmaya varılan siber güvenlik kontrolleri hakkında yeterli raporlama ile periyodik güvence sağlamaları önemlidir (IIA, 2016).

Uluslararası İç Denetçiler Enstitüsünün yayınlamış olduğu rehberde ikinci savunma hattında siber güvenlikle ilgili yaygın faaliyetler şöyle sıralanmıştır:

- Siber güvenlik politikaları, eğitimi ve testlerinin tasarlanması
- Siber risk değerlendirmelerinin yapılması
- Siber tehdit bilgilerinin toplanması
- Verilerin sınıflandırılması ve kısıtlı erişim rollerinin tasarlanması
- Olayların anahtar risk göstergelerinin izlenmesi ve iyileştirilmesi
- Sertifikalı IT risk personelinin işe alınması ve devamlılığı
- Üçüncü taraflarla, tedarikçilerle ve hizmet sağlayıcılar ile ilişkilerin değerlendirilmesi

- İş sürekliliği planlarının yapılması/test edilmesi ve olağanüstü durumları iyileştirme uygulamaları ve testlerine katılım

Üçüncü Savunma Hattı Sahipleri ve Temel Faaliyetleri

İşletmelerde yönetim, yönetim kurulu ve üst yönetiminin sorumluluğunda iken, yönetişimin değerlendirilmesi iç denetim biriminin birincil görevlerinden biridir. IIA 2110.A23 standardı uyarınca iç denetim biriminin, işletmenin bilgi teknolojisi yönetişiminin işletmenin stratejilerini ve hedeflerini destekleyip desteklemediğini değerlendirmesi gerekmektedir.

İşletmelerde üçüncü savunma hattı olarak iç denetim faaliyeti, ikinci savunma hattıyla koordinasyonlu bir biçimde hareket ederek özellikle siber güvenlik kapsamında önemli bir rol oynamaktadır. İç denetim birimi siber güvenlik hakkında aşağıda belirtilen konularda danışmanlık yapmaktadır (IIA, 2016):

- Siber güvenlik ve örgütsel riskler arasındaki ilişki
- Siber risklere verilecek tepkiler ve risklerle ilişkili kontrol faaliyetleri
- İşletmenin siber güvenlik risklerinin azaltılmasına yönelik denetim; örneğin, ayrıcalıklı erişim, ağ tasarımı, satıcı yönetimi ve izleme
- İyileştirme faaliyetlerinde güvence
- Birinci ve ikinci savunma hattı işlevlerinin tam anlamıyla yerine getirilemediği işletmelerde risk farkındalığını artırmak ve siber güvenlik risk yönetimi ile koordinasyon sağlama
- Siber risklerle ilgili konuların iş sürekliliği planları ve olağanüstü olayların iyileştirilme testleri kapsamına dahil edilip edilmediğini doğrulama

IIA Standardı 2120 uyarınca işletmenin risk yönetimi sürecinin etkinliğini değerlendirmenin bir parçası olarak, iç denetim faaliyetinin rolü, işletmenin diğer riskleriyle uyumlu bir biçimde siber güvenlik risklerini ve kontrollerini bağımsız olarak değerlendirmektir. Bu değerlendirme yapılırken, ikinci hattın belirlediği çerçeveler, standartlar, risk değerlendirmeleri ve yönetimle ilgili çalışmalarının yeterliliği de gözden geçirilmelidir (IIA, 2016).

Buna ek olarak, iç denetim birimi, birinci savunma hattındaki kontrollerin etkinliğini de değerlendirmelidir. BT genel kontrollerinin işletmenin siber güvenliğinin sağlanmasında temel oluşturduğunu, ancak siber güvenlik risklerini azaltmak için eksiksiz bir çözüm sunmadığını unutmamak önemlidir. Siber güvenlik süreçlerinin karmaşıklığı ve siber tehditlerin günden güne artması, saldırılar gerçekleştikçe tespit ve düzeltici eylemler gibi ek kontrol katmanları gerektirmektedir (IIA, 2016).

Geleneksel yöntemlere dayalı güvence hizmetleri, siber güvenlik riskinin hızına ayak uydurmak için yeterli olmadığından, yenilikçi bir güvence stratejisi belirlemek işletmeler için önem arz etmektedir. Güvenlik yapılandırmalarındaki değişiklikleri, ortaya çıkan risk aşırılıklarını ve eğilimlerini, yanıt sürelerini ve iyileştirme faaliyetlerini değerlendirmek için giderek artan bir şekilde sürekli denetim tekniklerine ihtiyaç duyulmaktadır (IIA, 2016).

IIA tarafından 2011 yılında yayımlanan “İç Denetimin Diğer Güvence Sağlayıcılarına Güvenmesi” (Reliance by Internal Audit on Other Assurance Providers) uygulama kılavuzuna göre, iç denetçiler yeniden uygulama, derinlemesine araştırma, soruşturma, belge inceleme veya doğrulama yapıp aynı sonuca varması durumunda ikinci savunma hattına güvenmelidir. Örneğin, İç denetçiler; BT birimi tarafından tamamlanan bir sızma testini yeniden uygulayabilir veya test ayrıntıları (kapsam dahil) inceleyerek ve sonuçların güvenilirliğine karar verebilir. Hatta mümkünse, iç denetçiler, işi yapan teknik personeli gözlemleyerek ve personel ile görüşerek sonuçları ve çıktıları gelecekteki siber güvenlik iç denetim prosedürlerine dahil etmelidir (IIA, 2011)

Aşağıda, bir iç denetim birimi yöneticisinin siber güvenlikle ilgili kuruluşun yönetimini değerlendirirken dikkate alması gereken 10 soru bulunmaktadır (IIA, 2016):

1. Üst yönetim ve yönetim organı (denetim komitesi, yönetim kurulu vb.) siber güvenlikle ilgili temel risklerin farkındalar mı? Siber güvenlik girişimleri öncelikli mi ve yeterli destek alıyor mu?
2. Yönetim, siber tehditlere veya güvenlik ihlallerine duyarlı varlıkları belirlemek için bir risk değerlendirmesi gerçekleştirdi mi ve potansiyel etki (finansal ve finansal olmayan) belirlendi mi?

3. Birinci ve ikinci savunma hatları, siber güvenlikle ilişkili yeni / ortaya çıkan riskler, yaygın zayıflıklar ve siber güvenlik ihlallerini güncel tutmak için sektördeki meslektaşlarıyla (ör. Konferanslar, ağ oluşturma forumları ve web yayınları) iş birliği yapıyor mu?
4. Siber güvenlik politikaları ve prosedürleri yürürlükte mi ve çalışanlar ve tedarikçiler/satıcılar/yükleniciler periyodik olarak siber güvenlik farkındalık eğitimi alıyor mu?
5. BT süreçleri spesifik olarak siber tehditleri tespit etmek için tasarlanmış mı ve çalışıyor mu? Yönetim yeterli izleme kontrollerine sahip mi?
6. Geri bildirim mekanizmaları, işletmenin siber güvenlik programlarının durumu hakkında üst yönetime ve yönetim kuruluna içgörü sağlamak için çalışıyor mu?
7. Yönetimin bir siber saldırı veya tehdit durumunda etkili bir yardım hattı veya acil durum prosedürü var mı? Varsa bu prosedürler çalışanlara, yüklenicilere ve hizmet sağlayıcılara iletildi mi?
8. İç denetim birimi, siber tehditleri azaltmak için süreçleri ve kontrolleri değerlendirebilecek yetkinlikte mi? Aksi takdirde iç denetim birimi müdürünün siber güvenlik uzmanlığına sahip diğer kaynakları dikkate alması gerekiyor mu?
9. İşletme, verileri harici olarak depolayanlar (ör. BT sağlayıcıları, bulut depolama sağlayıcıları, ödeme işlemcileri) dahil olmak üzere sistem erişimine sahip üçüncü taraf hizmet sağlayıcılarının bir listesini tutuyor mu? Hizmet sağlayıcısının kontrollerinin etkinliğini değerlendirmek için bağımsız bir siber güvenlik incelemesi yapıldı mı?
10. İç denetim, işletmenin karşı karşıya olduğu yaygın siber tehditleri (ör. suçlular, bilgisayar korsanları, ağa bağlı sistemler, bulut sağlayıcıları, tedarikçiler, sosyal medya sistemleri, kötü amaçlı yazılım) belirledi mi ve bunları iç denetim risk değerlendirme ve planlama süreçlerine dahil etti mi?

İç denetim birim yöneticisi, yukarıdaki soruları kullanarak siber güvenlikle ilgili tehlike işaretlerini belirlemelidir. İç denetim birim yöneticisi, ikinci savunma hattının stratejik olarak hareket edip etmediğini ve birinci savunma hattının riskleri belirleyip

bunlara yanıt verecek ve derhal düzeltici eylemi gerçekleştirecek şekilde konumlandırılıp konumlandırılmadığını değerlendirmelidir. Değerlendirmeler yapılırken öncelikle yönetim yapısı irdelenmelidir (IIA, 2016).

Bu sorulardan gelen ön yanıtları yorumlamak ve risk temelli yaklaşıma dayalı olarak tehdit altındaki alanları belirleme sürecini başlatmak iç denetim birimi yöneticisinin görevidir. İç denetim yöneticisinin mesleki yargısı, siber güvenlik uygulamaları ile tehditlerin karşılıklı ilişkilerinin tam olarak anlaşılmasında büyük bir rol oynayacaktır.

İç denetimin IIA tarafından yapılan tanımı “İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve tarafsız bir güvence ve danışmanlık faaliyetidir. İç denetim kurumunun risk yönetimi, kontrol ve kurumsal yönetim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistematik ve disiplinli bir yaklaşım geliştirerek, kurum hedeflerinin gerçekleştirilmesine yardımcı olur” şeklindedir.

İç denetim; işletmelerde kontrol mekanizması olarak çalışmakta ve işletmenin iş süreçlerinin uyumuna yönelik usulsüzlüklerini ve sistemin zayıflıklarını ortaya koymaktadır. İç denetimin temel amacı, örgütün; kişisel verilerin işlenmesini düzenlemek adına politika ve prosedür oluşturup oluşturmadığını, veri işlemenin bu politika ve prosedürlere göre gerçekleşip gerçekleşmediğini tespit etmek ve örgütün verilere yönelik sistematik hataları ele almada ne kadar başarılı olduğunu anlamaktır.

İç denetim faaliyeti, işletmelerin siber güvenlik risklerinin değerlendirilmesinde aşağıdaki unsurları göz önünde bulundurarak çok önemli bir rol oynamaktadır (IIA, 2016):

- İşletmenin en değerli bilgilerine kimler erişebilir?
- Siber saldırılar için en olası hedefler hangileridir?
- Olası bir saldırıda hangi sistemler en önemli kesintiye neden olur?
- Hangi veriler, yetkisiz taraflarca elde edilirse, işletmelerde finansal zarara, rekabet kaybına, yasal sonuçlara veya itibarın zarar görmesine neden olur?
- Yönetim, bir siber güvenlik olayı meydana gelirse zamanında tepki vermeye hazır mı?

Siber güvenlik riskinin kapsamını belirleme, iç denetim birimi ile ikinci savunma hattının ortaklaşa planlanma yapmasını gerektiren tüm aşamaları birbirine bağlı bir çalışmadır. İç denetim faaliyeti, iç denetim sırasında ve sonrasında iş birliği yapabilecekleri ve iş etki analizini gerçekleştirebilecek işletme organları/birimleri ile entegre edildiğinde daha etkili olmaktadır.

Siber güvenliğe ilişkin süreçler iç denetçiler ve bağımsız denetçiler tarafından gerçekleştirilen denetimlerin amacı ve kapsamı çerçevesinde ele alınmalıdır. Çünkü işletmelerde artık siber riske maruz kalmayan hiçbir süreç bulunmamaktadır. Blok zinciri, yapay zekâ, büyük veri, nesnelerin interneti gibi teknolojik gelişmelerin işletmelere etkileri göz önüne alındığında, finansal, operasyonel veya sistematik tüm süreçler siber riske maruz kalmaktadır (Selimoğlu & Altunel, 2019:13)

İç denetim birimi yöneticisi, iç denetim planının neleri kapsadığını tanımlamalı ve güvence sağlanamayan alanları not etmelidir. IIA 2050 numaralı Koordinasyon standardı uyarınca iç denetim faaliyetinin; işletme için önemli bilgilerin tanımlamak ve siber güvenlik riskinin uygun şekilde kapsamını belirlemek için birinci ve ikinci savunma hattıyla iş birliği yapması gerekecektir. İşletme için önemli bilgilerin korunmasına öncelik veren iç denetim faaliyeti, ilgili veri sahipleriyle birlikte çalışmalı, provizyon süreçlerini değerlendirmeli ve verilere kimin erişiminin olduğunu güncel olarak takip etmelidir (IIA, 2016)

İç denetim faaliyeti kritik bilgilere (örneğin, çalışan verileri, kişisel olarak tanımlanabilir bilgiler, müşteri kredi kartı numaraları, satın alma geçmişi) erişimi sağlayan sistemleri ve teknolojileri tanımlamak için işletme yönetimi ile çalışmalıdır. Yönetim ile çalışmak, siber güvenlik açıkları için ilgili unsurların sürekli olarak izlenmesine de yardımcı olacaktır.

Aşağıdaki sorular, kritik bilgileri tanımlama sürecinde kullanılmaktadır (IIA, 2016):

- Hangi bilgiler kritik kabul edilmektedir ve neden?
- Dolandırıcılar veya rakipler vb. için verilerin değeri nedir?
- Bilgiye nereden erişilmektedir, bilgiler nasıl işlenmekte ve saklanmaktadır?
- Bilgi nasıl iletilmektedir?

- Bilgiye erişim yetkisi verme veya erişimi iptal etme sürecinin kapsamı nedir, süreç titiz bir şekilde yürütülmekte midir?
- Erişim seviyeleri işletmedeki rollere göre belirlenmiş mi ve hangi roller yönetim erişimine sahiptir?
- Erişim nasıl atanmakta, onaylanmakta, izlenmekte ve kaldırılmaktadır?
- Bilgiler, yetkisiz erişime karşı ne kadar iyi korunmaktadır?
- Ne tür testler gerçekleştirilmektedir (sızma, erişim, izlenen değişiklikler vb.)?
- Kritik bilgilere işlevsel erişimi olanlar için siber güvenlik riski nasıl izlenmektedir?

Siber güvenlik gibi karmaşık ve hızlı değişen bir konu hakkında mutlak bilgi sahibi olunması mümkün olmamakla birlikte bir iç denetim biriminin siber güvenlik konusunu yakından takip etmesi ve konu hakkında bilgi sahibi olması çok önemlidir. Siber risk sadece bir teknoloji riski olmanın ötesinde işletmelerin tüm iş süreçlerini ve varlıklarını etkileyen bir risk unsurudur. Dolayısıyla iç denetim faaliyeti bu konuda önemli bir rol oynamaktadır. İç denetim faaliyeti, yalnızca siber güvenlik denetimlerinin yürütülmesi ile ilgili sorumluluklara değil aynı zamanda işletmeye, ileriye dönük ve stratejik düşünce liderliği sunmak suretiyle işletme için güvenilir danışmanlık hizmeti sunma misyonuna da sahiptir (IIA, 2016):

Siber güvenlik konusunda iç denetimin doğrudan etki edebileceği dört önemli alan bulunmaktadır. Bunlar (IIA, 2016):

- Siber tehditlere karşı hazırlık ve müdahale hakkında güvence vermek
- Üst yönetime işletmenin karşı karşıya olduğu risk seviyesini ve bu risk seviyelerine cevap vermek için sarf ettiği çabanın düzeyini bildirmek
- Etkili savunma ve müdahale mekanizmalarını temin etmek için bilgi teknolojileri birimi ve diğer bölümlerle birlikte çalışmak
- Risklerle ilgili olarak işletmede bulunan taraflar arasında iletişimi ve koordinasyonu sağlamak ve kolaylaştırmaktır.

Siber risklere ilişkin endişeler artıkça paydaşlar siber güvenlik risk programlarını takip etmektedir ve işletme yönetimi iç denetim biriminden siber güvenlik konusunda güvence talep etmektedir. Bu sebeple iç denetim birimi siber riskler konusunda bilgi

sahibi olmalı ve siber risklere karşı dirençli olmada rol üstlenmeli ve oynamalıdır. İç denetim biriminin risk değerlendirme stratejileri, siber güvenliğe özgü tüm riskleri içerecek şekilde geliştirilmeli, politika ve iç kontrollere uyulması konusunda güvence vermelidir. Dolayısıyla iç denetim birimi paydaşlara gerekli güvenceyi vermek adına siber sorunlarla ilgili denetim programı geliştirmesi gereklidir. Bu denetim programının etkinliği için kontrol ortamı, kontrol faaliyetleri, risk değerlendirme, iletişim ve izleme süreçlerinin kurulması ve siber güvenlik tedbirlerinin değerlendirilmesi için bir çerçevenin kurulması gereklidir (Selimoğlu & Altunel, 2019:14).

İç denetçiler, siber güvenlik risklerine karşı güvence sağlamak için güncellenmiş bir yaklaşıma ihtiyaç duymaktadır. BT genel kontrol değerlendirmeleri siber risklerden korunmak için yararlı olsa da siber güvenlik güvencesi sağlamak için yetersiz kalmaktadırlar. Bu bağlamda, siber güvenlik iddiaları hakkında değerli sonuçlar sağlayan güncellenmiş bir iç denetim yaklaşımına olan ihtiyaç önemini korumaktadır. (IIA, 2016).

3.5. İç Denetçilerin Siber Güvenlik Risklerini ve Kontrollerini Değerlendirmesine Yönelik Bir Yaklaşım

IIA tarafından yayımlanan “Siber Güvenlik Riskinin Değerlendirilmesi Üçlü Savunma Hattının Roller” kılavuzunda yer alan altı bileşen, yönetimin siber güvenlik kontrollerinin ve yönetişiminin tasarımını ve işletim etkinliğini değerlendirmek için kullanılmaktadır. Bileşenler birlikte iyi tasarlanmadığında veya çalışmadığında, işletme siber tehditleri ve ortaya çıkan riskleri karşısında savunmasız kalabilmektedir. Bileşenler aşağıda bölümde açıklanmıştır (IIA, 2016):

Siber Güvenlik Yönetişimi

İç denetim faaliyeti, işletmenin siber güvenlik uygulamalarına, süreçlerine ve yönetişimine hâkim olmalıdır. IIA 2100: İşin Niteliği standardı iç denetim faaliyetinin yönetişim, risk yönetimi ve kontrol süreçlerini değerlendirmesini ve iyileştirmesine katkıda bulunmasını gerektirmektedir. Yönetişim faaliyeti, rolleri ve sorumlulukları netleştirmeyi, hesap verebilirlik oluşturmayı, çok yıllık bir strateji benimsemeyi ve birden çok paydaşla stratejik iş birliğini içerecek şekilde eylem planlarına öncelik verme konularını kapsamaktadır.

Güçlü siber güvenlik yönetişimi şunlara bağlıdır:

- İşletmeyi etkileyebilecek tehditlere dayalı siber güvenlik risk istihbaratı toplama ve uzmanlar ile iş birliği yapma
- İşletmenin risk iştahı ve toleransını belirleme
- İş sürekliliğinde olası kesintilere karşı felaket kurtarma planı yapma
- Güvenlik ihlallerine anında yanıt verme
- Siber güvenlik riskleri ve tehditleri konusunda bir farkındalık kültürü oluşturma

Etkili yönetişim, açıkça tanımlanmış politikalar, ilgili araçlar, yeterli personel ve anlayışlı eğitim ile gerçekleştirilmektedir. Ayrıca farklı bakış açılarına sahip paydaşlar, yönetişimin kalitesinin güçlendirilmesine katkı sağlamaktadır. Siber güvenlik yönetişim komitesi genellikle üst yönetimi ve birinci, ikinci ve üçüncü savunma hatlarından temsilcileri içermektedir. Bu temsilcilere ek olarak sürece teknoloji ve süreç sahipleri, tedarikçiler, müşteriler, hizmet sağlayıcılar gibi potansiyel olarak kilit dış paydaşlarda katkı sağlamaktadır.

Siber güvenlik yönetişimi için iç denetim tarafından dikkate alınacak hususlar aşağıda sunulmuştur:

- Tanımlanmış roller ve sorumluluklar, açık ve stratejik amaç
- Uygun yetkilendirmeyi ve objektifliği sağlamak için raporlama hattı
- Güvenlik araçlarını dağıtma ve politikaları uygulama konusunda uzmanlık
- Aşağıdakileri içeren uygulama unsurları:
 - Risk iştahının tanımlanması ve iletilmesi.

- Siber güvenlik politikasının belirlenmesi.
- Tutarlı bir mantık ve metodolojiye dayalı olarak risk değerlendirmeleri yapılması
- İşletmenin ihtiyaçları değiştikçe sürdürülecek güvenlik izleme stratejisini uygulamak için gerekli donanıma sahip personel.
- Belirli mal veya hizmetleri üreten veya sağlayan üçüncü tarafların bağımsız siber güvenlik incelemesinin gerçekleştirilmesi
- Devam eden süreçlere ilişkin iletişim, ölçüm, raporlama ve izleme faaliyetleri.
- Olay yönetimi.
- Siber saldırı senaryoları ile ilgili iş sürekliliğinin planlanması
- Üst yönetim ve yönetim kurulunun süreçlere katılımı

Bilgi Varlıkları Envanteri

BT departmanı tüm bilgi varlıklarının güncel bir envanterini tutmalı ve işletmenin hedeflerini iletirmek ve operasyonları sürdürmek için en gerekli olanlara öncelik vermelidir. Stratejik kurumsal hedefleri ve girişimleri karşılamak için, bu varlıklar geleneksel BT genel kontrollerinden ve periyodik değerlendirmelerden daha fazlasını gerektirmektedir. Varlıkları korumak için tasarlanmış önleyici ve tespit edici kontroller, etkinliğin sürekliliğini sağlamak için sürekli olarak izlenmelidir.

İşletmenin bilgi varlıklarını değerlendirirken aşağıdakiler dikkate alınmalıdır:

Tablo 3.1. İşletmelerin Bilgi Varlıkları Değerlendirmesinde Dikkate Alması Gereken Unsurlar

Veri	İşlemsel veriler, BT yapılandırmasına ilişkin veriler, yapılandırılmamış veriler
	Sınıflandırma (standardizasyon ve önceliklendirme sağlamak amacıyla)
	Ortamlar (ör. veri ambarları, temel veri tabanları)
Teknoloji varlıklarının altyapı deposu	Sunucular
	Ağ Cihazları

	Depolama Alanları
	Son kullanıcı cihazları (ör. dizüstü bilgisayarlar, mobil cihazlar)
Uygulamalar	
Dış İlişkiler	Üçüncü taraflara ait ortamlar
	Veri dosyalarının harici kuruluşlarla paylaşılması (ör. satıcılar, düzenleyici kurumlar, hükümetler)

Kaynak: IIA, 2016

Ağlarda yer alan hangi yazılım ve cihazların etkileşimde bulunduğunu belirleme yeteneği, siber tehditlere karşı savunma yapabilmek için çok önemlidir. İşletmeler, bilinmeyen cihazlara ve yazılımlara yönelik ağ saldırılarına karşı etkin savunma yapamamaktadır. Çalışanların şahsi cihazlarını işe getirmelerine izin veren işletmeler, kurumsal ağ üzerinden daha az güvenilir olan farklı cihaz ve yazılımların işletmenin BT sistemlerine erişimine olanak sağlamaktadır. Çalışanların sahip olduğu cihazları ve ağa bağlanabilirliği kontrol etmek, yönetimin temel odak noktası olmalıdır. Günümüzde, daha fazla çalışanın günün her saatinde organizasyonel bilgilere daha fazla erişilebilirliğe sahip olması gerekmektedir. Bilinmeyen cihazları tespit etme, doğrulama ve envanterini alma yeteneği, işletmenin genel siber güvenlik stratejisinin etkili olmasını sağlamak için bu cihazlardaki değişiklikleri izlemesine, izlemesine ve ölçmesine olanak tanımaktadır.

Bilgi Güvenliği Varlıkları bileşeni kapsamında iç denetim tarafından dikkate alınacak hususlar aşağıda sunulmuştur:

Veri envanteri: İşletme, organizasyonun içinden veya dışından kritik ve hassas verilerin türlerini ve yerini belirlemeli ve sınıflandırmalıdır.

Yetkili ve yetkisiz cihaz envanteri: Yetkili donanım cihazları ağa erişmelidir ve bulunan yetkisiz cihazlar kaldırılmalıdır.

- İşletme ağındaki yetkisiz cihazların sayısı belirlenmelidir ve yetkisiz cihazların ağdan kaldırılması için geçen ortalama süreyi izlenmelidir.
- İşletmenin ağına erişmek için kullanıcı kimlik doğrulamasını kullanmayan sistemlerin yüzdesi belirlenmelidir.

- Ağ cihazlarının, sunucuların ve son kullanıcı cihazlarının güncel bir listesi tutulmalıdır.

Yetkili ve yetkisiz yazılım envanteri: Ağda yalnızca yetkili yazılımların kurulduğundan / yürütüldüğünden ve yetkisiz yazılımların kurulmasının önleendiğinden emin olunmalıdır. Yetkisiz yazılım tespit edilirse, zamanında kaldırılmalıdır. Aşağıda yer alan hususlar sürekli olarak izlenmelidir:

- Ağdaki yetkisiz yazılım örneklerinin sayısı ve yetkisiz yazılımın ağdan kaldırılması için geçen ortalama süre.
- Beyaz liste / kara liste yazılımı çalıştırmayan işletme sistemlerinin yüzdesi.
- İşletmenin beyaz listeye / kara listeye alma yazılımı tarafından engellenen yazılım uygulamalarının sayısı.
- Güçlendirilmiş sistemlerin yüzdesi.

Standart Güvenlik Yapılandırmaları

Merkezi, otomatikleştirilmiş konfigürasyon yönetimi yazılımı, cihazlar, işletim sistemleri ve uygulama yazılımları için temeller oluşturmak ve sürdürmek için kullanılabilir. Yeni tehdit türleri kullanılabilir hale geldikçe güvenli yapılandırmaların güncel kalmasını sağlamak için gerekli yamaları uygulama süreçlerinin yanı sıra yazılım ve donanım güncellemelerine de ihtiyaç vardır.

Standart Güvenlik Yapılandırmaları bileşeni kapsamında iç denetim tarafından dikkate alınacak hususlar aşağıda sunulmuştur:

Mobil cihazlarda, dizüstü bilgisayarlarda, iş istasyonlarında ve sunucularda donanım ve yazılım için güvenli yapılandırmalar: Güvenlik yapılandırmaları oluşturulmalı, uygulanmalı ve aktif olarak yönetilmelidir. Aşağıda yer alan hususlar sürekli olarak izlenmelidir:

- Onaylı yapılandırma standardına göre yapılandırılmamış işletme sistemlerinin yüzdesi.
- İşletmenin, teknik yapılandırma yönetimi uygulamaları tarafından zorunlu kılınmayan güvenlik yapılandırmasına sahip sistemlerinin yüzdesi.

- Mevcut işletim sistemi yazılımı güvenlik yamalarıyla güncel olmayan işletme sistemlerinin yüzdesi.
- Mevcut iş yazılımı uygulama güvenlik yamalarıyla güncel olmayan işletme sistemlerinin yüzdesi.

Güvenlik duvarları, yönlendiriciler ve anahtarlar gibi ağ cihazları için güvenli yapılandırmalar: Güvenlik yapılandırmaları oluşturulmalı, uygulanmalı ve aktif olarak yönetilmelidir. Aşağıda yer alan hususlar sürekli olarak izlenmelidir:

- Ağ sistemindeki yapılandırma değişikliklerinin hacmi ve sıklığı.
- Yönetimi yetkisiz yapılandırma değişiklikleri konusunda uyarmak için ortalama süre ve ağdaki değişiklikleri engellemek / karantinaya almak için ortalama süre.

Bilgi Erişim Yönetimi

İşletme yönetimi, işletme içi rollere ve sorumlulukları dikkate alarak kullanıcılara erişim sağlamak için önceden belirlenmiş süreç ve politikalara sahip olmalıdır. Buna ek olarak, çalışanların işletme içinde ne zaman hareket ettiğini tespit etmeye yönelik bir süreçler oluşturulması, kullanıcı erişiminin ayarlanmasını ve erişimlerin kullanıcıların görevleriyle alakalı olmasını sağlamaya yardımcı olacaktır. İç denetim faaliyeti, erişim seviyelerinin mevcut roller için doğru şekilde gerekçelendirildiğini doğrulamak için kilit verilere ve sistemlere erişimleri gözden geçirmelidir.

Ayrıcalıklı yönetim erişimi siber güvenlik açısından hayati öneme sahiptir. Çünkü, bilgiye erişme ve bilgi yayınlama becerisine sahip kullanıcılar, siber güvenlik riskine en çok duyarlı olanlardır. Kullanıcılar, kimlik avı girişimlerinin bir sonucu olarak yanlışlıkla şifrelerini ifşa ederek veya kötü amaçlı yazılım yükleyerek, yetkisiz erişimi önlemek için tasarlanmış sistematik kontrol katmanlarının aşılmasına sebebiyet verebilmektedir. Erişim izni vermek ve iptal etmek için önleyici kontrol faaliyetlerini doğrulamak ve ayrıcalıklı erişime sahip kullanıcıların duyarlılıklarını ve davranışlarını değerlendirmek, işletmenin siber güvenlik programının etkinliğinin en önemli göstergesidir.

Bilgi Erişim Yönetimi bileşeni kapsamında iç denetim tarafından dikkate alınacak hususlar aşağıda sunulmuştur:

Yönetici ayrıcalıklarının kontrollü kullanımı: Bilgisayarlarda, ağlarda ve uygulamalarda tanımlanan yönetici ayrıcalıklarının kullanımı, ataması ve yapılandırması izlenmelidir.

Hesap izleme ve kontrolü: Sistem ve uygulama hesaplarının yaşam döngüsü yönetilmelidir (oluşturma, kullanım, uyku hali ve silme).

Gizli bilginin ilgili görevli/yönetici tarafından mutlaka bilinmesi durumunda kontrollü erişim: Kritik varlıklara (ör. Bilgiler, kaynaklar, sistemler) güvenli erişimi izlenmeli, kontrol edilmeli, gerekirse önlenmeli ve düzeltilmelidir.

Kullanıcıların sayısı: Kullanıcı erişim süreçleri, dahili ve harici kullanıcılar dahil olmak üzere kritik verilere erişimi olan tüm kişileri kapsamalıdır. Çoğu işletmenin, verilere dahili ve harici olarak erişen çalışanları, danışmanları ve tedarikçileri bulunmaktadır. Dosya aktarımlarının gönderildiği üçüncü taraflar da süreçlere dahil edilmelidir.

Hızlı Yanıt Düzeltme

İşletmenin riskleri hızlı ve zamanında belirleme ve önleme yeteneği, siber güvenlik programının etkinliğini ve olgunluk düzeyini göstermektedir. Olgun programlar, yönetimin siber olaylara müdahale süresini sürekli olarak kısaltmaktadır. İkinci savunma hattının konuya ilişkin görev ve sorumlulukları aşağıdaki gibidir:

- Önemli riskleri yönetime iletmek
- İyileştirme yapmak
- Belirlenen sorunları, sorunlar çözülene kadar için takip etmek
- Siber varlıklara ilişkin çözüm raporu hazırlamak

Hızlı yanıt verme bileşeni kapsamında iç denetim tarafından dikkate alınacak hususlar aşağıda sunulmuştur:

- Siber güvenlik programının sürekli iyileştirilmesi
- Güvenlik açıklarının değerlendirilmesi, tehdit istihbaratının analiz edilmesi ve boşlukların belirlenmesi
- Performans ölçümleri, sektör karşılaştırmaları ve benzer işletmeler ile karşılaştırılmaların yapılması

- Programı desteklemek için gereken belirli bilgi, beceri ve yetenekleri belirlenmesi

Aşağıda bazı ölçüm örnekleri listelenmiştir:

- Konum / departman / çalışanlara göre sürekli iyileştirmenin miktarı ve yüzdesi.
- Konum / departman / çalışanlara göre BT güvenlik açıklarının ve politika istisnalarının sayısı.
- Konum / departmana göre platform uyumluluk puanları

Sürekli İzleme

Bu çerçevenin son bileşeni olan sürekli izleme; yukarıda açıklanan beş bileşenin her birinin sürekli denetimi, riskin nasıl yönetildiğini ve düzeltici faaliyetin ne kadar iyi işlediğini belirlemeye yardımcı olmaktadır

Bu bileşen kapsamında ikinci savunma hattından, aşağıdakileri içeren bir izleme stratejisi uygulaması beklenmektedir:

İlgili siber güvenlik riskini ölçmek için hassas bilgilere erişimi olan kişilerin izlenmesini içeren bir değerlendirme ve tarama yapılmalıdır.

Güvenlik açığı değerlendirmesi: Ortamdaki güvenlik açıklarını belirlemek için sistemlerin düzenli olarak taranması çok önemlidir. Güvenlik açıkları belirlendikten, sınıflandırıldıktan sonra tespit edilen güvenlik açıkları için iyileştirme faaliyetleri başlatılmalıdır.

Dışarıdan hizmet olarak alınan sistemler genellikle işletmeler için en yüksek riskleri oluşturmaktadır; Birinci ve ikinci hat kaynakları, SLA'ları tanımlamak ve üzerinde anlaşmak için işletme genelinde çalışmalı ve iç denetim, yönetimin tanımlanan SLA'lara uyup uymadığını değerlendirmelidir.

Üçüncü taraf risk değerlendirmeleri ve izleme: Programlar, üçüncü tarafların risklerini ve sağlanan hizmetlere bağlı olarak işletmeye yönelik güvenlik riski düzeyini değerlendirmeye yardımcı olacak şekilde tasarlanmalıdır.

Sızma testi: İkinci savunma hattı, önleyici teknik kontrollerin yanı sıra yönetimin saldırıları tespit etme ve bunlara yanıt verme becerisini değerlendirmek için

bilinen güvenlik açıkları için sızma testi yapılmalıdır. Sızma testleri, işletmenin yetenekleri ve gerçek dünyadaki siber saldırı durumlarına yanıt verme konusunda daha güvenilir ve objektif bir değerlendirme sağlamak için önceden duyurulmamış bileşenler içermelidir. Ancak, testlerin kapsamı makul olmalı, operasyonları aksatmamalı ve önceden ilgili yöneticiler tarafından onaylanmalıdır. Örneğin, ağın kötü niyetle kesintiye uğraması olan hizmet reddi saldırı senaryosunun test edilmesi, normal operasyonları aksatmamak için koordine edilmelidir.

Kötü amaçlı yazılım: Kötü amaçlı yazılım riskine karşı cihazları ve ürünleri düzenli olarak taramak, güvenlik açıklarını ve yama sistemlerini öncelik sırasına göre tanımlamak için süreçler tasarlanmalıdır.

Olay izleme ve yanıt: Bu süreç, işletmenin ihlalleri tespit etmesine, ihlallere müdahale etmesine, oluşan aksaklıkları düzeltmesine, süreçleri kurtarmasına ve yönetime rapor etmesine olanak tanımaktadır. Olayları kaydetme ve izleme teknolojilerinin yanı sıra yüksek eğitilmiş bir müdahale ekibi, bu kontrollerin hedeflere ulaşmada başarılı olmasını sağlamak için gereklidir.

İş dünyası ve faaliyette bulunan sektörlerde bulunan siber güvenlik risklerinin yanı sıra benzer işletmeler tarafından yaşanan olaylar, devam eden izleme stratejisinde zaman içinde ayarlamalar yapılmasını gerektirmektedir.

Sürekli izleme bileşeni kapsamında iç denetim tarafından dikkate alınacak hususlar aşağıda sunulmuştur:

Kötü amaçlı yazılımlara karşı savunma: Kötü amaçlı kodun yüklenmesi, yayılması ve yürütülmesi süreçleri kontrol edilmelidir. Savunma hızla güncellenmelidir, kötü amaçlı yazılımlara ilişkin veriler toplanmalı ve düzeltici eylemlerde bulunulmalıdır.

Ağ bağlantı noktalarının, protokollerin ve hizmetlerin sınırlandırılması ve kontrolü:

Ağ cihazlarında bağlantı noktalarının, protokollerin ve hizmetlerin operasyonel kullanımı sürekli olarak izlenmeli ve gerek duyulduğu takdirde düzeltilmelidir.

Uygulama yazılımı güvenliği: İşletme içi geliştirilen ve edinilen tüm yazılımların güvenlik zafiyetleri tespit edilmeli ve zafiyetler giderilmelidir.

Kablosuz erişim kontrolü: Kablosuz LAN'ların, erişim noktalarının ve kablosuz istemci sistemlerinin kullanımını izlenmeli ve gerekirse ilgili düzeltmeler yapılmalıdır.

Sınır güvenliği: Farklı güven seviyelerine sahip ağları aktaran bilgi akışı tespit edilmeli ve önlenmelidir.

Sızma testleri, kimlik avı testleri ve kırmızı takım egzersizleri: İşletmenin savunmasının (teknoloji, süreçler ve insanlar) genel gücü test edilmelidir.

Veri koruma / veri kaybını önleme: Veri hırsızlığının etkileri minimize edilmelidir; verilerin gizlilik ve bütünlüğü sağlamaya yardımcı araçlar uygulamaya koyulmalıdır.

DÖRDÜNCÜ BÖLÜM

BORSA İSTANBUL'DA FAALİYET GÖSTEREN İŞLETMELERİN SİBER GÜVENLİK FAALİYETLERİ SEVİYELERİNİN BELİRLENMESİ VE İÇ DENETİM BİRİMLERİNİN SİBER GÜVENLİK FAALİYETİNE ETKİSİNİN TESPİTİNE YÖNELİK BİR ARAŞTIRMA

Bu bölümün ilk kısmında, iç denetim ve siber güvenlik ile ilgili literatürde yer alan önceki çalışmaların kapsamına, amacına ve sonuçlarına yer verilmiştir. Çalışmalar öncelikle yayın tarihine göre listelenmiş ve açıklanmıştır. Daha sonra; araştırmanın amacı ve önemi, araştırmanın kapsamı, araştırmanın metodolojisi, araştırmanın sonuçlarıyla ilgili analiz ve bulgular, çalışmanın sonuçları ve öneriler başlıklarına yer verilmiştir.

4.1. Konuya İlişkin Literatür İncelemesi

Siber güvenlik ve iç denetim konularında yapılan akademik çalışmalar aşağıdaki bölümlerde sunulmuştur.

4.1.1. İç Denetim ve Siber Güvenlik

İç denetim ve siber güvenlik konularında yapılan çalışmalar, yayın tarihi sırasına göre gruplandırılarak sonuçları ile birlikte Tablo 4.1.'de özetlenmiştir.

Tablo 4.1. İç Denetim ve Siber Güvenlik Literatür İncelemesi

Yazar(lar)	Araştırmanın İsmi	Araştırmanın Türü
Lainhart, 2000	COBITTM: A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities	Araştırma Notu
Pathak, 2005	Risk management, internal controls and organizational vulnerabilities	Araştırma Notu

Wallace ve ark., 2011	Information security and Sarbanes-Oxley compliance	Keşifsel Araştırma
Li ve ark., 2012	The consequences of information technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports	Ampirik Araştırma-Regresyon Analizi
Steinbart ve ark., 2012	The relationship between internal audit and information security	Keşifsel Araştırma
Steinbart ve ark., 2013	Information-security professionals' perceptions about the relationship between the information security and IAFs	Ampirik Araştırma-En Küçük Kareler Yöntemi
Steinbart ve ark., 2015	SECURQUAL: An Instrument for Evaluating the Effectiveness of Enterprise Information Security Programs	Ampirik Araştırma-Faktör Analizi
Kurnaz ve Dindaroğlu, 2015	İç Denetim ve Bilgi Güvenliği İlişkisi: Bölgesel Bir Araştırma	Ampirik Araştırma
Rahimian ve ark., 2016	Estimation of deficiency risk and prioritization of information-security controls	Ampirik Araştırma-Tasarım Bilimi
Gyun No ve Vasarhelyi, 2017	Cybersecurity and Continuous Assurance	Araştırma Notu

Uludağ, 2017	Değişen Risk Algısı ve İç Denetim	Araştırma Notu
İslam ve ark., 2018	Factors associated with security/cybersecurity audit by IAF: An international study	Ampirik Araştırma-Regresyon Analizi
Kahyaoğlu ve Çaliyurt, 2018	Cyber security assurance process from the internal audit perspective	Kavramsal Araştırma
Stafford et al., 2018	The role of internal audit and user training in information-security policy compliance	Vak'a Analizi
Steinbart ve ark., 2018	The influence of a good relationship between the internal audit and information-security functions on information security outcomes	Ampirik Araştırma-Regresyon Analizi
Sabuncu, 2018	İç Denetim Anlayışındaki Değişiklikler ve Gelişmeler	Araştırma Notu
Mollaoğulları ve Özdoğan, 2018	İletişim Teknolojilerindeki Gelişmeler, Riskler ve İç Denetimin Rolü	Araştırma Notu
Güler ve Arkin, 2019	Siber Hijyenin Sağlanmasında İç Denetimin Rolü	Araştırma Notu
Öztürk, 2019	Siber Saldırıları, Siber Güvenlik Denetimleri ve Bütüncül Bir Denetim Modeli Önerisi	Analitik Araştırma
Selimoğlu ve Altunel, 2019	Siber Güvenlik Risklerinden Korunmada Köprü ve Katalizör Olarak İç Denetim	Araştırma Notu

Selimoğlu ve Saldı, 2019	İşletmelerde Siber Risklerin Analizinde, Haritalanmasında ve Değerlendirilmesinde İç Denetimin Rolü	Araştırma Notu
Akmeşe, 2020	Kamuda Dijital Dönüşümün Siber Güvenlik ve Dijital Güvence Boyutları ve İç Denetimin Rolü	Araştırma Notu
Bircan, 2020	İç Denetimde Yapısal Değişim ve Dönüşüm: İç Denetçilerin Farkındalığı ve Beklentileri Üzerine Bir Araştırma	Ampirik Araştırma

Lainhart (2000) çalışmasında COBIT çerçevesi ve BT denetimi konularını ele almış, küresel bilgi toplumunda bilginin etkin yönetiminin önemine dikkat çekmiştir.

Pathak (2005), çalışmasında teknolojik gelişmelerin işletmelerin iç kontrol sistemleri üzerindeki etkilerini açıklamış, kritik altyapılara yönelik siber saldırıların ve fiziksel saldırıların işletmeler için gerçek bir tehdit olduğunu, ancak böyle bir tehdide karşı kapsamlı bir savunma sağlamak için çok az şey yapıldığını savunmuştur.

Wallace ark. (2011), çalışmalarında ISO 17799 güvenlik çerçevesi tarafından önerilen Bilgi Teknolojisi (BT) kontrollerinin işletmelerin iç kontrol ortamlarına ne ölçüde entegre edildiğini incelemişlerdir. Araştırma sonuçları, BT kontrolleri ve bu kontrollerin uygulanma biçimlerinin işletmelerin özelliklerine göre farklılık gösterdiğini ortaya koymuştur.

Li ve ark. (2012), bilgi teknolojisi zayıflıklarını; veri işleme bütünlüğü, sistem erişimi ve güvenliği, sistem yapısı ve kullanımı olmak üzere 3 farklı boyutta ele almışlardır. Yazarlar, veri işleme bütünlüğü ile BT kontrol zayıflıkları için arasında güçlü bir ilişki olduğunu tespit etmişlerdir.

Steinbart ve ark. (2012), çalışmalarında işletmelerde iç denetim ve bilgi güvenliği birimlerinin iş birliği içerisinde olması gerektiğini belirtmişlerdir. Çalışmada iç denetim ve bilgi güvenliği arasındaki ilişkinin kalitesinin tespitine yönelik bir model önerisinde bulunulmuştur.

Steinbart ve ark. (2013), bilgi güvenliği çalışanlarının algılarını ölçtükleri çalışmalarında; iç denetçilerin sahip olduğu BT uzmanlık düzeyi ile bilgi güvenliği ve iç denetim departmanları arasındaki ilişkinin kalitesi arasında anlamlı bir ilişki olduğu sonucuna ulaşmışlardır.

Steinbart ve ark. (2015), COBIT 4.1 olgunluk modeli rubrikleri kullanarak geliştirdikleri SECURQUAL modeli puanlarının bilgi güvenliği programının etkinliğinin nesnel önlemlerini güvenilir bir şekilde tahmin ettiğini ispat etmişlerdir.

Kurnaz ve Dindaroğlu (2015), çalışmada, iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkiyi etkileyen faktörleri belirlemeyi amaçlamışlardır. Araştırma sonucunda iç denetçiler ile bilgi güvenliğinden sorumlu uzmanlar arasındaki ilişkiyi etkileyen unsurlar, iç denetçinin sahip olduğu kişisel ve mesleki özellikler, örgüt yapısı, iç denetim ve bilgi işlem departmanlarının fiziksel konumları olarak belirlenmiştir.

Rahimian ve ark. (2016), tasarım bilimi¹ yaklaşımını kullanarak, işletme verilerinin güvenlik seviyelerini sınıflandırmak için bir model önerisinde bulunmuşlardır. Araştırma sonuçları, OPL (Operational, Public Image, Legal) modelinin siber güvenlik bağlamında tüm kurumsal verilerin ayrıntılı bir risk değerlendirmesini oluşturmak için kullanılabileceğini göstermektedir.

Gyun No ve Vasarhelyi (2017), çalışmalarında siber güvenlik alanında güvence konusunda yeni yaklaşımlara duyulan ihtiyacı ele almışlardır.

Uludağ (2017), çalışmasında riske ilişkin değişen algıyı, iç denetim perspektifiyle değerlendirmiştir.

İslam ve ark. (2018), çalışmalarında iç denetim birimi tarafından gerçekleştirilen siber güvenlik denetiminin kapsamına ilişkin faktörleri incelemiştir. Yazarlar, siber güvenlik denetiminin kapsamının, iç denetim biriminin yönetim, risk ve kontrol konularında yetkinliği ile önemli ve olumlu bir şekilde ilişkili olduğunu tespit etmişlerdir.

¹ Tasarım bilimi, araştırma projelerinde değerlendirme ve yineleme için özel yönergeler sunan, sonuca dayalı bir bilgi teknolojisi araştırma metodolojisidir. Tasarım bilimi araştırması, yapay nesnenin işlevsel performansını iyileştirme niyetiyle yapay nesnelerin geliştirilmesi ve performansına odaklanır.

Kahyaoğlu ve Çalıyurt (2018), çalışmalarında, siber risk yönetimi aşamasında siber kontrollerle ilgili resmi dokümantasyonun sürdürülmesinin çok önemli olduğunu belirtmişlerdir. İç denetimin siber güvenlik güvence sürecinin ayrılmaz bir parçası olması gerektiğini savunmuşlardır.

Stafford ve ark. (2018), çalışmalarında bilgi sistemleri denetiminin işletmelerin siber güvenlik politikaları ve kurumsal risk yönetiminde aldığı rolü incelemişlerdir. Çalışma kapsamında denetçilerle derinlemesine görüşmeler yapılmıştır. Bulgular, kurumsal risk yönetiminin siber güvenlik denetimlerinden fayda sağladığını göstermiştir.

Steinbart ve ark. (2018), iç denetim ve bilgi güvenliği birimleri arasındaki ilişkinin kalitesinin, işletmelerin bilgi güvenliği çabalarının genel etkinliğini nasıl etkilediğini araştırmışlardır. Bu ilişkinin kalitesi, rapor edilen iç kontrol zafiyetleri ve gerçekleşen siber güvenlik olayları üzerinde anlamlı bir etkiye sahiptir.

Sabuncu (2018), çalışmasında iç denetimin günümüzdeki görünümü ve ülkemizdeki mevcut durumunu değerlendirmiş ve geleceğe yönelik birtakım öngörülerde bulunmuştur.

Mollaoğulları ve Özdoğan (2018), çalışmalarında gelişen bilgi teknolojisinin işletmelere getirdiği riskleri tanımlamış ve iç denetimin bu riskleri nasıl yöneteceği ve yeni duruma nasıl uyum sağlaması gerektiğini değerlendirmişlerdir.

Güler ve Arkın (2019) çalışmalarında, siber güvenlik ve siber hijyen bağlamında iç denetçilerin ve iç denetimin siber güvenlik süreçlerindeki rolünü değerlendirmişlerdir.

Öztürk (2019) çalışmasında, siber güvenlik denetimindeki tüm süreçlerin bütüncül bir biçimde ele alındığı bir model geliştirmiştir. Yazar tarafından geliştirilen model, siber güvenliğe ve denetime etki eden iç ve dış faktörler ile denetimin planlamasından itibaren denetim raporu ve güvenceye kadar geçen tüm süreci kapsamaktadır.

Selimoğlu ve Altunel (2019) çalışmalarında siber riskler ve siber risklerin yönetilmesine ilişkin bilgi vermişler ve siber güvenliğin sağlamasında iç denetimin rolünü açıklamışlardır.

Selimoğlu ve Saldı (2019) çalışmalarında, iç denetim perspektifinden siber risklerin analiz edilmesi, haritalanması ve değerlendirilmesi için hangi tekniklerin nasıl uygulanacağı ve kullanılacağı konularını ele almışlardır. Yazarlar, işletmelerde hangi tip siber risklerle karşılaşılabilir ve bunlara nasıl önlem alınacağı üzerine detaylı incelemeler yaparak, iç denetimin siber risklerin kontrolünde üstlenebileceği görevleri açıklamışlardır.

Akmeşe (2020) çalışmasında kamu sektörünün içerisinde olduğu dijital dönüşüm yolculuğunun temel bileşenlerini açıklamış ve iç denetimin siber güvenlik ve dijital güvence alanında organizasyonlara sağlayacağı katkıları değerlendirmiştir.

Bircan (2020), çalışmasında gelişen bilgi teknolojilerindeki gelişmelere paralel olarak iç denetimin değişen rolü, değişen iç denetim faaliyetleri ve değişen iç denetçi profilleri ve iç denetimde meydana gelen yapısal değişimi ve dönüşümü açıklanmıştır.

4.1.2. Bilgi Paylaşımı ve Siber Güvenlik

Bilgi paylaşımı ve siber güvenlik konularında yapılan çalışmalar, yayın tarihi sırasına göre gruplandırılarak sonuçları ile birlikte Tablo 4.2.'de özetlenmiştir.

Tablo 4.2. Bilgi Paylaşımı ve Siber Güvenlik Literatür İncelemesi

Yazar(lar)	Araştırmanın İsmi	Araştırmanın Türü
Gordon ve ark., 2003	Sharing information on computer systems security: An economic analysis.	Analitik Araştırma
Gansler ve Lucyshyn, 2005	Improving the security of financial management systems: What are we to do?	Araştırma Notu
Hausken, 2007	Information sharing among firms and cyberattacks	Analitik Araştırma

Gordon ve ark., 2015	The impact of information sharing on cybersecurity underinvestment: A real options perspective	Araştırma Notu

Gordon ve ark., (2003) çalışmalarında bilgi sistemleri güvenliğine ilişkin bilgilerin paylaşılmasının, ekonomik etkilerini incelemek için bir model sunmaktadır. Yazarlar, çalışmanın sonucunda güvenlik ihlalleri ile ilgili bilgi paylaşımının bilgi güvenliği seviyesini arttıracığı sonucuna ulaşmışlardır.

Gansler ve Lucyshyn (2005) çalışmalarında bilgi güvenliğinin sağlanmasında yaşanan zorlukları sıralamış ve bilgi güvenliğini sağlamak için atılacak adımları belirlemişlerdir. İşletmelerin siber saldırılardan kaçınmak için bir siber güvenlik programına sahip olması gerektiğini savunmuşlardır.

Hausken (2007), çalışmasında firmalar arası bilgi paylaşımları ve siber güvenlik yatırımlarının ilişiklisini tespit edecek bir model geliştirmiştir. Hausken, çalışmanın sonucunda bilgi paylaşımı ve güvenlik yatırımlarının maliyet ve faydalarının değerlendirilmesinin rekabet avantajı elde etmek için diğer stratejilerle bağlantılı olduğunu öne sürmüştür.

Gordon ve ark. (2015), çalışmalarında bilgi paylaşımının siber güvenlik yatırımlarına ve uygulamalarına etkisini açıklamışlardır. Gordon ve ark., siber güvenlik yatırımlarının, işletmelerin dış ve iç finansal raporlarının bütünlüğünü ve stratejik mülkiyet bilgilerini korumak için çok önemli olduğunu ifade etmişlerdir.

4.1.3. Siber Güvenlik Yatırımları

Siber güvenlik yatırımları konusunda yapılan çalışmalar, yayın tarihi sırasına göre gruplandırılarak sonuçları ile birlikte Tablo 4.3.'te özetlenmiştir.

Tablo 4.3. Siber Güvenlik Yatırımları Literatür İncelemesi

Yazar(lar)	Araştırmanın İsmi	Araştırmanın Türü
Gordon ve Loeb, 2002	The economics of information-security investment	Analitik Araştırma
Tanaka ve ark., 2005	Vulnerability and information-security investment: An empirical analysis of E-local government in Japan	Ampirik Araştırma-Regresyon Analizi
Hausken, 2006	Income, interdependence, and substitution effects affecting incentives for security investment	Analitik Araştırma
Gordon ve ark., 2008	Cybersecurity, Capital Allocations and Management Control Systems	Analitik Araştırma
Bose ve Luo, 2014	Investigating security investment impact on firm performance	Kavramsal Araştırma
Gordon ve ark., 2015	Externalities and the Magnitude of Cybersecurity Underinvestment by Private Sector Firms: A Modification of the Gordon–Loeb Model	Analitik Araştırma

Gordon ve Loeb (2002) çalışmalarında siber güvenliğe yatırım yapmak için en uygun miktarı belirleyen bir ekonomik model oluşturmayı amaçlamışlardır. Gordon-Loeb Modeline dayalı olarak bulgular, işletmelerin bilgi varlıklarını korumak için harcaması gereken miktarın genellikle beklenen kaybın sadece küçük bir kısmı olduğunu ortaya koymuştur.

Tanaka ve ark. (2005), Gordon-Loeb modelini kullanarak siber güvenlik yatırımı kararları ile işletmelerin siber güvenlik zafiyetlerinin bağlantılı olduğunu tespit etmişlerdir. Bulguları Gordon ve Loeb (2002) modelinin görüşlerini desteklemiştir.

Hausken (2006), çalışmasında işletmelerin siber güvenlik yatırımları yapmaya teşvik eden faktörleri incelemiştir. Çalışma sonucunda işletmelerin, güvenlik yatırımlarının getiri oranının siber saldırı maliyetlerini aşması durumunda veya yasal otoritelerin yatırımları zorunlu kılması durumunda, siber güvenlik yatırımları yaptıkları belirlenmiştir.

Gordon ve ark., (2008) çalışmalarında, yönetim kontrol sistemlerinin siber güvenlik ortamında ortaya çıkan problemlerle olan ilişkisini araştırmaktadır. Araştırma sonucunda yönetim kontrol sistemlerinin tasarımının ve kullanımının siber güvenlik sorunlarıyla başa çıkmada önemli bir faktör olduğu belirlenmiştir.

Bose ve Luo (2014), çalışmalarında bir işletmenin performansını etkileyen faktörleri belirlemek için BT ile ilgili ve BT ile ilgili olmayan güvenlik yatırım faktörlerinin kullanıldığı kapsamlı bir kavramsal çerçeve geliştirmişlerdir.

Gordon ve ark., (2015) uygun siber güvenlik yatırımı düzeyine karar vermede kullanılan Gordon – Loeb Modeline dışsallık değişkenini de dahil etmişlerdir. Analiz sonuçları, işletmelerin siber güvenliğe olan sosyal optimal yatırımının, beklenen dışsallık kaybının %37'sinden fazla olmadığını göstermektedir.

4.1.4. Siber Güvenlik Faaliyetlerine İlişkin Bilgilerin Açıklanması

Siber güvenlik faaliyetlerine ilişkin bilgilerin açıklanması konusunda yapılan çalışmalar, yayın tarihi sırasına göre gruplandırılarak sonuçları ile birlikte Tablo 4.4.'te özetlenmiştir.

Tablo 4.4. Siber Güvenlik Faaliyetleri Bilgilerinin Açıklanmasına Yönelik Literatür İncelemesi

Yazar(lar)	Araştırmanın İsmi	Araştırmanın Türü
Gordon ve ark., 2006	The impact of the Sarbanes-Oxley (SOX) Act on the corporate disclosures of information-security activities	Ampirik Araştırma-Regresyon Analizi
Gordon ve ark., 2010	Market value of voluntary disclosures concerning information security	Ampirik Araştırma-Regresyon Analizi
Li ve ark., 2018	SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors	Ampirik Araştırma-Regresyon Analizi
Ettredge ve ark., 2018	Trade Secrets and Cybersecurity Breaches	Ampirik Araştırma-Regresyon Analizi

Gordon ve ark. (2006), çalışmalarında, Sarbanes-Oxley yasasının (SOX) şirketlerin bilgi güvenliği açıklamaları üzerindeki etkisini araştırmışlardır. Sonuçlar, SOX'un gönüllü açıklama üzerinde olumlu bir etkisi olduğunu ortaya koymaktadır. Yazarlar, kurumsal bilgi güvenliği açıklamalarının SOX'un yürürlüğe girmesinden sonra artış gösterdiğini tespit etmişlerdir.

Gordon ve ark. (2010) çalışmalarında, bilgi güvenliği ile ilgili gönüllü açıklamaların piyasa değerini incelemeyi amaçlamışlardır. Bulgular, bilgi güvenliği ile ilgili faaliyetlerin gönüllü olarak açıklanmasının işletmelerin piyasa değeri ile olumlu bir şekilde ilişkili olduğunu ortaya koymaktadır.

Li ve ark. (2018) siber güvenlik riski açıklamasının gelecekteki siber güvenlik olayları için yeteri kadar bilgilendirici olup olmadığını araştırmıştır. Yazarlar, siber güvenlik risklerinin açıklanma süresinin, gelecekte meydana gelmesi muhtemel siber güvenlik olaylarıyla olumlu bir şekilde ilişkili olduğunu tespit etmişlerdir.

Ettredge ve ark. (2018) çalışmalarında işletmelerin yıllık raporlarında yer alan ticari sırlara yönelik açıklamaları ile maruz kalınan siber saldırı sıklığı arasındaki ilişkiyi incelemişlerdir. Çalışmanın bulguları, ticari sırların varlığından bahseden işletmelerin, konu ile ilgili açıklama yapmayan işletmelerden daha fazla saldırıya maruz kaldıklarını göstermiştir.

4.1.5. Güvenlik Tehditleri ve Güvenlik İhlalleri

Güvenlik tehditleri ve güvenlik ihlalleri konularında yapılan çalışmalar, yayın tarihi sırasına göre gruplandırılarak sonuçları ile birlikte Tablo 4.5.'te özetlenmiştir.

Tablo 4.5. Güvenlik Tehditleri ve Güvenlik İhlalleri Literatür İncelemesi

Yazar(lar)	Araştırmanın İsmi	Araştırmanın Türü
Ettredge ve Richardson, 2002	Information Transfer among Internet Firms: The Case of Hacker Attacks	Ampirik Araştırma- Regresyon Analizi
Boritz ve No, 2005	Security in XML-based financial reporting services on the Internet	Kavramsal Araştırma
Abu-Musa, 2006	Perceived security threats of computerized accounting information systems in the Egyptian banking industry	Ampirik Araştırma- ANOVA

Kwon ve ark., 2013	The Association between Top Management Involvement and Compensation and Information Security Breaches	Ampirik Araştırma-Regresyon Analizi
Yılmaz ve ark., 2015	Bilgi Toplumuna Geçiş ve Siber Güvenlik	Araştırma Notu
Higgs ve ark., 2016	The Relationship Between Board-Level Technology Committees and Reported Security Breaches	Ampirik Araştırma-Regresyon Analizi
Carré ve ark., 2018	Ascribing responsibility for online security and data breaches	Keşifsel Araştırma
Amir ve ark., 2018	Do firms underreport Information on cyberattacks? Evidence from capital markets	Ampirik Araştırma-Regresyon Analizi

Ettredge ve Richardson (2002) çalışmalarında, 2000 yılında meydana gelen siber saldırılar sonrası internet firmalarının hisse fiyatlarının değişimine odaklanmışlardır. Yapılan analiz sonucunda meydana gelen siber saldırılar ile birlikte siber güvenlik hizmet sağlayıcısı firmaların hisseleri değer kazanırken; bu firmalar dışında kalan internet firmalarının hisse fiyatlarında düşüş meydana geldiği tespit edilmiştir.

Boritz ve No, (2005) çalışmalarında, mevcut güvenlik teknolojilerinin güvenlik tehditlerini ve kısıtlamalarını açıklamışlardır. Yazarlar ayrıca XBRL ve XARL hizmetlerinin güvenilirliğini sağlamak için dikkate alınması gereken güvenlik gereksinimlerini de belirlemişlerdir.

Abu-Musa (2006) çalışmasında bilgisayara dayalı muhasebe bilgi sistemlerinin güvenlik tehditlerine yönelik algıyı araştırmıştır. Araştırmanın örneklemini Mısır

bankacılık sektörü çalışanları oluşturmıştır. Çalışma sonucunda, çalışanlar tarafından yanlışlıkla kötü verilerin girilmesi, çalışanlar tarafından verilerin imha edilmesi, bilgisayar virüsleri, doğal ve insan yapımı felaketler, çalışanların şifrelerinin güvenliğinin sağlanamaması ve bilgilerin yetkisiz kişilere dağıtılmasının en ciddi güvenlik tehditleri olduğu tespit edilmiştir.

Kwon ve ark., (2013) çalışmalarında, bilgi teknolojisi (BT) yöneticisinin üst yönetim ekibindeki konumu ve ücretlendirilmesi ile bilgi güvenliği ihlalleri arasındaki ilişkiyi incelemişlerdir. Sonuçlar, BT yöneticisinin üst yönetim ekibine katılımının bilgi güvenliği ihlalleri ile negatif ilişkili olduğunu göstermiştir. Ayrıca ücretlendirmenin de bilgi güvenlik ihlalleri ile negatif ilişkili olduğu tespit edilmiştir.

Yılmaz ve ark., (2015) çalışmalarında Türkiye’de uygulanan bilgi toplumu stratejisi, dünyada bilgi toplumuna geçiş süreci, bilgi teknolojileriyle oluşturulan kritik altyapı sistemleri, bu sistemlere karşı siber tehditler ve bu sistemlerin risk analizi yer almıştır.

Higgs ve ark., (2016) çalışmalarında, firmaların, güvenlik ihlallerini tespit etme ve bunlara müdahale etme yeteneklerini arttırmak için teknoloji komitesi oluşturması gerektiğini savunmuşlardır. Yapılan analiz sonucunda teknoloji komitelerine sahip firmaların siber saldırıları ve ihlalleri tespit etme yeteneğinin komitesi olmayan firmalara kıyasla daha güçlü olduğu belirlenmiştir.

Carré ve ark., (2018) çalışmalarında, güvenlik ihlalleri sonucu işletmelerin itibar kaybını en aza indirmeleri için en iyi yaklaşımı açıklamaktır.

Amir ve ark., (2018) çalışmalarında firmaların siber saldırılarla ilgili gönüllü olarak açıkladıkları veriler ve ikincil kaynaklardan elde ettikleri verileri kullanarak, firmaların siber saldırılarla ilgili bilgileri ne ölçüde sakladığını tahmin etmişlerdir. Bulgular, firmaların açıkladıkları siber saldırılara karşı piyasa tepkisinin küçük olduğunu, ancak gizlenen saldırılara karşı önemli ve olumsuz tepkilerin oluştuğunu ortaya çıkarmıştır.

4.2. Araştırmanın Amacı ve Önemi

İşletmeler varlıklarını korumak için; hile yolsuzluk, casusluk, sabotaj, doğal afetler vb. tehdit ve tehlikelere karşı koymanın yanı sıra virüs, casus ve kötü yazılım, bilgisayar

korsanları gibi siber tehditlere karşı da tetikte olmak durumundadır. Bu siber saldırıları ve tehditleri ortadan kaldırmak siber güvenliği sağlamakla mümkündür.

İşletmelerin faaliyet gösterdikleri sektör, işletmenin büyüklüğü, işletmenin iş hacmi, siber tehditlere maruz kalma durumlarını belirlerken önemli bir bağlam oluşturmaktadır.

Bilgi teknolojileri ve bu teknolojilerin yarattığı uygulamalara bağımlılık ve kritik bilgilere sahip olmak işletmeleri güvenlik açısından daha riskli hale getirmektedir. Bilginin üretim, transfer depolanma ve erişim süreçlerinin karmaşık hale gelmesi denetlenmesini de zorlaştırmaktadır.

Siber güvenlikte asıl amaç; işletmelerin bilgi varlıklarının güvenliğinin makul bir seviyede sağlanmasıdır. Bu bağlamda siber güvenliği sağlanmak için işletmelerin siber risklerinin tespiti ve yönetimi önemli bir unsurdur. Bu sebeple, risklerin tespit ve minimize edilmesi için iyi bir siber güvenlik yönetimi yapılmalı, mevcut teknikler, teknolojiler, politikalar, standartlar ve çözümler uygulanarak siber güvenlik kapsamında çalışmalar yürütülmelidir.

İşletmeler içindeki risk ve kontrol işlevlerinin etkinliğini ve verimliliğini iyileştirmek için en iyi uygulama yaklaşımı, IIA tarafından Ocak 2013'te yayınlanan "Etkili Risk Yönetimi ve Kontrolünde Üç Savunma Hattı" nda sunulmuştur.

İç denetim biriminin siber güvenlikteki rolünü değerlendirmenin en önemli adımı, üçlü savunma hattının uygun şekilde oluşturulduğundan ve her bir hattın etkin bir şekilde çalıştığından emin olmaktır.

Üçlü savunma hattının son basamağında görev yapan iç denetim birimi, üst yönetim ile yönetim kuruluna yönetişim, risk yönetimi ve iç kontroller konusunda bağımsız ve objektif güvence sağlamaktadır. Ayrıca iç denetim, birinci ve ikinci savunma hatları tarafından gerçekleştirilen faaliyetlerin siber güvenlik risklerini ve tehditlerini yönetme ve önleme konusunda rol almaktadır. İç denetim biriminin faaliyetleri işletmelerin siber güvenlik fonksiyonunu doğrudan etkilemektedir ve siber güvenlik süreçlerine değer katmaktadır.

Çalışmanın asıl amacı; siber risklere duyarlı sektörlerde faaliyet gösteren halka açık işletmelerin siber güvenlik yönetimine yaklaşımları ve siber güvenlik seviyeleri ile iç denetim faaliyetinin siber güvenlik konusundaki etkinliğini belirlemektir.

İç denetim faaliyetlerinin işletmeler için arz ettiği önem çeşitli çalışmalar ile geçmiş araştırmalarda ortaya konulmuştur. Ancak iç denetim ile siber güvenlik konularını birlikte ele alan çalışmalar çok kısıtlıdır. Bu konuda yabancı literatürde çeşitli çalışmalar bulunmaktadır. Şubat 2021 tarihi itibarıyla Türkiye’de YÖK tez merkezinde kayıtlı, “iç denetim ve siber güvenlik” konusunda yüksek lisans ve doktora tezi bulunmamaktadır. Bu açıdan bakıldığında çalışmanın iç denetim literatürüne yeni ve farklı bir bakış açısı kazandırması beklenmektedir.

4.3. Araştırmanın Kapsamı

İşletmelerin siber güvenlik faaliyetleri, işletme yönetimi, BT birimi ve iç denetim biriminin birlikte yürütmesi gereken bir süreçtir. İşletme yönetimi, verilerin, süreçlerin, risklerin ve kontrollerin sahibidir ve bunları yönetmekle yükümlüdür.

İşletme yönetiminin oluşturduğu süreçlerin ve kontrollerin varlığını ve etkin bir şekilde çalışmasını sağlamaktan sorumlu olan BT birimi siber risklere ilişkin, uygunluk, kontrol ve gözetim faaliyetlerini sürdürmektedir.

İşletmelerde yönetişim, yönetim kurulu ve üst yönetiminin sorumluluğunda iken, yönetişimin değerlendirilmesi iç denetim biriminin birincil rollerinden biridir. IIA 2110.A23 standart uyarınca iç denetim biriminin, işletmenin bilgi teknolojisi yönetişiminin işletmenin stratejilerini ve hedeflerini destekleyip desteklemediğini değerlendirmesi gerekmektedir.

Buna ek olarak iç denetim işletme yönetiminin oluşturduğu kontrollerin etkinliğini de değerlendirmektedir. Çünkü siber güvenlik süreçlerinin karmaşıklığı ve siber tehditlerin günden güne artması, saldırılar gerçekleştikçe tespit ve düzeltici eylemler gibi ek kontrol katmanları gerektirmektedir.

İç denetçiler, BT birimiyle koordinasyonlu bir biçimde hareket ederek özellikle siber güvenlik bağlamında önemli bir rol oynamaktadır. İç denetim birimi siber güvenlik

ile ilgili konularda BT birimine danışmanlık yapması süreçlerin sağlıklı bir şekilde ilerlemesi açısından önem arz etmektedir.

Ayrıca iç denetçiler siber güvenlik süreçlerinin yeterliliği ve etkinliğini gözden geçirmektedir. Bu değerlendirme yapılırken, BT biriminin belirlediği çerçeveler, standartlar, risk değerlendirmeleri ile ilgili çalışmalarının yeterliliğinin de gözden geçirilmesi gerekmektedir.

Sonuç olarak işletme yönetimi ve BT departmanı ile iletişimi ve etkileşimi göz önüne alındığında iç denetim departmanının siber güvenlik süreçlerine etkisi yadsınamayacak derecede önemlidir. Çünkü iç denetim birimi faaliyetleri ile işletme yönetimi ve BT departmanını ortak paydada buluşturmakta ve siber risklerin yönetilmesi süreçlerinde de son savunma hattını oluşturmaktadır.

Yukarıda açıklanan bilgiler ışığında bu çalışmada, Borsa İstanbul'a kote halka açık işletmelerin iç denetim birimi yöneticileri ve iç denetim çalışanları çalışmanın kapsamına dahil edilmiştir.

4.4. Araştırmanın Metodolojisi

Bu bölümde, araştırmayla ilgili veri toplama yöntemi, örnekleme süreci, araştırmanın hipotezleri, araştırmada kullanılan istatistiki yöntemler ve analiz sonuçları yer almaktadır.

4.4.1. Araştırmanın Yöntemi ve Veri Toplama

Çalışma deneysel olmayan nitel araştırma tasarımına sahiptir ve yapılaş yöntemine göre tarama modelidir. Araştırmada, örneklemden verilerin toplanması bakımından saha taraması kullanılmıştır. Örneklemden veri toplamada ise, katılımcıların görüşlerinin yazılı olarak alındığı bir veri toplama tekniği olan anket tekniği kullanılmıştır. Nicel araştırmalarda sayısal temsiliyet söz konusu olduğu için, araştırma evrenini temsil edecek örneklemin hatasız tespit edilmesi ve bu örnekleme doğru soruların sorulması önemlidir.

Anket formu denetim, iç denetim ve bilgi teknolojileri alanlarında çalışmakta olan kişilerin görüşleri de alınarak geliştirilmiş ve anketin daha anlaşılır hale getirilmesi sağlanmıştır.

Bu çalışma kapsamında işletmelerin siber güvenlik yönetimi düzeylerini belirlemek amacıyla ölçekler, Japonya Ticaret ve İnovasyon Bakanlığı'na bağlı Japonya Bilgi Teknolojileri Özendirme Ajansı'nın (IPA) Bilgi Güvenliği Yönetimi Kıyaslama Sistemi'nden (ISM Benchmark) uyarlanarak hazırlanmıştır (IPA, 2016). Ayrıca Steinbart ve ark. (2012; 2013; 2015; 2018) çalışmalarından da faydalanılmıştır. Bu araştırmada kullanılan değişkenlere ilişkin ölçek; alanında uzmanlar tarafından İngilizceden Türkçeye çevrilmiş, Türkçeleştirilen soruların geçerliliği ve güvenilirliği, alanında uzman meslek mensupları ve akademisyenler tarafından kontrol edilerek gerekli görülen düzenleme ve geliştirmeler yapılmıştır. Denetim, bilgi teknolojileri ve siber güvenlik alanında faaliyet gösteren yöneticilerin görüşleri doğrultusunda ankete son hali verilmiştir.

4.4.2. Örneklem Seçimi

Araştırma öncesinde yapılan ön görüşmelerde denetim ve bilgi teknolojileri alanlarında çalışmakta olan yöneticilerin görüşleri ve literatürde yer alan çalışmalar doğrultusunda Üretim, İnşaat, Kimya, Havacılık ve Uzay, Bankacılık, Madencilik/Metaller/Mineraller, Risk yönetimi/Sigorta, Enerji, İletişim, Medya ve Teknoloji sektörleri başta olmak üzere Borsa İstanbul'a kote şirketlerin iç denetim departmanlarında çalışan kişilere e-posta yoluyla anket uygulanmıştır.

Ampirik çalışmalarda örneklem sayının sağlam (robust) sonuçların alınmasını sağlayan bir yapıda olması, verilerin toplanma sürecinde yanlılıktan ve sistematik hatadan kaçınılması açısından önem arz eden bir durumdur.

Tablo 4.6: Örneklem Büyüklüğü Tablosu

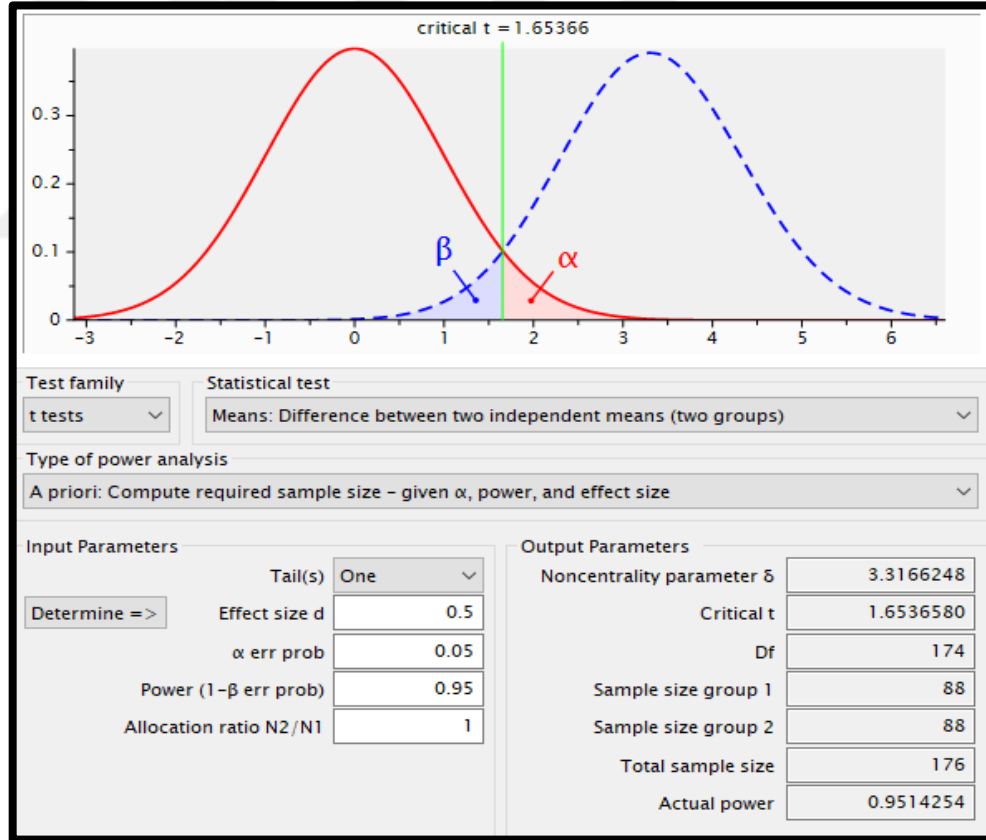
Anakütle Büyüklüğü	± 0.03 örneklem hatası (d)			± 0.05 örneklem hatası (d)			± 0.10 örneklem hatası (d)		
	p=0.5 q=0.5	p=0.8 q= 0.2	p=0.3 q=0.7	p=0.5 q=0.5	p=0.8 q= 0.2	p=0.3 q=0.7	p=0.5 q=0.5	p=0.8 q= 0.2	p=0.3 q=0.7
100	92	87	90	80	71	77	49	38	45
500	341	289	321	217	165	196	81	55	70
750	441	358	409	254	185	226	85	57	73
1000	516	406	473	278	198	244	88	58	75
2500	748	537	660	333	224	286	93	60	78
5000	880	601	760	357	234	303	94	61	79
10000	964	639	823	370	240	313	95	61	80
25000	1023	665	865	378	244	319	96	61	80
50000	1045	674	881	381	245	321	96	61	81
100000	1056	678	888	383	245	322	96	61	81
1000000	1066	682	896	384	246	323	96	61	81
100 milyon	1067	683	896	384	245	323	96	61	81

Kaynak: Yazıcıoğlu ve Erdoğan, 2004: 50

Çalışmanın anakütlesini, 2020 yılı itibariyle BİST'e kote 477 şirkette çalışmakta olan iç denetçiler oluşturmaktadır. Yapılan araştırmalar sonucunda söz konusu şirketlerde yaklaşık 2000 civarı iç denetçi çalıştığı tespit edilmiştir. Örneklem büyüklüğü tablosuna bakıldığında 222 analize elverişli anket cevabı ile yeterli örneklem sayısına ulaşılmıştır.

Güç analizi (power analysis); yapılacak analiz çalışması için en az kaç örneklemin gerekli olduğunun tespit edilmesini sağlamaktadır. Bu çalışmada grup farklılığı yapılacaktır. Anketi yapmayı kabul eden katılımcı sayısının robust (sağlam) sonuçlar üretebilme yeteneğini tespit edebilmek açısından Güç (power) analizi, G*POWER 3.1 sürümüyle yapılmıştır. Çalışmalarda, istatistiksel gücün $1-\beta= 0.95$ olmasının yeterli olduğu Cohen (1988) ve Parajapati vd. (2010)'nin yapmış oldukları çalışmalarda ortaya koyulmuş olup grup farklılığı hesaplanacağı belirtilerek sonuçlar elde edilmiştir. İstatistik anlamlılık düzeyi $\alpha=0,05$ olarak belirlenmiştir.

Şekil 4.1. Güç Analizi Sonuçları



Güç analizinin neticesinde grup farklılığı sınamalarında en az 176 örneklemlerle çalışılması halinde çalışmanın geçerli olacağı tespit edilmiştir. Bu çalışmada 222 örneklem kullanılmış ve gerçekleştirilecek analizlerin güvenilir olacağı ortaya koyulmuştur.

4.4.3. Araştırmanın Varsayımları ve Kısıtları

Çalışmanın ana kütlesini halka açık işletmeler oluşturmaktadır. Halka açık işletmelerin seçilme nedeni; çalışmada yer alması gereken işletmelerin gelişmiş bir kurumsal yapılanmaya, iç denetim ve BT departmanlarına sahip olması gerekliliğidir.

Özellikle Covid-19 döneminde yüz yüze anket toplamak mümkün olmamıştır. Bu nedenle anketler e-posta yoluyla yapılmıştır. Ayrıca anketin örneklem sayısının artırılmasında zorluklar yaşanmış, birçok kişi katılım göstermemiş veya katılım göstermeyeceğini beyan etmiştir. Ayrıca, ankete katılması beklenen kişilerin; orta ve üst kademe yöneticiler olması gerektiğinden, ankete katılıma olumlu bakmamaları önemli bir kısıt oluşturmuştur.

4.5. Araştırmanın Hipotezleri, Analizler, Bulgular ve Sonuçların Yorumlanması

Günümüz rekabetçi ortamında işletmeler; fiziksel işletme güvenlikleri ve personel güvenlikleri (işçi sağlığı vs.) için tedbirler aldıkları gibi daha stratejik bir alan olan siber güvenlik konusunda da tedbir ve mücadele yöntemleri geliştirmeli, kurumsal farkındalıklarını ileri düzeye taşımalıdır. Siber güvenlik faaliyetleri icra edilirken işletme yönetimlerinin en büyük destekçisi şüphesiz BT birimleri ve iç denetim birimleridir.

Çalışmanın üç temel amacı bulunmaktadır. Çalışmanın ilk amacı Türkiye’de faaliyet gösteren halka açık işletmelerin siber güvenlik faaliyetleri seviyelerini tespit etmek ve siber güvenlik düzeylerinin işletmelerin özelliklerine göre farklılaşıp farklılaşmadığını belirlemektir.

Çalışmanın ikinci amacı ise işletmelerde üçüncü savunma hattı olarak görev yapan iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliğini belirlemek ve iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliğinin işletmelerin özelliklerine göre farklılaşıp farklılaşmadığını tespit etmektir.

Bu çalışmanın son amacı ise işletmelerin siber güvenlik faaliyetleri seviyeleri ile iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliği arasında ilişki olup olmadığını incelemektir.

Bu bağlamda araştırmanın ilerleyen bölümlerinde; araştırma anketinin güvenilirlik analizine yer verilecek, normallik testleri ile araştırma katılımcılarının ve işletmelerin demografik bilgileri açıklanacaktır.

Araştırmanın temel konularını oluşturan “İşletmelerin Siber Güvenlik Faaliyetleri Seviyesi” ve “İç Denetim Birimlerinin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliği” ne ait hipotezler, frekans dağılımları ve fark testleri ise ayrı bölümlerde detaylı bir şekilde aktarılacaktır.

Son olarak çalışmanın araştırma bölümünde “İşletmelerin Siber Güvenlik Faaliyetleri Seviyesi” ve İç Denetim Birimlerinin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliği” arasındaki ilişkinin gücünü ve yönünü belirlemek amacıyla gerçekleştirilen korelasyon analizi sonuçlarına yer verilecektir.

4.5.1. Araştırma Anketinin Yapısı ve Anketin Güvenilirlik Analizi

Araştırma anketi iki ana bölümden oluşmaktadır. İlk bölümde BİST’e kote işletmelerin siber güvenlik yaklaşımlarının ve seviyelerinin belirlenmesine yönelik sorular yer almaktadır. İkinci bölümde; iç denetçilerin işletmelerin siber güvenlik süreçlerinin etkinliğinde aldıkları rollerin tespitine yönelik sorular yer almaktadır (EK-1).

Bir ölçeğin güvenilirliğinin test edilmesi için en yaygın uygulanan testler; “Cronbach Alpha, İkiye Bölme (split), Paralel ve Mutlak Kesin Paralel (strict)” şeklindedir. Cronbach Alpha testi sonucunda elde edilen değer $\geq 0,60$ ’in üzerinde olması anketin başarılı olduğunu ifade etmektedir. Kimi araştırmacılar tarafından ise bu değer $\geq 0,70$ ’in üzerinde olması beklenmektedir. Diğer güvenilirlik kriterlerinin de $\geq 0,70$ ’in üzerinde çıkması, anketin iç tutarlılığının sağlandığını ve çıkarımlara güvenilebileceğini göstermektedir.

Tablo 4.7. Güvenilirlik Analizi Sonuçları

	Anketin Güvenirlik Sonuçları
Cronbach Alpha	0,984
Split	0,962-0,980

Paralel	0,984
Strict	0,974

Tablo 4.7’ den görülebileceği üzere her dört testin sonucunda da belirtilen ve olması beklenen yüzde değerleri güven kriterini sağlamıştır. Dolayısıyla örneklem sonuçlarının yüksek güvenilirlik değerleriyle tutarlı ve güvenilir olduğu sonucuna ulaşılmıştır. Ele alınan bütün güvenilirlik kriterleri %70 değerini geçtiği için, uygulanan anketin başarılı olduğu, anketin kendi içinde tutarlılık gösterdiği, ulaşılabacak sonuçların gerçek değerleri yansıtacağı sonucu ortaya koyulmuştur.

4.5.2. Normallik Testi Sonuçları

Araştırmada yer alan önermeler için normallik testleri gerçekleştirilmiştir. Sonuçlar Tablo 4.8.’de sunulmuştur:

Tablo 4.8. Normal Dağılım Sonuçları

Değişkenler	Kolmogorov-Smirnov			Shapiro-Wilk		
	istatistik	s.d.	p	istatistik	s.d.	p
Siber Güvenliğe Kurumsal Yaklaşım	,096	222	,000	,945	222	,000
Fiziksel ve Çevresel Güvenlik Tedbirleri	,172	222	,000	,834	222	,000
Bilgi Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri	,134	222	,000	,907	222	,000
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tedbirleri	,126	222	,000	,919	222	,000
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	,181	222	,000	,922	222	,000
Siber Güvenlik Fonksiyonu Açısından İç Denetçinin Görev Tanımı Algısı	,150	222	,000	,913	222	,000

İç Denetim ve Bilgi Teknolojileri (BT) Departmanları Arasındaki İlişkinin Algısı	,137	222	,000	,953	222	,000
İç Denetim Departmanının Siber Güvenlik Bilgi Düzeyi Algısı	,109	222	,000	,943	222	,000
Siber Güvenlik İşlevi Açısından İç Denetim Departmanının Katma Değer Algısı	,205	222	,000	,918	222	,000
Siber Güvenlik Konusunda Üst Yönetimin Desteğine ilişkin İç Denetçi Algısı	,177	222	,000	,902	222	,000
İç Denetim Departmanının Siber Güvenliği Gözden Geçirme Sıklığı	,166	222	,000	,921	222	,000
Cari Dönem Vak'a Sayısı	,290	222	,000	,832	222	,000
Siber Güvenlik Vak'a trendi	,287	222	,000	,775	222	,000

Tablodan görüleceği üzere her bir önerme için $p < 0.05$ olduğundan normal dağılımın olmadığı tespit edilmiştir. Bu durumda grup farklılıkları analizi için non-parametrik yöntemler kullanılacaktır. Araştırmanın verileri normal dağılım göstermiyorsa, grup/koşul sayısı 3 veya 3'ten fazla ise ve tüm gruplarda/koşullarda farklı denekler kullanıldıysa Kruskal-Wallis testi uygulanmaktadır (Karagöz, 2010).

4.5.3. Araştırmaya Katılan İç Denetçilerin ve İşletmelerin Demografik Özellikleri (Frekans-Sıklık Dağılım Tabloları)

Araştırmaya 222 iç denetçi katılmıştır. Ankete katılan iç denetçilerin cinsiyetlerine göre frekans dağılım tablosu Tablo 4.9.'da verilmiştir.

Tablo 4.9. Araştırmaya Katılan İç Denetçilerin Cinsiyetlerine Göre Frekans Dağılımı

Cinsiyet	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Erkek	142	64	64	64
Kadın	80	36	36	100
Toplam	222	100	100	

Araştırmaya katılan iç denetçilerin %36'sı kadın, %64'ü erkektir. Araştırmaya katılan iç denetçilerin yaşa göre dağılımları Tablo 4.10.'da verilmiştir.

Tablo 4.10. Araştırmaya Katılan İç Denetçilerin Yaşlarına Göre Frekans Dağılımı

Yaş	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
25 ve altı	4	2	2	2
26-30	40	18	18	20
31-35	65	29	29	49
36-40	63	28	28	77
41-45	33	15	15	92
45 ve üzeri	17	8	8	100
Toplam	222	100	100	

Araştırmaya katılan iç denetçilerin %2'si 25 yaş ve altı, %18'i 26-30 yaş, %29'u 31-35 yaş, %28'i 36-40 yaş, %15'i 41-45 yaş ve %8' 45 yaş ve üzeri olarak belirlenmiştir. Araştırmaya katılan iç denetçilerin eğitim durumlarına göre dağılımları Tablo 4.11.'de verilmiştir.

Tablo 4.11. Araştırmaya İç Denetçilerin Eğitim Durumlarına Göre Frekans Dağılımı

Eğitim Durumu	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Lisans	109	49,1	49,1	49,1
Yüksek Lisans	101	45,5	45,5	94,6
Doktora	12	5,4	5,4	100
Toplam	222	100	100	

Araştırmaya katılan iç denetçilerin, %49,1'i lisans, %45,5'i yüksek lisans ve %5,4'ü doktora yapmıştır. Araştırmaya katılan iç denetçilerin mesleki deneyim sürelerine göre dağılımları Tablo 4.12.'de verilmiştir.

Tablo 4.12. Araştırmaya Katılan İç Denetçilerin Mesleki Deneyimlerine Göre Frekans Dağılımı

Mesleki Deneyim	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
5 yıldan az	34	15,3	15,3	15,3
5-9 yıl	76	34,2	34,2	49,5
10-14 yıl	56	25,2	25,2	74,8
15-19 yıl	37	16,7	16,7	91,4
20 yıl ve üzeri	19	8,6	8,6	100,0
Toplam	222	100	100	

Araştırmaya iç denetçilerin %15,3'ü 5 yıldan az %34,2'si 5-9 yıl, %25,2'si 10-14 yıl, %16,7'si 15-19 yıl ve %8,6'sı 20 yıl ve üzeri deneyim süresine sahiptir. Araştırmaya katılan iç denetçilerin çalıştıkları pozisyonlara göre dağılımları Tablo 4.13.'te verilmiştir.

Tablo 4.13. Araştırmaya Katılan İç Denetçilerin Çalıştıkları Pozisyonlara Göre Frekans Dağılımı

Çalıştıkları Pozisyon	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
İç Denetim Yöneticisi	106	47,7	47,7	47,7
İç Denetçi	98	44,1	44,1	91,9
İç Denetçi Yardımcısı	18	8,1	8,1	100,0
Total	222	100,0	100,0	

Araştırmaya katılan iç denetçilerden %47,7'si iç denetim yöneticisi, %44,1'i iç denetçi ve %8,1'i iç denetçi yardımcısı olarak görev yapmaktadır. Araştırmaya katılan iç denetçilerin mesleki sertifikasyona sahip olma durumlarına göre dağılımları Tablo 4.14.'te verilmiştir.

Tablo 4.14. Araştırmaya Katılan İç Denetçilerin Sahip Oldukları Mesleki Sertifika Sayısına Göre Frekans Dağılımı

Mesleki Sertifika Sayısı	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Hiç yok	84	37,8	37,8	37,8
1 Tane Var	65	29,3	29,3	67,1
2 Tane var	49	22,1	22,1	89,2
3 Tane Var	24	10,8	10,8	100,0
Total	222	100,0	100,0	

Araştırmaya katılan denetçilerden %37,8'i herhangi bir sertifikaya sahip değilken, %29,3'ü 1 adet, %22,1'i 2 adet, %10,8'i 3 adet sertifikaya sahiptir. Araştırmaya katılan iç denetçilerin çalıştıkları işletmelerin faaliyet gösterdikleri sektörlerin dağılımı Tablo 4.15.'te sunulmuştur:

Tablo 4.15. Araştırmaya Katılan İç Denetçilerin Çalıştıkları İşletmelerin Sektörüne Göre Frekans Dağılımı

Sektör	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Bankacılık	49	22,1	22,1	22,1
Üretim	45	20,3	20,3	42,3
Risk Yönetimi ve Sigorta	25	11,3	11,3	53,6
Enerji	22	9,9	9,9	63,5
Perakende	11	5,0	5,0	68,5
Havacılık ve Uzay	9	4,1	4,1	72,5
İletişim, Medya ve Teknoloji	9	4,1	4,1	76,6
İnşaat	9	4,1	4,1	80,6
Madencilik/Metaller/Mineraller	8	3,6	3,6	84,2
Kimya	7	3,2	3,2	87,4

Diğer	28	12,6	12,6	100,0
Total	222	100,0	100,0	

Araştırmaya katılan iç denetçilerden %22,1'i bankacılık, 20,3'ü üretim, %11,3'ü risk yönetimi ve sigorta, 9,9'u enerji, %5'i perakende, %4,1'i havacılık ve uzay, %4,1'i iletişim, medya ve teknoloji, %4,1'i inşaat, %3,6'sı madencilik/metaller/mineraller, %3,2'si kimya sektörlerinde faaliyet göstermektedir. 28 katılımcı ise (%12,6) diğer sektörlerde faaliyetlerini sürdürmektedir. Araştırmada yer alan işletmelerin aktif büyüklüklerine göre frekans dağılımı Tablo 4.16.'da sunulmuştur:

Tablo 4.16. Araştırmada Yer Alan İşletmelerin Aktif Büyüklüklerine Göre Frekans Dağılımı

Aktif Büyüklüğü	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
10 milyon TL altı	5	2,3	2,3	2,3
10 milyon TL- 100 Milyon TL	18	8,1	8,1	10,4
100 milyon TL- 1 milyar TL	53	23,9	23,9	34,2
1 milyar TL- 10 milyar TL	75	33,8	33,8	68,0
10 milyar TL üzeri	71	32,0	32,0	100,0
Total	222	100,0	100,0	

Araştırmada yer alan işletmelerin %2,3'ü 10 milyon TL ve altı, %8,1'i 10 milyon TL- 100 Milyon TL, %23,9'u 100 milyon TL- 1 milyar TL, %33,8'i 1 milyar TL- 10 milyar TL, %32'si 10 milyar TL üzeri aktif büyüklüğüne sahiptir. Araştırmada yer alan şirketlerin çalışan sayısına göre frekans dağılımı Tablo 4.17.'de sunulmuştur.

Tablo 4.17. Araştırmada Yer Alan İşletmelerin Çalışan Sayısına Göre Frekans Dağılımı

Çalışan Sayısı	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
100'ün altı	9	4,1	4,1	4,1

100-299	19	8,6	8,6	12,6
300-999	105	47,3	47,3	59,9
1000-4999	61	27,5	27,5	87,4
5000 ve üzeri	28	12,6	12,6	100,0
Toplam	222	100	100	

Araştırmada yer alan işletmelerin %4,1'i 10,100'ün altı, %8,6'sı 100-299 arası, %47,3'ü 300-999 arası, %27,5'i 1000-4999 arası, %12,6'sı 5000 ve üzeri çalışana sahiptir. Araştırmada yer alan şirketlerin teknoloji bağımlılıklarına göre frekans dağılımı Tablo 4.18.'de sunulmuştur:

Tablo 4.18. Araştırmada Yer Alan İşletmelerin Teknoloji Bağımlılıklarına Göre Frekans Dağılımı

Teknoloji Bağımlılığı	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Az bağımlı	55	24,8	24,8	24,8
Bağımlı	68	30,6	30,6	55,4
Çok bağımlı	99	44,6	44,6	100,0
Toplam	222	100	100	

Araştırmada yer alan işletmelerin teknoloji bağımlılığı sınıflandırması ise %24,8'i az bağımlı, %30,6'sı bağımlı, %44,6'sı ise çok bağımlı olarak gerçekleşmiştir. Araştırmada yer alan şirketlerin kritik bilgilere sahip olma durumlarına göre frekans dağılımı Tablo 4.19.'da sunulmuştur.

Tablo 4.19. Araştırmada Yer Alan İşletmelerin Kritik Bilgilere Sahip Olmalarına Göre Frekans Dağılımı

Kritik Bilgilere Sahip Olma	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Neredeyse yok	7	3,2	3,2	3,2
Az	73	32,9	32,9	36,0
Çok	44	19,8	19,8	55,9
Çoğunluğu Kritik	98	44,1	44,1	100,0
Toplam	222	100	100	

Araştırmada yer alan işletmelerin kritik bilgilere sahip olma durumları ise %3,2 “neredeyse yok”, %32,9’u “az”, %19,8’i “çok”, %44,1’i ise “çoğunluğu kritik” olarak belirlenmiştir. Araştırmada yer alan şirketlerin olası bir saldırı sonrası itibar kaybına uğrama ihtimallerine göre frekans dağılımı Tablo 4.20.’de sunulmuştur:

Tablo 4.20. Araştırmada Yer Alan İşletmelerin İtibar Riskine Göre Frekans Dağılımı

İtibar Riski	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Neredeyse yok	5	2,3	2,3	2,3
Az	58	26,1	26,1	28,4
Çok	81	36,5	36,5	64,9
Firmanın Geleceğini Etkiler	78	35,1	35,1	100,0
Toplam	222	100	100	

Araştırmada yer alan işletmelerin olası siber saldırı sonrası itibar riskleri %2,3 “neredeyse yok”, %26,1’i “az”, %35,6’sı “çok”, %35,1’i ise “firmanın geleceğini etkiler” olarak belirlenmiştir.

4.5.4. İşletmelerin Siber Güvenlik Faaliyetleri Seviyesine İlişkin Hipotezler, Frekans Dağılımları ve Farklılık Analizleri

Çalışmanın bu bölümünde sırasıyla işletmelerin siber güvenlik faaliyetleri seviyesine ilişkin hipotezler, frekans dağılımları ve farklılık analizlerine yer verilmiştir. Ayrıca analiz bulguları ve sonuçları yorumlanmıştır.

4.5.4.1. İşletmelerin Siber Güvenlik Faaliyetleri Seviyesine İlişkin Hipotezler

Bu araştırmanın temel konularından ilki; “Türkiye’de faaliyet gösteren halka açık işletmelerin siber güvenlik faaliyetleri seviyeleri ne durumdadır?” ve “İşletmelerin siber güvenlik düzeyleri işletmenin özelliklerine göre farklılaşmakta mıdır?” sorularından hareketle oluşturulmuştur.

Bu bağlamda siber güvenlik faaliyetlerinin seviyelerini belirlemek amacıyla aşağıdaki alt boyutlar belirlenmiştir:

- Siber Güvenlik Yönetimi ve Uygulamaları
- Fiziksel ve Çevresel Güvenlik Tedbirleri
- Bilgi Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri
- Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tedbirleri
- Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi

Yukarıda belirlenen alt boyutların işletmelerin çalışan sayısı, aktif büyüklüğü, BT bağımlılıkları, kritik bilgilere sahip olma durumları, siber saldırı sonrası olası itibar kayıpları ve sektörlerine göre farklılık gösterip göstermediklerini belirlemek için fark testleri uygulanacaktır. Türkiye’de faaliyet gösteren halka açık işletmelerin siber güvenlik faaliyetleri seviyelerine ilişkin hipotezler (Hipotez 1- Hipotez 6) ve araştırma modeli (Şekil 4.1.) aşağıda sunulmuştur:

H1: *Siber güvenlik faaliyetleri seviyesi işletmelerin çalışan sayısına göre anlamlı farklılık göstermektedir.*

- **H1a:** Siber güvenlik yönetiřimi ve uygulamaları iřletmelerin alıřan sayısına gre anlamlı farklılık gstermektedir.
- **H1b:** Fiziksel ve evresel güvenlik tedbirleri iřletmelerin alıřan sayısına gre anlamlı farklılık gstermektedir.
- **H1c:** Biliřim sistemleri ve iletiřim aęlarının iřletim ve bakım kontrolleri iřletmelerin alıřan sayısına gre anlamlı farklılık gstermektedir.
- **H1d:** Yazılım geliřtirme ve destek ařamalarında bilgi sistemleri eriřim kontrol güvenlik tedbirleri iřletmelerin alıřan sayısına gre anlamlı farklılık gstermektedir.
- **H1e:** Siber güvenlik ihlalleri ve iř srekliilięi ynetimi iřletmelerin alıřan sayısına gre anlamlı farklılık gstermektedir.

H2: *Siber güvenlik faaliyetleri seviyesi iřletmelerin byklęne gre anlamlı farklılık gstermektedir.*

- **H2a:** Siber güvenlik yönetiřimi ve uygulamaları iřletmelerin aktif byklęne gre anlamlı farklılık gstermektedir.
- **H2b:** Fiziksel ve evresel güvenlik tedbirleri iřletmelerin aktif byklęne gre anlamlı farklılık gstermektedir.
- **H2c:** Biliřim sistemleri ve iletiřim aęlarının iřletim ve bakım kontrolleri iřletmelerin aktif byklęne gre anlamlı farklılık gstermektedir.
- **H2d:** Yazılım geliřtirme ve destek ařamalarında bilgi sistemleri eriřim kontrol güvenlik tedbirleri iřletmelerin aktif byklęne gre anlamlı farklılık gstermektedir
- **H2e:** Siber güvenlik ihlalleri ve iř srekliilięi ynetimi iřletmelerin aktif byklęne gre anlamlı farklılık gstermektedir.

H3: *Siber güvenlik faaliyetleri seviyesi iřletmelerin bilgi teknolojilerine baęımlılık dzeyine gre anlamlı farklılık gstermektedir.*

- **H3a:** Siber güvenlik yönetiřimi ve uygulamaları iřletmelerin bilgi teknolojilerine baęımlılık dzeyine gre anlamlı farklılık gstermektedir.
- **H3b:** Fiziksel ve evresel güvenlik tedbirleri iřletmelerin bilgi teknolojilerine baęımlılık dzeyine gre anlamlı farklılık gstermektedir.

- **H3c:** Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri bilgi teknolojilerine bağımlılık düzeyine göre anlamlı farklılık göstermektedir.
- **H3d:** Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri bilgi teknolojilerine bağımlılık düzeyine göre anlamlı farklılık göstermektedir.
- **H3e:** Siber güvenlik ihlalleri ve iş sürekliliği yönetimi işletmelerin bilgi teknolojilerine bağımlılık düzeyine göre anlamlı farklılık göstermektedir.

H4: *Siber güvenlik faaliyetleri seviyesi siber saldırıların işletme imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.*

- **H4a:** Siber güvenlik yönetimi ve uygulamaları siber saldırıların işletme imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.
- **H4b:** Fiziksel ve çevresel güvenlik tedbirleri siber saldırıların işletme imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.
- **H4c:** Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri siber saldırıların işletme imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.
- **H4d:** Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri siber saldırıların işletme imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.
- **H4e:** Siber güvenlik ihlalleri ve iş sürekliliği siber saldırıların işletme imajı üzerindeki olası etkilerine göre anlamlı farklılık göstermektedir.

H5: *Siber güvenlik faaliyetleri seviyesi işletmelerin elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.*

- **H5a:** Siber güvenlik yönetimi ve uygulamaları işletmelerin elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.
- **H5b:** Fiziksel ve çevresel güvenlik tedbirleri işletmelerin elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.
- **H5c:** Bilişim sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri işletmelerin elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.

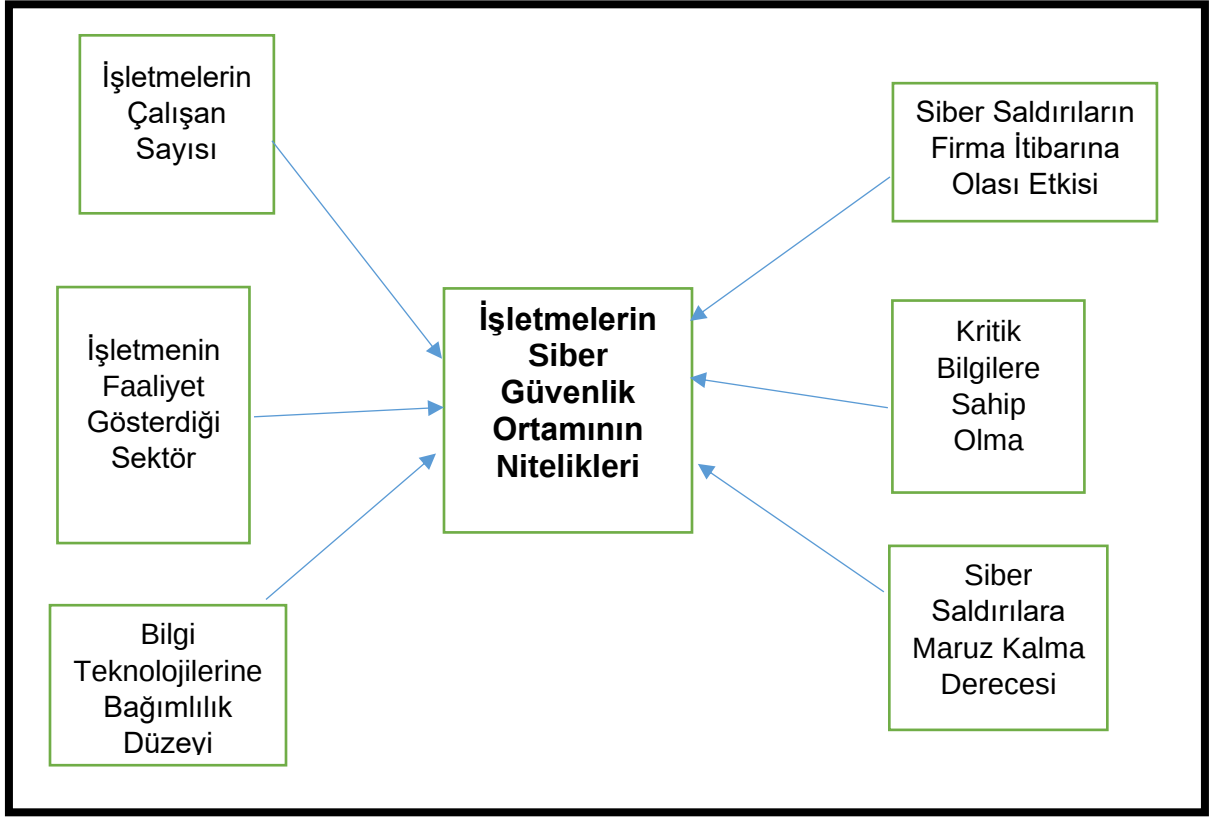
- **H5d:** Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri işletmelerin elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.
- **H5e:** Siber güvenlik ihlalleri ve iş sürekliliği işletmelerin elindeki kritik bilgilerin oranına göre anlamlı farklılık göstermektedir.

H6: *Siber güvenlik faaliyetleri seviyesi işletmelerin sektörüne göre anlamlı farklılık göstermektedir.*

- **H6a:** Siber güvenlik yönetiřimi ve uygulamaları işletmelerin sektörüne göre anlamlı farklılık göstermektedir.
- **H6b:** Fiziksel ve çevresel güvenlik tedbirleri işletmelerin sektörüne göre anlamlı farklılık göstermektedir.
- **H6c:** Biliřim sistemleri ve iletiřim aęlarının iřletim ve bakım kontrolleri işletmelerin sektörüne göre anlamlı farklılık göstermektedir.
- **H6d:** Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü güvenlik tedbirleri işletmelerin sektörüne göre anlamlı farklılık göstermektedir.
- **H6e:** Siber güvenlik ihlalleri ve iş sürekliliği işletmelerin sektörüne göre anlamlı farklılık göstermektedir

Yukarıda belirlenen alt boyutlar ve sonrasında oluşturulan hipotezler sonucu ortaya çıkan İşletmelerin Siber Güvenlik Faaliyetleri Seviyesine ilişkin araştırma modeli Şekil 4.1.'de sunulmuştur:

Şekil 4.1 Araştırma Modeli: İşletmelerin Siber Güvenlik Ortamının Nitelikleri



4.5.4.2. İşletmelerin Siber Güvenlik Faaliyetleri Seviyesine İlişkin Frekans Dağılımları

İç denetçilerin çalıştıkları işletmelerin siber güvenlik ortamının niteliklerini belirlemek üzere yöneltilen sorulara verilen cevaplar aşağıdaki bölümlerde verilmiştir. Çalışmada 5'li likert ölçeği kullanılmış ve araştırmaya katılan iç denetçilerden, aşağıdaki seçeneklerden birini işaretlemeleri beklenmiştir.

- 1- Hiç uygulanmıyor
- 2- Kısmen uygulanıyor
- 3- Uygulanıyor
- 4- Çoğunluğu uygulanıyor
- 5- Tamamen uygulanıyor

Cevaplara 1-5 arası ağırlık verilerek, her ifade için frekans, ağırlıklı ortalama ve standart sapma hesaplanmıştır.

4.5.4.2.1. Siber Güvenlik Yönetişimi ve Uygulamaları-Frekans Dağılımları

Siber güvenlik yönetişimi ve uygulamaları alt boyutuna ait frekans dağılımları, ortalama ve standart sapma değerleri Tablo 4.21.'deki gibidir:

Tablo 4.21. Siber Güvenlik Yönetişimi ve Uygulamaları Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri Dağılımı

	Hiç uygulanmıyor	Kısmen Uygulanıyor	Uygulanıyor	Çoğunlukla Uygulanıyor	Tamamen Uygulanıyor	Ort. ± Ss.		
İşletmemizin siber güvenliğe ilişkin yazılı kural ve politikaları vardır.	2,3	7,2	15,3	42,8	32,4	3,9595	±	,98549
İşletmemiz siber güvenliğe ilişkin yazılı kural ve politikaları oluştururken hayati öneme sahip alanlarda oluşabilecek tehlike ve güvenlik açıklarını dikkate almıştır.	2,7	10,4	20,7	31,5	34,7	3,8514	±	1,09316
İşletmemizin siber güvenliğe ilişkin kural ve politikaları, ülkemizdeki ilgili kanun ve yönetmeliklere uygundur.	0,9	7,7	9,9	30,2	51,4	4,2342	±	,97438
İşletmemiz kritik bilgi teknolojilerini	2,7	17,1	18,5	33,3	28,4	3,6757	±	1,13888

önem derecesine göre sınıflandırıp, bu sistemleri oluşturulan sınıflandırmaya göre yönetmektedir.								
İşletmemiz bilgi yaşam döngüsünün tüm aşamalarında gerekli güvenlik önemlerini almaktadır. (Bilgi yaşam döngüsü: bilginin oluşturulması, kullanılması, depolanması, iletilmesi, işlenmesi ve imha edilmesi)	2,7	18,5	20,3	31,5	27,0	3,6171	±	1,14642
İşletmemiz bilgi teknolojilerine yönelik hizmet alımlarında, gerekli güvenlik önlemlerini sözleşme maddelerine dahil etmektedir.	7,2	16,7	20,3	26,6	29,3	3,5405	±	1,26765
İşletmemiz tüm çalışanlara siber güvenliğe ilişkin yükümlülükleri açıkça bildirmektedir.	5,4	19,4	22,5	22,1	30,6	3,5315	±	1,25716
İşletmemiz tüm çalışanlara düzenli olarak bilgi güvenliği ve siber güvenlik eğitimleri vermektedir.	16,7	28,4	17,1	13,5	24,3	3,0045	±	1,43800

Önerme 1: İşletmemizin siber güvenliğe ilişkin yazılı kural ve politikaları vardır.

Bu önermeye araştırmaya katılan iç denetçilerin %2,3'ü "Hiç uygulanmıyor", %7,2'si "Kısmen uygulanıyor", 15,3'ü "Uygulanıyor", 42,8'si "Çoğunlukla uygulanıyor", 32,4'si "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,9595 ve standart sapması ,98549 olarak bulunmuştur. Frekans dağılımı sonuçlarına göre araştırmaya katılan işletmelerin tamamına yakınında yazılı kural ve politikalar bulunduğu belirlenmiştir. Önermenin ortalamasının 3,9595 olduğu görülmektedir. Buna göre işletmelerin yazılı kural ve politikaların çoğunlukla uygulandığı sonucuna ulaşılmaktadır.

Önerme 2: İşletmemiz siber güvenliğe ilişkin yazılı kural ve politikaları oluştururken hayati öneme sahip alanlarda oluşabilecek tehlike ve güvenlik açıklarını dikkate almıştır.

Bu önermeye araştırmaya katılan iç denetçilerin %2,7'si "Hiç uygulanmıyor", %10,4'ü "Kısmen uygulanıyor", 20,7'si "Uygulanıyor", 31,5'i "Çoğunlukla uygulanıyor", 34,7'si "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,8514 ve standart sapması 1,09316 olarak bulunmuştur. Buna göre, işletmelerin çoğunlukla yazılı kural ve politikaları oluştururken hayati öneme sahip alanlarda oluşabilecek tehlike ve güvenlik açıklarını dikkate aldığı sonucu ortaya çıkmaktadır.

Önerme 3: İşletmemizin siber güvenliğe ilişkin kural ve politikaları, ülkemizdeki ilgili kanun ve yönetmeliklere uygundur.

Bu önermeye araştırmaya katılan iç denetçilerin %0,9'u "Hiç uygulanmıyor", %7,7'si "Kısmen uygulanıyor", 9,9'u "Uygulanıyor", 30,2'si "Çoğunlukla uygulanıyor", 51,4'ü "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 4,2342 ve standart sapması ,97438 olarak bulunmuştur. Buna göre, işletmelerin siber güvenliğe ilişkin kural ve politikalarının ülkemizdeki ilgili kanun ve yönetmeliklere uygun olduğu anlaşılmaktadır.

Önerme 4: İşletmemiz kritik bilgi teknolojilerini önem derecesine göre sınıflandırıp, bu sistemleri oluşturulan sınıflandırmaya göre yönetmektedir.

Bu önermeye araştırmaya katılan iç denetçilerin %2,7'si "Hiç uygulanmıyor", %17,1'i "Kısmen uygulanıyor", 18,5'i "Uygulanıyor", 33,3'ü "Çoğunlukla uygulanıyor", 28,4'ü "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,6757 ve

standart sapması 1,13888 olarak bulunmuştur. Ankete katılan iç denetçilerin 3'te 1'i işletmelerinin çoğunlukla kritik bilgi teknolojilerini önem derecesine göre sınıflandırıp, bu sistemleri oluşturulan sınıflandırmaya göre yönettikleri yönünde cevap vermişlerdir. İşletmelerin büyük bir çoğunluğu kritik bilgi teknolojilerini önem derecesine göre sınıflandırmakta ve sistemleri oluşturulan sınıflandırmalara göre yönetmektedir.

Önerme 5: İşletmemiz bilgi yaşam döngüsünün tüm aşamalarında gerekli güvenlik önemlerini almaktadır. (Bilgi yaşam döngüsü: bilginin oluşturulması, kullanılması, depolanması, iletilmesi, işlenmesi ve imha edilmesi)

Bu önermeye araştırmaya katılan iç denetçilerin %2,7'si "Hiç uygulanmıyor", %18,5'i "Kısmen uygulanıyor", 20,3'ü "Uygulanıyor", 31,5'i "Çoğunlukla uygulanıyor", 27,0'si "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,6171 ve standart sapması 1,14642 olarak bulunmuştur. Önermenin ortalaması dikkate alındığında, işletmelerin genelinin bilgi yaşam döngüsünün tüm aşamalarında gerekli güvenlik önemlerini aldığı sonucu ortaya çıkmaktadır.

Önerme 6: İşletmemiz bilgi teknolojilerine yönelik hizmet alımlarında, gerekli güvenlik önlemlerini sözleşme maddelerine dahil etmektedir.

Bu önermeye araştırmaya katılan iç denetçilerin %0,9'u "Hiç uygulanmıyor", %7,2'si "Kısmen uygulanıyor", 16,7'si "Uygulanıyor", 20,3'ü "Çoğunlukla uygulanıyor", 29,3'ü "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,5405 ve standart sapması 1,26765 olarak bulunmuştur. Buna göre, işletmelerin yarısına yakınının bilgi teknolojilerine yönelik hizmet alımlarında, gerekli güvenlik önlemlerini sözleşme maddelerine dahil ettiği anlaşılmaktadır.

Önerme 7: İşletmemiz tüm çalışanlara siber güvenliğe ilişkin yükümlülükleri açıkça bildirmektedir.

Bu önermeye araştırmaya katılan iç denetçilerin %5,4'ü "Hiç uygulanmıyor", %19,4'ü "Kısmen uygulanıyor", 22,5'i "Uygulanıyor", 22,1'i "Çoğunlukla uygulanıyor", 30,6'sı "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,5315 ve standart sapması 1,25716 olarak bulunmuştur. Buna göre, işletmelerin yarısından fazlası

alıřanlarına siber gvenlięe iliřkin sorumluluklarını oęunlukla veya tamamen bildirmektedir.

nerme 8: İřletmemiz tm alıřanlara dzenli olarak bilgi gvenlięi ve siber gvenlik eęitimleri vermektedir.

Bu nermeye arařtırmaya katılan i denetilerin %16,7'si "Hi uygulanmıyor", %28,4' "Kısmen uygulanıyor", 17,1'i "Uygulanıyor", 13,5'i "oęunlukla uygulanıyor", 24,3' "Tamamen uygulanıyor" řeklinde cevaplamıřlardır. Bu nermenin ortalaması 3,0045 ve standart sapması 1,43800 olarak bulunmuřtur. Arařtırmadaki ortalamalar ierinde en dřk ortalama bu nermeye aittir. Bu nermeye verilen cevaplar incelendięinde iřletmelerin yaklařık %17'sinin alıřanlarına hi eęitim vermedięi grlmektedir. Bu durum siber gvenlik konusunun iřletmeler aısından nemi dřnldęnde dikkat ekici bir sonutur.

4.5.4.2.2. Fiziksel ve evresel Gvenlik Tedbirleri- Frekans Daęılımları

Fiziksel ve evresel gvenlik tedbirleri alt boyutuna ait frekans daęılımları, ortalama ve standart sapma deęerleri Tablo 4.22.'deki gibidir:

Tablo 4.22. Fiziksel ve evresel Gvenlik Tedbirleri Frekans Daęılımları, Ortalama ve Standart Sapma Deęerleri

	Hi uygulanmıyor	Kısmen Uygulanıyor	Uygulanıyor	oęunlukla Uygulanıyor	Tamamen Uygulanıyor	Ort. ± Ss.		
İřletmemize ait tesislerin gvenlięini iyileřtirmek iin gerekli gvenlik nlemleri alınmaktadır.	2,3	0,9	8,1	47,7	41,0	4,2432	±	,82073

İşletmemize ait tesislere giriş-çıkışı düzenleyen yazılı kurallar vardır.	0,0	1,4	6,3	31,5	60,8	4,5180	±	,67746
İşletmemizde bilgi teknolojilerine yönelik her türlü tehlikeye (doğal afetler veya insan kaynaklı zararlar) karşı koruyucu önlemler alınmıştır.	0,9	3,2	7,7	33,8	54,5	4,3784	±	,82992
İşletmemizde taşınabilir bilgisayarlar ve harici depolama aygıtlarının kullanımına ilişkin güvenlik önlemleri alınmıştır.	0,9	2,3	8,6	37,8	50,5	4,3468	±	,80241

Önerme 1: İşletmemize ait tesislerin güvenliğini iyileştirmek için gerekli güvenlik önlemleri alınmaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %2,3'ü "Hiç uygulanmıyor", %0,9'u "Kısmen uygulanıyor", 8,1'i "Uygulanıyor", 47,7'si "Çoğunlukla uygulanıyor", 41,0'i "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 4,2432 ve standart sapması ,82073 olarak bulunmuştur. Önermenin ortalaması dikkate alındığında, işletmelerin güvenlik önlemleri uygulamaları konusunda çok iyi seviyede oldukları anlaşılmaktadır.

Önerme 2: İşletmemize ait tesislere giriş-çıkışı düzenleyen yazılı kurallar vardır.

Bu önermeye araştırmaya katılan iç denetçilerin %1,4'ü "Kısmen uygulanıyor", 6,3'ü "Uygulanıyor", 31,5'i "Çoğunlukla uygulanıyor", 60,8'i "Tamamen uygulanıyor" şeklinde

cevaplamışlardır. Bu önermenin ortalaması 4,5180 ve standart sapması 0,67746 olarak bulunmuştur. Bu önermenin ortalaması dikkate alındığında, işletmelerin neredeyse tamamının işletmelerin tesislerine giriş çıkışı düzenleyen kurallar bulunduğu ve bunların düzgün bir şekilde uygulandığı anlaşılmaktadır.

Önerme 3: İşletmemizde bilgi teknolojilerine yönelik her türlü tehlikeye (doğal afetler veya insan kaynaklı zararlar) karşı koruyucu önlemler alınmıştır.

Bu önermeye araştırmaya katılan iç denetçilerin %0,9'u "Hiç uygulanmıyor", %3,2'si "Kısmen uygulanıyor", 7,7'si "Uygulanıyor", 33,8'i "Çoğunlukla uygulanıyor", 54,5'i "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 4,3784 ve standart sapması ,82992 olarak bulunmuştur. Bu önermenin ortalaması dikkate alındığında, işletmelerin neredeyse tamamının her türlü tehlikeye karşı koruyucu önlemler aldığı ve bunları uyguladıkları anlaşılmaktadır.

Önerme 4: İşletmemizde taşınabilir bilgisayarlar ve harici depolama aygıtlarının kullanımına ilişkin güvenlik önlemleri alınmıştır

Bu önermeye araştırmaya katılan iç denetçilerin %0,9'u "Hiç uygulanmıyor", %2,3'ü "Kısmen uygulanıyor", 8,6'sı "Uygulanıyor", 37,8'i "Çoğunlukla uygulanıyor", 50,5'i "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 4,3468 ve standart sapması 0,80241 olarak bulunmuştur. Bu önermenin ortalaması dikkate alındığında, işletmelerin neredeyse tamamının bilgisayarlar ve diğer aygıtların kullanımına ilişkin güvenlik önlemlerini aldığı görülmektedir.

İşletmelerin fiziksel ve çevresel güvenlik önlemleri ortalamaları, araştırmada yer alan önermeler içerisindeki en yüksek ortalamalardır. İşletmelerin varlıklarını her türlü zarardan korumak için sıkı güvenlik önlemleri almaları, siber güvenlik konusundan bağımsız olarak düşünüldüğünde de beklenen bir durumdur ve bu önermelere ait ortalamaların yüksek olmasını açıklamaktadır.

4.5.4.2.3. Bilgi Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri-Frekans Dağılımları

Bilgi sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri alt boyutuna ait frekans dağılımları, ortalama ve standart sapma değerleri Tablo 4.23.'teki gibidir:

Tablo 4.23. Bilgi Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri

	Hiç uygulanmıyor	Kısmen Uygulanıyor	Uygulanıyor	Çoğunlukla Uygulanıyor	Tamamen Uygulanıyor	Ort. ± Ss.		
İşletmemiz bilgi teknolojileri verilerini (sistem konfigürasyon ve yedekleri) uygun bir şekilde korumaktadır.	4,1	14,4	19,8	33,3	28,4	3,6757	±	1,15074
İşletmemizde bilgi teknolojileri kurulum ve kullanım süreçleri siber güvenlik hususları dikkate alınarak icra edilmektedir.	5,4	16,2	18,0	33,8	26,6	3,5991	±	1,19448
İşletmemiz verilerini uygun bir şekilde yedeklemektedir.	1,8	15,3	16,7	30,2	36,0	3,8333	±	1,13128
İşletmemiz kötü amaçlı yazılımlara (virüs, trojan, vb.) karşı önlemler almaktadır.	1,4	11,3	16,2	29,3	41,9	3,9910	±	1,07624
İşletmemiz bilgi sistemlerinin güvenlik açıklarını azaltmak için	2,3	9,5	17,6	30,6	40,1	3,9685	±	1,07791

önlemler almaktadır.								
İşletmemiz bilgi sistemlerine bağlantıları güvenli bir şekilde tesis etmektedir.	4,5	7,7	22,1	27,0	38,7	3,8784	±	1,14496
İşletmemiz tüm cihaz ve aygıtların çalınma riskine karşı gereken önlemleri almaktadır.	,9	4,5	16,7	37,4	40,5	4,1216	±	,90678

Önerme 1: İşletmemiz bilgi teknolojileri verilerini (sistem konfigürasyon ve yedekleri) uygun bir şekilde korumaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %4,1'i "Hiç uygulanmıyor", %14,4'ü "Kısmen uygulanıyor", 19,8'i "Uygulanıyor", %33,3'ü "Çoğunlukla uygulanıyor", %28,4'ü "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,6757 ve standart sapması 1,15074 olarak bulunmuştur. Bu önermeye verilen yanıtlar ve önermenin ortalaması incelendiğinde, işletmelerin tamamına yakınının BT verilerini uygun bir şekilde korudukları sonucuna varılmaktadır.

Önerme 2: İşletmemizde bilgi teknolojileri kurulum ve kullanım süreçleri siber güvenlik hususları dikkate alınarak icra edilmektedir.

Bu önermeye araştırmaya katılan iç denetçilerin %5,4'ü "Hiç uygulanmıyor", %16,2'si "Kısmen uygulanıyor", 18'i "Uygulanıyor", %33,8'i "Çoğunlukla uygulanıyor", %26,6'sı "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,5991 ve standart sapması 1,19448 olarak bulunmuştur. Bu önermeye verilen yanıtlar ve önermenin ortalaması incelendiğinde, işletmelerin tamamına yakınının BT kurulum ve kullanım süreçlerini siber güvenlik hususlarını dikkate alarak gerçekleştirdikleri sonucu ortaya çıkmaktadır.

Önerme 3: İşletmemiz verilerini uygun bir şekilde yedeklemektedir.

Bu önermeye araştırmaya katılan iç denetçilerin %1,8'i "Hiç uygulanmıyor", %15,3'ü "Kısmen uygulanıyor", %16,7'si "Uygulanıyor", %30,2'si "Çoğunlukla uygulanıyor", %36'sı "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,8333 ve standart sapması 1,13128 olarak bulunmuştur. Bu önermeye verilen yanıtlar ve önermenin ortalaması incelendiğinde, işletmelerin tamamına yakınının verilerini uygun şekilde yedekledikleri sonucuna ulaşılmaktadır.

Önerme 4: İşletmemiz kötü amaçlı yazılımlara (virüs, trojan, vb.) karşı önlemler almaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %1,4'ü "Hiç uygulanmıyor", %11,3'ü "Kısmen uygulanıyor", %16,2'si "Uygulanıyor", %29,3'ü "Çoğunlukla uygulanıyor", %41,9'u "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,9910 ve standart sapması 1,07624 olarak bulunmuştur. Bu önermeye verilen yanıtlar ve önermenin ortalaması incelendiğinde, işletmelerin neredeyse tamamının kötü amaçlı yazılımlara karşı önlem aldıkları anlaşılmaktadır.

Önerme 5: İşletmemiz bilgi sistemlerinin güvenlik açıklarını azaltmak için önlemler almaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %2,3'ü "Hiç uygulanmıyor", %9,5'i "Kısmen uygulanıyor", %17,6'sı "Uygulanıyor", %30,6'sı "Çoğunlukla uygulanıyor", %40,1'i "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,9685 ve standart sapması 1,07791 olarak bulunmuştur. Bu önermeye verilen yanıtlar ve önermenin ortalaması incelendiğinde, işletmelerin neredeyse tamamının güvenlik açıklarını azaltmak amacıyla önlem aldıkları anlaşılmaktadır.

Önerme 6: İşletmemiz bilgi sistemlerine bağlantıları güvenli bir şekilde tesis etmektedir.

Bu önermeye araştırmaya katılan iç denetçilerin %4,5'ü "Hiç uygulanmıyor", %7,7'si "Kısmen uygulanıyor", %22,1'i "Uygulanıyor", %27'si "Çoğunlukla uygulanıyor", %38,7'si "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,8784 ve

standart sapması 1,14496 olarak bulunmuştur. Bu önermeye verilen yanıtlar ve önermenin ortalaması incelendiğinde, işletmelerin neredeyse tamamının bilgi sistemlerine bağlantıları güvenli bir şekilde gerçekleştirdikleri anlaşılmaktadır.

Önerme 7: İşletmemiz tüm cihaz ve aygıtların çalınma riskine karşı gereken önlemleri almaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %0,9'u "Hiç uygulanmıyor", %4,5'i "Kısmen uygulanıyor", %16,7'si "Uygulanıyor", %37,4'ü "Çoğunlukla uygulanıyor", %40,5'si "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 4,1216 ve standart sapması 0,90678 olarak bulunmuştur. Buna göre, araştırmadaki işletmelerin %99'u sahip oldukları cihazların çalınmasını önlemek için gerekli önlemleri almaktadırlar.

4.5.4.2.4. Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tedbirleri- Frekans Dağılımları

Yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü tedbirleri alt boyutuna ait frekans dağılımları, ortalama ve standart sapma değerleri Tablo 4.24.'teki gibidir:

Tablo 4.24. Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tedbirleri Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri

	Hiç uygulanmıyor	Kısmen Uygulanıyor	Uygulanıyor	Çoğunlukla Uygulanıyor	Tamamen Uygulanıyor	Ort. ± Ss.		
İşletmemiz bilgi sistemlerine bağlantı için gerekli kimlik denetimlerini gerçekleştirmektedir.	5,9	14,0	21,6	29,3	29,3	3,6216	±	1,20747

İşletmemizde bilgi teknolojilerine kimlerin hangi şartlarda erişebileceği düzenlenmiştir.	5,9	12,2	18,5	33,3	30,2	3,6982	±	1,18966
İşletmemiz yerel ağlar üzerinde yetki denetimi uygulamaktadır.	9,0	12,2	18,0	27,5	33,3	3,6396	±	1,29945
İşletmemiz yazılım geliştirme projelerinin güvenlik gereksinimlerini tanımlamakta ve bu gereksinimleri projelere dahil etmektedir.	12,6	17,6	17,6	29,3	23,0	3,3243	±	1,33970
İşletmemiz yazılım ürünlerinin seçimi, satın alınması ve/veya bakım işlerinde güvenlik kontrolleri gerçekleştirmektedir.	8,6	18,9	17,6	28,4	26,6	3,4550	±	1,29575

Önerme 1: İşletmemiz bilgi sistemlerine bağlantı için gerekli kimlik denetimlerini gerçekleştirmektedir.

Bu önermeye araştırmaya katılan iç denetçilerin %5,9'u "Hiç uygulanmıyor", %14'ü "Kısmen uygulanıyor", %21,6'sı "Uygulanıyor", %29,3'ü "Çoğunlukla uygulanıyor", %29,3'ü "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması

3,6216 ve standart sapması 1,20747 olarak bulunmuştur. Bu önermenin ortalama değeri dikkate alındığında, işletmelerin çoğunlukla bilgi sistemleri kimlik denetimlerini gerçekleştirdikleri sonucuna ulaşılmaktadır.

Önerme 2: İşletmemizde bilgi teknolojilerine kimlerin hangi şartlarda erişebileceği düzenlenmiştir.

Bu önermeye araştırmaya katılan iç denetçilerin %5,9'u "Hiç uygulanmıyor", %12,2'si "Kısmen uygulanıyor", %18,5'i "Uygulanıyor", %33,3'ü "Çoğunlukla uygulanıyor", %30,2'si "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,6982 ve standart sapması 1,18966 olarak bulunmuştur. Bu önermenin ortalama değeri dikkate alındığında, işletmelerin çoğunlukla bilgi teknolojilerine kimlerin hangi şartlarda erişebileceğini düzenledikleri sonucuna ulaşılmaktadır.

Önerme 3: İşletmemiz yerel ağlar üzerinde yetki denetimi uygulamaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %9'u "Hiç uygulanmıyor", %12,2'si "Kısmen uygulanıyor", %18'i "Uygulanıyor", %27,5'i "Çoğunlukla uygulanıyor", %33,3'ü "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,6396 ve standart sapması 1,29945 olarak bulunmuştur. Bu önermenin ortalama değeri dikkate alındığında, işletmelerin çoğunlukla yerel ağlar üzerinde yetki denetimi uyguladıkları anlaşılmaktadır.

Önerme 4: İşletmemiz yazılım geliştirme projelerinin güvenlik gereksinimlerini tanımlamakta ve bu gereksinimleri projelere dahil etmektedir.

Bu önermeye araştırmaya katılan iç denetçilerin %12,6'sı "Hiç uygulanmıyor", %17,6'sı "Kısmen uygulanıyor", %17,6'sı "Uygulanıyor", %29,3'ü "Çoğunlukla uygulanıyor", %23'ü "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,3243 ve standart sapması 1,33970 olarak bulunmuştur. Bu önermenin ortalama değeri dikkate alındığında, işletmelerin yazılım geliştirme projelerinin güvenlik gereksinimlerini tanımladıkları ve bunları projelere dahil ettikleri sonucuna varılmaktadır.

Önerme 5: İşletmemiz yazılım ürünlerinin seçimi, satın alınması ve/veya bakım işlerinde güvenlik kontrolleri gerçekleştirmektedir.

Bu önermeye araştırmaya katılan iç denetçilerin %8,6'sı “Hiç uygulanmıyor”, %18,9'u “Kısmen uygulanıyor”, %17,6'sı “Uygulanıyor”, %28,4'ü “Çoğunlukla uygulanıyor”, %26,6'sı “Tamamen uygulanıyor” şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,4550 ve standart sapması 1,29575 olarak bulunmuştur. Bu önermenin ortalama değeri dikkate alındığında, işletmelerin büyük çoğunluğunun yazılım ürünlerinin seçimi, satın alınması ve/veya bakım işlerinde gerekli güvenlik kontrollerini gerçekleştirdikleri anlaşılmaktadır.

4.5.4.2.5. Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi- Frekans Dağılımları

Siber güvenlik ihlalleri ve iş sürekliliği yönetimi yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü tedbirleri alt boyutuna ait frekans dağılımları, ortalama ve standart sapma değerleri Tablo 4.25.'teki gibidir:

Tablo 4.25. Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri

	Hiç uygulanmıyor	Kısmen Uygulanıyor	Uygulanıyor	Çoğunlukla Uygulanıyor	Tamamen Uygulanıyor	Ort. ± Ss.		
İşletmemiz bilgi sistemleri arızalarının kurum faaliyetlerini aksatmaması için gerekli önlemleri almaktadır.	5,4	10,4	18,5	44,1	21,6	3,6622	±	1,09226
İşletmemizde olası bilgi sistemi kaynaklı problemler için uygulanacak acil eylemleri belirten	6,8	15,8	20,7	30,6	26,1	3,5360	±	1,22421

yazılı prosedürler bulunmaktadır.								
İşletmemizin bilgi sistemleri arızalarına karşı mücadeleyi ele alan bir İş Sürekliliği Yönetimi bulunmaktadır.	10,8	15,8	19,8	29,7	23,9	3,4009	±	1,29970

Önerme 1: İşletmemiz bilgi sistemleri arızalarının kurum faaliyetlerini aksatmaması için gerekli önlemleri almaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %5,4'ü "Hiç uygulanmıyor", %10,4'ü "Kısmen uygulanıyor", %18,5'i "Uygulanıyor", %44,1'i "Çoğunlukla uygulanıyor", %21,6'sı "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,6622 ve standart sapması 1,09226 olarak bulunmuştur. Buna göre, işletmelerin büyük çoğunluğu BT arızalarının faaliyetlerini aksatmaması için gereken önlemleri almaktadır.

Önerme 2: İşletmemizde olası bilgi sistemi kaynaklı problemler için uygulanacak acil eylemleri belirten yazılı prosedürler bulunmaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %6,8'i "Hiç uygulanmıyor", %15,8'i "Kısmen uygulanıyor", %20,7'si "Uygulanıyor", %30,6'sı "Çoğunlukla uygulanıyor", %26,1'i "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,5360 ve standart sapması 1,22421 olarak bulunmuştur. Buna göre, işletmelerin büyük çoğunluğu bilgi sistemi kaynaklı problemler için uygulanacak acil eylemleri belirten yazılı prosedürlere sahiptir.

Önerme 3: İşletmemizin bilgi sistemleri arızalarına karşı mücadeleyi ele alan bir İş Sürekliliği Yönetimi bulunmaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %10,8'i "Hiç uygulanmıyor", %15,8'i "Kısmen uygulanıyor", %19,8'i "Uygulanıyor", %29,7'si "Çoğunlukla uygulanıyor", %23,9'u "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması

3,4009 ve standart sapması 1,29970 olarak bulunmuştur. Buna göre, işletmelerin büyük çoğunluğu İş Sürekliliği Yönetimi'ne sahiptir.

4.5.4.3. İşletmelerin Siber Güvenlik Faaliyetleri Seviyelerine İlişkin Kruskal-Wallis Testleri Sonuçları ve Yorumları

İşletmelerin siber güvenlik faaliyetleri seviyelerinin işletmelerin özelliklerine göre farklılık gösterip göstermediğini belirlemek amacıyla farklılık testleri yapılmıştır. Normallik testi sonuçlarına göre (Tablo 4.8.) araştırmanın verileri normal dağılım göstermediğinden non parametrik farklılık testi olan Kruskal-Wallis testleri gerçekleştirilmiştir. Test sonuçları aşağıdaki bölümlerde aktarılmıştır.

4.5.4.3.1. Siber Güvenlik Faaliyetleri Seviyeleri- Çalışan Sayısına Göre Kruskal-Wallis Testi Sonuçları ve Yorumları

Siber güvenlik faaliyetleri seviyeleri ve alt boyutlarının işletmelerin çalışan sayılarına göre farklılık gösterip göstermediği Kruskal-Wallis testi yapılarak sınanmıştır. Test sonuçları Tablo 4.26.'da yer almaktadır:

Tablo 4.26. Siber Güvenlik Faaliyetleri Seviyeleri-Çalışan Sayısına Göre Kruskal-Wallis Testi

Değişkenler	Çalışan Sayısı	N	Ortalama Sıra	Ki-Kare değeri	p
Siber Güvenliğe Kurumsal Yaklaşım	100'ün altı	9	144,22	26,464	,000*
	100-299	19	108,58		
	300-999	105	89,81		
	1000-4999	61	130,53		
	5000 ve üzeri	28	142,82		
Fiziksel ve Çevresel Güvenlik Tedbirleri	100'ün altı	9	96,89	6,941	,118
	100-299	19	120,68		
	300-999	105	97,46		
	1000-4999	61	128,22		
	5000 ve üzeri	28	126,20		
Bilgi Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri	100'ün altı	9	145,67	42,875	,000*
	100-299	19	126,08		
	300-999	105	82,29		
	1000-4999	61	135,93		
	5000 ve üzeri	28	146,95		
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tedbirleri	100'ün altı	9	156,33	54,413	,000*
	100-299	19	112,11		
	300-999	105	79,82		
	1000-4999	61	139,26		

	5000 ve üzeri	28	154,98		
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	100'ün altı	9	162,83	54,900	,000*
	100-299	19	117,16		
	300-999	105	80,33		
	1000-4999	61	133,10		
	5000 ve üzeri	28	161,00		
Genel Ortalama	100'ün altı	9	148,11	45,629	,000*
	100-299	19	118,66		
	300-999	105	81,98		
	1000-4999	61	135,69		
	5000 ve üzeri	28	152,89		

Test sonuçlarına göre; H1b (Fiziksel ve Çevresel Güvenlik Tedbirleri) hipotezi hariç tüm hipotezlerin p değerleri 0,05' den küçük olarak hesaplanmıştır. $P < 0.05$ olduğundan H1 hipotezi ve H1b hariç tüm alt hipotezler kabul edilmiştir.

Araştırmaya katılan işletmelerin siber güvenlik faaliyetleri seviyesi ve buna bağlı alt boyutlar işletmelerin çalışanlarının sayısı dikkate alındığında bir anlamlı farklılığa sahiptir. Farklılığın yönünü belirlemek amacı ile post hoc testlerinden Tamhane's T2 testi yapılmıştır. Test sonuçlarına göre 300-999 çalışan sayısına sahip işletmelerin ortalamaları 1000-4999 ve 5000 üzeri çalışanı olan işletmelere göre daha düşüktür. Çalışan sayısı fazla olan işletmelerin siber güvenlik yaklaşımları ve seviyeleri az çalışanı olan işletmelere kıyasla daha iyidir.

4.5.4.3.2. Siber Güvenlik Faaliyetleri Seviyeleri- İşletmelerin Aktif Büyüklüklerine Göre Kruskal-Wallis Testi Sonuçları ve Yorumları

Siber güvenlik faaliyetleri seviyesi ve alt boyutlarının işletmelerin aktif büyüklüklerine göre farklılık gösterip göstermediği Kruskal-Wallis testi yapılarak sınanmıştır. Test sonuçları Tablo 4.27.'de yer almaktadır:

Tablo 4.27. Siber Güvenlik Faaliyetleri Seviyeleri -Aktif Büyüklüğüne Göre Kruskal-Wallis Testi

Değişkenler	Aktif Büyüklüğü	N	Ortalama Sıra	Ki-Kare değeri	p
	10 milyon TL ve altı	5	128,10	28,880	,000*

Siber Güvenliğe Kurumsal Yaklaşım	10 milyon TL-100 milyon TL	18	124,39		
	100 milyon TL-1 milyar TL	53	74,78		
	1 milyar TL-10 milyar TL	75	110,03		
	10 milyar TL üzeri	71	136,02		
Fiziksel ve Çevresel Güvenlik Tedbirleri	10 milyon TL ve altı	5	96,80	31,530	,000*
	10 milyon TL-100 milyon TL	18	127,92		
	100 milyon TL-1 milyar TL	53	72,82		
	1 milyar TL-10 milyar TL	75	113,56		
	10 milyar TL üzeri	71	135,07		
Bilgi Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri	10 milyon TL ve altı	5	128,20	30,406	,000*
	10 milyon TL-100 milyon TL	18	128,47		
	100 milyon TL-1 milyar TL	53	78,76		
	1 milyar TL-10 milyar TL	75	102,92		
	10 milyar TL üzeri	71	139,52		
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tedbirleri	10 milyon TL ve altı	5	156,30	29,713	,000*
	10 milyon TL-100 milyon TL	18	122,42		
	100 milyon TL-1 milyar TL	53	83,26		
	1 milyar TL-10 milyar TL	75	99,21		
	10 milyar TL üzeri	71	139,64		
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	10 milyon TL ve altı	5	159,20	29,496	,000*
	10 milyon TL-100 milyon TL	18	125,83		
	100 milyon TL-1 milyar TL	53	78,69		
	1 milyar TL-10 milyar TL	75	104,45		
	10 milyar TL üzeri	71	136,44		

Genel Ortalama	10 milyon TL ve altı	5	140,90	35,481	,000*
	10 milyon TL-100 milyon TL	18	127,75		
	100 milyon TL-1 milyar TL	53	74,74		
	1 milyar TL-10 milyar TL	75	103,82		
	10 milyar TL üzeri	71	140,87		

Araştırmaya katılan işletmelerin siber güvenlik faaliyetleri seviyesi ve buna bağlı tüm alt boyutlar işletmelerin aktif büyüklüklerine göre anlamlı farklılık göstermektedir ($p<0,05$). Farklılığın yönünü test edebilmek amacı ile post hoc testlerinden Tamhane's T2 testi yapılmıştır. Test sonuçlarına göre aktif büyüklüğü 100 milyon TL-1 Milyar TL olan işletmelerin ortalamaları, aktif büyüklüğü 1 milyar TL-10 milyar TL ile 10 milyar TL üzeri olan işletmelere göre daha düşüktür. Aktif büyüklüğü arttıkça işletmelerin siber güvenlik yaklaşımları ve seviyeleri daha iyi olmaktadır.

İşletmelerin büyüklükleri ile alakalı varsayımlar içeren ilk iki hipoteze ait sonuçlar değerlendirildiğinde; işletmelerin büyüklükleri arttıkça siber güvenlik faaliyetleri seviyelerinin de arttığı sonucuna ulaşılmıştır. Sonuç olarak, işletmelerin büyüklüklerinin artmasına paralel siber güvenlik ve BT olan yatırımlarının artması ve etkin bir kurumsal yönetim ve iç kontrol sisteminin gerekliliği bu sonuçların ortaya çıkmasında önemli role sahiptir ve beklenen bir durumdur.

4.5.4.3.3. Siber Güvenlik Faaliyetleri Seviyeleri- İşletmelerin BT Bağımlılıklarına Göre Kruskal-Wallis Testi Sonuçları ve Yorumları

Siber güvenlik faaliyetleri seviyesi ve alt boyutlarının işletmelerin BT bağımlılıklarına göre farklılık gösterip göstermediği Kruskal-Wallis testi yapılarak sınanmıştır. Test sonuçları Tablo 4.28.'de yer almaktadır:

Tablo 4.28. Siber Güvenlik Faaliyetleri Seviyeleri -BT Bağımlılıklarına Göre Kruskal-Wallis Testi

Değişkenler	BT Bağımlılığı	N	Ortalama Sıra	Ki-Kare değeri	p
Siber Güvenliğe Kurumsal Yaklaşım	Az bağımlı	55	39,35	114,642	,000*
	Bağımlı	68	107,17		
	Çok bağımlı	99	154,56		
Fiziksel ve Çevresel Güvenlik Tedbirleri	Az bağımlı	55	66,04	48,006	,000*
	Bağımlı	68	107,99		
	Çok bağımlı	99	139,17		
Bilgi Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri	Az bağımlı	55	40,84	112,210	,000*
	Bağımlı	68	106,01		
	Çok bağımlı	99	154,53		
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tedbirleri	Az bağımlı	55	42,82	105,519	,000*
	Bağımlı	68	106,37		
	Çok bağımlı	99	153,18		
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	Az bağımlı	55	36,03	121,627	,000*
	Bağımlı	68	110,20		
	Çok bağımlı	99	154,32		
Genel Ortalama	Az bağımlı	55	37,17	122,167	,000*
	Bağımlı	68	106,45		
	Çok bağımlı	99	156,26		

Araştırmaya katılan işletmelerin siber güvenlik faaliyetleri seviyesi ve buna bağlı tüm alt boyutlar işletmelerin BT bağımlılık seviyelerine göre anlamlı farklılık

göstermektedir ($p < 0,05$). Farklılığın yönünü belirleyebilmek adına post hoc testlerinden Tamhane's T2 testi yapılmıştır. Test sonuçlarına göre "Az bağımlı" işletmelerin ortalamaları "Bağımlı" ve Çok bağımlı işletmelerden; "Bağımlı" işletmelerin ortalamaları ise "Çok bağımlı" işletmelerden daha düşüktür. "Bağımlı Değil" sınıflandırılmasının hiçbir katılımcı tarafından seçilmemesi de dikkate değer bir husustur. Ancak araştırmanın ana kütlesini oluşturan Borsa İstanbul şirketlerinin kurumsal yapılanmaları ve faaliyetlerinin büyüklüğü göz önüne alındığında işletmelerin BT bağımlılıklarının bulunması normal bir durumdur. Test sonuçlarına göre işletmelerin BT bağımlılıkları arttıkça siber güvenlik faaliyeti seviyeleri de pozitif yönde artmaktadır.

4.5.4.3.4. Siber Güvenlik Faaliyetleri Seviyeleri- Siber Saldırıların İşletme İtibarına Etkisine Göre Kruskal-Wallis Testi Sonuçları ve Yorumları

Siber güvenlik faaliyetleri seviyesi ve alt boyutlarının siber saldırıların işletme itibarına etkisine göre farklılık gösterip göstermediği Kruskal-Wallis testi yapılarak sınanmıştır. Test sonuçları Tablo 4.29.'da yer almaktadır:

Tablo 4.29. Siber Güvenlik Faaliyetleri Seviyeleri-Siber Saldırıların İşletme İtibarına Etkisine Göre Kruskal-Wallis Testi

Değişkenler	Siber Saldırıların İşletme İtibarına Etkisi	N	Ortalama Sıra	Ki-Kare değeri	p
Siber Güvenliğe Kurumsal Yaklaşım	Neredeyse yok	5	66,10	92,797	,000*
	Az	58	53,75		
	Çok	81	109,74		
	İşletmenin Geleceğini Etkileyecek Kadar Fazla	78	159,18		
Fiziksel ve Çevresel Güvenlik Tedbirleri	Neredeyse yok	5	102,60	44,667	,000*
	Az	58	72,79		

	Çok	81	107,35		
	İşletmenin Geleceğini Etkileyecek Kadar Fazla	78	145,16		
Bilgi Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri	Neredeyse yok	5	92,10	82,153	,000*
	Az	58	51,73		
	Çok	81	116,89		
	İşletmenin Geleceğini Etkileyecek Kadar Fazla	78	151,59		
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tedbirleri	Neredeyse yok	5	122,60	72,175	,000*
	Az	58	54,86		
	Çok	81	115,48		
	İşletmenin Geleceğini Etkileyecek Kadar Fazla	78	148,78		
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	Neredeyse yok	5	93,60	81,334	,000*
	Az	58	50,38		
	Çok	81	120,96		
	İşletmenin Geleceğini Etkileyecek Kadar Fazla	78	148,27		
Genel Ortalama	Neredeyse yok	5	95,20	87,679	,000*
	Az	58	50,97		
	Çok	81	113,99		
	İşletmenin Geleceğini Etkileyecek Kadar Fazla	78	154,97		

Araştırmaya katılan işletmelerin siber güvenlik faaliyetleri seviyesi ve alt boyutları siber saldırıların işletme itibarına etkisine göre anlamlı farklılık göstermektedir. ($P<0,05$). Farklılığın yönünü test edebilmek amacı ile post hoc testlerinden Tamhane's T2 testi yapılmıştır. Test sonuçlarına göre itibar riski "Az" olan işletmelerin ortalamaları itibar riski "Çok" ve "İşletmenin Geleceğini Etkileyecek Kadar Fazla" olan işletmelerden daha düşük ortalama sahiptir. Kısacası itibar riski arttıkça işletmelerin siber güvenlik faaliyeti seviyeleri de bu risklere paralel olarak artmaktadır.

4.5.4.3.5. Siber Güvenlik Faaliyetleri Seviyeleri- İşletmelerin Kritik Bilgilere Sahip Olmalarına Göre Kruskal-Wallis Testi Sonuçları ve Yorumları

Siber güvenlik faaliyetleri seviyesi ve alt boyutlarının işletmelerin kritik bilgilere sahip olmasına göre farklılık gösterip göstermediği Kruskal-Wallis testi yapılarak sınanmıştır. Test sonuçları Tablo 4.30.'da yer almaktadır:

Tablo 4.30. Siber Güvenlik Faaliyetleri Seviyeleri-İşletmelerin Kritik Bilgilere Sahip Olmalarına Göre Kruskal-Wallis Testi

Değişkenler	Kritik Bilgilere Sahip Olma	N	Ortalama Sıra	Ki-Kare değeri	p
Siber Güvenliğe Kurumsal Yaklaşım	Neredeyse yok	7	68,50	92,797	,000*
	Az	73	71,05		
	Çoğunlukla kritik	44	98,81		
	Tamamı Kritik	98	150,40		
Fiziksel ve Çevresel Güvenlik Tedbirleri	Neredeyse yok	7	71,43	44,667	,000*
	Az	73	78,44		
	Çoğunlukla kritik	44	114,13		

	Tamamı Kritik	98	137,81		
Bilgi Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri	Neredeyse yok	7	94,07	82,153	,000*
	Az	73	67,64		
	Çoğunlukla kritik	44	106,15		
	Tamamı Kritik	98	147,82		
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tedbirleri	Neredeyse yok	7	115,43	72,175	,000*
	Az	73	69,49		
	Çoğunlukla kritik	44	108,28		
	Tamamı Kritik	98	143,96		
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	Neredeyse yok	7	94,93	81,334	,000*
	Az	73	68,16		
	Çoğunlukla kritik	44	112,56		
	Tamamı Kritik	98	144,49		
Genel Ortalama	Neredeyse yok	5	95,20	87,679	,000*
	Az	58	50,97		
	Çoğunlukla kritik	81	113,99		
	Tamamı Kritik	78	154,97		

Araştırmaya katılan işletmelerin siber güvenlik faaliyetleri seviyesi ve alt boyutları işletmelerin kritik bilgilere sahip olmasına göre anlamlı farklılığa sahiptir ($P < 0,05$). Farklılığın yönünü test edebilmek amacı ile post hoc testlerinden Tamhane's T2 testi yapılmıştır. Test sonuçlarına göre "Az" kritik bilgiye sahip olan işletmelerin ortalamaları bilgileri "Çoğunlukla kritik" ve "Tamamı kritik" olan işletmelerden daha düşük ortalamaya

sahiptir. İşletmelerin sahip olduğu kritik bilgilerin oranı arttıkça işletmelerin siber güvenlik faaliyeti seviyeleri artmaktadır.

H3, H4 ve H5 hipotezleri ve bu hipotezlere bağlı alt hipotezlerde işletmeler bilgi teknolojilerine bağımlılık, kritik bilgilere sahip olma ve itibar risklerine göre sınıflandırılmıştır. Yapılan analizler sonucunda işletmelerin BT bağımlılık düzeyleri, kritik bilgileri ve itibar riskleri arttıkça siber güvenlik faaliyeti seviyesinin de arttığı anlaşılmıştır.

21. yüzyılda bilgi teknolojilerinin her alanda kullanılması ve vazgeçilmez bir hale gelmesi, özellikle nerdeyse tüm faaliyetlerin dijital ortamlarda yürütülmeye başlanması, bilgi hacminin artması ve bilginin en önemli rekabet aracı olması bilginin ve bilgiyi sağlayan kaynakların korunmasını zorunlu hale getirmiştir. Daha önce çalışmanın 2. bölümünde de açıklandığı üzere bilgi teknolojilerine dayalı uygulamaların barındırdığı birtakım riskler bulunmaktadır. İşletmelerin faaliyetlerini tehlikeye atacak her türlü zarardan ve riskten korunmak için siber güvenlik faaliyetlerine önem vermesi kaçınılmazdır. Tüm bunların bir sonucu olarak işletmelerin BT bağımlılıkları, kritik bilgileri ve itibar riski arttıkça bir savunma mekanizması olarak siber güvenlik faaliyetleri seviyelerinin de pozitif yönde artması öngörülebilir bir durumdur.

4.5.4.3.6. Siber Güvenlik Faaliyetleri Seviyeleri- Faaliyet Gösterilen Sektöre Göre Kruskal-Wallis Testi Sonuçları ve Yorumları

Siber güvenlik faaliyetleri seviyesi ve alt boyutlarının işletmelerin sektörüne göre farklılık gösterip göstermediği Kruskal-Wallis testi yapılarak sınanmıştır. Test sonuçları Tablo 4.31.'de yer almaktadır:

Tablo 4.31. Siber Güvenlik Faaliyetleri Seviyeleri-Faaliyet Gösterilen Sektöre Göre Kruskal-Wallis Testi

Değişkenler	Faaliyet Gösterilen Sektör	N	Ortalama Sıra	Ki-Kare değeri	p
Siber Güvenliğe Kurumsal Yaklaşım	Üretim	45	69,30	105,143	,000*
	Bankacılık	49	167,24		
	Havacılık ve Uzay	9	124,72		
	Madencilik/Metaller/Mineraller	8	56,31		

	Risk Yönetimi ve Sigorta	25	163,46		
	Enerji	22	99,95		
	İletişim, Medya ve Teknoloji	9	101,78		
	Kimya	7	47,00		
	Perakende	11	116,00		
	İnşaat	9	23,00		
	Diğer	28	101,89		
Fiziksel ve Çevresel Güvenlik Tedbirleri	Üretim	45	85,43	42,905	,000*
	Bankacılık	49	143,58		
	Havacılık ve Uzay	9	126,28		
	Madencilik/Metaller/Mineraller	8	88,06		
	Risk Yönetimi ve Sigorta	25	154,70		
	Enerji	22	112,27		
	İletişim, Medya ve Teknoloji	9	106,56		
	Kimya	7	89,36		
	Perakende	11	85,23		
	İnşaat en kötü	9	81,17		
	Diğer	28	87,21		
Bilgi Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri	Üretim	45	68,00	98,347	,000*
	Bankacılık	49	165,14		
	Havacılık ve Uzay	9	122,61		
	Madencilik/Metaller/Mineraller	8	59,06		
	Risk Yönetimi ve Sigorta	25	156,38		
	Enerji	22	100,34		
	İletişim, Medya ve Teknoloji	9	102,94		
	Kimya	7	49,79		
	Perakende	11	122,91		

	İnşaat	9	22,06		
	Diğer	28	110,09		
Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tebdirleri	Üretim	45	71,76	94,553	,000*
	Bankacılık	49	167,70		
	Havacılık ve Uzay	9	105,61		
	Madencilik/Metaller/Mineraller	8	49,94		
	Risk Yönetimi ve Sigorta	25	137,82		
	Enerji	22	110,64		
	İletişim, Medya ve Teknoloji	9	97,78		
	Kimya	7	44,07		
	Perakende	11	116,14		
	İnşaat	9	19,00		
	Diğer	28	122,86		
Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi	Üretim	45	65,40	91,576	,000*
	Bankacılık	49	161,20		
	Havacılık ve Uzay	9	114,67		
	Madencilik/Metaller/Mineraller	8	60,56		
	Risk Yönetimi ve Sigorta	25	146,26		
	Enerji	22	110,70		
	İletişim, Medya ve Teknoloji	9	105,39		
	Kimya	7	55,79		
	Perakende	11	135,77		
	İnşaat	9	20,00		
	Diğer	28	117,50		
Genel Ortalama	Üretim	45	67,17	102,543	,000*
	Bankacılık	49	168,47		
	Havacılık ve Uzay	9	117,06		

	Madencilik/Metaller/Mineraller	8	55,44		
	Risk Yönetimi ve Sigorta	25	155,88		
	Enerji	22	105,55		
	İletişim, Medya ve Teknoloji	9	101,44		
	Kimya	7	49,43		
	Perakende	11	117,27		
	İnşaat	9	22,44		
	Diğer	28	107,45		

Araştırmaya katılan işletmelerin siber güvenlik faaliyetleri seviyesi ve alt boyutları işletmelerin sektörlerine göre anlamlı farklılık göstermektedir. ($P < 0,05$). Farklılığın yönünü test edebilmek amacı ile post hoc testlerinden Tamhane's T2 testi yapılmıştır. Yapılan test sonucunda İnşaat ve Üretim sektörlerinin ortalamaları Enerji, Risk Yönetimi ve Sigorta ve Bankacılık sektörlerinin ortalamalarından düşük olduğu belirlenmiştir.

Enerji, Risk Yönetimi ve Sigorta ve Bankacılık sektörleri diğer sektörlerle kıyasla daha kritik altyapıları ve bilgileri barındırmaktadır. Ayrıca bu sektörler siber güvenliğe ilişkin yasal düzelmelere tabidir. Özellikle Sigortacılık ve Bankacılık sektörleri ekonomiye verdikleri yön gerek işlem hacimleri ve gerekse sahip oldukları müşteri bilgileri ile siber güvenlik açısından en kritik sektörlerdendir. Enerji sektörü ise sahip olduğu kritik altyapılar ve herhangi bir kesinti ve zarara uğraması durumunda ortaya çıkacak yıkıcı sonuçlar nedeniyle siber güvenlik konularına duyarlı bir sektördür. Bu sektörlerde faaliyet gösteren işletmelerin siber güvenlik faaliyetleri seviyelerinin diğer sektörlerle kıyasla daha iyi olması beklenen bir durumdur.

4.5.5. İşletmelerin İç Denetim Birimlerinin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliğine İlişkin Hipotezler, Frekans Dağılımları ve Farklılık Analizleri

Çalışmanın bu bölümünde sırasıyla işletmelerin iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliğine ilişkin hipotezler, frekans dağılımları ve farklılık analizlerine yer verilmiştir. Ayrıca analiz bulguları ve sonuçları yorumlanmıştır.

4.5.5.1. İç Denetim Birimlerinin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliğine İlişkin Hipotezler

Bu araştırmanın ikinci konusu ise; “Türkiye’de faaliyet gösteren halka açık işletmelerin iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliği ne durumdadır?” ve “İşletmelerin iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliği işletmelerin özelliklerine göre farklılaşmakta mıdır?” sorularından hareketle oluşturulmuştur.

Bu bağlamda iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliğini belirlemek amacıyla aşağıdaki alt boyutlar belirlenmiştir:

- İç Denetim Departmanının Siber Güvenliği Gözden Geçirme Sıklığı
- İç Denetim ve Bilgi Teknolojileri (BT) Departmanları Arasındaki İlişkinin Algısı
- İç Denetim Departmanının Siber Güvenlik Bilgi Düzeyi Algısı
- Siber Güvenlik Konusunda Üst Yönetimin Desteğine İlişkin İç Denetçi Algısı

Yukarıda belirlenen alt boyutların işletmelerin aktif büyüklüğü, BT bağımlılıkları, kritik bilgilere sahip olma durumları ve sektörlerine göre farklılık gösterip göstermediklerini belirlemek için fark testleri uygulanacaktır. Türkiye’de faaliyet gösteren halka açık işletmelerin Türkiye’de faaliyet gösteren halka açık işletmelerin iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliğine ilişkin hipotezler (Hipotez 7-9) ve araştırma modeli (Şekil 4.2.) aşağıda sunulmuştur:

H7: İç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği işletmelerin büyüklüğüne göre anlamlı farklılık göstermektedir.

- **H7a:** İç denetçinin BT bilgi düzeyi işletmelerin büyüklüğüne göre anlamlı farklılık göstermektedir.
- **H7b:** İç denetim biriminin siber güvenliği gözden geçirme sıklığı işletmelerin büyüklüğüne göre anlamlı farklılık göstermektedir.
- **H7c:** Siber güvenlik konusunda üst yönetimin iç denetime verdiği destek işletmelerin aktif büyüklüğüne göre anlamlı farklılık göstermektedir.
- **H7d:** İç denetim ve BT departmanları arasındaki ilişkinin kalitesi işletmelerin aktif büyüklüğüne göre anlamlı farklılık göstermektedir.

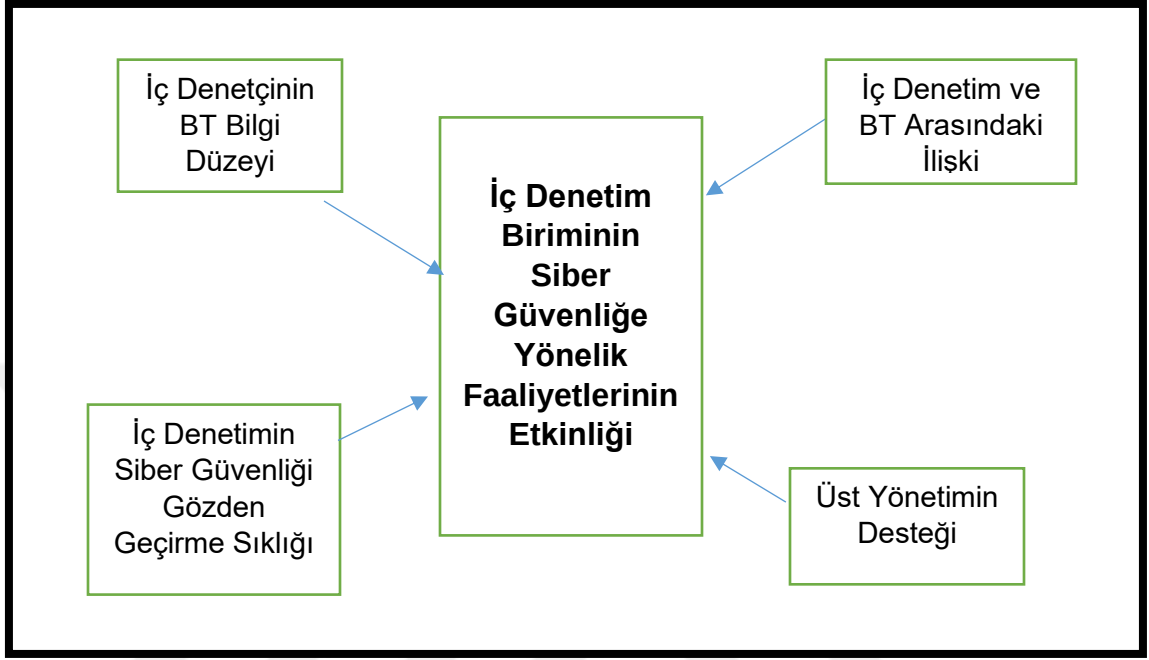
H8: İç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği işletmelerin sektörüne göre anlamlı farklılık göstermektedir.

- **H8a:** İç denetçinin BT bilgi düzeyi faaliyet gösterdiği işletmenin sektörüne göre anlamlı farklılık göstermektedir.
- **H8b:** İç denetim biriminin siber güvenliği gözden geçirme sıklığı faaliyet gösterdiği işletmenin sektörüne göre anlamlı farklılık göstermektedir.
- **H8c:** Siber güvenlik konusunda üst yönetimin iç denetime verdiği destek işletmenin sektörüne göre anlamlı farklılık göstermektedir.
- **H8d:** İç denetim ve BT departmanları arasındaki ilişkinin kalitesi işletmenin sektörüne göre anlamlı farklılık göstermektedir.

H9: İç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği işletmelerin bilgi teknolojilerine bağımlılık düzeyine göre anlamlı farklılık göstermektedir.

- **H9a:** İç denetçinin BT bilgi düzeyi işletmelerin bilgi teknolojilerine bağımlılık düzeyine göre anlamlı farklılık göstermektedir.
- **H9b:** İç denetim biriminin siber güvenliği gözden geçirme sıklığı işletmelerin bilgi teknolojilerine bağımlılık düzeyine göre anlamlı farklılık göstermektedir.
- **H9c:** Siber güvenlik konusunda üst yönetimin iç denetime verdiği destek işletmelerin bilgi teknolojilerine bağımlılık düzeyine göre anlamlı farklılık göstermektedir.
- **H9d:** İç denetim ve BT departmanları arasındaki ilişkinin kalitesi işletmelerin bilgi teknolojilerine bağımlılık düzeyine göre anlamlı farklılık göstermektedir.

Yukarıda belirlenen alt boyutlar ve sonrasında oluşturulan hipotezler sonucu ortaya çıkan iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliğine ilişkin araştırma modeli Şekil 4.2.'de sunulmuştur:



Şekil 4.2. Araştırma Modeli: İç Denetçilerin Siber Güvenlik Faaliyetlerinin Etkinliği

4.5.5.2. İç Denetim Biriminin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliğine İlişkin Frekans Dağılımları

İç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliğini belirlemek üzere yöneltilen sorulara verilen cevaplar aşağıda sunulmuştur. Çalışmada 5’li likert ölçeği kullanılmış ve araştırmaya katılan iç denetçilerden, aşağıdaki seçeneklerden birini işaretlemeleri beklenmiştir.

- 1- Hiç katılmıyorum
- 2- Kısmen katılıyorum
- 3- Kararsızım
- 4- Katılıyorum
- 5- Tamamen katılıyorum

ve

- 1- Hiç yapılmaz
- 2- Nadiren yapılır

3- Bazen yapılır

4- Sıklıkla yapılır

5- Çok sıklıkla yapılır

Cevaplara 1-5 arası ağırlık verilerek, her ifade için frekans, ağırlıklı ortalama ve standart sapması hesaplanmıştır.

4.5.5.2.1. İç Denetim ve Bilgi Teknolojileri (BT) Departmanları Arasındaki İlişkinin Algısı-Frekans Dağılımları

İç denetim ve bilgi teknolojileri (BT) departmanları arasındaki ilişkinin algısı alt boyutuna ait frekans dağılımları, ortalama ve standart sapma değerleri Tablo 4.32.'deki gibidir:

Tablo 4.32. İç Denetim ve Bilgi Teknolojileri (BT) Departmanları Arasındaki İlişkinin Algısı Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri

	Hiç Katılmıyorum	Kısmen Katılmıyorum	Kararsızım	Katılıyorum	Tamamen Katılıyorum	Ort. ± Ss.		
Çalıştığım işletmede iç denetim ile BT departmanları arasında uyumsuzluk/anlaşmazlık vardır.	76,1	14,9	3,6	3,6	1,8	1,4009	±	0,86490
Çalıştığım işletmede iç denetim ve BT personeli arasındaki ilişki yakın ve kişiseldir.	41,4	25,2	22,5	9,0	1,8	2,0450		1,07953
Çalıştığım işletmede, iç denetim ile BT personeli arasında iyi bir iş ilişkisi vardır.	1,4	1,4	16,2	56,8	24,3	4,0135	±	0,76389

BT ve iç denetim çalışanları, bilgi sistemlerinin güvenilir olmasını sağlamak için birlikte çalışmaktadır.	2,3	4,1	18,9	40,1	34,7	4,0090	±	0,95126

Önerme 1: Çalıştığım işletmede iç denetim ile BT departmanları arasında uyumsuzluk/anlaşmazlık vardır.

Bu önermeye araştırmaya katılan iç denetçilerin %76,1'i "Hiç Katılmıyorum", %14,9'u "Kısmen Katılıyorum", %3,6'sı "Kararsızım", %3,6'sı "Katılıyorum", %1,8'i "Tamamen Katılıyorum" şeklinde cevaplamışlardır. Bu önermenin ortalaması 1,4009 ve standart sapması 0,86490 olarak bulunmuştur. Bu sonuçlara göre, iç denetçilerin büyük çoğunluğunun BT çalışanları ile uyum içerisinde çalışmakta olduğu anlaşılmaktadır.

Önerme 2: Çalıştığım işletmede iç denetim ve BT personeli arasındaki ilişki yakın ve kişiseldir.

Bu önermeye araştırmaya katılan iç denetçilerin %41,4'ü "Hiç Katılmıyorum", %25,2'si "Kısmen Katılıyorum", %22,5'si "Kararsızım", %9'u "Çoğunlukla Katılıyorum", %1,8'i "Tamamen Katılıyorum" şeklinde cevaplamışlardır. Bu önermenin ortalaması 2,0450 ve standart sapması 1,07953 olarak bulunmuştur. Buna göre iç denetçilerin büyük çoğunluğunun, "iç denetim ve BT personeli arasındaki ilişki yakın ve kişiseldir" önermesine katılmadıkları anlaşılmaktadır.

Önerme 3: Çalıştığım işletmede, iç denetim ile BT personeli arasında iyi bir iş ilişkisi vardır.

Bu önermeye araştırmaya katılan iç denetçilerin %1,4'ü "Hiç Katılmıyorum", %1,4'ü "Kısmen Katılıyorum", %16,2'si "Kararsızım", %56,8'i "Çoğunlukla Katılıyorum", %24,3'ü "Tamamen uygulanıyor" şeklinde cevaplamışlardır. Bu önermenin ortalaması 4,0135 ve standart sapması 0,76389 olarak bulunmuştur. Buna göre, araştırmaya katılan iç denetçiler BT personeli arasında iyi bir iş ilişkisi olduğuna çoğunlukla katılmaktadırlar.

Önerme 4: BT ve iç denetim çalışanları, bilgi sistemlerinin güvenilir olmasını sağlamak için birlikte çalışmaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %2,3'ü "Hiç Katılmıyorum", %4,1'i "Kısmen Katılıyorum", %18,9'u "Kararsızım", %40,1'i "Çoğunlukla Katılıyorum", %34,7'si "Tamamen katılıyorum" şeklinde cevaplamışlardır. Bu önermenin ortalaması 4,0090 ve standart sapması 0,95126 olarak bulunmuştur. Buna göre iç denetçilerin, BT ve iç denetim çalışanlarının bilgi sistemlerinin güvenilir olmasını sağlamak için birlikte çalıştıkları önermesine çoğunlukla katıldıkları anlaşılmaktadır.

4.5.5.2.2. İç Denetim Departmanının Siber Güvenlik Bilgi Düzeyi Algısı- Frekans Dağılımları

İç denetim departmanının siber güvenlik bilgi düzeyi algısı alt boyutuna ait frekans dağılımları, ortalama ve standart sapma değerleri Tablo 4.33.'teki gibidir:

Tablo 4.33. İç Denetim Departmanının Siber Güvenlik Bilgi Düzeyi Algısı Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri

	Hiç Katılmıyorum	Kısmen Katılıyorum	Kararsızım	Katılıyorum	Tamamen Katılıyorum	Ort. ± Ss.		
İç denetim birimi, siber güvenlik konusunda bilgi sahibi kişilerden oluşmaktadır.	4,5	15,3	14,0	47,3	18,9	3,6081	±	1,09484
İç denetim birimi siber güvenlik konusunda uzman kişilerden oluşmaktadır.	17,6	35,1	19,4	20,7	7,2	2,6486		1,19689
İç denetim birimi siber güvenlik hakkında güncel gelişmeleri takip etmektedir.	1,4	10,4	20,7	35,1	32,4	3,8694	±	1,02726

Önerme 1: İç denetim birimi, siber güvenlik konusunda bilgi sahibi kişilerden oluşmaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %4,5'i "Hiç Katılmıyorum", %15,3'ü "Kısmen Katılıyorum", %14'ü "Kararsızım", %47,3'ü "Çoğunlukla Katılıyorum", %18,9'u "Tamamen Katılıyorum" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,6081 ve standart sapması 1,09484 olarak bulunmuştur. Bu önermeye verilen cevaplara göre, iç denetçilerin büyük çoğunluğu, çalıştıkları birimde görev yapan iç denetçileri siber güvenlik konusunda bilgi sahibi olarak tanımlamaktadır.

Önerme 2: İç denetim birimi siber güvenlik konusunda uzman kişilerden oluşmaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %17,6'sı "Hiç Katılmıyorum", %35,1'i "Kısmen Katılıyorum", %19,4'ü "Kararsızım", %20,7'si "Çoğunlukla Katılıyorum", %7,2'si "Tamamen Katılıyorum" şeklinde cevaplamışlardır. Bu önermenin ortalaması 2,6486 ve standart sapması 1,19689 olarak bulunmuştur. Bu önermeye verilen cevaplar ve önermenin ortalaması incelendiğinde, iç denetim birimlerinin önemli bir çoğunluğunun siber güvenlik konusunda uzman çalışanlara sahip olmadığı anlaşılmaktadır.

Önerme 3: İç denetim birimi siber güvenlik hakkında güncel gelişmeleri takip etmektedir.

Bu önermeye araştırmaya katılan iç denetçilerin %1,4'ü "Hiç Katılmıyorum", %10,4'ü "Kısmen Katılıyorum", %20,7'si "Kararsızım", %35,1'i "Çoğunlukla Katılıyorum", %32,4'ü "Tamamen Katılıyorum" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,8694 ve standart sapması 1,02726 olarak bulunmuştur. Buna göre iç denetlerin tamamına yakını siber güvenlik hakkında güncel gelişmeleri takip ettiği anlaşılmaktadır.

4.5.5.2.3. Siber Güvenlik Konusunda Üst Yönetimin Desteğine ilişkin İç Denetçi Algısı-Frekans Dağılımları

Siber güvenlik konusunda üst yönetimin desteğine ilişkin iç denetçi algısı alt boyutuna ait frekans dağılımları, ortalama ve standart sapma değerleri Tablo 4.34.'teki gibidir:

Tablo 4.34. Siber Güvenlik Konusunda Üst Yönetimin Desteğine İlişkin İç Denetçi Algısı
Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri

	Hiç Katılmıyorum	Kısmen Katılmıyorum	Kararsızım	Katılıyorum	Tamamen Katılıyorum	Ort. ± Ss.		
Çalıştığım işletmede üst yönetim siber güvenlik için yeterli kaynakları sağlamaktadır.	5,0	9,0	20,7	45,0	20,3	3,6667	±	1,05362
Çalıştığım işletmede, üst yönetim çalışanlarla siber güvenliğin önemi hakkında düzenli olarak iletişim kurmaktadır.	8,6	10,8	27,9	35,1	17,6	3,4234		1,15378
Çalıştığım işletmede üst yönetim siber güvenliğin önemli bir konu olduğuna inanmaktadır.	6,3	9,5	22,1	38,3	23,9	3,6396		1,13195
Çalıştığım işletmede üst yönetim siber güvenlik konularında reaktif olmaktan ziyade daha proaktiftir.	5,4	10,8	23,4	35,1	25,2	3,6396	±	1,13195

Önerme 1: Çalıştığım işletmede üst yönetim siber güvenlik için yeterli kaynakları sağlamaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %5'i "Hiç Katılmıyorum", %9'u "Kısmen Katılıyorum", %20,7'si "Kararsızım", %45'i "Çoğunlukla Katılıyorum", %20,3'ü "Tamamen

Katılıyorum” şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,6667 ve standart sapması 1,05362 olarak bulunmuştur.

Önerme 2: Çalıştığım işletmede, üst yönetim çalışanlarla siber güvenliğin önemi hakkında düzenli olarak iletişim kurmaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %8,6’sı “Hiç Katılmıyorum”, %10,8’i “Kısmen Katılıyorum”, %27,9’u “Kararsızım”, %35,1’i “Çoğunlukla Katılıyorum”, %17,6’ü “Tamamen Katılıyorum” şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,4234 ve standart sapması 1,15378 olarak bulunmuştur.

Önerme 3: Çalıştığım işletmede üst yönetim siber güvenliğin önemli bir konu olduğuna inanmaktadır.

Bu önermeye araştırmaya katılan iç denetçilerin %6,3’ü “Hiç Katılmıyorum”, %9,5’i “Kısmen Katılıyorum”, %22,1’i “Kararsızım”, %38,3’ü “Çoğunlukla Katılıyorum”, %23,9’u “Tamamen Katılıyorum” şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,6396 ve standart sapması 1,13195 olarak bulunmuştur.

Önerme 4: Çalıştığım işletmede üst yönetim siber güvenlik konularında reaktif olmaktan ziyade daha proaktiftir.

Bu önermeye araştırmaya katılan iç denetçilerin %5,4’ü “Hiç Katılmıyorum”, %10,8’i “Kısmen Katılıyorum”, %23,4’ü “Kararsızım”, %35,1’i “Çoğunlukla Katılıyorum”, %25,2’si “Tamamen Katılıyorum” şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,6396 ve standart sapması 1,13195 olarak bulunmuştur.

İç denetçilerin “Siber Güvenlik Konusunda Üst Yönetimin Desteğine” ilişkin önermelere verdikleri yanıtlar ve önermelerin ortalamaları dikkate alındığında, işletmelerin yöneticilerinin siber güvenlik konularında çalışanlarına yeterli seviyede destek oldukları anlaşılmaktadır.

4.5.5.2.4. İç Denetim Departmanının Siber Güvenliği Gözden Geçirme Sıklığı-Frekans Dağılımları

İç denetim departmanının siber güvenliği gözden geçirme sıklığına alt boyutuna ait frekans dağılımları, ortalama ve standart sapma değerleri Tablo 4.35.'teki gibidir:

Tablo 4.35. İç Denetim Departmanının Siber Güvenliği Gözden Geçirme Sıklığı Frekans Dağılımları, Ortalama ve Standart Sapma Değerleri

	Hiç Yapılmaz	Nadiren Yapılır	Bazen Yapılır	Sıklıkla Yapılır	Çok Sıklıkla Yapılır	Ort. ± Ss.		
İş sürekliliği ve olağanüstü durum kurtarma planları iç denetim tarafından yapılır.	16,2	23,9	19,4	34,7	5,9	2,9009	±	1,21047
Kimlik ve erişim yönetimi kontrolleri iç denetim yapılır.	14,0	18,9	20,3	31,5	15,3	3,1532		1,28829
Verilerin kaydedilmesi ve izlenmesi iç denetim tarafından yapılır	18,0	20,7	17,6	32,0	11,7	2,9865		1,31294
Güvenlik duvarları ve diğer ağ erişim cihazları iç denetim tarafından yapılır.	20,3	24,8	17,6	28,4	9,0	2,8108		1,29401
Kriptolama (şifreleme yönetimi dahil) iç denetim tarafından yapılır.	22,5	23,9	19,8	25,7	8,1	2,7297		1,28652
Yedekleme prosedürleri iç denetim tarafından yapılır.	22,1	21,6	19,4	27,5	9,5	2,8063		1,31244

Değişim yönetimi kontrolleri iç denetim tarafından yapılır.	21,6	24,8	18,5	27,0	8,1	2,7523		1,28580
Güvenlik politikaları kontrolü iç denetim tarafından yapılır.	17,1	13,5	14,0	40,5	14,9	3,2252	±	1,33308

Önerme 1: İş sürekliliği ve olağanüstü durum kurtarma planları iç denetim tarafından yapılır.

Bu önermeye araştırmaya katılan iç denetçilerin %16,2'si "Hiç yapılmaz", %23,9'u "Nadiren yapılır", %19,4'ü "Bazen yapılır", %34,7'si "Sıklıkla yapılır", %5,9'u "Çok sıklıkla yapılır" şeklinde cevaplamışlardır. Bu önermenin ortalaması 2,9009 ve standart sapması 1,21047 olarak bulunmuştur.

Önerme 2: Kimlik ve erişim yönetimi kontrolleri iç denetim tarafından yapılır.

Bu önermeye araştırmaya katılan iç denetçilerin %14'ü "Hiç yapılmaz", %18,9'u "Nadiren yapılır", %20,3'ü "Bazen yapılır", %31,5'i "Sıklıkla yapılır", %15,3'ü "Çok sıklıkla yapılır" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,1532 ve standart sapması 1,28829 olarak bulunmuştur.

Önerme 3: Verilerin kaydedilmesi ve izlenmesi iç denetim tarafından yapılır.

Bu önermeye araştırmaya katılan iç denetçilerin %18'i "Hiç yapılmaz", %20,7'si "Nadiren yapılır", %17,6'sı "Bazen yapılır", %32'si "Sıklıkla yapılır", %11,7'si "Çok sıklıkla yapılır" şeklinde cevaplamışlardır. Bu önermenin ortalaması 2,9865 ve standart sapması 1,31294 olarak bulunmuştur.

Önerme 4: Güvenlik duvarları ve diğer ağ erişim cihazları iç denetim tarafından yapılır.

Bu önermeye araştırmaya katılan iç denetçilerin %20,3'ü "Hiç yapılmaz", %24,8'i "Nadiren yapılır", %17,6'sı "Bazen yapılır", %28,4'ü "Sıklıkla yapılır", %9'u "Çok sıklıkla yapılır" şeklinde cevaplamışlardır. Bu önermenin ortalaması 2,8108 ve standart sapması 1,29401 olarak bulunmuştur.

Önerme 5: Kriptolama (şifreleme yönetimi dahil) iç denetim tarafından yapılır.

Bu önermeye araştırmaya katılan iç denetçilerin %22,5'i "Hiç yapılmaz", %23,9'u "Nadiren yapılır", %19,8'i "Bazen yapılır", %25,7'si "Sıklıkla yapılır", %8,1'i "Çok sıklıkla yapılır" şeklinde cevaplamışlardır. Bu önermenin ortalaması 2,7297 ve standart sapması 1,28652 olarak bulunmuştur.

Önerme 6: Yedekleme prosedürleri iç denetim tarafından yapılır.

Bu önermeye araştırmaya katılan iç denetçilerin %22,1'i "Hiç yapılmaz", %21,6'sı "Nadiren yapılır", %19,4'ü "Bazen yapılır", %27,5'i "Sıklıkla yapılır", %9,5'i "Çok sıklıkla yapılır" şeklinde cevaplamışlardır. Bu önermenin ortalaması 2,8063 ve standart sapması 1,31244 olarak bulunmuştur.

Önerme 7: Değişim yönetimi kontrolleri iç denetim tarafından yapılır.

Bu önermeye araştırmaya katılan iç denetçilerin %21,6'sı "Hiç yapılmaz", %24,8'i "Nadiren yapılır", %18,5'i "Bazen yapılır", %27'si "Sıklıkla yapılır", %8,1'i "Çok sıklıkla yapılır" şeklinde cevaplamışlardır. Bu önermenin ortalaması 2,7523 ve standart sapması 1,28580 olarak bulunmuştur.

Önerme 8: Güvenlik politikaları kontrolleri iç denetim tarafından yapılır.

Bu önermeye araştırmaya katılan iç denetçilerin %17,1'i "Hiç yapılmaz", %13,5'i "Nadiren yapılır", %14'ü "Bazen yapılır", %40,5'i "Sıklıkla yapılır", %14,9'u "Çok sıklıkla yapılır" şeklinde cevaplamışlardır. Bu önermenin ortalaması 3,2252 ve standart sapması 1,33308 olarak bulunmuştur.

"İç Denetim Departmanının Siber Güvenliği Gözden Geçirme Sıklığı"na ilişkin önermelere verilen yanıtlar ve önermelerin ortalamalar incelendiğinde, iç denetçilerin siber güvenliği gözden geçirme aralığının "Bazen yapılır" seviyesinde olduğu anlaşılmaktadır. Siber güvenlik konularında farkındalığın ve uzmanlığın artmasına paralel iç denetim birimlerinin siber güvenliğe yönelik incelemelerinin de artması beklenmektedir.

4.5.5.2.5. Siber Güvenlik Vakalarına Yönelik Frekans Dağılımları

Araştırmaya katılan iç denetçilere Siber güvenlik vakalarına yönelik sorulara verilen cevaplara ilişkin frekans dağılımları aşağıdaki gibidir.

Araştırmada yer alan şirketlerin cari dönem siber güvenlik vak'a sayısı frekans dağılımı Tablo 4.36.'da sunulmuştur:

Tablo 4.36. Cari Dönem Vaka/Veri İhlali Sayısı Frekans Dağılımı

Cari Dönem Vak'a/Veri İhlali Sayısı	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
0	65	29,3	29,3	29,3
1-10	104	43,8	43,8	76,1
11-20	43	19,4	8,1	95,5
21 ve üzeri	10	4,6	4,6	100,0
Toplam	222	100	100	

Araştırmada yer alan işletmelerin cari dönem siber güvenlik vak'a sayıları; %29,3'ü 0; %43,8'i 1-10; %19,4'ü 11-20; %4,6'sı 21 ve üzeri olacak şekilde gerçekleşmiştir.

Araştırmada yer alan şirketlerin cari dönem siber güvenliğine ilişkin iç denetim bulgularının yüzdesi frekans dağılımı Tablo 4.37.'de yer almaktadır:

Tablo 4.37. Cari Dönem Siber Güvenliğine İlişkin İç Denetim Bulgularının Yüzdesi Frekans Dağılımı

Siber Güvenliğine İlişkin İç Denetim Bulgularının Yüzdesi	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
0	54	24,3	24,3	24,3
%1-%10	112	50,5	50,5	74,8
%11-%20	26	11,7	11,7	86,5

%21 ve üzeri	30	13,5	13,5	100,0
Toplam	222	100	100	

Araştırmada yer alan işletmelerin cari dönem siber güvenlik vak'a sayıları; %24,3'ü 0; %50,5'i %1-10; %11,7'si %11-20; %13,5'i %21 ve üzeri olacak şekilde gerçekleşmiştir.

Araştırmada yer alan şirketlerin iç denetim biriminin siber güvenlik konusunda aktif olarak rol alması Frekans Dağılımı Tablo 4.38.'de yer almaktadır:

Tablo 4.38. İç Denetim Biriminin Siber Güvenlik Konusunda Aktif Olarak Rol Alması Frekans Dağılımı

Siber Güvenlik Konusunda Aktif Olarak Rol Alması	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
0-3	113	50,9	50,9	50,9
4-6	43	19,4	19,4	70,3
7-10	43	19,4	19,4	89,6
10 yıldan fazla	23	10,4	10,4	100,0
Toplam	222	100	100	

Araştırmada yer alan işletmelerin iç denetim biriminin siber güvenlik konusunda aktif olarak rol almasına yönelik frekans dağılımları incelendiğinde; işletmelerin %50,9'unda iç denetim birimlerinin 0-3 yıldır; %19,4'ünde 4-6 yıl; %19,4'ünde 7-10 yıl; %10,4'ünde ise 10 yıldan fazla süredir siber güvenlik konusunda aktif olarak rol aldığı anlaşılmaktadır.

Araştırmada yer alan şirketlerin iç denetim biriminin siber güvenlik konusunda aktif olarak rol alması sonrası meydana gelen siber güvenlik vak'a trendi frekans dağılımı Tablo 4.39.'da yer almaktadır:

Tablo 4.39. Siber Güvenlik Vaka Trendi Frekans Dağılımı

Siber Güvenlik Vak'a Trendi	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Önemli Ölçüde Azaldı	22	9,9	9,9	9,9
Azaldı	93	41,9	41,9	51,8
Aynı Oranda Kaldı	61	27,5	27,5	79,3
Önemli Ölçüde Arttı	2	,9	,9	80,2
Hiç Yaşanmadı	44	19,8	19,8	100,0
Toplam	222	100	100	

Araştırmada yer alan işletmelerin iç denetim biriminin siber güvenlik konusunda aktif olarak rol almasından sonra meydana gelen siber güvenlik vak'alarının trendi analiz edildiğinde; işletmelerden %9,9'unda vak'aların önemli ölçüde azaldığı; %41,9'unda vak'aların azaldığı; %27,5'inde aynı oranda kaldığı; %0,9'unda önemli ölçüde arttığı; %19,8'inde ise hiç vak'a yaşanmadığı görülmektedir.

4.5.5.3. İç Denetim Biriminin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliğine İlişkin Kruskal-Wallis Testleri

İşletmelerin iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliğinin işletmelerin özelliklerine göre farklılık gösterip göstermediğini belirlemek amacıyla farklılık testleri yapılmıştır. Normallik testi sonuçlarına göre (Tablo 4.8.) araştırmanın verileri normal dağılım göstermediğinden non parametrik farklılık testi olan Kruskal-Wallis testleri gerçekleştirilmiştir. Test sonuçları aşağıdaki bölümlerde aktarılmıştır.

4.5.5.3.1. İç Denetim Biriminin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliği- Çalışan Sayısına Göre Kruskal-Wallis Testi Sonuçları ve Yorumları

İç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği ve alt boyutlarının işletmelerin aktif büyüklüğüne göre farklılık gösterip göstermediği Kruskal-Wallis testi yapılarak sınanmıştır. Test sonuçları Tablo 4.40.'ta sunulmuştur:

Tablo 4.40. Aktif Büyüklüğüne Göre Kruskal-Wallis Testi

Değişkenler	Çalışan Sayısı	N	Ortalama Sıra	Ki-Kare değeri	P
İç Denetim Departmanının Siber Güvenlik Bilgi Düzeyi Algısı	10 milyon TL ve altı	5	131,40	29,096	,000*
	10 milyon TL-100 milyon TL	18	129,22		
	100 milyon TL-1 milyar TL	53	72,34		
	1 milyar TL-10 milyar TL	75	114,53		
	10 milyar TL üzeri	71	131,63		
İç Denetim Departmanının Siber Güvenliği Gözden Geçirme Sıklığı	10 milyon TL ve altı	5	174,10	27,202	,000*
	10 milyon TL-100 milyon TL	18	118,39		
	100 milyon TL-1 milyar TL	53	78,28		
	1 milyar TL-10 milyar TL	75	108,95		
	10 milyar TL üzeri	71	132,84		
Siber Güvenlik Konusunda Üst Yönetimin Desteğine ilişkin İç Denetçi Algısı	10 milyon TL ve altı	5	122,40	27,387	,000*
	10 milyon TL-100 milyon TL	18	135,00		
	100 milyon TL-1 milyar TL	53	74,72		

	1 milyar TL- 10 milyar TL	75	111,90		
	10 milyar TL üzeri	71	131,81		
İç Denetim ve Bilgi Teknolojileri (BT) Departmanları Arasındaki İlişkinin Algısı	10 milyon TL ve altı	5	148,90	5,459	,243
	10 milyon TL-100 milyon TL	18	106,83		
	100 milyon TL-1 milyar TL	53	101,56		
	1 milyar TL- 10 milyar TL	75	107,29		
	10 milyar TL üzeri	71	121,92		
Genel Ortalama	10 milyon TL ve altı	5	143,80	28,347	,000*
	10 milyon TL-100 milyon TL	18	124,28		
	100 milyon TL-1 milyar TL	53	75,43		
	1 milyar TL- 10 milyar TL	75	109,43		
	10 milyar TL üzeri	71	135,09		

Araştırmaya katılan işletmelerin iç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği ve “İç Denetim ve Bilgi Teknolojileri (BT) Departmanları Arasındaki İlişki” hariç tüm alt boyutları işletmelerin aktif büyüklüklerine göre anlamlı farklılığa sahiptir ($p<0,05$). Farklılığın yönünü belirleyebilmek amacı ile post hoc testlerinden Tamhane's T2 testi yapılmıştır. Test sonuçlarına göre aktif büyüklüğü 100 milyon TL-1 Milyar TL olan

işletmelerin ortalamaları, aktif büyüklüğü 1 milyar TL-10 milyar TL ile 10 milyar TL üzeri olan işletmelere göre daha düşüktür. Buna göre, aktif büyüklüğü arttıkça iç denetim birimlerinin siber güvenlik faaliyetlerinin etkinliği de artmaktadır.

4.5.5.3.2. İç Denetim Biriminin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliği- Faaliyet Gösterilen Sektöre Göre Kruskal-Wallis Testi Sonuçları ve Yorumları

İç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği ve alt boyutlarının işletmelerin sektörüne göre farklılık gösterip göstermediği Kruskal-Wallis testi yapılarak sınanmıştır. Test sonuçları Tablo 4.41.'de yer almaktadır:

Tablo 4.41. Faaliyet Gösterilen Sektöre Göre Kruskal-Wallis Testi

Değişkenler	Çalışan Sayısı	N	Ortalama Sıra	Ki-Kare değeri	p
İç Denetim Departmanının Siber Güvenlik Bilgi Düzeyi Algısı	Üretim	45	82,68	70,463	,000*
	Bankacılık	49	152,17		
	Havacılık ve Uzay	9	121,28		
	Madencilik/Metaller/Mineraller	8	78,56		
	Risk Yönetimi ve Sigorta	25	159,20		
	Enerji	22	107,57		
	İletişim, Medya ve Teknoloji	9	98,94		
	Kimya	7	52,79		
	Perakende	11	103,36		
	İnşaat	9	20,94		
	Diğer	28	104,43		
İç Denetim Departmanının Siber Güvenliği Gözden Geçirme Sıklığı	Üretim	45	63,41	103,001	,000*
	Bankacılık	49	165,76		
	Havacılık ve Uzay	9	155,17		
	Madencilik/Metaller/Mineraller	8	75,44		
	Risk Yönetimi ve Sigorta	25	152,80		

	Enerji	22	101,68		
	İletişim, Medya ve Teknoloji	9	110,56		
	Kimya	7	39,00		
	Perakende	11	123,82		
	İnşaat en kötü	9	29,22		
	Diğer	28	100,98		
Siber Güvenlik Konusunda Üst Yönetimin Desteğine İlişkin İç Denetçi Algısı	Üretim	45	65,32	82,085	,000*
	Bankacılık	49	151,52		
	Havacılık ve Uzay	9	137,17		
	Madencilik/Metaller/Mineraller	8	67,94		
	Risk Yönetimi ve Sigorta	25	160,42		
	Enerji	22	121,30		
	İletişim, Medya ve Teknoloji	9	94,11		
	Kimya	7	59,36		
	Perakende	11	115,09		
	İnşaat	9	33,39		
	Diğer	28	110,82		
İç Denetim ve Bilgi Teknolojileri (BT) Departmanları Arasındaki İlişkinin Algısı	Üretim	45	81,30	39,329	,000*
	Bankacılık	49	133,61		
	Havacılık ve Uzay	9	109,61		
	Madencilik/Metaller/Mineraller	8	106,63		
	Risk Yönetimi ve Sigorta	25	132,82		
	Enerji	22	128,16		
	İletişim, Medya ve Teknoloji	9	119,17		
	Kimya	7	56,21		
	Perakende	11	144,91		
	İnşaat	9	45,50		

	Diğer	28	110,66		
Genel Ortalama	Üretim	45	67,38	104,901	,000*
	Bankacılık	49	166,10		
	Havacılık ve Uzay	9	137,28		
	Madencilik/Metaller/Mineraller	8	75,00		
	Risk Yönetimi ve Sigorta	25	161,24		
	Enerji	22	110,86		
	İletişim, Medya ve Teknoloji	9	102,06		
	Kimya	7	39,21		
	Perakende	11	115,27		
	İnşaat	9	20,61		
	Diğer	28	93,93		

Araştırmaya katılan işletmelerin iç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği ve alt boyutları işletmelerin sektörlerine göre anlamlı farklılığa sahiptir ($P<0,05$). Farklılığın yönünü test edebilmek amacı ile post hoc testlerinden Tamhane's T2 testi gerçekleştirilmiştir. Yapılan test sonucunda İnşaat ve Üretim sektörlerinin ortalamaları Enerji, Risk Yönetimi ve Sigorta ve Bankacılık sektörlerinin ortalamalarından düşük olduğu belirlenmiştir. Bu sonuçlardan hareketle, Enerji, Risk Yönetimi ve Sigorta ve Bankacılık sektörlerinde faaliyet gösteren işletmelerin iç denetim faaliyetlerinin İnşaat ve Üretim sektörlerindeki işletmelerden daha iyi seviyede olduğu çıkarımını yapabiliriz.

4.5.5.3.3. İç Denetim Biriminin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliği- İşletmelerin BT Bağımlılıklarına Göre Kruskal-Wallis Testi Sonuçları ve Yorumları

İç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği ve alt boyutlarının işletmelerin BT bağımlılıklarına göre farklılık gösterip göstermediği Kruskal-Wallis testi yapılarak sınanmıştır. Test sonuçları Tablo 4.42.'de yer almaktadır:

Tablo 4.42. BT Bağımlılığına Göre Kruskal-Wallis Testi

Değişkenler	Çalışan Sayısı	N	Ortalama Sıra	Ki-Kare değeri	p
İç Denetim Departmanının Siber Güvenlik Bilgi Düzeyi Algısı	Az bağımlı	55	50,41	73,399	,000*
	Bağımlı	68	116,63		
	Çok bağımlı	99	141,91		
İç Denetim Departmanının Siber Güvenliği Gözden Geçirme Sıklığı	Az bağımlı	55	47,12	94,060	,000*
	Bağımlı	68	105,75		
	Çok bağımlı	99	151,22		
Siber Güvenlik Süreçlerine Üst Yönetimin Desteğine ilişkin İç Denetçi Algısı	Az bağımlı	55	46,45	91,663	,000*
	Bağımlı	68	109,32		
	Çok bağımlı	99	149,14		
İç Denetim ve Bilgi Teknolojileri (BT) Departmanları Arasındaki İlişkinin Algısı	Az bağımlı	55	64,90	40,439	,000*
	Bağımlı	68	122,93		
	Çok bağımlı	99	129,54		
Genel Ortalama	Az bağımlı	55	44,00	97,272	,000*
	Bağımlı	68	109,36		
	Çok bağımlı	99	150,47		

İç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği ve alt boyutları işletmelerin BT bağımlılıklarına göre anlamlı farklılığa sahiptir ($p<0,05$). Farklılığın yönünü test edebilmek amacı ile post hoc testlerinden Tamhane's T2 testi yapılmıştır.

Test sonuçlarına göre “Az bağımlı” işletmelerin ortalamaları “Bağımlı” ve “Çok bağımlı” işletmelerden; “Bağımlı” işletmelerin ortalamaları ise “Çok bağımlı” işletmelerden daha düşüktür. Test sonuçlarına göre işletmelerin BT bağımlılıkları arttıkça iç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği de pozitif yönde artmaktadır.

IIA tarafından yayımlanan ve işletmeler içindeki risk ve kontrol işlevlerinin etkinliğini ve verimliliğini iyileştirmek için en iyi uygulama yaklaşımını belirleyen **“Etkili Risk Yönetimi ve Kontrolünde Üçlü Savunma Hattı”** ve **“Siber Güvenlik Riskinin Değerlendirilmesi Üç Savunma Hattının Rollerini”** kılavuzlarında siber güvenliğe ilişkin rolleri açıkça tanımlanan iç denetim biriminin siber güvenlik faaliyetlerini icra edilmesi süreçlerine katılımı ve konu hakkında güncel ve yeterli bilgi sahibi olması oldukça önemlidir.

İç denetim birimi, iç kontrol, yönetim ve risk yönetimi konularında bağımsız ve tarafsız bir şekilde güvence sağlamaktadır. Ayrıca birinci ve ikinci savunma hatları tarafından gerçekleştirilen faaliyetlerin siber güvenlik risklerini ve tehditlerini yönetme ve önleme konusunda genel etkinliğini değerlendirmekte üçüncü savunma hattının önemli görevlerinden biridir. H7, H8 ve H9 hipotezlerinin test sonuçları da “Üçüncü Savunma Hattı” olarak faaliyet gösteren iç denetim biriminin faaliyetlerinin etkinliğinin işletmelerin risklerine (Sektör, büyüklük ve BT bağımlılığı) paralel arttığını göstermektedir. Tablo 4.33 ve 4.34 incelendiğinde araştırmaya dahil olan işletmelerin büyük çoğunluğunda işletmelerin iç denetim birimlerinin siber güvenlik konularında aktif rol almasından sonra siber vak’aların sayısının azaldığı veya hiç yaşanmadığı sonucu ortaya çıkmaktadır. Bu durum iç denetim biriminin siber riskleri yönetme ve engelleme konusunda aldığı rolü ve iç denetim faaliyetinin işletmeler için önemini doğrular niteliktedir.

4.5.6. İşletmelerin Siber Güvenlik Faaliyetleri Seviyesi ile İç Denetim Birimlerinin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliğine İlişkin Korelasyon Analizleri

Üçüncü araştırma konusu ise; “İç denetim departmanlarının siber güvenlik faaliyetleri işletmelerin siber güvenlik seviyelerine ne ölçüde etki etmektedir?” sorusu şekillendirmektedir. Bu bağlamda, işletmelerin siber güvenlik faaliyetleri seviyesi ile iç

denetim departmanlarının siber güvenlik faaliyetleri seviyesi arasındaki ilişkiyi tespit etmek amacıyla korelasyon testi uygulanacaktır. Üçüncü araştırma sorusundan hareketle oluşturulan hipotez ve alt hipotezler aşağıdaki gibidir:

H10: İç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği ile işletmelerin siber güvenlik faaliyetleri seviyesi arasında anlamlı bir ilişki vardır.

- H10a: İç denetçinin BT bilgi düzeyi ile işletmelerin siber güvenlik faaliyetleri seviyesi arasında anlamlı bir ilişki vardır.
- İç denetim biriminin siber güvenliği gözden geçirme sıklığı ile işletmelerin siber güvenlik faaliyetleri seviyesi arasında anlamlı bir ilişki vardır.
- İç denetim ve BT departmanları arasındaki ilişkinin kalitesi ile işletmelerin siber güvenlik faaliyetleri seviyesi arasında anlamlı bir ilişki vardır.
- Siber güvenlik konusunda üst yönetimin iç denetime verdiği destek ile işletmelerin siber güvenlik faaliyetleri seviyesi arasında anlamlı bir ilişki vardır.

İç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliğine ilişkin hipotezlere ait test sonuçları incelendiğinde sonuçların işletmelerin siber güvenlik faaliyeti seviyelerine yönelik test sonuçları ile benzer sonuçların çıktığı görülmektedir.

İç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği ve işletmelerin siber güvenlik faaliyeti seviyeleri arasındaki ilişkinin ortaya konulması amacıyla korelasyon analizi gerçekleştirilmiştir.

Tablo 4.43. İşletmelerin Siber Güvenlik Faaliyetleri Seviyesi ile İç Denetim Birimlerinin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliğine İlişkin Korelasyon Analizi

	Siber güvenlik faaliyetleri seviyesi	İç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği
Siber güvenlik faaliyetleri seviyesi	1,000	,803**
İç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği	,803**	1,000

Tablo 4.43.'te verilen Spearman korelasyon analizine göre işletmelerin siber güvenlik faaliyetleri seviyesi ve iç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği arasında çok güçlü düzeyde ve pozitif bir ilişki vardır. ($r = ,803$; $p < 0,05$).

Literatürde farklı sınıflandırmalar olmakla birlikte, genelde ($,00- ,30$) zayıf; ($,31- ,49$) orta; ($,50- ,69$) güçlü; ($,70- ,100$) çok güçlü ilişki olduğu şeklinde yorumlanmaktadır (Tavşancıl, 2006).

Tablo 4.44. İşletmelerin Siber Güvenlik Faaliyetleri Seviyesi ile İç Denetim Birimlerinin Siber Güvenliğe Yönelik Faaliyetlerinin Etkinliğinin Alt Boyutlarının Korelasyon Analizi

	Siber güvenlik faaliyetleri seviyesi	İç denetçinin BT bilgi düzeyi	İç denetim biriminin siber güvenliği gözden geçirme sıklığı	İç denetim ve BT departmanları arasındaki ilişkinin kalitesi	Siber güvenlik konusunda üst yönetimin iç denetime verdiği destek
Siber güvenlik faaliyetleri seviyesi	1,000	,661**	,739**	,471**	,779**

İç denetçinin BT bilgi düzeyi		1,000	,712**	,438**	,671**
İç denetim biriminin siber güvenliği gözden geçirme sıklığı			1,000	,587**	,695**
İç denetim ve BT departmanları arasındaki ilişkinin kalitesi				1,000	,466**
Siber güvenlik konusunda üst yönetimin iç denetime verdiği destek					1,000

Tablo 4.44.'te verilen Spearman korelasyon analizine göre işletmelerin siber güvenlik faaliyetleri seviyesi ve iç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliğinin alt boyutları arasında orta, güçlü ve çok güçlü düzeyde ve pozitif bir ilişki vardır. “İşletmelerin siber güvenlik faaliyetleri seviyesi” ile “İç denetçinin BT bilgi düzeyi” arasında güçlü ($r = ,661$; $p < 0,05$) derecede ve pozitif; “İşletmelerin siber güvenlik faaliyetleri seviyesi” ile “İç denetim biriminin siber güvenliği gözden geçirme sıklığı” arasında çok güçlü ($r = ,739$; $p < 0,05$) derecede ve pozitif; “İşletmelerin siber güvenlik faaliyetleri seviyesi” ile “İç denetim ve BT departmanları arasındaki ilişkinin kalitesi” arasında orta ($r = ,471$; $p < 0,05$) derecede ve pozitif; “İşletmelerin siber güvenlik faaliyetleri seviyesi” ile “Siber güvenlik konusunda üst yönetimin iç denetime verdiği destek” arasında çok güçlü ($r = ,779$; $p < 0,05$) derecede ve pozitif ilişki bulunmaktadır.

SONUÇ ve ÖNERİLER

Günümüzde teknolojik gelişmelerin sonucu olarak, bilgi ve iletişim altyapısı geniş coğrafyalara yayılmıştır. 80'li yıllarda internet kullanımının yaygınlaşmaya başlaması, 1995 yılında tamamen serbest bırakılmasıyla bu dönem “Bilgi Çağı (Information Age)” olarak adlandırılmaya başlanmıştır. Bu gelişmeler bilgi ve teknoloji odaklı bir dünya yaratmıştır.

Bilgi teknolojisinin hızla gelişmesi sonucu sanayi toplumu bilgi toplumuna evrilmiştir. Bilgi toplumunda temel üretim faktörü bilgidir. Bilgi toplumunda konvansiyonel ağır sanayi anlayışı yerini bilgi teknolojilerine bırakmıştır. Bilginin işlenmesinde ve depolanmasında kullanılan bilgisayar ve iletişim teknolojileri iş hayatının merkezine yerleşmiştir. Buna bağlı olarak iş dünyasının da iş yapış şekilleri ve değer yargıları tamamen değişmiştir.

Günümüzde bilgi teknolojilerinin kullanımının giderek artması ve nerdeyse tüm faaliyetlerin dijital ortamlarda yürütülmeye başlanması, bilgi hacminin artması ve bilginin en önemli rekabet aracı olması bilginin ve bilgiyi sağlayan kaynakların korunmasını zorunlu hale getirmiştir.

Bilgi teknolojileri kullanımının artması ve hayatımızın her alanına entegre olması, bilgi güvenliğine dair problemleri de beraberinde getirmiştir. Bu dijitalleşme sürecinde işletmelerin bilgi kaynaklarının ve veri tabanlarının da dijitalleşmesi nedeniyle analog bilgi kullanımı azalmış ve bu durum bilgi güvenliği ve siber güvenlik kavramlarının iç içe geçmesine sebebiyet vermiştir. Her ne kadar bilgi güvenliği kavramı ve siber güvenlik kavramları birbirlerinin yerine kullanılsa da bu unsurların farklılıkları ve kesişen özellikleri mevcuttur. Her iki unsorda işletmeler açısından eşit derecede öneme sahiptir.

Günümüz dünyasında fiziksel güvenlik kadar siber güvenlik uygulamaları da işletmeler açısından büyük önem taşımaktadır. İşletmelerde bilgi güvenliği ve siber güvenliğe dair uyumluluğun sağlanması, bilgi güvenliği ve siber güvenlik yönetişimin işletmelerin odak noktası olması çağımızın en büyük gerekliliğidir. Ayrıca maliyeti ne

olursa olsun gerekli altyapı yatırımlarının yapılması, sistemlerin kurulması, yetkin ve tecrübeli BT personellerinin çalıştırılması da bir diğer önemli noktadır.

Tüm bunlara ek olarak süreç işletmelerin faaliyetlerinin, kontrol ortamının ve varlıklarının her türlü zarar ve saldırıdan korunmasını içerdiğinden iç denetçilere de bu süreçte önemli görevler düşmektedir.

İç denetimin IIA tarafından yapılan tanımında “*İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve tarafsız bir güvence ve danışmanlık faaliyetidir. İç denetim kurumunun risk yönetimi, kontrol ve kurumsal yönetim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistematik ve disiplinli bir yaklaşım geliştirerek, kurum hedeflerinin gerçekleştirilmesine yardımcı olur*” şeklinde ifade edilmiştir.

İç denetim; işletmelerde kontrol mekanizması olarak çalışmakta ve işletmenin iş süreçlerinin uyumuna yönelik usulsüzlüklerini ve sistemin zayıflıklarını ortaya koymaktadır.

IIA tarafından “**Etkili Risk Yönetimi ve Kontrolünde Üçlü Savunma Hattı**” ve “**Siber Güvenlik Riskinin Değerlendirilmesi Üçlü Savunma Hattının Roller**” siber risklerin analizinde üçlü savunma hattının ve özellikle de iç denetçilerin rolleri açıklanmıştır. İşletmelerde üçüncü savunma hattı olarak iç denetim faaliyeti, birinci (işletme yönetimi) ve ikinci (BT departmanı) savunma hattıyla koordinasyonlu bir biçimde hareket ederek özellikle siber güvenlik kapsamında önemli bir rol oynamaktadır.

Bu çalışmada iç denetimin kapsamı, iç denetim türleri ve iç denetimin unsurları açıklanarak iç denetimle ilgili genel bilgilere yer verilmiştir. İç denetim, kurumsal yönetişim, iç kontrol ve risk yönetimi ilişkisi açıklanmıştır. Ayrıca iç denetimle alakalı yasal düzenlemeler ve uluslararası standartlar ve iç denetim süreci açıklanmaya çalışılmıştır.

Çalışmada bilgi teknolojileri ve bunlara bağlı olarak ortaya çıkan uygulamalar anlatılmıştır. Çalışmada ayrıca bilgi güvenliği ve siber güvenliğe ilişkin genel kavramlar ve unsurlara yer verilmiştir. Siber uzay, siber olay, siber tehditler ve işletmelerde sınır güvenliği sistemleri ve bunlara ilişkin kavramların üzerinde durulmuştur. Siber güvenlikle

ilgili olaylar ve bu olayların sonuçlarının yer aldığı güncel istatistiki bilgiler ile konunun ülkeler ve işletmeler için arz ettiği öneme dikkat çekilmiştir.

Tüm bunlara ek olarak çalışmada işletmelerde siber güvenlik yönetiřimi ve siber güvenlik yönetiřimine iliřkin kabul görmüş uluslararası standartlar açıklanmıştır. İşletmelerde siber tehditlerin önlenmesi ve minimize edilmesi konusunda işletme yönetimi, BT çalışanları ve iç denetçilere düşen roller ve görevler anlatılmıştır. IIA tarafından siber güvenlik konularında yayımlanan çerçeveler dikkate alınarak iç denetçilerin siber güvenlik risklerini ve kontrollerini değerlendirmesi konusuna ışık tutulmaya çalışılmıştır.

Siber güvenlik ve iç denetim konularında yapılan literatür taramasıyla, konuyla ilişkili çalışmalar sınıflandırılmış ve açıklanmıştır. Literatür incelemesinin alt başlıkları; iç denetim ve siber güvenlik, bilgi paylaşımı ve siber güvenlik, siber güvenlik yatırımları, siber güvenlik faaliyetlerine ilişkin bilgilerin açıklanması, güvenlik tehditleri ve güvenlik ihlalleri konularından oluşmuştur.

Çalışmanın uygulama bölümündeki amaçlar üç temelde boyutlandırılmıştır. Çalışmanın ilk amacı Türkiye’de faaliyet gösteren halka açık işletmelerin siber güvenlik faaliyetleri seviyelerini tespit etmek ve siber güvenlik düzeylerinin işletmelerin özelliklerine göre farklılaşıp farklılaşmadığını belirlemektir.

Çalışmanın ikinci amacı ise işletmelerde üçüncü savunma hattı olarak görev yapan iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliğini belirlemek ve iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliğinin işletmelerin özelliklerine göre farklılaşıp farklılaşmadığını tespit etmektir.

Bu çalışmanın son amacı ise işletmelerin siber güvenlik faaliyetleri seviyeleri ile iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliği arasında ilişki olup olmadığını incelemektir. Bu bağlamda çalışmada toplam 10 hipotez ve bu hipotezlere bağlı alt hipotezler oluşturulmuştur. Hipotezleri test etmek amacıyla gruplar arası fark analizi (Kruskal Wallis) ve korelasyon (Spearman) analizi yapılmıştır. Yapılan analizler sonucunda araştırmanın hipotezlerinin neredeyse tamamı (H1b ve H7d hariç) kabul edilmiştir.

Araştırma bulgularında; çalışan sayısı fazla olan işletmelerin siber güvenlik düzeylerinin çalışan sayısı az olan işletmelerden daha iyi seviyede olduğu tespit edilmiştir. Ayrıca aktif büyüklüğü arttıkça işletmelerin siber güvenlik düzeylerinin daha iyi seviyelere çıktığı görülmüştür.

Günümüzde meydana gelen siber saldırıların işletmeler açısından yıkıcı sonuçları olmaktadır. Finansal zararların yanı sıra bu tip saldırılar, paydaşların işletmelere olan güvenin sarsmakta ve itibar kaybı da yaratmaktadır. Saldırıları aynı zamanda kişilerin ve işletmelerin ve ülkelerin güvenliklerini de tehdit etmektedirler.

Elde edilen sonuçlar işletmelerin BT bağımlılıkları arttıkça siber güvenlik faaliyeti seviyelerinin de pozitif yönde arttığını ortaya koymaktadır. Ayrıca, işletmelerin itibar riski arttıkça ve sahip olduğu kritik bilgilerin oranı arttıkça da işletmelerin siber güvenlik faaliyeti seviyelerinin artmakta olduğu anlaşılmıştır.

Araştırma sonuçları sektörel açıdan değerlendirildiğinde; Enerji, Risk Yönetimi ve Sigorta ve Bankacılık sektörlerinde faaliyet gösteren işletmelerin iç denetim faaliyetlerinin İnşaat ve Üretim sektörlerindeki işletmelerden daha iyi seviyede olduğu sonucu ortaya çıkmaktadır. Bu durumun oluşmasında bu sektörlerin tabi olduğu yasal düzenlemeler ve sektörde yer alan işletmelerin kurumsal yapıları önemli rol oynamaktadır. Bu sektörlerde faaliyet gösteren işletmelerin etkin bir kurumsal yapıya, iç kontrol sistemine ve risk yönetimi süreçlerine sahip olmaları gerekmektedir. Tüm faaliyetlerin etkin bir biçimde devam etmesi iç denetim faaliyetlerinin kalitesine bağlıdır. Bu nedenle Enerji, Risk Yönetimi ve Sigorta ve Bankacılık gibi siber risklere duyarlı sektörlerde iç denetimin siber güvenlik faaliyetlerinin diğer sektörlerle göre daha etkin şekilde yürütülmesi normal bir durumdur.

İç denetim faaliyeti işletmelerin varlıklarını her türlü zarardan korumakta ve işletmelerin faaliyetlerine ve süreçlerine değer katmaktadır. İşletmelerin fiziksel varlıklarının yanı sıra siber varlıklarının korunmasında da iç denetim faaliyeti önemli roller üstlenmektedir. Araştırma sonuçları araştırmaya dahil olan işletmelerin büyük çoğunluğunda iç denetim birimlerinin siber güvenlik konularında aktif rol almasından sonra siber vak'aların sayısının azalmış veya hiç yaşanmamış olduğunu göstermiştir. Bu durum iç denetim faaliyetinin işletmelerin siber risklerinin belirlenmesi, analizi ve bertaraf

edilmesinde aldığı rolün önemini bir kez daha gözler önüne sermektedir. İç denetim birimi işletme yönetimi ve BT departmanları ile birlikte hareket ederek siber güvenlik konularında işletmelere değer katmaktadır.

Türkiye’de faaliyet gösteren halka açık işletmeler göz önüne alındığında işletme üst yönetiminin siber süreçlere katkısı, iç denetim ve BT departmanları ilişkileri, iç denetçilerin BT ve siber güvenlik bilgi düzeyinin iyi seviyelerde olduğu sonucu ortaya çıkmıştır. Ayrıca iç denetimin siber güvenliği gözden geçirme düzeyi ortalama seviyededir. Araştırmaya katılan işletmelerin yaklaşık yarısında iç denetim birimlerinin 0-3 yıldır siber güvenlik konularında rol almasına rağmen siber güvenlik ortamının iyi seviyelerde olması dikkat çekicidir ve ülkemiz işletmeleri adına sevindirici bir durumdur. İlerleyen yıllarda siber güvenliğe verilen önemin artmasıyla birlikte siber güvenlik uygulamalarının ve iç denetim birimlerinin konuya yönelik faaliyetlerinin pozitif yönde ilerleyeceği öngörülebilir.

Araştırma sonuçlarına göre aktif büyüklüğü arttıkça, iç denetim birimlerinin siber güvenlik faaliyetlerinin etkinliğinin de arttığı anlaşılmıştır. Ayrıca işletmelerin BT bağımlılıkları arttıkça, iç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği de pozitif yönde artmaktadır.

Ayrıca çalışmada; iç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği ve işletmelerin siber güvenlik faaliyeti seviyeleri arasındaki ilişkinin yönünün ve seviyesinin belirlenmesi amacıyla yapılan analizde elde edilen sonuçlara göre; işletmelerin siber güvenlik faaliyetleri seviyesi ve iç denetim biriminin siber güvenliğe yönelik faaliyetlerinin etkinliği arasında çok güçlü düzeyde ve pozitif bir ilişki bulunmuştur.

Günümüzde bilgi teknolojilerinde meydana gelen gelişmelerin ardından iç denetimin görev alanları da genişlemiştir. Söz konusu teknolojik gelişmeler işletme risklerini ve risklere karşı alınacak önlemleri tamamen değiştirmiş, iç denetim birimi kendilerine tanınan bağımsızlık ve tarafsızlık özelliklerinin de desteğiyle; işletme süreçlerinin iyileştirilmesi, işletmeye değer kazandırma ve işletme risklerini önleme konularında önemli roller edinmiştir. İç denetim üstlenmiş olduğu bu misyonla hem yönetsel kontrol hem de diğer işletme faaliyetleri kapsamında önemli bir konum

kazanmıştır ve faaliyetleri işletmenin süreçlerine doğrudan etki eder bir hal almıştır. Dolayısıyla iç denetim biriminin siber güvenlik konusunda bilgi sahibi olması, farkındalığının olması ve doğrudan aksiyon alması işletmelerin siber güvenlik seviyelerini doğrudan etkilemekte ve tüm sürece değer katmaktadır.

Araştırmaya katılan işletmelerin siber güvenlik faaliyetleri seviyeleri ve iç denetim birimlerinin siber güvenliğe yönelik faaliyetlerinin etkinliğinin iyi seviyelerde olduğu görülmektedir. Her ne kadar bu seviyeler işletme özelliklerine göre (büyüklük, sektör v.b.) farklılık gösterse de genel olarak değerlendirildiğinde, Türkiye’de faaliyet gösteren halka açık işletmelerin siber güvenlik konularında pozitif bir farkındalığa ve iyi uygulamalara sahip olmaları gelecek için umut vericidir.

İşletmelerde, iç denetim birimleri yürüttükleri faaliyetlerle, siber güvenlik süreçlerine doğrudan etki etmektedirler. Özellikle son yıllarda iç denetim birimleri, siber güvenlik konularında işletmelerde etkin bir biçimde faaliyet göstermeye başlamışlardır. Araştırma sonuçları incelendiğinde, iç denetim birimlerinin faaliyetleri işletmelerin siber güvenlik faaliyetlerini pozitif yönde etkilediği anlaşılmaktadır. İlerleyen yıllarda iç denetçilerin siber güvenlik konularında tecrübelerinin ve uzmanlıklarının artmasına paralel olarak siber güvenlik faaliyetlerinin etkinliğinin daha iyi seviyelere çıkması da muhtemeldir.

Araştırma sonuçları literatürde yer alan “İç denetim ve siber güvenlik” konulu araştırmaların sonuçlarını destekler niteliktedir.

Bu çalışmada siber güvenlik konusu; Borsa İstanbul’a kote halka açık işletmeler özelinde incelenmiştir. Gelecekte yapılacak çalışmaların evreni tüm Türkiye’yi kapsayacak şekilde genişletilebilir ve daha büyük gruplar üzerinde araştırmalar yapılabilir. Ayrıca gelecekteki araştırmalarda Türkiye’deki işletmelerin siber güvenlik seviyeleri ve iç denetim birimlerinin konuya ilişkin faaliyetleri, farklı ülkelerle veya kültürlerle kıyaslanabilir. Ayrıca, gelecekteki yapılacak çalışmaların BT birimi çalışanlarını da kapsayacak şekilde genişletilmesi önerilir.

KAYNAKÇA

- ABU-MUSA, A. A.: 2006 "Perceived Security Threats of Computerized Accounting Information Systems in The Egyptian Banking Industry", **Journal of Information Systems**, 20(1), 187-203.
- ACCENT URE: 2019 **2019 the cost of cybercrime.**
- ADİLOĞLU, B.: 2010 İç Denetim Süreci ve Temel İşletme Faaliyetlerinin Kontrol Prosedürleriyle Değerlendirilmesi: Bir Uygulama, **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Doktora Tezi.
- ADIR, A. E.: 2019 Kurumlar İçin Siber Güvenlik Laboratuvarı Altyapısının Oluşturulması. **KTO Karatay Üniversitesi Fen Bilimleri Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi.
- AHMAD, Z., İBRAHİM, R.: 2017 "Mobile Commerce (M-Commerce) Interface Design: A Review of Literature", **IOSR Journal of Computer Engineering**, 19(3), 66-70.
- AKARKA RASU, N.: 2000 **Halka Açık Şirketlerde İç Denetim ve Denetim Kurullarının Etkinleştirilmesi için Öneriler**, İstanbul, SPK Yeterlilik Etüdü.
- AKARSLA N, H.: 2011 Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Ayrımı. **T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi.
- AKAY, İ.G.: 2014 Bilgi Güvenliği Yönetim Sistemleri: Bilgi Güvenliği Uygulama Mülakatları, **Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi.
- AKBIYIK, S.:2005 **Vergi Uygulamaları Yönüyle Denetim ve Raporlama**, Ankara, Ekin Kitapevi.
- AKÇAY, G.: 2011 "Kurumsal Risk Yönetiminde İç Denetimin Rolü ve Kamu İdarelerinde Yaşanan Gelişmeler", **Denetişim**, (7), 25-46.
- AKDAŞ, H.: 2019 Üniversitelerin Bilgi İşlem Birimlerinin ITIL Çerçevesinde İncelenmesi ve Etkin Bir Yönetim Modeli Önerisi, **İstanbul Üniversitesi**, Yüksek Lisans Tezi.

- AKMEŞE, S.: 2020 “Kamuda Dijital Dönüşümün Siber Güvenlik ve Dijital Güvence Boyutları ve İç Denetimin Rolü”, **Denetişim**, (20), 108-119.
- AKPINAR, Y.: 2010 “610 No’lu Uluslararası Denetim Standardı Hükümleri ile Türkiye Uygulamaları Çerçevesinde İç Denetim ve İç Denetim Çalışmaları”, **Trakya Üniversitesi Sosyal Bilimler Dergisi**, 12(2), 174-200.
- AKSOY, T.: 2007 **Tüm Yönleriyle Denetim**, 2. bs, Ankara, Yetkin Yayınları.
- AKTAN, C.C., VURAL, İ.: 2016 “Bilgi Toplumu, Yeni Temel Teknolojiler ve Yeni Ekonomi”, **Yeni Türkiye**, 88(1), 1-37.
- AKYEL R.: 2010 “Türkiye’de İç Kontrol Kavramı, Unsurları ve Etkinliğinin Değerlendirilmesi”, **Yönetim ve Ekonomi: Celal Bayar Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, 83-97.
- AKYEŞİL MEN, N.: 2018 **Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik**. Ankara: Orion Kitabevi.
- ALBAYRA K A.: 2015 Bilgisayar Ağlarında Güvenlik Politikaları ve Bulut Bilişim, **Beykent Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Doktora Tezi.
- ALP, A., KILIÇ, S.: 2014 **Kurumsal Yönetim Nasıl Yönetilmeli**, 1. bs., İstanbul, Doğan Kitap.
- ALPAY B. N.: 2008 ITIL (Information Technology Infrastructure Library) Güvenlik Yönetimi Süreçlerinin Orta/Büyük Şirketlerde Uygulanması, **Haliç Üniversitesi SBE**, Yayınlanmamış Yüksek Lisans Tezi
- ALPMAN, G.: 2007 “İç Kontrol Sisteminin Etkinliğinin Sağlanması” (Çevrimiçi), <https://ms.hmb.gov.tr/uploads/2019/06/6822-00BE62E558580D9C11802D8B45F95F89BA49A4B8.pdf>, 16 Kasım 2019.
- ALPTÜRK , E.: 2008 **Finans, Muhasebe ve Vergi Boyutlarında İç Denetim Rehberi**, 1. bs., Ankara, Seçkin Yayıncılık.
- ALPTÜRK , E.: 2008 **Finans, Muhasebe ve Vergi Boyutlarında İç Denetim Rehberi**, Ankara, Maliye ve Hukuk Yayınları.

ALTUNIŞI K, R.: “Büyük Veri: Fırsatlar Kaynağı Mı Yoksa Yeni Sorunlar Yumağı Mı?”, **Yildiz Social Science Review**, 1(1), 45-76. 2015

AMİR, E., LEVİ, S., & LİVNE, T.: “Do Firms Underreport Information On Cyber-Attacks? Evidence From Capital Markets”, **Review of Accounting Studies**, 23(3), 1177-1206. 2018

ANDERS ON, U.: **Assurance and Consulting Services**, IIA Research Foundation. 2003

ANDERS ON, U.L., HEAD M.J., RAMAMO RTI, S. RİDDLE C., SALAMA SİCK, M., SOBEL, P.J.: **Internal Auditing: Assurance & Advisory Services**, Canada, Internal Audit Foundation. 2017

ARENS, A. VE LOEBBE CKE, J.: **Auditing an Integrated Approach**, Prentice Hall, USA. 2000

ARENS, A., RANDAL J.E., BEASLEY , M.S., HOGAN C.E.: **Auditing and Assurance Services**, 16. ed., Pearson. 2017

- ARSLAN, M.E.: 2016 "Siber Güvenlik ve Siber Saldırı Türleri", 03.05.2016, (Çevrimiçi), https://d1wqtxts1xzle7.cloudfront.net/52122013/SIBER_GUVENLIK_VE_SIBER_SALDIRI_TURLERI.pdf?, 12.04.2020
- ASLAN, B.: 2010 "Bir Yönetim Fonksiyonu Olarak İç Denetim", **Sayıştay Dergisi**, 77, 63-86.
- AVUNDUK, H., ASAN, H.: 2018 "Blok Zinciri (Blockchain) Teknolojisi ve İşletme Uygulamaları: Genel Bir Değerlendirme." **Dokuz Eylül Üniversitesi İktisadi İdari Bilimler Fakültesi Dergisi**, 33(1), 369-384.
- AYVAZ, B.: 2006 Tedarik Zinciri Yönetiminde Kullanılan Elektronik Veri Değişimi Sisteminin Performansını Etkileyen Faktörler, **İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi.
- BADARA, S.: 2012 "The Role of Internal Auditors İn Ensuring Effective Financial Control at Local Government Level: The Case of Alkaleri L.G.A., Bauchi State", **Research Journal Of Finance And Accounting**, 3(4), 57-65.
- BAĞCI, H.: 2009 "Sosyal Mühendislik ve Denetim", 2009, (Çevrimiçi), <http://Kidder.Org.Tr/Wp-Content/Uploads/Denetisim/1.%20SAYI.Pdf>, 01.05.2020.
- BAKKAL, H., KASIMOĞLU, A.: 2012 "İç Kontrol Sistemine Karşılaştırmalı Bir Bakış COSO ve COCO Modeli", **Mevzuat Dergisi**, 15, 1-14.
- BALAY, R.: 2004 "Küreselleşme, Bilgi Toplumu Ve Eğitim", **Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi**, 37(2), 61-82.
- BANK FOR INTERNATIONAL SETTLEMENTS., 2020 "About BIS – Overview", (Çevrimiçi) <https://www.bis.org/about/index.htm?m=1%7C1>, 20 Ocak 2021.
- BANK FOR INTERNATIONAL SETTLEMENTS., 2020 "Internal Audit in Banks and The Supervisor's Relationship With Auditors", (Çevrimiçi) <https://www.bis.org/publ/bcbs84.pdf>, 5 Aralık 2020.

ENTS.:
2001

BAYKAR A, M.,
DAŞ, R.,
KARADOĞAN, İ.:
2013

“Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi”, **In 1st International Symposium on Digital Forensics and Security (ISDFS’13)**, 231-239.

BAYKAR A, S.T.:
2014

“OECD Ülkelerinde İç Denetim”, **Kamu İç Denetçileri Derneği Denetışim Dergisi**, 14, 42-58.

BELLİNO, C.,
WELLS, J., HUNT, S.: 2007

“Auditing Application Controls”, (Çevrimiçi)
<https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%20%20-%20Auditing%20application%20controls.pdf>, 14 Mart 2019.

BENSGHİR, T.:
1996

Bilgi Teknolojileri ve Örgütsel Değişim, Ankara, Türkiye ve Orta Doğu Amme İdaresi Enstitüsü.

BEYHAN, M.: 2018

Yerel Yönetimlerde İç Denetim Yapısının Kurumsal Risk Yönetimi Vizyonuna Etkisi; İstanbul İlçe Belediyeleri Üzerine Bir Alan, **İşık Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU:
2020

“Bilgi Teknolojileri ve İletişim Kurumu Dünyada ve Ülkemizde Sayısal Dönüşüm: Endüstri 4.0, Yapay Zekâ ve Büyük Veriye İlişkin Gelişmeler”, (Çevrimiçi) <https://www.btk.gov.tr/uploads/pages/arastirma-raporlari/sayisal-donusum-rapor.pdf>, 21.01.2020.

BİLGİN, B. Ö.:
2016

Bilgi Teknolojileri Denetimi ve Bir Uygulama, **Marmara Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi.

BİRCAN, N. G.:
2020

“İç Denetimde Yapısal Değişim ve Dönüşüm: İç Denetçilerin Farkındalığı ve Beklentileri Üzerine Bir Araştırma”, **Muhasebe Enstitüsü Dergisi**, (63), 67-83.

BLASEA:
2017

“Blok zincirinin faydaları nelerdir?”, (Çevrimiçi) <https://blasea.org/block-zincirinin-faydalari-nelerdir/>, 24.02.2020.

- BLOOMB
ERG:
2017 “Uber paid hackers to delete stolen data on 57 million people”, (Çevrimiçi),
<https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data>, 25.05.2020
- BMC:
2020 The Complete Guide to ITIL 4. (Çevrimiçi),
<https://Www.Bmc.Com/Blogs/Itil-4/> 04.06.2020.
- BODNAR,
G. H.,
HOPWOO
D W. S.:
2013 **Accounting Information Systems**, 11. ed., Pearson.
- BORITZ,
J. E., &
NO, W.
G.: 2005 “Security in XML-Based Financial Reporting Services on The
Internet”, **Journal of Accounting and Public Policy**, 24(1), 11-35.
- BOURGE
OİS, D.:
2014 **Information Systems For Business and Beyond**, Saylor Foundation.
- BOZKUR
T, N.:
2012 **Denetim, Denetim Standartları ve Uygulamaları**, TÜRMOB Bağımsız
Denetim Eğitimi Ders Notları, Ankara, TÜRMOB.
- BOZÜYÜ
K, T.,
YAĞCI,
C.,
GÖKÇE,
İ., AKAR,
G.: 2005 Yapay Zekâ Teknolojisinin Endüstrideki Uygulamaları. **Marmara
Üniversitesi Teknik Bilimler Meslek Yüksek Okulu Elektrik
Programı**, Yayınlanmamış Yüksek Lisans Tezi.
- BURTON,
G. F.,
EMETT,
S. A.,
SİMON,
C. A.,
WOOD,
D. A.:
2012 “Corporate Managers' Reliance on Internal Auditor Recommendations”.
Auditing: A Journal of Practice & Theory, 31(2), 151-166.

- BYSTRÖM, H.: 2016 “Blockchains, Real-Time Accounting and The Future of Credit Risk Modeling” **Working Paper/Department of Economics, School of Economics and Management, Lund University**, (4), 1-11.
- CACKETT, D.: 2013 **Information Management and Big Data, A Reference Architecture**. Redwood Shores: Oracle Corporation.
- ÇAĞLIYA N, V.: 2012 “Kurumsal Kaynak Planlama Yazılımı Kullanımının İşletme Performansı Üzerine Etkisi: Örnek Olay Çalışması”, **Niğde Üniversitesi İİBF Dergisi**, 5(1), 159-178.
- CANBEK, G., SAĞIROĞLU Ş.: 2006 “Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme”, **Politeknik Dergisi**, 9(3), 165-174.
- CANBERK, G. VE SAĞIROĞLU, Ş.: 2006 **Bilgi ve Bilgisayar Güvenliği Casus Yazılımlar ve Korunma Yöntemleri**, Grafiker Ltd. Şti., Ankara.
- CANGEMI, M. P., SINGLETON, T.: 2003 **Managing The Audit Function: A Corporate Audit Department Procedures Guide**, 3. ed, New Jersey, John Wiley & Sons, Inc.
- CANNADY, J.: 1998 Artificial Neural Networks for Misuse Detection, **In National Information Systems Security Conference**.
- CANTÜRK, S.: 2013 “Bilgi Teknolojileri Yönetişimi İçin Yeni Bir Adım: COBIT 5”, **KPMG Gündem Dergisi**, 17, 36-37.
- ÇARIKÇI, O., YILDIRIM, A.: 2020 “Risk Odaklı İç Denetimin Stratejik Yönetim Anlayışı Açısından Değerlendirilmesi”, **Süleyman Demirel Üniversitesi Vizyoner Dergisi**, (11)26, 302–313.
- CARRE, J. R., CURTIS, S. R.: “Ascribing Responsibility For Online Security and Data Breaches”, **Managerial Auditing Journal**, 436-446.

JONES,
D. N.:
2018

ÇEK, E.: Kurumsal Bilgi Güvenliği Yönetimi ve Bilgi Güvenliği İçin İnsan
2017 Faktörünün Önemi, **İstanbul Bilgi Üniversitesi SBE**, Yayınlanmamış YL Tezi.

CELAYİR, İç Denetimde Riskin Değerlendirilmesi, **İstanbul Ticaret Üniversitesi**
D.: 2011 **Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi.

ÇELİK, A.: "Bilgi Toplumu Üzerine Bazı Notlar", **Hacettepe Üniversitesi Edebiyat**
1998 **Fakültesi Dergisi**, 15(1), 53-59.

ÇELİK, S., "Güncel Siber Güvenlik Tehditleri: Fidyeye Yazılımlar", **Cyberpolitik**
ÇELİKTA **Journal**, 2(4), 296-323.
Ş, B: 2017

CENGİZ, S.: 2013 "İşletmelerde Kurumsal Yönetim Kapsamında İç Denetimin Yeri ve
Önemi: Borsa İstanbul'da Bir Araştırma", **Afyon Kocatepe Üniversitesi İİBF Dergisi**, 403-448.

CERAN, Y.: 2009 "Türk Bankacılık Sektöründe İç Denetim", **Niğde Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, 2(2), 168-178.

CEYHAN, İ.F., "COSO İç Kontrol Modelinin Yapısal Eşitlik Modeli ile İncelenmesi: Bir
Hastane Uygulaması", **Mehmet Akif Ersoy Üniversitesi SBE Dergisi**,
APAN, M.: 6 (10), 179-198.
2014

CHAPMAN, C., **Implementing The Professional Practices Framework**, Florida, The
N, C., Institute of Internal Auditors.
ANDERS
ON, U.:
2003

CHERDANTSEVA, Y., & "A Reference Model of Information Assurance & Security", In **2013**
HILTON, J.: **International Conference on Availability, Reliability And Security**,
546-555.
2013

CODERR, E, D., **Internal Auditing: Efficiency Through Automation**, New Jersey, John
2009 Wily & Sons, Inc.

- ÇOLAK
DEMİR,
S.,
ÖZMİZRA
K, M.:
2014
- “Bilgi Teknolojileri Sürüm ve Geliştirme Yönetimi Uygulaması”, **İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi**, 13(25), 35-44.
- ÇOLAK,
F.: 2020
- NIST Cyber Security Framework Nedir?, (Çevrimiçi),
<https://www.Fatihcolak.Com.Tr/Nist-Cyber-Security-Framework-Nedir.Html> 04.07.2020
- COLLIER,
P. M.,
BERRY,
A. J.,
BURKE
G. T.:
2006
- Risk and Management Accounting: Best Practice Guidelines For Enterprise-Wide Internal Control Procedures**, Elsevier, USA.
- CÖMERT,
N.: 2008
- “Türk Ticaret Kanunu Tasarısı Kapsamında İç Denetim ve İç Kontrol”, **İç Denetim Dergisi**, 21, 24-28.
- COMMITT
EE OF
SPONSO
RING
ORGANIZ
ATIONS
OF
TREADW
AY
COMMIS
SION:
2017
- “Guidance on Enterprise Risk Management”, (Çevrimiçi)
<https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf>, 7 Şubat 2020.
- CONKLİN
, A.,
WHITE,
G. B.:
2006
- “E-Government and Cyber Security: The Role of Cyber Security Exercises”, **In Proceedings Of The 39th Annual Hawaii International Conference On System Sciences (HICSS'06)**
- CSO
ONLINE:
2020
- “Top cybersecurity facts, figures and statistics” (Çevrimiçi),
<https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html>, 29.05.2020

- CYBERS
ECURİTY
MEDİA:
2020 “300 billion passwords by 2020, report predicts”, (Çevrimiçi),
[https://www.scmagazine.com/home/research/video-300-billion-
passwords-by-2020-report-predicts/](https://www.scmagazine.com/home/research/video-300-billion-passwords-by-2020-report-predicts/) 25.05.2020.
- CYBERS
ECURİTY
VENTUR
ES: 2018 “Cybercrime to cost the world \$10.5 trillion annually by 2025”, (Çevrimiçi),
[https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-
2021/](https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/), 25.05.2020
- CYBİNT
SOLUTİ
NS: 2020 “15 alarming cyber security facts and stats.”, (Çevrimiçi),
<https://www.cybintsolutions.com/cyber-security-facts-stats/>, 25.05.2020
- DABBAG
OGLU, K.:
2009 “İç Kontrol Sistemi”, **Journal of Qafqaz University**, (26), 109-115.
- DABBAO
ĞLU, K.:
2007 “İç Kontrol Sistemi”, **Mali Çözüm Dergisi**, 82, 159-170.
- DAĞLI, M.
K.: 2000 **Aracı Kurumlarda İç Kontrol Sisteminin Önemi ve İç Kontrol
Sisteminin Etkinleştirilmesi**, Sermaye Piyasası Kurulu Yeterlilik Etüdü,
Yayın no 145.
- DATABAS
E: 2020 (Çevrimiçi), <https://database.com.tr/urun/cryptolockerviruscozumleri/>
23.01.2020
- DELOİTT
E: 2012 “The Changing Role of Internal Audit”, (Çevrimiçi)
[https://www2.deloitte.com/content/dam/Deloitte/in/Documents/audit/in-
audit-internal-audit-brochure-noexp.pdf](https://www2.deloitte.com/content/dam/Deloitte/in/Documents/audit/in-audit-internal-audit-brochure-noexp.pdf), 5 Mayıs 2020.
- DELOİTT
E: 2018 “Blokzincir Potansiyelinin Keşfi: 2018 Yılı Türkiye Blokzincir Araştırması”,
(Çevrimiçi)
[https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/consulting/
blokzincir-potansiyelinin-kesfi.pdf](https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/consulting/blokzincir-potansiyelinin-kesfi.pdf)., 22 Haziran 2020.
- DELOİTT
E: 2020 “BT Denetim”, (Çevrimiçi)
https://www.denetimnet.net/Pages/bt_denetimm.aspx, 6 Ekim 2020.
- DİONNE,
G.: 2013 “Risk Management: History, Definition, And Critique”, **Risk
Management And Insurance Review**, 16(2), 147-166.
- DİTTENH
OFER, M.
A.,
RAMAMO **Behavioral Dimensions of Internal Auditing**, Altamonte Spring, FL:
IIA Research Foundation.

ORTİ, S.
C.,
ZİEGENF
US, C. D.
E.,
EVANS,
C. R. L.:
2010

DOYDUK, H.B.B., TİFTİK, C. (2017). "Nesnelerin İnterneti: Kapsamı, Gelecek Yönelimi ve İş Fırsatları", **Third Sector Social Economic Review**, 52(3), 127-147.

DRUCKE R, F.P.: 1994 **Yeni Gerçekler**, Çev. Birtane Karanakçı, Türkiye İş Bankası Kültür Yayınları.

EFE, A.: 2016 "Kamu Yönetiminde Bir Yönetişim Hedefi Olarak Kaynak Optimizasyonu: Kalkınma Ajanslarında COBIT-5 Çerçevesinde Bir Analiz", **Uluslararası Ekonomi ve Yenilik Dergisi**, 2(1), 43-65.

ELİBOL, H., KESİCİ, B.: 2004 "Çağdaş İşletmecilik Açısından Elektronik Ticaret", (Çevrimiçi) http://www.sosyalbil.selcuk.edu.tr/sos_mak/makaleler/Burcu, 25 Mart 2020.

ENISA: 2014 **ENISA Cyber Europe 2014 - After Action Report**

EQUIFAX: 2017 "Equifax Announces cybersecurity incident involving consumer information", (Çevrimiçi), <https://investor.equifax.com/news-and-events/press-releases/2017/09-07-2017-213000628>, 28.05.2020.

ERGEN, Z.: 2016 "Kamu Mali Yönetiminde Yeniden Yapılanma: Muhasebe-İ Umumiye Kanunundan 5018 Sayılı Kanuna Bütçe Ve Harcama Usullerinde Dönüşüm", **Ekonomi Bilimleri Dergisi**, 8(1), 46-58.

EROL, M., ATMACA, M., ŞAHİN, 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.

ERTİKİN, K.: 2017 "Hile Denetimi: Kırmızı Bayrakların Tespiti İçin Kullanılan Proaktif Yaklaşımlar", **Muhasebe ve Finansman Dergisi**, 71-94.

- ESEN, L.: 2008-2017 Yılları Arası Kamu İç Denetim Genel Raporlarının Analizi, **Nevşehir Hacı Bektaş Veli Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi.
- ESET: 2020A Güvenlik Duvarı (Firewall), (Çevrimiçi), <https://www.Eset.Com/Tr/Firewall/> 08.09.2020
- ESET: 2020B “Antivirüs Nedir?”, (Çevrimiçi), <https://www.Eset.Com/Tr/Antivirus-Software/>, 18.08.2020.
- EŞKAZAN, A. R.: 2004 “İç Denetim Sonuçlarının Yönetime Sunulması”, **İç Denetim Dergisi**, 32-33.
- ETTREDGE, M. L., & RICHARDSON, V. J.: 2003 “Information Transfer Among Internet Firms: The Case of Hacker Attacks”, **Journal of Information Systems**, 17(2), 71-82.
- ETTREDGE, M., GUO, F., LI, Y.: 2018 “Trade Secrets and Cyber Security Breaches”, **Journal of Accounting and Public Policy**, 37(6), 564-585.
- EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING, 2020 “The history of ECIIA”, (Çevrimiçi) <https://www.eciia.eu/the-history-of-eciia/>, 5 Şubat 2021.
- EUROPEAN COURT OF AUDITORS: 2019 **Annual Report: 2019 EU Accounts: Clean, But Too Many Spending Errors.**
- EUROPEAN **ENISA Threat Landscape Report 2017.**

NETWORK
K AND
INFORMA
TION
SECURIT
Y
AGENCY:
2018

EUROPE AN
NETWORK
K AND
INFORMA
TION
SECURIT
Y
AGENCY:
2019

ENISA Threat Landscape Report 2018.

EY &
IAPP:
2018

Annual Privacy Governance Report 2018.

FARAHM AND, F.,
NAVATH E, S. B.,
SHARP, G. P.,
ENSLOW, P. H.:
2005

"A Management Perspective on Risk of Security Threats to Information Systems", *Information Technology and Management*, 6(2), 203-225.

FARABÍ:
1986

Fusulü'l-Müntezza, (Nşr. Fevzi m. En-Neccar), Beyrut l.

FASANG HARI, M.,
NASSER ESLAMİ,
F.,
NAGHAVİ
, M.: 2008

"IT Governance Standard Selection Based on Two Phase Clustering Method", In 2008 Fourth International Conference On Networked Computing And Advanced Information Management (Vol. 2, Pp. 513-518). IEEE.

FORBES:
2018

"83% of enterprise workloads will be in the cloud by 2020", (Çevrimiçi), <https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of->

enterprise-workloads-will-be-in-the-cloud-by-2020/?sh=72932ce6261a, 23.05.2020.

GANSLE R, J., LUCYSH YN, W. (2005). "Improving The Security of Financial Management Systems: What Are We to Do?", **Journal of Accounting and Public Policy**. 24. 1-9.

GANTZ, S.: 2014 **The Basics of IT Audit: Purposes, Processes, and Practical Information**, Elsevier, USA.

GARTNER: 2018 "Gartner forecasts worldwide information security spending to exceed \$124 billion in 2019.", (Çevrimiçi), <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>, 25.05.2020.

GELINAS, U., DULL, R., WHEELER, P.: 2015 **Accounting Information Systems**, 10th ed., Cengage Learning.

GÖKÇEN, G., TİPİ, O.: 2019 "İşletmelerde Hilelerin Önlenmesine Yönelik İç Kontroller ve BİST İmalat Sektöründe Bir Araştırma", **Marmara Üniversitesi İktisadi ve İdari Bilimler Dergisi**, 41(1), 145-169.

GÖKMEN, K.: 2019 **Bilgi Toplumunda Elektronik Ticaret ve Türkiye Örneği, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi.

GÖNEN, S.: 2009 "İç Kontrol Sisteminin Unsurlarından Kontrol Ortamının İncelenmesine Yönelik Bir Araştırma", **Muhasebe Bilim Dünyası Dergisi**, 1, 192-217.

GORDON, L. A., & LOEB, M. P.: 2002 "The Economics of Information Security Investment", **ACM Transactions On Information And System Security (TISSEC)**, 5(4), 438-457.

GORDON, L. A., LOEB, M. P., LUCYSH YN, W., "The Impact of The Sarbanes-Oxley Act on The Corporate Disclosures of Information Security Activities", **Journal of Accounting and Public Policy**, 25(5), 503-530.

SOHAİL,
T.: 2006

GORDON , L. A., LOEB, M. P.,
LUCYSH YN, W.,
ZHOU, L.:
2014

“Externalities and The Magnitude of Cyber Security Underinvestment by Private Sector Firms: a Modification of The Gordon-Loeb Model”, **Journal of Information Security**, 6(1), 24-30.

GORDON , L. A., LOEB, M. P.,
LUCYSH YN, W.,
ZHOU, L.:
2015

“The Impact of Information Sharing On Cybersecurity Underinvestment: A Real Options Perspective”, **Journal of Accounting and Public Policy**, 34(5), 509-519.

GORDON , L. A., LOEB, M. P.,
LUCYSH YN, W.:
2003

“Sharing Information on Computer Systems Security: An Economic Analysis”, **Journal of Accounting and Public Policy**, 22(6), 461-485.

GORDON , L. A., LOEB, M. P.,
SOHAİL,
T. (2010).

“Market Value of Voluntary Disclosures Concerning Information Security”, **MIS Quarterly**, 567-594.

GORDON , L. A., LOEB, M. P.,
SOHAİL,
T.,
TSENG,
C. Y.,
ZHOU, L.:
2008).

“Cybersecurity, Capital Allocations and Management Control Systems”, **European Accounting Review**, 17(2), 215-241.

- GÖSTERİ Cİ, H.: 2006 “Kamu İç Mali Kontrol Sisteminde İç Denetimin Bağımsızlığı-Fonksiyonel Bağımsızlık”, **Vergi Dünyası Dergisi**, 295, 177-187.
- GRİFFİTH S, P.: 2005 **Risk-Based Auditing**, USA, Routledge.
- GÜLER, A., ARKIN, A.K.: 2019 “Siber Hijyenin Sağlanmasında İç Denetimin Rolü”, **Denetışim**, (19), 17-40.
- GÜLER, E.: 2010 “Sigorta İşletmelerinde İç Denetim Uygulamalarının İç Denetim Standartları İle Birlikte Değerlendirilmesi”, **Sosyal Ekonomik Araştırmalar Dergisi**, 10(19), 385-402.
- GÜNDOĞ AN, B.: 2016 “Bilgi Sistemleri Denetiminde ISO/IEC 27001 ve ISO/IEC 27002 Standartlarının Yeri”, **Muhasebe Ve Denetim Dünyası Dergisi**, 1(2), 15-28.
- GÜNDÜZ, M. Z., & DAŞ, R.: 2016 (Çevrimiçi), <http://Www.Bingol.Edu.Tr/Documents/Sosyal%20M%C3%Bchendislikyayg%C4%B1n%20Ataklar%20ve%20G%C3%Bcve nlik%20%C3%96nlemleri.Pdf>
- GÜNEŞ, R., DURSUN, G.D.: 2019 “İç Kontrol Sistemi Etkinliğinin İncelenmesinde SWOT Analizi”, **Dicle Üniversitesi İİBF Dergisi**, 298-2019.
- GÜNGÖR M.: 2015 Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma, **Uzmanlık Tezi**.
- GÜREDİN , E.: 2014 **Denetim ve Güvence Hizmetleri**, 14. bs., İstanbul, Türkmen Kitabevi.
- GÜRKAY NAK, M., İREN, A. A.: 2011 “Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler”, **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, 16(2), 263-279.
- GUY, D.M., ALDERM AN C.W., **Auditing**, New York, The Dryden Press.

WINTERS
A.J.: 1996

HALLAM-BAKER,
P.: 2016 Ransomware, Everywhere: What's The Science Behind It?

HASS, S.,
AABDOL
MOHAMM
ADI, M.J.,
BURNAB
Y, P.:
2006 "The America's Literature Review on Internal Auditing", **Managerial Auditing Journal**, 21(8), 835-844.

HAUSKE
N, K.
(2007). "Information Sharing Among Firms and Cyber Attacks", **Journal of Accounting and Public Policy**, 26(6), 639-688.

HAUSKE
N, K.:
2006 "Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment", **Journal of Accounting and Public Policy**, 25(6), 629-665.

HEKIM,
H.,
BAŞIBÜY
ÜK, O.:
2013 „Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları“, **Uluslararası Güvenlik ve Terörizm Dergisi**, 4(2), 13-158.

HİGGS, J.
L.,
PİNSKER,
R. E.,
SMİTH, T.
J., &
YOUNG,
G. R.:
2016 "The Relationship Between Board-Level Technology Committees And Reported Security Breaches", **Journal of Information Systems**, 30(3), 79-98.

HOFFER,
J. A.,
STRAUB,
D. W.:
1989 "The 9 to 5 Underground: Are You Policing Computer Crimes", **Sloan Management Review**, 30(4), 35-43.

- HUNTON, J. E., WRIGHT, A. M., WRIGHT, S.: 2004, "Are financial Auditors Overconfident in Their Ability to Assess Risks Associated With Enterprise Resource Planning Systems?(Retracted)", **Journal of Information Systems**, 18(2), 7-28.
- İBİŞ, C., ÇATIKKAŞ, Ö.: 2012, "İşletmelerde İç Kontrol Sistemine Genel Bakış", **Sayıştay Dergisi**, 85, 95-21.
- İÇ DENETİM KOORDİNASYON KURULU: 2013, "Kamu İç Denetim Genel Tebliği", (Çevrimiçi) <https://www.resmigazete.gov.tr/eskiler/2013/04/20130419-5.htm>, 7 Ağustos 2020.
- ID THEFT RESOURCE CENTER: 2020, (Çevrimiçi), <https://www.idtheftcenter.org/data-breaches/> 25.05.2020
- IIA: 2008 International Standards For The Professional Practice of Internal Auditing (Standards), (Çevrimiçi), <https://na.theiia.org/standards-guidance/public%20documents/ippf%202013%20english.pdf>, 08.09.2019
- IIA: 2009 "IIA Uluslararası İç Denetim Standartları", (Çevrimiçi) https://global.theiia.org/translations/PublicDocuments/Standards_2011_Turkish.pdf, 9 Mart 2019.
- IIA: 2013 "Etkili Risk Yönetimi ve Kontrolünde Üç Savunma Hattı", (Çevrimiçi), <https://global.theiia.org/translations/PublicDocuments/PP-The-Three-Lines-of-Defense-in-Effective-Risk-Management-and-Control-Turkish.pdf>, 23.04.2020.
- IIA: 2016 Global Technology Audit Guide (GTAG) Assessing Cybersecurity Risk Roles of The Three Lines of Defense.
- IIA: 2017 International Standards for The Professional Practice of Internal Auditing (Standards)

- IIA: 2018 Global Bakış Açıları ve Anlayışlar: 2018 Global Risk Raporu-İç Denetim Yöneticilerinin Karşılaştığı En Büyük Riskler.
- IIA: 2019 “The IIA Tops 200,000 Members”, (Çevrimiçi)
[https://global.theiia.org/news/press-releases/Pages/The-IIA-Tops-Two-Hundred-Thousand-Members.aspx#:~:text=The%20Institute%20of%20Internal%20Auditors%20\(IIA\)%20is%20the%20internal%20audit,than%20170%20countries%20and%20territories,](https://global.theiia.org/news/press-releases/Pages/The-IIA-Tops-Two-Hundred-Thousand-Members.aspx#:~:text=The%20Institute%20of%20Internal%20Auditors%20(IIA)%20is%20the%20internal%20audit,than%20170%20countries%20and%20territories,) 6 Şubat 2021.
- INTERNATIONAL AUDITING AND ASSURANCE STANDARDS BOARD: 2013 “ISA 610 (Revised 2013), Using The Work of Internal Auditors and Related Conforming Amendments”, (Çevrimiçi)
[https://www.ifac.org/system/files/publications/files/ISA-610-\(Revised-2013\).pdf](https://www.ifac.org/system/files/publications/files/ISA-610-(Revised-2013).pdf), 4 Kasım 2020.
- INTERNATIONAL BUSINESS MACHINES: 2020 “Elektronik veri değişimi”, (Çevrimiçi), <https://www.ibm.com/tr-tr/supply-chain/edi-electronic-data-interchange>, 21.05.2020.
- INTERNATIONAL BUSINESS MACHINES: 2020 “Elektronik Veri Değişimi”, (Çevrimiçi) <https://www.ibm.com/tr-tr/supply-chain/edi-electronic-data-interchange>, 3 Mart 2020.
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: 2005 “ISO/IEC 27002:2005 Information Technology — Security Techniques — Code of Practice for Information Security Management”, 2005, (Çevrimiçi), <https://www.iso.org/standard/50297.html>, 15.05.2020

- ISACA: 2009A. **The Risk IT Framework.**
- ISACA: 2012 **COBIT 5: A Business Framework for The Governance And Management of Enterprise IT.** Rolling Meadows, IL: ISACA.
- İŞGÜDEN , B.: 2012 Bilgi Teknolojilerinin İç Denetimde Yarattığı Değişimler ve İç Denetim Birimlerinin Değişimleri Değerlendirmesine Yönelik İMKB-100 İşletmelerinde Bir Uygulama, **Anadolu Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Doktora Tezi.
- İSLAM, M. S., FARAH, N., STAFFORD, T. F.: 2018 “Factors Associated With Security/Cybersecurity Audit by Internal Audit Function”, **Managerial Auditing Journal**, 377-409.
- İSMAGİL OVA, E., HUGHES, L., DWİVEDİ, Y. K., & RAMAN, K. R.: 2019 “Smart Cities: Advances In Research—An Information Systems Perspective”, **International Journal of Information Management**, 47, 88-100.
- ISO/IE: 2012 ISO/IEC 27032:2012 Information Technology — Security Techniques — Guidelines For Cybersecurity, (Çevrimiçi), <https://Www.Iso.Org/Standard/44375.Html> , 23.04.2020
- ISO/IEC: 2010 ISO/IEC 27003:2010 Information Technology — Security Techniques — Information Security Management System Implementation Guidance, (Çevrimiçi), <https://Www.Iso.Org/Standard/42105.Html> , 20.04.2020.
- ISO/IEC: 2018 ISO/IEC 27005:2018 Information Technology — Security Techniques — Information Security Risk Management, (Çevrimiçi), <https://Www.Iso.Org/Standard/75281.Html> , 21.04.2020
- ISO/IEC:2 020 ISO/IEC 27007:2020 Information Security, Cybersecurity and Privacy Protection — Guidelines for Information Security Management Systems

- Auditing, (Çevrimiçi), <https://Www.Iso.Org/Standard/77802.Html>, 22.04.2020.
- ISSA: “Global challenges 10 for social security”, (Çevrimiçi), 2017 <https://ww1.issa.int/sites/default/files/documents/publications/Ten%20global%20challenges%20for%20social%20security-204700.pdf>, 25.05.2020
- IT GOVERNANCE:2012 What is COBIT?, (Çevrimiçi), <https://Www.Itgovernance.Co.Uk/Cobit>
- KAGERMAN, H., KINNEY W., KÜTING K., WEBER, C.: 2008 **Internal Audit Handbook**, Springer-Verlag, Berlin Heidelberg.
- KAHYAO GLU, S. B., CALİYUR T, K.: 2018 “Cyber Security Assurance Process from the Internal Audit Perspective”, **Managerial Auditing Journal**, 360-376.
- KALKINO ĞLU, M.: 2003 “İç Kontrol Sistemi”, **Vergi Dünyası**, 265, 70-78.
- KARAÇAY, G.: 2011 “E-Ticarette Karşılaşılan Sorunlar ve Çözüm Önerileri”, (Çevrimiçi) <http://enm.blogcu.com/e-ticarette-karsilasilan-sorunlar-ve-cozumonerileri/>, 5 Nisan 2020.
- KARADE NİZ, D.: 2019 NIST Cyber Security Framework Nedir? (Çevrimiçi), <https://Medium.Com/@Duhankkaradeniz/Nist-Cyber-Security-Framework-Nedir-381968a24616> 05.07.2020
- KASPER SKY: 2018 Yanıltma Nedir?, 2018, (Çevrimiçi), <https://www.Kaspersky.Com.Tr/Resource-Center/Definitions/İp-And-Email-Spoofing>, 25.03.2020

- KAVAL, H.: 2005 **Muhasebe Denetimi: Uluslararası Finansal Raporlama Standartları Uygulama Örnekleriyle**, 2. bs., Ankara, Gazi Kitabevi.
- KAVCI, R.: 2016 **İşletmelerde Satın Alma Sürecinde İç Kontrol Sistemi ve Denetimi, İstanbul Ticaret Üniversitesi, Sosyal Bilimler Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi.
- KAVUT, L.: 2010 "Kurumsal Yönetim, Kurumsal Sosyal Sorumluluk Ve Çevresel Raporlama: İMKB 100 Şirketlerinin Çevresel Açıklamalarının İncelenmesi", **İstanbul Üniversitesi İşletme Fakültesi İşletme İktisadi Enstitüsü Dergisi**, 21(66): 1-36.
- KEPEKÇİ, C.: 1982 **İşletmelerde İç Kontrol Sisteminin Etkinliğini Sağlamada İç Denetimin Rolü**, Eskişehir, Eskişehir İktisadi ve Ticari İlimler Akademisi Basımevi.
- KEPEKÇİ, C.: 2004 **Bağımsız Denetim**, 5. bs., Avcı Ofset Matbaacılık.
- KESKİN, D. A.: 2006 **İç Kontrol Sistemi Kontrol Öz Değerlendirme**, 1. bs., İstanbul, Beta Basım A.Ş.
- KESKİN, D. A.: 2009 "Kamu ve Özel Sektör Yönetiminde İç Kontrol Sistemi Ve Değerlendirilmesi", **Denetişim**, 14-21.
- KESTANE A., KURNAZ, N.: 2019 "ERP Sistemlerinin Muhasebe Bilgi Sistemine Entegrasyonu ve Finansal Raporlamaya Yansımaları", **Dumlupınar Üniversitesi Sosyal Bilimler Dergisi**, 145-158.
- KIZILBOĞ A, R., ÖZŞAHİN, F.: 2013 "Etkin Bir İç Kontrol Sisteminin İç Denetim Faaliyetine ve İç Denetçilere Katkısı", **Niğde Üniversitesi İİBF Dergisi**, 6(2), 220–236.
- KNORR, K., & RÖHRIG, S.: 2001 **Security Requirements of E-Business Processes**. In Towards The E-Society Springer, Boston, MA.
- KOBAN, A.O., 2019 **Sanayi İşletmelerinde İç Denetim ve Kurumsal Risk Yönetiminin Etkileşimi**, Ankara, Gazi Kitabevi.
- KOÇ, S., ŞEKER, "Bilişim Teknolojileri (BT) Denetiminde Bilgi Güvenliği ile İlgili Uluslararası Standartlar ve Türkiye'deki Uyum Çabalarının İncelenmesi",

- S.,
ŞEKER
F.: 2019
- Uluslararası Muhasebe ve Finans Araştırmaları Dergisi**, 1(2): 121-139.
- KOHNKE,
A.,
SHOEMA
KER, D., &
SİGLER,
K.: 2016
- The Complete Guide to Cybersecurity Risks and Controls**, Boca Raton, FL: CRC Press, Taylor & Francis Group.
- KOHNKE,
A.,
SHOEMA
KER, D.,
SİGLER,
K. E.:
2016
- The Complete Guide to Cybersecurity Risks and Controls**. CRC Press.
- KOHNKE,
A.,
SHOEMA
KER, D.:
2015
- "Making Cybersecurity Effective: The Five Governing Principles For Implementing Practical IT Governance And Control", **EDPACS**, 52(3), 9-17.
- KORGA,
S.,
ASLANO
ĞLU, S.:
2020
- "İç Kontrol Sisteminin Unsurları İle Risk Yönetimi Arasındaki İlişkinin İncelenmesi: Bankacılık Sektöründe Bir Uygulama", **Muhasebe Ve Denetime Bakış**, 60, 95-116.
- KORKMA
Z, U.:
2007
- "Kamuda İç Denetim", **Bütçe Dünyası Dergisi**, 2-25.
- KORUYA
N, K.,
BİNGÖL,
F. İ.: 2015
- "Bulut Bilişim Hizmet Sağlayıcılarının Veriyi Koruyamamaları Durumuyla İlgili Türk, Avrupa Birliği ve Amerikan Hukukundaki Düzenlemeler." **Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, 17(3), 367-388.
- KPMG:
2017
- "BT Denetim Standartları ve Uygulamaları", (Çevrimiçi)
<https://assets.kpmg/content/dam/kpmg/tr/pdf/2018/05/bt-denetim-standartlari-ve-uygulamalari.pdf>, 6 Ocak 2021.
- KRUTZ,
R.,
- The CISSP And CAP Prep Guide**, Platinum Ed (With Cd). John Wiley & Sons.

VİNES, R.
D.: 2007

KÜÇÜKS
ÖZEN, C.,
KÜÇÜKK
OCAOĞL
U, G.:
2005

“Kurumsal Şirket Yönetiminde Finansal Tabloların Rolü”, **Muhasebe ve Denetime Bakış**, 16, 1-5.

KURNAZ,
N., &
DİNDARO
ĞLU, A.
K.: 2016

İç Denetim ve Bilgi Güvenliği İlişkisi: Bölgesel Bir Araştırma. **Bilgi Ekonomisi ve Yönetimi Dergisi**, 10(1), 51-63.

KURNAZ,
N.,
ÇETİNOĞ
LU T.:
2010

İç Denetim: Güncel Yaklaşımlar, Kocaeli, Umuttepe Yayınları.

KWON, J.,
ULMER,
J. R., &
WANG,
T.: 2013

“The Association Between Top Management Involvement and Compensation and Information Security Breaches”, **Journal of Information Systems**, 27(1), 219-236.

LAINHAR
T IV, J.
W.: 2000

“COBIT [TM]: A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities.” **Journal Of Information Systems**, 21-21.

LANKTO
N, N.,
PRICE, J.
B.,
KARİM,
M.: 2020

“Cybersecurity Breaches and Information Technology Governance Roles in Audit Committee Charters”, **Journal of Information Systems**, 0000-0000.

LAUDON,
K.,
LAUDON,
J.: 2006

Management Information Systems: Managing The Digital Firm, 9th ed., New Jersey, Prentice Hall.

LEE, S.,
LEE, K.,

“Efficiency Analysis of Controls In EDI Applications”, **Information & Management**, 42(3), 425-439.

KANG W.:
2005

Lİ, C., "The Consequences of Information Technology Control Weaknesses on
PETERS, Management Information Systems: The Case Of Sarbanes-Oxley
G. F., Internal Control Reports", **MIS Quarterly**, 179-203.
RİCHARD
SON, V.
J.,
WATSON,
M. W.:
2012

Lİ, H., NO, "SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity
W. G., Risk Factors", *International Journal of Accounting Information Systems*,
WANG, 30, 40-55.
T.: 2018

LİU, M. C., "Investigating Security Investment Impact on Firm
BOSE, R., Performance", **International Journal of Accounting & Information
LUO, X. Management**, 194-208.
R.: 2014

LUGGAT.: "İlm", (Çevrimiçi) <https://www.luggat.com/index.php#ceviri>, 8 Ekim 2020.
2020

MADEND **Kurumsal Risk Yönetiminde İç Denetimin Rolü**, Yayınlanmamış
ERE, TİDE Dokümanı, İstanbul.
M.A.:
2005

MAİLGUA (Çevrimiçi), [https://www.Mailguard.Com.Au/Blog/Phishing-Email-Scam-](https://www.Mailguard.Com.Au/Blog/Phishing-Email-Scam-Spoofs-Dropbox-Office-365-Uses-New-Po-To-Deliver-Attack)
RD: 2020 [Spoofs-Dropbox-Office-365-Uses-New-Po-To-Deliver-Attack](https://www.Mailguard.Com.Au/Blog/Phishing-Email-Scam-Spoofs-Dropbox-Office-365-Uses-New-Po-To-Deliver-Attack) 29.02.2020

MANTAR, İç Denetim Sürecinin Kontrol Faaliyetleri Üzerindeki Rolü: Kamu Mali
A.: 2013 Yönetimi ve Kontrol Kanunu Açısından Bir Araştırma, **Eskişehir
Osmangazi Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış
Yüksek Lisans Tezi.

MARİNOS **ENISA Threat Landscape 2015**, European Union Agency For Network
, L., And Information Security.
BELMON
TE, A.,
REKLEİTİ
S, E.:
2016

MARYLA ND
ÜNİVERSİTESİ:
2020

“Study: Hackers attack every 39 seconds”, (Çevrimiçi), <https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds>, 25.05.2020.

MELL, P.,
GRANCE,
T.: 2011

“The NIST Definition of Cloud Computing.”,2011, (Çevrimiçi) <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>, 27.05.2020.

MEMİŞ,
M.Ü.:
2008

“Etkin ve Başarılı İç Denetim İçin Gerekli Koşullar”, **Mali Çözüm Dergisi**, 85, 75–91.

MERRİAM-
WEBSTER:
2020

“Internet”, (Çevrimiçi) merriam-webster.com/dictionary/Internet, 28 Şubat 2020.

MİTNICK,
K. D.,
SİMON,
W. L.:
2003

The Art of Deception: Controlling The Human Element of Security. John Wiley & Sons.

MOELLE R.,
R.:
2014

Executive's Guide to COSO Internal Controls-Understanding and Implementing The New Framework, John Wiley & Sons Inc.

MOLLAOĞULLARI
B.: 2018

Denetim Komitesinin İç Denetim Birimi Çalışmalarına Etkisi: Türkiye'de İç Denetim Birimi Yöneticilerinin Algısı Araştırması, **Manisa Celal Bayar Üniversitesi Sosyal Bilimler Enstitüsü**, Yayımlanmamış Doktora Tezi.

MOLLAOĞULLARI,
B., &
ÖZDOĞA
N, B.:
2018

“İletişim Teknolojilerindeki Gelişmeler, Riskler ve İç Denetimin Rolü”, **Yönetim Ve Ekonomi: Celal Bayar Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi**, 25(3), 625-639.

MORABIT O,
V.:
2015

Big Data And Analytics: Strategic and Organisational Impacts, Springer.

- MUKHOPADHYAY, I., CHAKRA BORTY, M. CHAKRA BARTI, S.: 2011 "A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems", **Journal of Information Security**, 2, 28-38.
- MUNRO, L., STEWARD J.: 2010 External Auditors' Reliance on Internal Audit: The Impact of Sourcing Arrangements and Consulting Activities. **Accounting & Finance**, 50(2), 371-387.
- NEW YORK TIMES: 2017 "All 3 billion yahoo accounts were affected by 2013 attack", (Çevrimiçi), <https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html>, 24.05.2020.
- NO, W. G., VASARHELYI, M. A.: 2017 "Cybersecurity and Continuous Assurance", **Journal of Emerging Technologies in Accounting**, 14(1), 1-12.
- ÖĞÜT, A.: 2003 **Bilgi Çağında Yönetim**, 2. bs., Ankara, Nobel Yayın Dağıtım.
- OKSAY, S., ACAR, O.: 2007 **Avrupa Birliği ve Türk Sigorta Sektöründe Denetim**, Türkiye Sigorta ve Reasürans Şirketleri Birliği Yayın No: 23, Sigorta Araştırma ve İnceleme Yayınları.
- ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT: 2004 "OECD Principles of Corporate Governance", (Çevrimiçi) <http://www.oecd.org/corporate/ca/corporategovernanceprinciples/31557724.pdf>, 18 Haziran 2020.
- ÖZBEK, Ç.: 2012 **İç Denetim Kurumsal Yönetim Risk Yönetimi İç Kontrol**, İstanbul, Türkiye İç Denetim Enstitüsü Yayınları No:3, Cilt 1.

- ÖZBİLGİN, S.: 2017 Bilgi Teknolojileri Servis Yönetiminin ITIL Çerçevesinde Perakende Firması İçin İncelenmesi ve ITIL Uygulaması Önerisi, **Maltepe Üniversitesi, Fen Bilimleri Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi.
- ÖZDOĞA N., B., KARGİN, S.: 2018 “Blok Zinciri Teknolojisinin Muhasebe ve Finans Alanlarına Yönelik Yansımaları ve Beklentiler.” **Muhasebe ve Finansman Dergisi**, (80), 161-176.
- ÖZDOĞA N., B.: 2014 İç Denetçilerin Gelişen İç Denetim Uygulamalarına ve Paydaş Beklentilerine Uyum, **Celal Bayar Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Doktora Tezi.
- ÖZEREN, B.: 2000 **İç Denetim, Standartları ve Mesleğin Yeni Açılımları**, Sayıştay Araştırma/ İnceleme/ Çeviri Dizisi, Ankara.
- ÖZGÜ, C., AKBAŞ, M.: 2014 “Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması”, **TÜBAV Bilim Dergisi**, 7(2), 16-31.
- ÖZOĞLU, B., MERCAN, C., ÇAKIROĞLU, S.: 2010 **Bir Güvence ve Danışmanlık Hizmeti İç Denetim**, İstanbul, İ.B.B. İç Denetim Birim Başkanlığı Yayınları No. 1.
- ÖZTÜRK, M. S.: 2018 “Siber Saldırıları, Siber Güvenlik Denetimleri ve Bütüncül Bir Denetim Modeli Önerisi”, **Muhasebe ve Vergi Uygulamaları Dergisi**, 208-232.
- PAMUKÇU, F.: 2011 “Finansal Raporlama ile Kamuyu Aydınlatma ve Şeffaflıkta Kurumsal Yönetimin Önemi”, **Muhasebe ve Finansman Dergisi**, 133-148.
- PANKO, R.: 2009 **Business Computer and Network Security**. Englewood Cliffs, NJ: Prentice-Hall.
- PAŞAOĞLU, D., TOKGÖZ, N., ŞAKAR, N., ERGUN

ÖZLER,
D.,
ÖZALP, İ.:
2013

PATHAK, J.: 2005 "Risk Management, Internal Controls and Organizational Vulnerabilities", **Managerial Auditing Journal**, 569-577.

PEHLİVA NLI, D.: 2008 Kurumsal Risk Yönetimi Temelli İç Denetim ve Türkiye Uygulamaları, **Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü**, Yayımlanmamış Doktora Tezi.

PENBER-BEY, G.: 2012 **The Parkerian Hexad: The CIA Triad Model Expanded.**

PICKETT, K. H.: 2005 **The Internal Audit Handbook.** England, John Willey and Sons.

PICKETT, K.H.: 2011 **The Essential Guide to Internal Auditing**, 2. ed., England, John Willey and Sons.

PONEMON
N
INSTITUTE
E
RESEARCH
CH
REPORT:
2013 "2013 Cost Of Data Breach Study: Global Analysis", 2013, (Çevrimiçi), <https://www.Ponemon.Org/Local/Upload/File/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.Pdf> 25.05.2020

PUBLIC
COMPANY
ACCOUNTING
OVERSIGHT
BOARD,:
2007 "AS 2201: An Audit of Internal Control Over Financial Reporting That is Integrated With an Audit of Financial Statements", (Çevrimiçi) <https://pcaobus.org/oversight/standards/auditing-standards/details/AS2201>.

RAHİMİA
N, F.,
BAJAJ,
A., "Estimation of Deficiency Risk and Prioritization of Information Security Controls: A Data-Centric Approach", **International Journal of Accounting Information Systems**, 20, 38-64.

BRADLEY
, W.:2016

REEDER- "Reducing Racial Disparities in Breast Cancer Care: The Role of Big
HAYES, Data", **Oncology (08909091)**, 31(10), 756-762.
K. E.,
TROEST
ER, M. A.,
MEYER,
A. M.:
2017

REIDER, **The Complete Guide to Operational Auditing**, USA, John Wiley&Sons.
H. R.:
1994

REIDER, **The Complete Guide to Operational Auditing**, USA, Wiley.
R.: 1994

RICHARD **2011 CSI Computer Crime And Security Survey**. Computer Security
SON, R.: Institute.
2011

RISK "Data breach quickview report 2019 year end", (Çevrimiçi),
BASED: <https://pages.riskbasedsecurity.com/2019-year-end-data-breach-quickview-report#:~:text=There%20were%207%2C098%20breaches%20reported,what%20it%20means%20for%202020>, 23.05.2020.
2019

SABUNC "İç Denetim Anlayışındaki Değişiklikler ve Gelişmeler", **Muhasebe Bilim**
U, B.: **Dünyası Dergisi**, 20, 779-789.
2018

SABUNC "İç Denetim Anlayışındaki Değişiklikler ve Gelişmeler", **Muhasebe Bilim**
U, B.: **Dünyası Dergisi**, 20 (Özel Sayı), 779–789.
2018

SAFEATL "Ransomware statistic", (Çevrimiçi),
AST: <https://safeatlast.co/blog/ransomware-statistics/>, 27.05.2020
2020

SAĞIROĞ **Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler**.
LU Ş.: Siber Güvenlik ve Savunma.
2018

SAĞIROĞ **Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık**. Ankara,
LU, Ş., Grafiker Yayınları.

ALKAN,
M.: 2018

ŞAHİNAS LAN, E., KANDEMI R, R., KANTÜR K, A.:
2010 Bilgi Güvenliği Risk Yönetim Metodolojileri ve Uygulamaları Üzerine İnceleme, **Ağ ve Bilgi Güvenliği Ulusal Sempozyumu Bildirileri**.

ŞAHİNAS LAN, Ö.:
2013 Siber Saldırılarına Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma, **Trakya Üniversitesi Fen Bilimleri Enstitüsü**, Yayınlanmamış Yüksek Lisans Tezi.

SAWYER, L. B., DITTNER, M. A., SCHEINE R, J.H.:
2003. **Sawyer's Internal Auditing: The Practice of Modern Internal Auditing**, 5. ed., Florida, USA, The Internal Audit Foundation.

SCHMIDT, N.: 2016 **Super-Empowering of Non-State Actors in Cyberspace**, World International Studies Committee 2014.

SECURIT Y EXCHANGE COMMISSION: 2002 "Sarbanes-Oxley Act", (Çevrimiçi) https://pcaobus.org/About/History/Documents/PDFs/Sarbanes_Oxley_Act_of_2002.pdf, 6 Aralık 2020.

SELAHAT TİN, K. O. Ç., ŞEKER, S., ŞEKER, F.: 2019 "Bilişim Teknolojileri (BT) Denetiminde Bilgi Güvenliği İle İlgili Uluslararası Standartlar ve Türkiye'deki Uyum Çabalarının İncelenmesi", **Uluslararası Muhasebe ve Finans Araştırmaları Dergisi**, 1(2), 121-139.

SELİMOĞ LU, S. K., SALDI, M. H.: 2019 "İşletmelerde Siber Risklerin Analizinde, Haritalanmasında ve Değerlendirilmesinde İç Denetimin Rolü", **Muhasebe ve Denetim Bakış= Accounting & Auditing Review**, 19(57), 1-18.

- SELİMOĞ
LU, S.,
ALTUNEL
, M.: 2019 “Siber Güvenlik Risklerinden Korunmada Köprü ve Katalizör Olarak İç Denetim”. **Denetim**, (19), 5-16.
- SELİMOĞ
LU, S.K.: 1999 “Faaliyet Denetimi”, **Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, 15(1), 193-206.
- SELVİ,
Ö.: 2011 “Bilgi Toplumu, Bilgi Yönetimi, ve Halkla İlişkiler”, **Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi**, 191-214.
- ŞEN, Ş.,
YERLİKA
YA, T.: 2013 **ISO 27001 Kurumsal Bilgi Güvenliği Standardı**, Akademik Bilişim.
- SERÇEM
ELİ, M.: 2015 İç Denetim Stratejisinde Sürekli Denetim Yaklaşımı BIST-100 Şirketlerinde Bir Araştırma, **Atatürk Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Doktora Tezi.
- SERMAY
E
PİYASASI
KURULU:
2011 “Kurumsal Yönetim İlkelerinin Belirlenmesine Ve Uygulanmasına İlişkin Tebliğ”, (Çevrimiçi) <https://www.spk.gov.tr/Sayfa/Dosya/66>, 11 Mayıs 2020.
- SEVİM,
A.: 2009 **Dijital Muhasebe**, Eskişehir, Eskişehir T.C. Anadolu Üniversitesi Yayınları No: 1903 İktisadi ve İdari Bilimler Fakültesi Yayınları No: 208.
- SİBERBÜ
LTEN:
2019 “Yapay Zeka, Siber Güvenlik İçin Tehdit Mi Çözüm Mü?”, (Çevrimiçi) <https://siberbulten.com/yapayzeka/yapay-zeka-siber-guvenlik-icin-tehdit-mi-cozum-mu/>, 8 Haziran 2020.
- SİBERTİ
ME: 2020 COBIT 5, (Çevrimiçi), <https://Sibertime.Com.Tr/Danismanlik/Cobit/> 05.06.2020
- SİBERTİ
ME: 2020 COBIT 5, (Çevrimiçi), <https://Sibertime.Com.Tr/Danismanlik/Bilgi-Teknolojileri-Altyapi-Kutuphanesi/> 11.06.2020.
- SILVERİO
-
FERNÁN
DEZ, M., “What Is A Smart Device?-A Conceptualisation Within The Paradigm of The Internet of Things.”, **Visualization in Engineering**, 6(1), 1-10.

RENUKA
PPA, S.,
SURESH,
S.: 2018

SOBEL, P. J.: 2005 **Auditor's Risk Management Guide Integrating Auditing and ERM**, USA, CCH Incorporated.

SOLMS, R., VAN NIEKERK, J.: 2013 "From Information Security to Cyber Security", **Computers and Security**, 38, 97-102.

SÖZÜER, A., GÖKÇEN, Z., ARSLANT AŞ, C. C.: 2012 "Yönetim Kurulu Özellikleri Ve Şirket Performansları: İMKB Kurumsal Yönetim ve İMKB 50 Endekslerindeki İşletmelerin Karşılaştırılması", **Yönetim Dergisi: İstanbul Üniversitesi İşletme Fakültesi İşletme İktisadi Enstitüsü**, 72, 77-89.

STAFFORD, D. T., DEITZ, G., LI, Y.: 2018 "The Role of Internal Audit and User Training In Information Security Policy Compliance", **Managerial Auditing Journal**, 410-424.

STEICHE, N., P.: 2012 "Principles and Fundamentals of Security Methodologies of Information Systems – Introduction" 2012, (Çevrimiçi), http://Pst.Libre.Lu/M2ssic-Metz/01_Intro-Art.Pdf, 02.02.2020.

STEINBAUM, P. J., RASCHKE, R. L., GAL, G., DILLA, W. N.: 2012 "The Relationship Between Internal Audit and Information Security: An Exploratory Investigation", **International Journal of Accounting Information Systems**, 13(3), 228-243.

STEINBAUM, P. J., RASCHKE, R. L., GAL, G.: "Information Security Professionals' Perceptions About The Relationship Between The Information Security and Internal Audit Functions", **Journal of Information Systems**, 27(2), 65-86.

DİLLA, W.
N.: 2013

STEİNBA
RT, P. J.,
RASCHK
E, R. L.,
GAL, G.,
DİLLA, W.
N.: 2016

“SECURQUAL: An Instrument For Evaluating The Effectiveness of Enterprise Information Security Programs”, **Journal Of Information Systems**, 30(1), 71-92.

STEİNBA
RT, P. J.,
RASCHK
E, R. L.,
GAL, G.,
DİLLA, W.
N.: 2018

“The Influence of A Good Relationship Between The Internal Audit and Information Security Functions on Information Security Outcomes”, **Accounting, Organizations And Society**, 71, 15-29.

SWİNTO
N. S.:
2019

Cybersecurity Governance, Part 1: 5 Fundamental Challenges.

SYMANT
EC: 2019

“Endpoint defense starts with prevention”, (Çevrimiçi), <https://symantec-enterprise-blogs.security.com/blogs/product-insights/endpoint-defense-starts-prevention>, 20.05.2020

T.C.
HAZİNE
VE
MALİYE
BAKANLI
ĞI: 2019

“Kurumsal Risk Yönetimi Bütünleşik Çerçeve-COSO”, (Çevrimiçi) <https://ms.hmb.gov.tr/uploads/2019/01/Kurumsal-Risk-Y%C3%B6netimi-B%C3%BCt%C3%BCnle%C5%9Fik-%C3%87er%C3%A7eve-COSO.pdf>, 3 Mart 2019.

T.C.
ULAŞTIR
MA
BAKANLI
ĞI: 2016

2016-2019 Ulusal Siber Güvenlik Stratejisi, Ankara: T.C Ulaştırma Denizcilik Ve Haberleşme Bakanlığı.

TAKÇI,
H.,
TÜRKER
AKYÜZ,
A. U.,
KARABA
Ğ, R.,
SOĞUKPI

“Bilgi Güvenliği Yönetiminde Varlıkların Risk Değerlendirmesi İçin Bir Model”, **Ağ ve Bilgi Güvenliği Sempozyumu.**

NAR, İ.:
2010

TANAKA, H.,
MATSUURA, K.,
SUDOH, O.: 2005
“Vulnerability and Information Security Investment: an Empirical Analysis of E-Local Government In Japan”, **Journal of Accounting and Public Policy**, 24(1), 37-59.

TANRIVERDİ, M.,
UYSAL, M.,
ÜSTÜNDAG, M. T.:
2019
“Blokzinciri Teknolojisi Nedir? Ne Değildir?: Alanyazın İncelemesi.” **Bilişim Teknolojileri Dergisi**, 12(3), 203-217.

TAPERA, J.: 2014
“The Importance of Strategic Management to Business Organizations”, **International Journal of Social Science Management**, 122-131.

TECHCRUNCH:
2019
“French data protection watchdog fines Google \$57 million under the GDPR”, (Çevrimiçi), <https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/>, 25.05.2020

TECHNOLOGY
INQUIRER:
2017
“At least 100,000 groups in 150 countries hit by Ransomware” (Çevrimiçi), <https://technology.inquirer.net/62619/least-100000-groups-150-countries-hit-ransomware>, 25.05.2020

TEKBAŞ, İ.: 2019
Muhasebenin Dijital Dönüşümü ve Mali Mühendislik, İstanbul, Hümanist Kitap Yayıncılık.

TEKEREK, A.,
GEMCİ, C., BAY, Ö.: 2016
“Web Tabanlı Saldırı Önleme Sistemi Tasarımı ve Gerçekleştirilmesi: Yeni Bir Hibrit Model”, **Gazi Üniversitesi Mühendislik- Mimarlık Fakültesi Dergisi**, 31 (3), 645–653.

THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADW
“Internal Control – Integrated Framework”, (Çevrimiçi) <https://www.coso.org/Pages/default.aspx>, 9 Şubat 2020.

AY
COMMISSION:
2013

THE
FINANCIAL
REPORTING
COUNCIL
: 2015

Internal Control: Revised Guidance for Directors on the Combined Code, London.

THE
INSTITUTE OF
INTERNAL
AUDITORS:
2009

“International Professional Practices Framework” (Çevrimiçi)
<https://na.theiia.org/>, (4 Nisan 2020).

THE
INSTITUTE OF
INTERNAL
AUDITORS:
2013

“Umuç”, (Çevrimiçi) https://www.tide.org.tr/uploads/UMUC_2013.pdf, 14
Ağustos 2020.

THE
INSTITUTE OF
INTERNAL
EDITORS:
2020

“Internal Auditing”, (Çevrimiçi) <https://na.theiia.org/standards-guidance/mandatory-guidance/pages/definition-of-internal-auditing.aspx>,
8 Eylül 2020.

TOFAN,
D.C.:
2011

“Information Security Standards. Journal of Mobile”, **Embedded and Distributed Systems**, 3 (3), 128-135

TONTA,
Y.: 1999

“Bilgi Toplumu ve Bilgi Teknolojisi”, **Türk Kütüphaneciliği**, 13 (4), 363-375.

TÖRENLİ,
N., 2003

EİT Dolayımında Kapitalist Üretim İlişkilerinin Yeniden Yapılandırılması:
Enformasyon Toplumu ve Düşündükleri, **SBF Dergisi**, 58, 191-219.

- TRUSTW ARE: 2018 **2018 Trustwave Global Security Report.**
- TURAN, M.: 2020 NIST – Cyber Security Framework V.1.1., (Çevrimiçi), <https://Mturan.Net/Blog/Nist-Cyber-Security-Framework-V-1-1/> 07.07.2020
- TÜREDİ H., KOBAN, A.O.: 2016 “COSO İç Kontrol Modelinde Risk Değerlendirme Faaliyetleri”, **Marmara Üniversitesi Öneri Dergisi**, 12(46), 155-177.
- TÜREDİ, H., KOBAN A.O., KARAKAYA, G.: 2015 “COSO İç Kontrol (ABD) Modeli ile İngiliz (Turnbull) ve Kanada (Coco) Modellerinin Karşılaştırılması”, **Sayıştay Dergisi**, 99, 95-120.
- TÜREDİ, H.: 2000 **Denetim**, Trabzon, Celepler Matbaacılık Yayın ve Dağıtım.
- TÜREL, A.: 2018 **Muhasebe Bilgi Sistemleri**, İstanbul, Çağlayan Kitapevi.
- TÜRK DİL KURUMU: 2020 “Bilgi”, (Çevrimiçi) <https://sozluk.gov.tr/>, 21 Ocak 2021.
- TÜRK SANAYİCİLERİ VE İŞ İNSANLARI DERNEĞİ : 2017 “Dijitalleşen Dünyada Ekonominin İtici Gücü E-ticaret”, (Çevrimiçi) http://www.eticaretraporu.org/wp-content/uploads/2017/04/TUSIAD_E-Ticaret_Raporu_2017.pdf, 8 Mayıs 2020.
- TÜRKİYE İÇ DENETİM ENSTİTÜSÜ: 2011 “İç Denetim Terimler Sözlüğü”, (Çevrimiçi) <https://www.tide.org.tr/file/documents/pdf/IcDenetimTerimlerSozlugu.pdf>, 15 Ekim 2020.

- TÜRKİYE
İÇ
DENETİM
ENSTİTÜ
SÜ: 2017
- “Küresel Bakış Açıları ve Anlayışlar: Yapay Zekâ – İç Denetim Mesleğine İlişkin Dikkate Alınması Gerekenler”, (Çevrimiçi)
<https://global.theiia.org/translations/PublicDocuments/GPI-Artificial-Intelligence-Part-I-Turkish.pdf>, 7 Haziran 2020.
- TÜRKİYE
İÇ
DENETİM
ENSTİTÜ
SÜ: 2020
- “Uluslararası Mesleki Uygulama Çerçevesi”, (Çevrimiçi)
<https://www.tide.org.tr/page/22/UMUC>, 7 Ekim 2020.
- TÜRKİYE
KURUMS
AL
YÖNETİM
DERNEĞİ
,
DELOİTT
E: 2006
- “Nedir Bu Kurumsal Yönetim?” (Çevrimiçi)
http://www.tkyd.org/files/downloads/faaliyet_alanlari/yayinlarimiz/tkyd_yayinlari/nedir_bu_kurumsal_yonetim.pdf., 27 Eylül 2019.
- TÜRKME
N, S. Y.,
DURBILM
EZ, S.E.:
2018
- “Blockchain Teknolojisi ve Türkiye Finans Sektöründeki Durumu”
Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 33(1), 369-384.
- UĞURLU,
Y.: 2019
- İç Denetimde Farklı Kaynak Kullanımlarının Hileleri Önleme ve Ortaya Çıkarmadaki Rolü, **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Doktora Tezi.
- ÜLGİN,
H.,
MİRZE,
S.K.: 2004
- İşletmelerde Stratejik Yönetim**, İstanbul, Literatür Yayınları.
- ULUDAG,
S.: 2017
- Değişen Risk Algısı ve İç Denetim. **Muhasebe ve Denetime Bakış= Accounting & Auditing Review**, 17(51), 93-101.
- ULUSAL
SİBER
OLAYLAR
A
MÜDAHA
LE
- Siber Güvenliğe İlişkin Temel Bilgiler, 2014, (Çevrimiçi),
<https://www.Usom.Gov.Tr/Dosya/1418807122-USOM-SGFF-001>

MERKEZİ
: 2014

ÜNAL, S: "İnternet Üzerinde İzinli Pazarlama Yaklaşımı", **Öneri Dergisi**, 155-162.
2010

UNDER ARMOR: "Under armour notifies myfitnesspal users of data security issue" (Çevrimiçi), <http://www.uabiz.com/news-releases/news-release-details/under-armour-notifies-myfitnesspal-users-data-security-issue>, 25.05.2020

ÜNVER, M., CANBAY, C., MİRZAOĞLU, A.: **Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler**. Ankara: Bilgi Teknolojileri ve İletişim Kurumu.
2011

UYAR, S.: **İç Kontrol ve İç Denetim, 5018 Sayılı Kanun Açısından Değerlendirme**, Ankara, Gazi Kitabevi.
2009

UZAY, Ş.: **Muhasebe Denetimi**, Ankara, Gazi Kitabevi.
2009

UZUN, A.K.: 2009 "Şirketlerde İç Kontrollerin Yeterliliğinde İç Denetimin Rolü", (Çevrimiçi) <http://www.icdenetim.net>, 7 Aralık 2019.

VACCA, R. J: 2006 **Guide to Wireless Network Security**, Pomeroy, OH: Springer Science & Business Media LLC.

VALLABH ANENİ, R.S.: 2005 **Wiley CIA Exam Review Volume 2: Conducting The Internal Audit Engagement**, USA, John Wiley & Sons.

VAN GREMBE RGEN, W., DE HAES, S., GULDEN TOPS, E.: 2004 "Structures, Processes and Relational Mechanisms For IT Governance", **In Strategies For Information Technology Governance**, 1-36

VARONİS : 2019 "2019 global data risk report from the varonis data lab.", (Çevrimiçi), <https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf>, 27.05.2020

- VARONIS : 2019 “2019 global data risk report from the varonis data lab” (Çevrimiçi), <https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf>, 26.05.2020
- VERIZON : 2018 **2018 Data Breach Investigations Report.**
- VERIZON : 2018 **2018 Data Breach Investigations Report.**
- VERIZON : 2019 **2019 Data Breach Investigations Report.**
- WALLAC E, L., LİN, H., CEFARAT Tİ, M. A.: 2011 “Information Security and Sarbanes-Oxley Compliance: An Exploratory Study”, **Journal of Information Systems**, 25(1), 185-211.
- WARD, J. S. & BARKER, A.: 2013 **Undefined by data: A Survey of Big Data Definitions**, arXiv preprint arXiv:1309.5821.
- WEBSTE R, F.: 2001 **Theories of The Information Age**, Routledge.
- WEISS, M., SOLOMO N, M. G.: 2015 **Auditing IT Infrastructures for Compliance**, Jones & Bartlett Publishers.
- WEITZNE R, D., ABELSON, H., BERNER S-LEE, T., FEIGENBAUM, J., HENDLER, J. VE SUSSMAN : 2011 “Information Accountability”, **Communications Of The ACM**, 51(6), 82–87.

N, G.:
2008

WHITMAN, M. E., & MATTORD, H. J.:
Risk Management: Controlling Risk, ME Whitman, & HJ Mattord, Management of Information Security.
2017

YAN, Y., QIAN, Y. H. VE TIPPER, D.:
“A Survey on Cyber Security For Smart Grid Communications”, **IEEE Communications Surveys and Tutorials**, 14(4), 998-1007.
2012

YAVANOĞLU, U., SAĞIROĞLU, Ş., ÇOLAK, İ.:
“Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler”, **Politeknik Dergisi**, 15(1), 15–27.
2012

YAYLA, M.:
“Hukuki Bir Terim Olarak Siber Savaş”, **TBB Dergisi**, (104), 177-202.
2013

YERELİ, A.N., ÖZDOĞA N. B.:
Genel Kabul Görmüş Denetim Standartlarının Türkiye Açısından Değerlendirilmesi, Manisa, Celal Bayar Üniversitesi Matbaası.
2009

YILANCI, M.:
İç Denetim ve İç Kontrol Değerleme Rehberi, Detay Yayıncılık.
2015

YILDIZ, M.:
Siber Suçlar ve Kurum Güvenliği, **Denizcilik Uzmanlık Tezi**, Ankara: Ulaştırma Denizcilik ve Haberleşme Bakanlığı Bilgi İşlem Daire Başkanlığı.
2014

YILDIZ, M.:
Siber Suçlar ve Kurum Güvenliği, **Ulaştırma Denizcilik ve Haberleşme Bakanlığı Denizcilik Uzmanlık Tezi**.
2014

- YILMAZ, A.: 2015 **Türkiye’deki Dolandırıcılık Tipolojileri: Dolandırıcılık Olaylarının Kategorik Tasnifi ve Yapılış Şekilleri.**
- YILMAZ, E., HALİL, U., GÖNEN, S.: 2015 “Bilgi Toplumuna Geçiş ve Siber Güvenlik”, **Bilişim Teknolojileri Dergisi**, 8(3), 133-145.
- YÖRÜKE R, S.: 2004 **Başka Ülke Örnekleri Temelinde Kontrol, Denetim, Teftiş ve Soruşturma; Kavramsal Bir Çerçeve**, Ankara, Tesev Yayınları.
- YÜCEL, A., MANDACI, P., KURT, G.: 2007 “İşletmelerin Finansal Risk Yönetimi ve Türev Ürün Kullanımı: İMKB 100 Endeksinde Yer Alan İşletmelerde Bir Uygulama”, **Muhasebe ve Finansman Dergisi**, (36), 1-9.
- ZENGİN N.: 2018 Elektronik Ticaretin Kullanımında Kritik Başarı Faktörlerinin Etkisi ve Türkiye’de Faaliyet Gösteren Elektronik Ticaret İşletmelerinde Bir Araştırma, **Beykent Üniversitesi Sosyal Bilimler Enstitüsü**, Yayınlanmamış Doktora Tezi.

EK

EK – 1 Anket Formu Örneđi

Sayın Katılımcı,

Bu yazının ekinde sunduđumuz anket formu İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü İşletme Fakóltesi Muhasebe Anabilim Dalı Doktora Programında Nevzat GÜNGÖR tarafından hazırlanmakta olan “İç Denetimde Bilgi Teknolojileri ve Siber Güvenlik: Bir Uygulama” konulu doktora tez çalışmasının araştırma bölümü için hazırlanmıştır.

Araştırmanın temel amacı işletmelerin mevcut siber güvenlik uygulamaları hakkında durum tespiti yapmak ve iç denetçilerin siber güvenlik süreçlerinde aldıkları rolü ve süreçlere verdikleri katkıları tespit etmektir.

Araştırmanın sonuçları katılımcıların istekleri doğrultusunda kendilerine rapor olarak gönderilecektir. **Anketimizi cevaplamanız bilimsel araştırmamızın tamamlanmasında büyük öneme sahiptir.**

Bilimsel araştırmamıza desteđiniz ve katkılarınız için teşekkür ederiz.

Prof. Dr. Fatma Lerzan KAVUT

Arş. Grv. Nevzat GÜNGÖR

Bölüm-1 Demografik Bilgiler

1) Cinsiyet

☐ Erkek

☐ Kadın

2) Kaç Yaşındasınız?

☐ 25 ve altı

☐ 26-30

☐ 31-35

☐ 36-40

☐ 41-45

☐ 45 ve üstü

3) Eğitim Durumunuz

☐ Lisans

☐ Yüksek Lisans

☐ Doktora

4) İç denetim departmanında hangi pozisyonda görev yapıyorsunuz?

☐ İç denetim yöneticisi

☐ İç denetçi

☐ İç denetçi yardımcısı

5) Bilgi Teknolojileri ve Siber Güvenlik konularında kendinizi nasıl tanımlarsınız?

☐ Bilgi teknolojileri ve siber güvenlik konularında yeterli bilgiye sahibim.

☐ Bilgi teknolojileri ve siber güvenlik konularında eğitim aldım ve uzmanlık derecesinde bilgi sahibiyim.

☐ Bilgi teknolojileri ve siber güvenlik konularında herhangi bir tecrübeye sahip değilim.

6) Sahip Olduğunuz Mesleki Sertifikasyonlar (1'den fazla seçilebilir)

☐ CPA/CA

☐ CISA (Certified Information Systems Auditor)

☐ CIA (Certified Internal Auditor)

☐ CISSP (Certified Information Systems Security Professional)

☐ Diğer (CRMA, CRISC, CGEIT, vb.,)

☐ Yok

7) İşletmeniz siber güvenlik ve bilgi teknolojileri konularında dışarıdan hizmet almakta mıdır?

- ☐ İşletmemiz, siber güvenlik ve bilgi teknolojileri konularında dışarıdan hizmet almaktadır.
- ☐ İşletmemiz siber güvenlik ve bilgi teknolojileri konularında sadece danışmanlık hizmeti almaktadır.
- ☐ İşletmemiz siber güvenlik ve bilgi teknolojileri faaliyetleri BT/Siber Güvenlik departmanları tarafından yürütülmektedir.

8) Çalıştığınız İşletmenin Sektörü

- ☐ Üretim
- ☐ Bankacılık
- ☐ Havacılık ve Uzay
- ☐ Madencilik/Metaller/Mineraller
- ☐ Risk yönetimi/Sigorta
- ☐ Enerji
- ☐ İletişim, Medya ve Teknoloji
- ☐ Kimya
- ☐ Perakende
- ☐ İnşaat
- ☐ Diğer

9) Çalıştığınız İşletmenin Çalışan Sayısı

- ☐ 100'ün altı
- ☐ 100-299
- ☐ 300-999
- ☐ 1000-4999
- ☐ 5000 ve üzeri

10) Çalıştığınız İşletmenin Toplam Aktif Büyüklüğü ne kadardır?

- ☐ 100,000 TL altı
- ☐ 100,001 TL- 500,000 TL
- ☐ 500,001 TL-1,000,000 TL
- ☐ 1,000,001 TL-10,000,000 TL
- ☐ 10,000,001 TL – 100,000,000 TL
- ☐ 100,000,000 TL üzeri

11) İç Denetçilik Mesleki Tecrübeniz (Yıl)

- ☐ 5 yıldan az
- ☐ 5-9
- ☐ 10-14
- ☐ 15-19
- ☐ 20 ve üzeri

12) Sizce işletmeniz Ticari/Üretim/Hizmet faaliyetlerinde bilgi teknolojilerine ne derece bağımlı?

- ☐ Bağımlı değil
- ☐ Az bağımlı
- ☐ Bağımlı
- ☐ Çok bağımlı

13) Sizce işletmenizi hedef alan ve kişisel bilgilerin (müşteri bilgisi vb.) sızdırılması ile sonuçlanan bir siber saldırının firma itibarı üzerine etkileri ne oranda olur?

- ☐ Neredeyse yok
- ☐ Az
- ☐ Çok
- ☐ Firmanın geleceğini etkileyecek kadar fazla olur

14) Kritik bilgiler; ulusal sırlar, ticari sırlar, müşterilere ait özel bilgiler vb. olarak sınıflandırılmaktadır. Sizce bu kritik bilgilerin, işletmenizin elinde tuttuğu, yönettiği ve kullandığı tüm bilgiler arasındaki oranı ne kadardır?

- ☐ Neredeyse yok
- ☐ Az
- ☐ Bilgilerin yarısı
- ☐ İşletmenin sahip olduğu verilerin çoğunluğu kritik öneme sahiptir.

Bölüm-2 Siber Güvenliğe Kurumsal Yaklaşım,

	Hiç uygulanmıyor	Kısmen uygulanıyor	Uygulanıyor	Çoğunluğu uygulanıyor	Tamamen uygulanıyor
15) İşletmemizin siber güvenliğe ilişkin yazılı kural ve politikaları vardır.					
16) İşletmemiz siber güvenliğe ilişkin yazılı kural ve politikaları oluştururken hayati öneme sahip alanlarda oluşabilecek tehlike ve güvenlik açıklarını dikkate almıştır.					
17) İşletmemizin siber güvenliğe ilişkin kural ve politikaları, ülkemizdeki ilgili kanun ve yönetmeliklere uygundur.					
18) İşletmemiz kritik bilgi teknolojilerini önem derecesine göre sınıflandırıp, bu sistemleri oluşturulan sınıflandırmaya göre yönetmektedir.					
19) İşletmemiz bilgi yaşam döngüsünün tüm aşamalarında gerekli güvenlik önemlerini almaktadır. (Bilgi yaşam döngüsü: bilginin oluşturulması, kullanılması, depolanması, iletilmesi, işlenmesi ve imha edilmesi)					
20) İşletmemiz bilgi teknolojilerine yönelik hizmet alımlarında, gerekli güvenlik önlemlerini sözleşme maddelerine dahil etmektedir.					
21) İşletmemiz tüm çalışanlara siber güvenliğe ilişkin yükümlülükleri açıkça bildirmektedir.					
22) İşletmemiz tüm çalışanlara düzenli olarak bilgi güvenliği ve siber güvenlik eğitimleri vermektedir.					

Bölüm-3 Fiziksel ve Çevresel Güvenlik Tedbirleri

	Hiç uygulanmıyor	Kısmen uygulanıyor	Uygulanıyor	Çoğunluğu uygulanıyor	Tamamen uygulanıyor
23) İşletmemize ait tesislerin güvenliğini iyileştirmek için gerekli güvenlik önlemleri alınmaktadır.					
24) İşletmemize ait tesislere giriş-çıkışı düzenleyen yazılı kurallar vardır.					
25) İşletmemizde bilgi teknolojilerine yönelik her türlü tehlikeye (doğal afetler veya insan kaynaklı zararlar) karşı koruyucu önlemler alınmıştır.					
26) İşletmemizde taşınabilir bilgisayarlar ve harici depolama aygıtlarının kullanımına ilişkin güvenlik önlemleri alınmıştır.					

Bölüm-4 Bilgi Sistemleri ve İletişim Ağlarının İşletim ve Bakım Kontrolleri

	Hiç uygulanmıyor	Kısmen uygulanıyor	Uygulanıyor	Çoğunluğu uygulanıyor	Tamamen uygulanıyor
27) İşletmemiz bilgi teknolojileri verilerini (sistem konfigürasyon ve yedekleri) uygun bir şekilde korumaktadır.					
28) İşletmemizde bilgi teknolojileri kurulum ve kullanım süreçleri siber güvenlik hususları dikkate alınarak icra edilmektedir.					
29) İşletmemiz verilerini uygun bir şekilde yedeklemektedir.					
30) İşletmemiz kötü amaçlı yazılımlara (virüs, trojan, vb.) karşı önlemler almaktadır.					
31) İşletmemiz bilgi sistemlerinin güvenlik açıklarını azaltmak için önlemler almaktadır.					
32) İşletmemiz bilgi sistemlerine bağlantıları güvenli bir şekilde tesis etmektedir.					
33) İşletmemiz tüm cihaz ve aygıtların çalınma riskine karşı gereken önlemleri almaktadır.					

Bölüm-5 Yazılım Geliştirme ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tedbirleri

	Hiç uygulanmıyor	Kısmen uygulanıyor	Uygulanıyor	Çoğunluğu uygulanıyor	Tamamen uygulanıyor
34) İşletmemiz bilgi sistemlerine bağlantı için gerekli kimlik denetimlerini gerçekleştirmektedir.					
35) İşletmemizde bilgi teknolojilerine kimlerin hangi şartlarda erişebileceği düzenlenmiştir.					
36) İşletmemiz yerel ağlar üzerinde yetki denetimi uygulamaktadır.					
37) İşletmemiz yazılım geliştirme projelerinin güvenlik gereksinimlerini tanımlamakta ve bu gereksinimleri projelere dahil etmektedir.					
38) İşletmemiz yazılım ürünlerinin seçimi, satın alınması ve/veya bakım işlerinde güvenlik kontrolleri gerçekleştirmektedir.					

Bölüm-6 Siber Güvenlik İhlalleri ve İş Sürekliliği Yönetimi

	Hiç uygulanmıyor	Kısmen uygulanıyor	Uygulanıyor	Çoğunluğu uygulanıyor	Tamamen uygulanıyor
39) İşletmemiz bilgi sistemleri arızalarının kurum faaliyetlerini aksatmaması için gerekli önlemleri almaktadır.					
40) İşletmemizde olası bilgi sistemi kaynaklı problemler için uygulanacak acil eylemleri belirten yazılı prosedürler bulunmaktadır.					
41) İşletmemizin bilgi sistemleri arızalarına karşı mücadeleyi ele alan bir İş Sürekliliği Yönetimi bulunmaktadır.					

Bölüm-7 Siber Güvenlik Fonksiyonu Açısından İç Denetçinin Görev Tanımı Algısı

	Hiç katılmıyorum	Kısmen katılıyorum	Kararsızım	Katılıyorum	Tamamen katılıyorum
42) İç denetim birimi üst yönetimin belirlediği plan ve politikalarının uygulanmasından sorumludur.					
43) İç denetim birimi işletmenin diğer departmanlarına danışmanlık hizmeti vermektedir.					
44) İç denetim birimi işletmedeki eksiklikleri tespit etmekte ve raporlamaktır.					

Bölüm-8 İç Denetim Departmanının Siber Güvenlik Bilgi Düzeyi Algısı

	Hiç katılmıyorum	Kısmen katılıyorum	Kararsızım	Katılıyorum	Tamamen katılıyorum
45) İç denetim birimi, siber güvenlik konusunda bilgi sahibi kişilerden oluşmaktadır.					
46) İç denetim birimi siber güvenlik konusunda uzman kişilerden oluşmaktadır.					
47) İç denetim birimi siber güvenlik hakkında güncel gelişmeleri takip etmektedir.					

Bölüm-9 İç Denetim Departmanının Siber Güvenliği Gözden Geçirme Sıklığı

	Hiç yapılmaz	Nadiren yapılır	Bazen yapılır	Sıklıkla yapılır	Çok sıklıkla yapılır
48) İş sürekliliği ve olağanüstü durum kurtarma planları iç denetim tarafından;					
49) Kimlik ve erişim yönetimi kontrolleri iç denetim tarafından;					
50) Verilerin kaydedilmesi ve izlenmesi iç denetim tarafından;					
51) Güvenlik duvarları ve diğer ağ erişim cihazları iç denetim tarafından;					
52) Kriptolama (şifreleme yönetimi dahil) iç denetim tarafından;					
53) Yedekleme prosedürleri iç denetim tarafından;					
54) Değişim yönetimi kontrolleri iç denetim tarafından;					
55) Güvenlik politikaları iç denetim tarafından;					

Bölüm-10 Siber Güvenlik İşlevi Açısından İç Denetim Departmanının Katma Değer Algısı

	Hiç katılmıyorum	Kısmen katılmıyorum	Kararsızım	Katılıyorum	Tamamen katılıyorum
56) Çalıştığım işletmede, iç denetim bulguları / raporları siber güvenlik işlevine yararlı bilgiler sağlamaktadır.					
57) Çalıştığım işletmede, iç denetim bulguları / raporları üst yönetime siber güvenliğin etkinliği hakkında yararlı bilgiler sağlamaktadır.					
58) Çalıştığım işletmede, siber güvenliği gözden geçirme konusunda iç denetim departmanı etkin bir şekilde çalışmaktadır.					

Bölüm-11 İç Denetim ve Bilgi Teknolojileri (BT) Departmanları Arasındaki İlişkinin Algısı

	Hiç katılmıyorum	Kısmen katılıyorum	Kararsızım	Katılıyorum	Tamamen katılıyorum
59)Çalıştığım işletmede iç denetim ile BT departmanları arasında uyumsuzluk/anlaşmazlık vardır.					
60) Çalıştığım işletmede iç denetim ve BT personeli arasındaki ilişki yakın ve kişiseldir.					
61) Çalıştığım işletmede, iç denetim ile BT personeli arasında iyi bir iş ilişkisi vardır.					
62) BT ve iç denetim çalışanları, bilgi sistemlerinin güvenilir olmasını sağlamak için birlikte çalışmaktadır.					

Bölüm-12 Siber Güvenlik Konusunda Üst Yönetimin Desteğine İlişkin İç Denetçi Algısı:

	Hiç katılmıyorum	Kısmen katılıyorum	Kararsızım	Katılıyorum	Tamamen katılıyorum
63) Çalıştığım işletmede üst yönetim siber güvenlik için yeterli kaynakları sağlamaktadır.					
64) Çalıştığım işletmede, üst yönetim çalışanlarla siber güvenliğin önemi hakkında düzenli olarak iletişim kurmaktadır.					
65) Çalıştığım işletmede üst yönetim siber güvenliğin önemli bir konu olduğuna inanmaktadır.					
66) Çalıştığım işletmede üst yönetim siber güvenlik konularında reaktif olmaktan ziyade daha proaktiftir.					

Bölüm- 13 Siber Güvenlik Vak'aları

67) Geçtiğimiz yıl içerisinde işletmenizde kaç adet siber güvenlik vak'ası (Phishing, veri ihlali vb.) gerçekleşti?

- ☐ 0
- ☐ 1-5
- ☐ 6-10
- ☐ 11-15
- ☐ 16-20
- ☐ 21-25
- ☐ 25'den fazla

68) Cari yılın mevcut iç denetim raporlarındaki toplam bulgu sayısını göz önünde bulundurduğunuzda, siber güvenliğine ilişkin iç denetim bulgularının yüzdesi kaçtır?

- ☐ %0
- ☐ %1-5
- ☐ %6-10
- ☐ %11-15
- ☐ %16-20
- ☐ %21-25
- ☐ %25'den fazla

69) İşletmenizin iç denetim birimi siber güvenlik konusunda kaç yıldır aktif olarak rol almaktadır?

- ☐ 0-3
- ☐ 4-6
- ☐ 7-10
- ☐ 10 yıldan fazla

70) İç denetim biriminin siber güvenlik konusunda aktif olarak faaliyet göstermesiyle siber güvenlik vak'aları;

- ☐ Önemli ölçüde azaldı
- ☐ Azaldı
- ☐ Aynı oranda kaldı
- ☐ Arttı
- ☐ Önemli ölçüde arttı
- ☐ Hiç Yaşanmadı

ÖZGEÇMİŞ

Nevzat Güngör, ilk, orta ve lise eğitimini Mersin’de tamamlamıştır. 2014 yılında İstanbul Üniversitesi İşletme Fakültesi İngilizce İşletme Bölümü’nden mezun olmuştur. 2017 yılında İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Muhasebe Tezli Yüksek lisans Programını “ENTEĞRE RAPORLAMA VE ENTEĞRE RAPOR ÇERÇEVESİNİN DÜNYA’DA VE TÜRKİYE’DE UYGULANMASI ÜZERİNE BİR İNCELEME” adlı tez çalışması ile tamamlamıştır.

2015 yılında Yıldız Teknik Üniversitesi İşletme Bölümü’nde araştırma görevlisi olarak çalışmaya başlamıştır. Aynı yıl içerisinde İstanbul Üniversitesi İşletme Fakültesi Muhasebe Anabilim Dalı’na araştırma görevlisi olarak geçiş yapmıştır. 2017 yılında İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Muhasebe Doktora Programına kabul edilmiştir. Evli olan Nevzat Güngör, İstanbul Üniversitesi’nde araştırma görevlisi olarak çalışmaya devam etmektedir.