DİJİTAL DÖNÜŞÜMÜN İÇ KONTROL SİSTEMİNDE YARATTIĞI RİSKLER VE BU RİSKLERİN YÖNETİMİNDE İÇ DENETİM FONKSİYONU: TÜRKİYE'DEKİ FARKINDALIĞIN ARAŞTIRILMASI

Doktora Tezi

MEHTAP ALTUNEL

Eskişehir 2023

DİJİTAL DÖNÜŞÜMÜN İÇ KONTROL SİSTEMİNDE YARATTIĞI RİSKLER VE BU RİSKLERİN YÖNETİMİNDE İÇ DENETİM FONKSİYONU: TÜRKİYE'DEKİ FARKINDALIĞIN ARAŞTIRILMASI

MEHTAP ALTUNEL

DOKTORA TEZİ

İşletme (Muhasebe) Anabilim Dalı

Danışman: Prof. Dr. Seval SELİMOĞLU

Eskişehir

Anadolu Üniversitesi

Sosyal Bilimler Enstitüsü

Haziran 2023

Bu tez çalışması BAP Komisyonunca kabul edilen 2108E221 no.lu proje kapsamında desteklenmiştir.

JÜRİ VE ENSTİTÜ ONAYI

Mehtap ALTUNEL'ın "Dijital Dönüşümün İç Kontrol Sisteminde Yarattığı Riskler ve Bu Risklerin Yönetiminde İç Denetim Fonksiyonu: Türkiye'deki Farkındalığın Araştırılması" başlıklı tezi **05 Haziran 2023** tarihinde, aşağıdaki jüri tarafından Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin 37. Maddesi uyarınca ilgili maddeleri uyarınca **İşletme Anabilim Dalı Muhasebe Bilim Dalında, Doktora** tezi olarak değerlendirilerek kabul edilmiştir.

İmza

Üye (Tez Danışmanı)	**: Prof. Dr. Seval SELİMOĞLU**
Üye	**:Prof. Dr. Necdet SAĞLAM**
Üye	**:Prof. Dr. Gülsün KURUBACAK**
Üye	**:Prof. Dr. Birol YILDIZ**
Üye	**:Doç. Dr. Şafak AĞDENİZ**

Prof. Dr. Saime ÖNCE
Anadolu Üniversitesi
Sosyal Bilimler Enstitüsü Müdürü

ÖZET

DİJİTAL DÖNÜŞÜMÜN İÇ KONTROL SİSTEMİNDE YARATTIĞI RİSKLER VE BU RİSKLERİN YÖNETİMİNDE İÇ DENETİM FONKSİYONU: TÜRKİYE'DEKİ FARKINDALIĞIN ARAŞTIRILMASI

Mehtap ALTUNEL

İşletme Anabilim Dalı Muhasebe Bilim Dalı

Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü, Haziran 2023

Danışman: Prof. Dr. Seval SELİMOĞLU

Bu çalışmanın amacı dijital dönüşüm sürecinde karşılaşılan riskleri yönetmek için iç denetim fonksiyonunun nasıl bir yol izlediği/izleyeceği yönünde Türkiye'de farkındalık araştırması yapılması ve bu araştırma sonucunda önerilerin sunulmasıdır. Bu çerçevede iki aşamalı Delphi tekniği kullanılmıştır. Birinci aşamada akademisyenler, kamu, bağımsız denetim kurumu ve yasal yapıcı kuruluşlarda çalışan iç denetçilerden oluşan 13 katılımcı ile yarı yapılandırılmış görüşme gerçekleştirilmiştir. Bu aşama çalışmanın nitel kısmını oluşturmaktadır. Görüşmeler neticesinde ikinci aşamada, 65 ifadeden oluşan anket formu katılımcılara sunularak görüşleri alınmış ve analiz edilerek görüş birliği sağlanamayan ifadeler ayıklanarak üçüncü aşama için 60 ifadeden oluşan son anket formu hazırlanarak katılımcılardan görüşleri alınmıştır. İkinci ve üçüncü aşama çalışmanın nicel kısmını oluşturmaktadır. Çalışma sonucunda örneklem çerçevesinde katılımcıların dijital dönüşümün iç denetim üzerinde etkileri konusunda farkındalıklarının olduğu ve kurumların dijital dönüşüm sürecinde iç denetim fonksiyonundan danışmanlık rolü çerçevesinde beklentilerinin olduğuna ulaşılmıştır.

Anahtar Sözcükler: Dijital dönüşüm, İç denetim fonksiyonu, İç denetçi, Delphi tekniği

ABSTRACT

RISKS IN THE CREATION OF THE INTERNAL CONTROL SYSTEM OF DIGITAL TRANSFORMATION AND INTERNAL AUDIT FUNCTION IN MANAGEMENT OF THE RISKS :RISK AWARENESS INVESTIGATION IN TURKEY

Mehtap ALTUNEL

Department of Business

Programme in Accounting

Anadolu University, Graduate School of Social Sciences, June 2023

Supervisor: Prof. Dr. Seval SELİMOĞLU

The purpose of this study is to conduct awareness research in Turkey on how the internal audit function follows/will follow in order to manage the risks encountered in the digital transformation process and to present suggestions as a result of this research. In this framework, two-phase Delphi technique was used. In the first phase, semi-structured interviews were conducted with 13 participants, consisting of academics, internal auditors working in public, independent auditing institutions and law-making institutions. This stage constitutes the qualitative part of the study. As a result of the interviews, in the second stage, the survey form consisting of 65 statements was presented to the participants and their opinions were taken. The second and third phases constitute the quantitative part of the study. As a result of the study, it was found that the participants were aware of the effects of digital transformation on internal audit and that the institutions had expectations from the internal audit function within the framework of the consultancy role in the digital transformation process.

Keywords: Digital transformation, Internal auditing function, Internal auditor, Delphi technique

ÖNSÖZ

Bu çalışmanın yanında birçok çalışmada ve doktora sürecimde desteğini esirgemeyen başta kıymetli danışman hocam Prof. Dr. Seval SELİMOĞLU'na sonsuz teşekkürlerimi sunarım. Ayrıca değerli katkılarıyla tez izleme jürimde bulunan Prof. Dr. Necdet SAĞLAM ve Prof. Dr. Birol YILDIZ hocalarıma, tezin uygulama aşamasında kullandığım yöntem konusunda yol gösteren, desteğini esirgemeyen Prof. Dr. Gülsün KURUBACAK hocama teşekkür ederim. Birlikte akademik çalışmalarda yer aldığım Doç. Dr. Gül YEŞİLÇELEBİ'ye desteği için teşekkürlerimi sunarım.

Bu çalışmaya katkı vermeyi kabul ederek, değerli vakitlerini ayıran ve değerli bilgiler paylaşan tüm katılımcılara da ayrı ayrı teşekkür ederim.

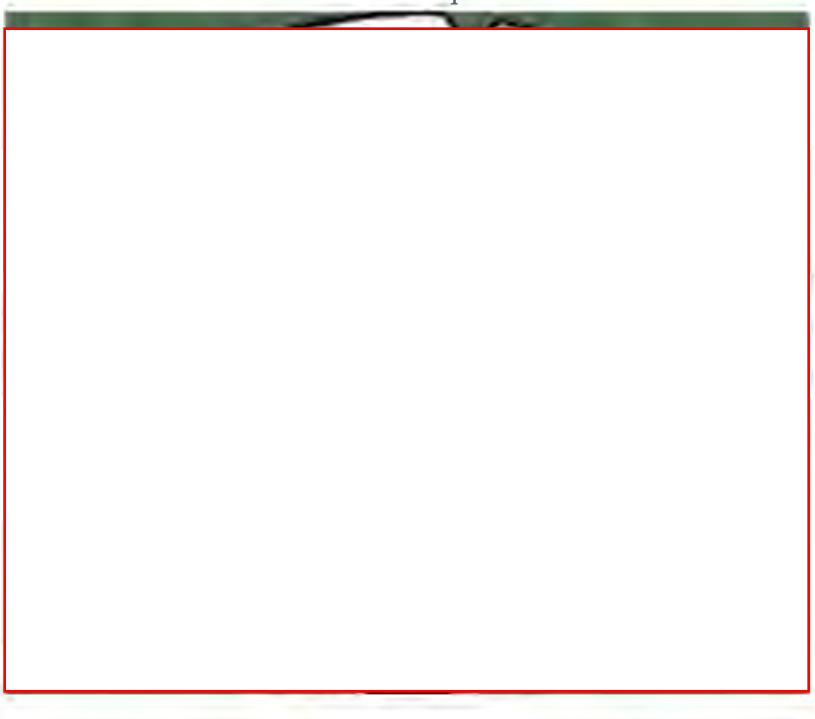
Doktora ve öncesi eğitim sürecimde sabır ve anlayışları ile bu yolculuğumda desteklerini hep hissettiğim annem Mihriye ALTUNEL, babam Osman ALTUNEL, kardeşlerim Hatice, Elif ve Merve ALTUNEL'e teşekkürlerimi sunuyorum.

05.06.2023

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tezin bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmanın Anadolu Üniversitesi tarafından kullanılan "bilimsel intihal tespit programı"yla tarandığını ve hiçbir şekilde "intihal içermediğini" beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçları kabul ettiğimi bildiririm.

Mehtap ALTUNEL



İÇİNDEKİLER

TABLOLAR DİZİNİ

Sayfa

ŞEKİLLER DİZİNİ

Sayfa

KISALTMALAR DİZİNİ

AICPA :Association of International Certified Professional Accountants
BDDK :Bankacılık Düzenleme ve Denetleme Kurumu
BGYS :Bilgi güvenliği yönetim sistemi
BT :Bilgi Teknolojisi
CBOK :Global Internal Audit Common Body of Knowledge
CCTA :Central Computer and Telecommunications Agency
CIO :Chief Information Officer
CIS CSC :The Center for Internet Security, Critical Security Controls
CISA :Certified Information Systems Auditor
CISO :Chief Information Security Officer
COBIT :Control Objectives for Information and Related Technology
COSO :Committee of Sponsoring Organizations
CPA :Certified Public Accountant
CPS :Cyber Physical Systems
CSF :Cyber Security Framework
CSO :Chief Security Officer
CTO :Chief Technology Officer
DDO :Dijital Dönüşüm Ofisi
EGIT :Enterprise Governance Of Information And Technology
ERM :Enterprise Risk Management
GSM :Global System for Mobile Communications
IIA :Institute of Internal Auditors
IoT :Internet of Things
ISA :International Society of Automation
ISACA :Information Systems Audit and Control Association
ISO :International Organization for Standardization
ITGI :Information Technology Governance Institute
ITIL :Information Technology Infrastructure Library
IQR :Interquartile range
İDDK :İç Denetim Koordinasyon Kurulu
KRY :Kurumsal Risk Yönetimi
MES :Manufacturing Execution System(Üretim Yürütme Sistemi)

MT Connect	:Manufacturing Teknology Connect
NIST	:National Institute of Standards and Technology
NIST CSF	:NIST Cyber Security Framework
RFID	:Radyo Frekans Tanımlama
RPA	:Robotic Process Automation
SCM	:Supply Chain Management
SLA	:Service Level Agreements
SOC	:System and Organization Controls/ Service Organization Control
SPK	:Sermaye Piyasası Kurulu
TİDE	:Türkiye İç Denetim Enstitüsü
TSE	:Türk Standartları Enstitüsü
UMUÇ	:Uluslararası Mesleki Uygulama Çerçevesi

GİRİŞ

Dördüncü sanayi devrimi ile yaşanan dijital dönüşüm etkisinin gün geçtikte devam edeceği göz önünde bulundurulduğunda kurumların[1] iş ortamındaki değişikliğin süreceğinin göstergesidir. Dijital teknolojiler bireylerin davranışlarından kurumların iş yapış şekillerine kadar birçok konuda değişikliği zorunlu hale getirmiştir (Verhoefa vd., 2021, s. 890). İş ortamında yaşanan dijitalleşme kurumlara rekabet avantajı, etkinlik ve verimlilik yönünde avantajlar sunmasına rağmen birtakım riskleri de beraberinde getirmektedir. Literatürde iç denetimin farklı düzeylerde risk yönetimine daha aktif destek sağlayarak değer katmaya ve kurumun stratejik hedefleriyle uyumlu hareket ederek iç denetimin stratejik risklere odaklanmasının önemi vurgulanmaktadır (Allegrini and D'Onza, 2003, s. 199). Diğer taraftan Endüstri 4.0 teknolojileri iç denetim fonksiyonunun yürüttüğü faaliyetlerde değişiklik gerektirirken dijitalleşmenin hızla büyümesi ve iç denetim fonksiyonunun rolü hakkında soruları gündeme getirmektedir (Betti, Sarens and Poncin, 2021, s. 873). Dijital dönüşümün iç denetimde üç alanda etkilendiğine ulaşılmıştır. Birincisi denetimin kapsamını genişlettiği, ikincisi iç denetimin rolü çerçevesinde danışmanlığa olan ihtiyacın artışı ve üçüncü olarak iç denetimin çalışma uygulamaları kapsamında ihtiyaç duyulan denetçi yetkinliğinde ve teknoloji kullanımında artış şeklindedir (Betti and Sarens, 2021). Bu alanla ilgili literatüre katkı sağlamak amacıyla dijital dönüşüm sürecinin yarattığı riskler karşısında iç denetim fonksiyonunun ne yönde katkı sağladığı iç denetçinin kendisinin süreci doğru yönetmek adına hangi özelliklere sahip olması gerektiği ve yasal düzenlemeler konularında görüşmeler yapılarak öneriler sunulmuştur.

Bu çalışma üç bölümden oluşmaktadır. Birinci bölümde sanayi devrimlerinin gelişmeleri, dördüncü sanayi devrimi teknolojileri, dördüncü sanayi devrimiyle yaşanan teknolojik gelişmenin yarattığı riskler ve dördüncü sanayi devrimi ile yaşanan dönüşümün kurum fonksiyonlarına yansımaları ele alınmıştır. Dijital dönüşümün kurum fonksiyonuna yansımaları kapsamında üretim, pazarlama, muhasebe fonksiyonlarına yansımaları kısa şekilde ele alınmış olup, çalışmanın konusu itibariyle iç denetim fonksiyonuna yansımaları üzerinde ağırlıklı açıklama yapılmıştır.

---

[1]Çalışma boyunca "kurumlar" ifadesi hem özel hem kamu kurumlarını kapsayacak şekilde kullanılmıştır.

İkinci bölüm kapsamında dördüncü sanayi devriminin denetim sürecine yansımalarını ortaya koymak adına Denetim 1.0'dan Denetim 4.0'a kadar gelişmeler ele alınarak, bu sürecin iç denetime yansımaları ortaya konulmaya çalışılmıştır. Ayrıca diğer önemli konu olan iç denetçinin dijital dönüşüm sürecinde sahip olması gereken yetkinlik ele alınarak IIA (2021) tarafından sunulan raporda ikinci sırada risk olarak sunulan yetenek yönetimi riski ile ilişkilendirilmiştir. Diğer taraftan dördüncü sanayi teknolojilerden olan yapay zeka, nesnelerin interneti, büyük veri ve veri analizinin iç denetim uygulamalarına yansımalarına ilişkin bilgiler yer almaktadır. Dijital dönüşümün yarattığı riskleri doğru yönetmek adına uluslararası ve ulusal çerçevede yapılan düzenlemeler iki başlık halinde ele alınmıştır. Uluslararası çerçevede ISO 27000, COSO, COBIT, ITIL, NIST, AICPA kapsamında açıklamalar sunulurken; ulusal çerçevede BDDK, SPK ve T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından düzenlemelere yer verilmiştir. Son olarak bu bölümde, yine IIA (2021) raporunda kurumların başlıca karşılaştığı risk olarak sıralanan siber güvenlik riski çerçevesinde iç denetim fonksiyonunun kurumlara sağlayacağı katkıyı ortaya koymak adına üçlü hat modeli kapsamında bilgiler sunulmuştur.

Üçüncü bölüm kapsamında çalışmanın uygulama kısmına yer verilmiştir. Bu çerçevede dijital dönüşümün yarattığı riskler ve bu risklerin yönetiminde iç denetim fonksiyonuna ilişkin Türkiye'de farkındalığın ortaya konulmasına yönelik Delphi tekniği ve araştırmaya ilişkin detaylar sunulmuştur. Bu bölümde önceki bölümlerden yola çıkılarak hazırlanan görüşme soruları çerçevesinde uzman kişilerle yapılan görüşmeler sonucu dijital dönüşüm algıları, dijital dönüşümden kaynaklı başlıca gördükleri riskler, dijital dönüşüm karşısında iç denetimin rolü, dijital dönüşüm sürecinde etkin olmak adına iç denetçinin sahip olması gereken yetkinlik ve yasal düzenlemelere ilişkin algılar saptanarak, değerlendirmeler yapılmıştır. Bu doğrultuda bu bölümde araştırma problemi, uluslararası ve ulusal literatürde yapılan araştırmalar, araştırmanın amacı, araştırmanın önemi, sayıltılar, sınırlılıklar, yöntem (araştırma deseni, Delphi tekniği, evren ve örneklem, veri toplama araçları ve analizi), bulgular ve yorumlar, sonuç ve öneriler başlıklarına yer verilmiştir.

BİRİNCİ BÖLÜM

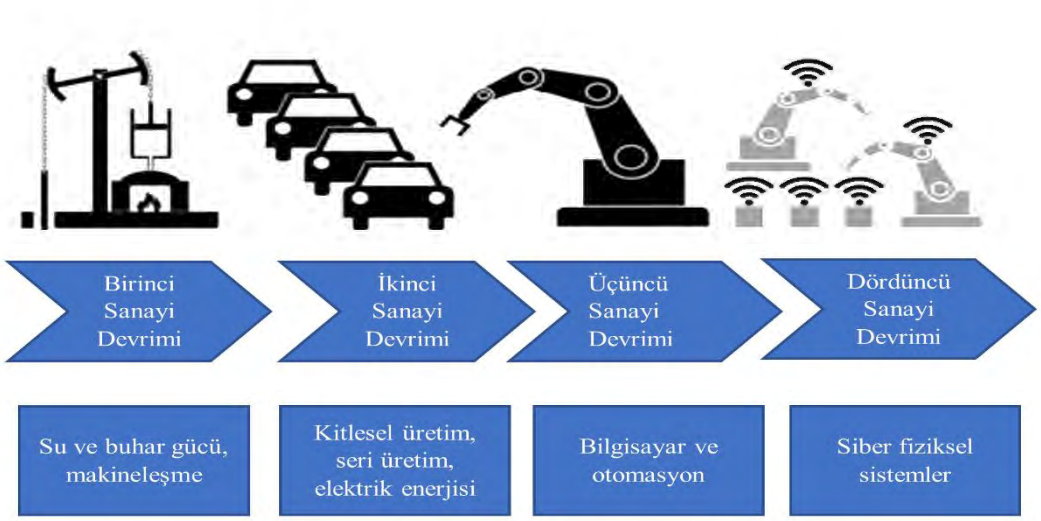
Endüstri 4.0 kurumlara rekabet üstünlüğü, maliyet azaltma, verimlilik artışı vb. konularda faydalar sunmanın yanında kullanılan teknolojiden kaynaklı yaşanacak riskleri de barındırdığı göz ardı edilmemelidir. Tezin bu bölümünde, bahsi geçen etkilere geçmeden evvel, birinci, ikinci ve üçüncü sanayi devrimlerinden kısaca bahsedilmiştir. Ardından Dördüncü Sanayi Devrimi olarak da ifade edilen Endüstri 4.0 kavramı, dördüncü sanayi devriminin ne zaman ve nasıl ortaya çıktığı, Endüstri 4.0'ın dinamikleri olan teknolojileri ve kurumlara etkileri ele alınmıştır.

1.TARİHSEL SÜREÇTE SANAYİ DEVRİMLERİ

Bu kısımda dördüncü sanayi devrimine kadar olan sanayi devrimleri kapsamında açıklamalara yer verilmiştir.

1.1. Birinci Sanayi Devrimi (Endüstri 1.0)

Sanayi devrimleri yeni teknolojilerin geliştirildiği ve tanıtıldığı basit dönemlerden daha fazlasıdır. Sanayi devrimleri geniş toplumsal dönüşümle eş zamanlı olarak belirli bir dizi özelliğe sahip teknolojik değişim zamanları olarak ifade edilebilir (Philbeck and Davis, 2018, s. 19). Dünyanın dört sanayi devrimiyle birlikte evrildiği genel kabul görmektedir. Bu devrimler arasındaki geçişler, Şekil 1.1'de görüldüğü üzere her devrimde yer alan teknoloji üstüne yeni teknolojilerin gelişmesiyle gerçekleşmiştir.



Şekil 1. 1. *Sanayi devrimleri (Stancioiu, 2017, s. 74)*

Birinci Sanayi Devrimi (Endüstri 1.0) küreselleşme sürecinin dört ana aşamasından ilkini oluşturmaktadır. Bu ilk aşamanın başlangıç noktası konusunda çeşitli fikir ayrılıkları olmakla birlikte birçok araştırmacı Birinci Sanayi Devrimi'nin 1760-1840 yılları arasında etkisinin görüldüğü konusunda ortak kanıya sahiptirler. Sanayi devrimlerinin başlangıç noktası olan Birinci Sanayi Devrimi, demiryollarının inşası ve buhar makinesinin devreye girmesiyle üretime öncülük etmiş ve devrimlerin başlangıç noktası olarak kabul edilmiştir (Schwab, 2016, s. 16). Birinci Sanayi Devrimi döneminde insan gücünden makine gücüne doğru bir evrim yaşanmıştır. Ayrıca makineler nitelik ve nicelik olarak artış göstermekle birlikte buhar gücüyle işlev kazanmışlardır. Bu dönemde odun ve bio-yakıt yerine kömür kullanımının başlanması makinelerin yaygınlaşmasındaki diğer bir etkendir (EBSO, 2015, s. 4). Birinci sanayi devrimin ilk olarak İngiltere'de başlamasının temelinde ülkede tekstilin en önemli sektör olması ve sahip olduğu demir ve kömür rezervlerinin yanında; sermaye ve enerji maliyetlerinin daha ucuz, ücretlerin ise yüksek olmasıdır (Braudel, 1991, s. 202-203; Kabaklarlı, 2016, s. 34).

1.2. İkinci Sanayi Devrimi (Endüstri 2.0)

Birinci Sanayi Devrimi'nin ardından 1840'lı yıllardan itibaren teknolojinin gelişimindeki artış ile birlikte İkinci Sanayi Devrimi'nin (Endüstri 2.0) temellerinin atılması sağlanmıştır. İkinci sanayi devrimi 1840-1870 dönemini kapsar ve teknoloji devrimi olarak adlandırılır (EBSO, 2015, s. 5). İkinci sanayi devriminde yaşanan gelişmelerden örnekler aşağıda sıralanmıştır:

- Elektrik teknolojisi geliştirilerek üretim hatlarında kullanılmaya başlanmıştır. Buhar gücüne kıyasla daha kuvvetli olması sebebiyle daha gelişmiş makinelerin ortaya çıkmasına ve yüksek miktarda üretim yapılarak dünyada seri üretim kavramının tanınmasına ön ayak olmuştur. En bilindik örneği Henry Ford'un Ford Motor Şirketi'dir (EBSO, 2015, s. 5).
- Kimya sektöründe yaşanan gelişmeler tıp alanında olumlu yönde (difteri ve tüberküloza karşı geliştirilen ilaçlar) gelişmelerin yaşanmasını sağlamıştır. Ayrıca suni gübre, yapay boya, patlayıcı ürünler üretilmiştir (Fülberth, 2011, s. 175).
- İkinci Sanayi Devrimi'nde diğer önemli bir gelişme ise çelik üretiminin yaygınlaşmasıdır (Mokyr and Strotz, 1998, s. 3).

- Birinci sanayi devriminde buhar makinesinin gelişmesi ulaşım alanına uygulanması büyük bir gelişme sağlamamakla birlikte dizel motor ve elektrikli lokomotiflerin kullanımı demiryollarının gelişimini olumlu yönde etkilemiştir. Bunun yanında gemilerde gelişim yaşanmıştır. Gemilerin çelik ile yapımına başlanmasıyla daha büyük gemiler inşa edilmiştir (Mokyr and Strotz, 1998, s. 7).
- Yukarıda sıralanan örneklerin yanı sıra ikinci sanayi devriminde sosyal yapılar, ev/meskene ait teknolojiler, tarım, yiyecek üretimi, petrol üretimi, kağıt gibi çeşitli alanlarda gelişmeler yaşanmıştır (Mohajan, 2020)

İkinci sanayi devrimi, birçok yönden birincisinin devamı niteliğinde olmasına rağmen yine de birçok önemli açıdan ondan farklıdır. İkinci sanayi devriminin birinci sanayi devriminden temel farklılığı teknolojik liderliğin coğrafi odağının İngiltere'den daha dağınık bir yere, ABD, Japonya'ya kayması olarak görülmektedir (Mokyr and Strotz, 1998, s. 14; H. Y. Taş, 2018, s. 1821). İkinci sanayi devriminin önemli gelişmesi olan seri üretim, sayısal artışın yanında kalite ve verimliği de etkilemiştir. Bu gelişmeler pazarlama stratejilerini de olumlu yönde etkilemiştir (Eğilmez, 2019, s. 133).

1.3 Üçüncü Sanayi Devrimi

Üçüncü Sanayi Devrimi'nin ilk yarısında iki büyük dünya savaşının gerçekleşmesinden kaynaklı önceki devrimler ile karşılaştırıldığında sanayi ve teknolojik ilerlemede yavaşlamanın meydana geldiğine ulaşılmıştır. Savaşların yanı sıra bu dönemi etkileyen diğer bir konu ise 1929 yılında gerçekleşen küresel ekonomik krizdir (EBSO, 2015, s. 6).

Üçüncü Sanayi Devrimi, 1960'larda yarı iletkenlerin ve ana bilgisayarların, 1970-1980 arasındaki dönemde kişisel bilgisayarların ve 1990'larda internetin katalizörlüğünde geliştiği "bilgisayar devrimi" veya "dijital devrim" olarak ifade edilmektedir (Schwab, 2016, s. 16). Üçüncü Sanayi Devrimi'nde bilgisayar ve internet kapsamındaki gelişmeler yanında güneş ve rüzgar gibi yenilenebilir enerji kaynakları, enerji depolama teknolojileri, internet ve üç boyutlu baskı gibi dijital üretim teknolojileri gelişimine devam etmiştir (Heinonen, Karjalainen and Ruotsalainen, 2015, s. 10). 1970'li yıllar itibariyle elektronik, bilgi ve iletişim teknolojilerinin gelişmesi sonucu üretimde otomasyonun yer alması, Üçüncü Sanayi Devrimi'nde en önemli özelliklerinden birisi

olan üretimde otomasyonun artışıyla insan gücüne olan ihtiyacın azalması sağlanmıştır (MÜSİAD, 2017, s. 34; Çetinkaya, 2020, s. 29).

Üçüncü sanayi devriminde bilgisayar kullanımı, akıllı telefon ve internetin kullanımının yaygın hale gelmesi üretimi etkilemenin yanında e-ticaret kavramının ortaya çıkışında ön ayak olarak ticaret ve endüstrinin küreselleşmesini sağlamıştır. Üçüncü Sanayi Devrimi'nde kişiye özel üretim anlayışın, seri üretim anlayışının yerini almaya başlamıştır. Ayrıca Üçüncü Sanayi Devrimi'nde bilgisayar ve iletişim teknolojilerinin daha kullanışlı şekilde günlük yaşantımıza girmesini sağlayarak iş hayatında olduğu gibi insanların günlük yaşantısında da insan gücüne olan ihtiyacın azalmasını neden olmuştur (Çetinkaya, 2020, s. 33; EBSO, 2015, s. 6; Eğilmez, 2019, s. 143).

2. DÖRDÜNCÜ SANAYİ DEVRİMİ (ENDÜSTRİ 4.0) ve DİJİTAL DÖNÜŞÜM SÜRECİ

Dördüncü Sanayi Devrimi (Endüstri 4.0) öncesinde yaşanan sanayi devrimleriyle birlikte gerek üretim şekilleri ve miktarlarında gerekse teknolojideki ilerlemeden kaynaklı yaşam biçimlerinde büyük oranda değişim yaşanmıştır. Her sanayi devrimindeki gelişmeler göz önünde bulundurulduğunda üretim yapısı, çıktıları konusunda farklılıklar yaşandığı, ekonomik ve sosyal anlamda değişmelerin gerçekleştiği görülmektedir. Dolayısıyla çalışmanın amacını yönelik Endüstri 4.0'ın ortaya çıkışı ve geldiği nokta büyük önem taşımaktadır. Bu kısımda bölümde Dördüncü Sanayi Devrimi yarattığı yıkıcı değişimlere her geçen gün yeni bir gelişmeyi eklediğini ortaya koymak, Endüstri 4.0 ve beraberinde gelen dijital dönüşüm kavramı, Endüstri 4.0'ın yaşanmasında etkili olan teknolojiler, Endüstri 4.0 kapsamında yaşanan riskler, dijital dönüşüm sürecinin işletme fonksiyonlarına yansıması kapsamında açıklamalara yer verilmiştir.

2.1.Dördüncü Sanayi Devrimi (Endüstri 4.0)

20 yy. sonu itibariyle bilişim teknolojisindeki ilerleme, beraberinde internet teknolojisinin ortaya çıkışı ve yaygınlaşması ardından bilişim teknolojisindeki kullanımın yaygınlaşmasını getirmiştir (A. Şahin, 2017). Endüstri 4.0'da gelinen noktaya bakıldığında imalat ve hizmet sistemlerinde birçok yeni gelişmenin yaşanmasını sağlamıştır. Üretimde ve teknolojideki hızlı ve dikkat çekici değişimler teknoloji, üretim, hizmet alanlarında bütünleşik gelişimden kaynaklanan yeni bir ortak gücün oluşmasını sağlamıştır. Dolayısıyla bu ortak güç sayesinde hem üretim hem de hizmet alanlarında

artan şekilde üretkenliğin önü açılmıştır (Salkin vd., 2018, s. 3). Tüm bu gelişmeler ilk kez 2011 yılında Alman hükümeti tarafından Hannover Fuarında ***Endüstri 4.0*** terimi olarak ifade edilmiştir (Bartevyan, 2015, s. 2). Endüstri 4.0 kavramını birçok yazar tarafından Tablo 1.1'de görüldüğü üzere benzer ifadeler kullanılarak ifade edilmekle birlikte kavrama ilişkin net bir tanımlama bulunmamaktadır.

Tablo 1. 1.*Endüstri 4.0 kavramı (Yazar tarafından oluşturulmuştur.)*

YAZAR	TANIM
Kagermann, Wahlster and Helbig (2013, s.19)	Üretim ortamında, dikey ağ oluşturma, uçtan uca mühendislik ve giderek daha akıllı hale gelen ürün ve sistemlerin tüm değer ağı boyunca yatay entegrasyon, sanayileşmenin dördüncü aşaması olan Endüstri 4.0'ın başlangıcı şeklinde ifade edilmiştir.
Qina, Liua and Grosvenor (2016, s.175)	Endüstri 4.0 üretimin bilgiyi keşfeden, kararlar alan ve eylemi bağımsız ve akıllı bir şekilde gerçekleştiren akıllı olmasını gerektirmektedir. Akıllı teknolojiler kullanılarak üretim ağlarından ham veriler toplanarak analiz edilir. Birlikte çalışabilirlik, Endüstri 4.0'ın güvenilir ortamı olarak birbirine bağlı birkaç ağ kurar. Bilinç, yapay zeka işlevleriyle Endüstri 4.0'ın özünü sunmaktadır.
Schwab (2016, s.24-37)	Bütün gelişmeler ve teknolojiler ortak bir özelliğe sahip dijitalleşme ve enformasyon teknolojileri ile her yere nüfus etme gücüdür. Schwab (2016) Endüstri 4.0' ın teknolojik itici güçlerini fiziksel, dijital ve biyolojik olmak üzere üç grupta toplamaktadır. Dördüncü sanayi devrim olarak ifade edilen teknolojiler ekonomiyi, iş yaşamını ülkeler, toplumlar ve bireyler üzerinde geniş etkiye sahip olduğu vurgulanmaktadır.
Mrugalska & Wyrwicka (2017, s.466)	Dördüncü sanayi devrimi akıllı bir fabrikaya sahip olmak için tüm değer zincirinde makineler, ürünler, bileşenler, özellikler, bireyler ve bilgi iletişim teknoloji sistemlerinden oluşan akıllı bir ağ oluşturmaya olanak tanıması şeklinde ifade edilmiştir.

Endüstrileşmenin dördüncü dönüşümü; Almanya' da "Platform Endüstri 4.0", ABD'de "Endüstriyel İnternet" (Nesnelerin Endüstriyel İnterneti), Japonya'da "Toplum 5.0", Çin'de "İnternet +", Güney Kore'de "Akıllı Fabrika" ve "Akıllı Şehir" şeklinde ifade edilmektedir. Endüstri 4.0'ı tanımlamak üzere çeşitli kavramlar öne sürülmektedir. "Sanayi 4.0", "Dijital Sanayi Çağı", "Akıllı Fabrika-Akıllı Üretim", "Makineden Makineye", "Endüstriyel İnternet" bu kavramların bir kısmıdır. Görüldüğü üzere,

dördüncü sanayi devriminin kavramsallaştırılmasında ve tanımlanmasında ortak bir ifade yoktur (Gür, Ünay ve Dilek, 2017, s. 69-73).

Schwab'a (2016, s. 11) göre üçüncü sanayi devriminden farklı olarak dördüncü sanayi devriminin gelişimine ilişkin temel üç göstergenin olduğu vurgulanmaktadır. Bu üç temel gösterge hız, genişlik ve derinlik, sistem etkisi şeklinde sınıflandırılmıştır.

- Hız, dördüncü sanayi devriminin önceki sanayi devrimlerinden farklı olarak doğrusal değil üstel bir hızla geliştiğine ilişkindir. Bu durum içinde bulunulan durumun bağlantılı, çok yönlü dünyanın ve teknolojinin sürekli yeni teknolojilerinin önünü açmasından kaynaklıdır.
- Genişlik ve derinlik, dördüncü sanayi devrimi dijital devrim üzerinde yükselerek ekonomide, iş dünyasında, toplumlarda, bireylerde değişime neden olacak çok çeşitli teknolojileri barındırmaktadır. Bu dönüşüm ile birlikte sadece "ne" ve "nasıl" sorularını değil aynı zamanda "biz kimiz" sorusunu değiştirmiştir.
- Sistem etkisi, bu teknolojik devrimin şirketlerin, ülkelerin, sektörlerin bireylerin, toplumdaki sistemin yani makro ve mikro oranda bir dönüşümü içermektedir.

Hermann, Pentek ve Otto (2016)'nun yürüttüğü çalışma incelendiğinde Endüstri 4.0'ın temel sorunlarından birinin uygulayıcıların Endüstri 4.0 tasarım ilkelerinin mevcut olmamasını vurgulamaktadır. Hermann, Pentek ve Otto (2016) tarafından Endüstri 4.0 tasarım ilkeleri olarak dört husus sıralanmaktadır. Bunlar: Birbirine Bağlı Olma, Bilgi Şeffaflığı, Merkezi Olmayan Kararlar ve Teknik Destek şeklindedir. Diğer taraftan Hermann, Pentek ve Otto (2016) tarafından yapılan çalışmayı destekleyici diğer bir çalışmada akıllı fabrikaların Endüstri 4.0'ın amacına hizmet edecek şekilde aşağıda sıralanan özellikleri taşıması gerektiği vurgulanmıştır (Jazdi, 2014, s. 1-2).

- Akıllı Ağ Oluşturma: Otomatik sistemler ve ekipmanlar, dahili lojistik sistemler ve işletim malzemeleri, kablosuz ve kablolu iletişim hizmetleri, akıllı aktüatörler ve sensörler ve telekomünikasyon teknolojileri gibi siber teknolojinin yardımıyla sürekli olarak birbirine bağlanır. Bu, onlara üst düzey süreçlere ve hizmetlere doğrudan erişim sağlar. Bu durum optimum

kaynak kullanımını ve akıllı kontrolü destekleyen katma değer ve iş modellerine sahip tamamen yeni inovasyonlara yol açmaktadır.

- Hareketlilik: Akıllı telefonlar ve tabletler gibi mobil cihazlar, endüstriyel otomasyonda ilerleme kaydetmiştir. Otomatikleştirilmiş sistemlerin süreçlerine ve hizmetlerine zamansal ve mekânsal olarak bağımsız erişim sağlarlar. Bu durum sistemlerin teşhisinde, bakımında ve çalıştırılmasında yeni bir boyut yaratmaktadır.
- Esneklik: Endüstri 4.0, hem geliştirme, tanılama ve bakım hem de otomatikleştirilmiş sistemlerin çalıştırılmasında yüksek esneklik sağlar. Bu sistemlerin geliştirilmesinde, geniş bir bileşen, modül ve hizmet tedarikçisi havuzundan en iyi teklifi seçilmesine yardımcı olur. Teşhis kısmen kullanıcı tarafından yapılabilir. Burada büyük veriye erişim, otomasyona yardımcı olur. Bilgiler talep üzerine alınabilir, akıllıca kullanılabilir ve bağlanabilir böylece otomatik bir teşhis elde edilebilir. Yedek parçalar, en ucuz üreticilerden otomatik olarak sipariş edilebilir böylece beceri eksikliği sorununu ortadan kaldırmaktadır.
- Müşterilerin Entegrasyonu: Endüstri 4.0 ile ürünlerin müşterilerin özel ve bireysel ihtiyaçlarına göre özelleştirilmesi mümkün olacaktır. 21. yüzyılın otomatik sistemleri her yaş grubundaki kullanıcıların ihtiyaç ve yeteneklerine uyum sağlar. Örneğin modern bir bilet satış makinesi, farklı engelli insanlar tarafından kullanılmasına izin vermek için çeşitli işletim seçenekleri sağlar. Otomatik sistemler, insanları her durumda destekleyecek ve onlara yaşamın farklı aşamalarında yardımcı olacaktır. Böylece sürdürülebilir, sağlıklı ve mobil kalmalarını sağlayacaktır.
- Yenilikçi İş Modelleri: Gelecekteki üretim dağıtılacak ve esnek olacaktır. Yeni geliştirme süreçleri, altyapı ve hizmetler ortaya çıkacaktır. Ürünler modüler ve yapılandırılabilir hale gelecek böylece ürün özel gereksinimlere uyarlanabilecektir.

2.2. Dördüncü Sanayi Devrimi Teknolojileri

Dördüncü sanayi devrimi teknolojileri geniş bir yelpaze oluşturmakla birlikte literatürde yoğun şekilde bahsedilen teknolojilere aşağıda sırasıyla yer verilmiştir.

2.2.1. Büyük Veri Analitiği

İngilizce bir kavram olan "Big Data" kavramı Türkçede yer edinmekle birlikte "Büyük Veri" şeklinde ifade edilmektedir. Literatür incelendiğinde büyük veri kapsamında net bir tanım bulunmamakla birlikte üç ana özelliğini (çeşitlilik, hız, miktar) vurgulayan tanımlanmanın büyük oranda yer aldığına ulaşılmıştır. Bu kapsamda, ABD'li bilgi teknolojisi araştırma uzmanı ve danışmanı olan Gartner tarafından büyük veri, gelişmiş bakış açısı ve karar alma için uygun maliyetli, yenilikçi bilgi işleme biçimleri talep eden yüksek hacimli, hızlı ve çeşitli bilgi varlıkları şeklinde ifade edilmiştir (Gartner, 2013).

Büyük veride iki temel olgu mevcuttur. Bunlardan ilki ilgilenilen alanlarda büyük miktardaki verilerin toplanıp depolanmasıdır. İkincisi ise bu büyük veri yığının analizidir. Büyük veri, internet sunucularındaki kayıtlardan, sosyal medya içeriklerinden, bloglardan, internet istatistiklerinden, GSM operatörlerinden gelen arama kayıtlarından şeklinde sıralanan birçok mecradan elde edilen büyük hacimli verilerden oluşmaktadır. Dolayısıyla doğru analiz yöntemleriyle yorumlandığı takdirde kurumların stratejik kararlarını doğru biçimde almaları, riskleri etkin şekilde yönetmeleri, işlerde ve ürünlerde inovasyon yapılması konusunda faydası söz konusudur (Banger, 2018, s. 48-49).

Büyük veriyi tanımlarken üç özellik ayırt edici olmakla birlikte ek olarak iki kavram eklenerek Büyük Verinin 5V'si şeklinde büyük verinin özellikleri ifade edilmektedir. 5V kavramı, Şekil 1.2'de gösterildiği üzere Velocity (Hız), Variety (Çeşitlilik), Volume (Miktar), Value (Değer), Veracity (Gerçeklik-Doğruluk) ifadelerinin İngilizce karşılıklarının baş harfleri sonucu oluşturulmuştur (Hadı vd., 2015, s. 20).

Şekil 1. 2.*Büyük verinin özellikleri (Hadı vd., 2015, s.20'den uyarlanmıştır.)*

Büyük verinin beş bileşenine ilişkin açıklamalar aşağıda kısaca ifade edilmiştir:

- **Hacim:** Milyonca cihaz ve uygulamadan sürekli olarak büyük veri üretilmesini ifade etmektedir. Büyük veri sistemine giriş verileri sosyal ağlardan, web sunucusu kayıtlarından, trafik akış sensörlerinden, uydu görüntülerinden, yayın ses akışlarından, bankacılık işlemlerinden, web sayfalarının içeriğinden, finansal piyasa verileri vb. şeklinde sıralanan birçok alandan gelmektedir. Bu durumun başlıca sebebi olarak Endüstri 4.0 ile birlikte dijital teknolojilerin gelişmesi, ölçme ve kaydetme imkanlarının artışıdır (Khan, Uddin and Gupta, 2014, s. 2; Oussous vd., 2018, s. 433; Altunışık, 2015, s. 52).
- **Hız:** Verinin sürekli hareket halinde olmasını ifade eder. Veri üretim hızı çok yüksektir. Bu noktada özellikle verinin işlenmesi, analiz edilmesi verinin hızıyla aynı olması gerekmektedir (Cyganek vd., 2016, s. 499; Gerhardt, Griffin and Klemann, 2012, s. 3).
- **Çeşitlilik:** Çeşitlilik büyük verinin içereceği veri türünü ifade etmektedir. Büyük veriler her zaman yapılandırılmış verilerden oluşmazlar. Büyük veri, metin, sensör verileri, ses, video, tıklama akışları, günlük dosyaları vb. yapılandırılmış ve yapılandırılmamış verileri kapsayan her türlü veriden oluşmaktadır (Hadı vd., 2015, s. 21). Dolayısıyla bu durum verinin çeşitliliğini artırmaktadır.

- **Değer:** Toplanan verilerin amaçlanan sürece, aktiviteye veya tahmine dayalı analizin getirebileceği katma değeri ifade etmektedir. Büyük veriye erişimde her şey uygun şekilde yürütülüyorsa onun potansiyel değerinin çok fazla olduğu fakat aksi durumda fayda sağlamayacağı unutulmamalıdır (Kalbandi and Anuradha, 2015, s. 321).
- **Gerçeklik-Doğruluk:** Verinin hız, hacim ve çeşitliliğinden kaynaklı tüm verilerin %100 doğru olması mümkün değildir. Verinin hız, hacim ve çeşitliliğinden kaynaklı veriye güven sorununu ortaya çıkarmaktadır. Dolayısıyla verinin üç özelliği sebebiyle kirli verilerin olması söz konusudur (Kalbandi and Anuradha, 2015, s. 321). Yöneticilerin kararlarını etkileyen bir faktör olması itibariyle bilgiye güvenmesi önemlidir (Hadı vd., 2015, s. 21).

Büyük verinin yukarıdaki özelliklerine Khan, Uddin ve Gupta (2014) tarafından Volatility (Oynaklık) ve Validity (Geçerlik) olmak üzere 7V, Firican (2017) tarafından Vulnerability (Hassaslık), Variability (Değişkenlik) ve Visualization (Görselleştirme) ilave edilerek 10V kavramlarını da kapsayacak şekilde genişletilmiştir.

2.2.2. Nesnelerin İnterneti

İnternet hem insanların profesyonel hayatlarında hem de özel hayatlarında iletişim ve iş yapış şekillerini büyük oranda etkilemektedir. Nesnelerin interneti ise nesneler arası iletişimi sağlayarak bu duruma yeni bir boyut kazandırmış ve her zaman, her yerde, her medya da ve her nesne arasında iletişimin sağlanmasına yol açmıştır (Atzori, Iera and Morabito, 2010, s. 2803). Diğer taraftan dijital bir kurumun kurulmasındaki temel ihtiyaçlardan bir tanesi sistemin parçası olan bütün cihazların ve insanların kullanacağı ortak bir dilin oluşturulmasıdır (Lee vd., 2018, s. 1001). Ortak dil, bilgisayar bilimi, bilişim ve iletişim teknolojileri ile üretim bilimi ve teknolojileri üzerine kurulu siber fiziksel sistemleri mümkün kılan en temel öge olan nesnelerin internetidir (Lee, Zhang and Ng, 2017, s. 336).

Nesnelerin interneti, veri yakalama ve iletişim yeteneklerinden yararlanarak fiziksel ve sanal nesneleri birbirine bağlayan küresel bir ağ altyapısıdır. Nesnelerin interneti için temel bir teknolojilerden biri olan mikroçiplerin kimlik bilgilerini kablosuz iletişim yoluyla bir okuyucuya iletmesine olanak tanıyan Radyo Frekans Tanımlama

(RFID) teknolojisidir. RFID okuyucuları kullanarak, insanlar RFID etiketleriyle bağlanan her nesneyi otomatik olarak tanımlar, takip eder ve izlemektedir (Jia vd., 2012, s. 1282). Nesnelerin interneti için bir başka temel teknoloji, algılama ve izleme için esas olarak birbirine bağlı akıllı sensörleri kullanan kablosuz sensör ağlarıdır. Bu teknoloji kapsamındaki uygulama alanları çevresel izleme, sağlık bakımı izleme, endüstriyel izleme, trafik izleme vb. şeklinde sıralanabilir. Başarılı bir nesnelerin interneti tabanlı ürün ve hizmetlerin dağıtımı için bahsedilen yaygın iki teknoloji, nesnelerin internetinin gelişimine önemli ölçüde katkıda bulunmaktadır. Ek olarak, Şekil 1.3'te sıralandığı üzere barkodlar, akıllı telefonlar, sosyal ağlar ve bulut bilişim gibi diğer birçok teknoloji ve cihaz nesnelerin internetini desteklemek için kapsamlı bir ağ oluşturmak için kullanılmaktadır (Xu, He and Li, 2014, s. 2233-2234).

Şekil 1. 3.*Nesnelerin interneti ile ilişkili teknolojiler (Xu vd., 2014, s.2234)*

Nesnelerin interneti kavramını Haller, Karnouskos ve Schroth (2008, s. 15) tarafından nesnelerin interneti fiziksel nesneler ile bilgi ağının birbirine entegre edildiği ve aktif katılımcı olarak fiziksel nesnelerin iş süreçlerinde yer aldığı bir dünya olarak nitelendirilmektedir. Nesnelerin internetinde güvenlik ve mahremiyet konuları göz ardı edilmeden internet üzerinden akıllı nesneler ile etkileşim kurulduğu hizmetleri kapsamaktadır. Hizmetlerin interneti, kurum, müşteriler, aracılar, toplayıcılar ve

tedarikçiler gibi iç ve dış her paydaş arasındaki hizmet sağlama ve tüketim için iş ağlarının oluşturulduğu hizmetlerin interneti vizyonunu kolaylaştıran gelişmiş iş modellerini kapsayan teknolojilerdir (Cardoso, Voigt and Winkler, 2008, s. 15-16). Hizmetlerin interneti kavramını nesnelerin interneti kavramından ayıran durum, fiziksel nesneler yerine hizmetler ile internetin bağlantısının kurulduğu bir iş modeli olmasıdır (Pereira and Romero, 2017, s. 1211-1212).

Nesnelerin interneti vizyonuna yukarıda da ifade edildiği üzere farklı türdeki pek çok cihaz ağa bağlanmakta ve iletişim döngüsünü sürdürülebilir kılmaktadır. İletişim döngüsü içerisinde insanlar olabildiği gibi, cihazlar, makineler gibi nesneler de bulunabilmektedir (Lee vd., 2013, s. 258). Nesnelerin İnterneti kavramını karşılamak için üç farklı iletişim şekli kullanılabilmektedir. Bunlar şöyledir (Lee and Crespi, 2010, s. 403):

- **İnsandan- İnsana İletişim:** İnsanların bir nesne/cihaz aracılığıyla iletişimde olmasını ifade etmektedir.
- **İnsandan- Nesneye İletişim:** İnsanların cihazla özel bir bilgiyi (IPTV içeriği, dosya transferi gibi) elde etmek amacıyla iletişim kurmasını ifade etmektedir. Nesnelerin uzak erişimli olarak insanlar tarafından erişilebilmesini de kapsamaktadır.
- **Nesneden- Nesneye iletişim:** Nesnenin bilgiye (özellikle sensör tabanlı bilgiye) ulaşmasında diğer bir nesne ile veya insan dışı bir cihaz ile iletişim kurarak elde etmesidir.

Nesnelerin interneti uygulamaları ile ilgili olarak literatürde binalara akıllı cihazların yerleştirilmesi ile akıllı altyapıların sağlanması, hastaların sensörler ile izlenerek doktorlara bilgi aktarılması ve tedarik zincirlerinde güncel ve ayrıntılı bilginin sunulması, doğal afetlerin tahmini ile önceden önlem alınması, tarımsal uygulamalar ile arazinin uygunluğu hakkında bilgi verilmesi şeklinde birbirinden farklı örnek uygulamalar sıralanmaktadır. Lojistik, üretim, perakende, eczacılık gibi farklı birçok alanda kullanılabilecek olan nesnelerin internetinin başarısı, birlikte çalışabilirlik, uyumluluk, güvenilirlik ve küresel ölçekte etkili operasyonlar sağlayan standardizasyona bağlıdır (Xu, He and Li, 2014, s. 2234; Khan vd., 2012, s. 259). Tüm bu örneklerden görüldüğü üzere bu teknolojinin benimsenmesindeki temel etkenlerden biri olan rekabetçi

baskılar firmaları yenilik yapmaya ve kendilerini dönüştürmeye ittikçe hızla ivme kazanmaktadır. Nesnelerin interneti teknolojisi ilerledikçe ve artan sayıda firma teknolojiyi benimsedikçe, maliyet-fayda analizi büyük ilgi konusu haline gelecektir. Nesnelerin internetinin potansiyel ancak belirsiz faydaları ve yüksek yatırım maliyetleri nedeniyle, şirketlerin kaynaklarının makul bir şekilde harcanmasını sağlamak için nesnelerin internetinden kaynaklı her fırsat ve zorluğu değerlendirmesi önemlilik arz etmektedir (I. Lee and K. Lee, 2015, s. 432).

2.2.3. Siber Fiziksel Sistemler

Endüstri 4.0 kapsamında yaşanan gelişmelerin ortaya çıkışını hazırlayan bir teknoloji olan siber fiziksel sistemler (Cyber Physical Systems-CPS) terimi, doğal ve insan yapımı sistemlerin (fiziksel mekan) hesaplama, iletişim ve kontrol sistemleri (siber uzay) ile sıkı bir şekilde entegre edildiği sistemler şeklinde kısaca ifade edilmiştir (Bagheri vd., 2015, s. 1622). Gelişmekte olan bir teknoloji olarak CPS, mevcut birçok endüstriyel sistemin işleyişini ve rolünü dönüştürmek için umut verici çözümler sunması beklenmektedir (Lu, 2017, s. 6). Monostori vd. (2016, s. 621) siber fiziksel sistemleri, çevredeki fiziksel dünya ve devam eden süreçlerle yoğun bağlantı içinde olan, sağlayan ve kullanan aynı zamanda internette bulunan hizmetlerin veri erişimi ve veri işlemesi, ortak çalışan sayısal öğelerin sistemleri şeklinde ifade etmektedir.

Siber fiziksel sistemler çok sayıda uzamsal ve zamansal ölçekte yüksek derecede karmaşıklık, hesaplama ve fiziksel bileşenleri entegre eden yüksek düzeyde ağ bağlantılı iletişimi kapsamaktadır. CPS, yeni nesil akıllı sistemlere olanak tanımakta ve bundan kaynaklı son derece yüksek seviyede ekonomik etkileri olabilir. Siber ve fiziksel dünyaları birleştirerek ortaya çıkan yıkıcı teknolojinin sonucunda geniş bir endüstri yelpazesi için bir inovasyon lokomotifi ve büyüme için tamamen yeni pazarlar ve platformların oluşturulma imkanı vermektedir. Üretimde; akıllı üretim ekipmanı, süreçler, otomasyon, kontrol ve ağlar, yeni ürün tasarımı imkanlar sunarken ulaşımda; akıllı araçlar ve trafik kontrolü, akıllı yapılar ve kaldırımlar şeklinde örnekler gösterilebilir. (NIST, 2013, s. 1).

CPS, Endüstri 4.0'a zemin hazırlamak için hizmetlerin interneti ile birleşen nesnelerin internetinin oluşturulması için temel sağlamaktadır. Diğer taraftan siber fiziksel sistemlerin yapısını nesnelerin internetinin yapısından ayıran özellik, fiziksel ve

işlemsel bileşenleri daha yüksek oranda kombine etmesidir (Rad vd., 2015, s. 75). Siber fiziksel sistemler gerçek ve sanal dünya arasındaki sınırları kaldırarak birden çok yenilikçi uygulama ve süreci gerçeğe dönüştüren teknolojidir (GTAI, 2014, s. 8). Endüstri 4.0'ın özü akıllı fabrikaların geliştirmesi için CPS kullanılmaktadır. Dolayısıyla CPS akıllı fabrika üretim süreçlerinde önemli role sahiptir. Bu sayede geleneksel üretim sistemleriyle karşılaştırıldığında gerçek zamanlı kalite, maliyet ve kaynak avantajı sağlamaktadır (GTAI, 2014, s. 10). Ayrıca siber fiziksel sistemlerin uygulanması bileşenlerin öz farkındalık ve öngörü, makinelerin kıyaslama yapma ve fabrikanın kendini yapılandırma ve sürdürülebilir kılma özelliklerini kazanmasını sağlamaktadır (Lee, Bagheri and Kao, 2015, s. 19). Bunların yanında siber fiziksel sistemlerin siber güvenlik, ekonomiklik, birlikte çalışabilirlik, gizlilik, güvenlik ve güvenirlilik ve siber fiziksel sistemin sosyo-teknik yönleri konuları uygulama alanlarında ortak engeller olarak sıralanmaktadır (Monostori vd., 2016, s. 623).

Lee Bagheri ve Kao (2015, s. 19-20) tarafından CPS yapısı oluşturulurken beş kademeli bir model önerilmiştir. Önerilen beş kademeli CPS yapısı (5C mimarisi[2]) üretim uygulaması için bir CPS geliştirmek ve dağıtmak için adım adım bir kılavuz sağlamaktadır. Genel olarak, bir CPS iki ana işlevsel bileşenden oluşur:

- Fiziksel dünyadan gerçek zamanlı veri alımını ve siber alandan bilgi geri bildirimini sağlayan gelişmiş bağlantı; ve
- Siber alanı oluşturan akıllı veri yönetimi, analitik ve hesaplama yeteneği.

Ancak, bu tür bir gereklilik çok soyuttur ve genel olarak uygulama amacı için yeterince spesifik değildir. Buna karşılık, burada sunulan 5C mimarisi, sıralı bir iş akışı yöntemiyle ilk veri toplamadan analitiğe ve nihai değer yaratmaya kadar bir siber fiziksel sistemlerin nasıl oluşturulacağını açıkça tanımlamaktadır. Şekil 1.4'te gösterildiği gibi, ayrıntılı 5C mimarisi aşağıdaki kısaca özetlenmiştir:

1. Akıllı Bağlantı: Makinelerden ve bileşenlerinden doğru ve güvenilir verilerin elde edilmesi bir siber fiziksel sistem uygulaması geliştirmenin ilk adımıdır. Veriler doğrudan sensörler tarafından ölçülebilir veya denetleyici veya ERP, MES ve SCM gibi kurumsal üretim sistemlerinden elde

[2] *5C Mimarisi* denilmesinin sebebi "Akıllı Bağlantı", "Siber", "Veriden Bilgiye Dönüşüm", "Bilişim Uygulama", Yapılandırma Seviyesi" kademelerin başlıklarından kaynaklı adlandırma tercih edilmiştir.

edilebilir. Bu seviyedeki iki önemli faktör dikkate alınmalıdır. İlk olarak, çeşitli veri türlerini göz önünde bulundurarak, MT Connect [3](Manufacturing Teknology Connect) ve benzeri gibi belirli protokollerin etkili bir şekilde yararlı olduğu durumlarda, veri toplama prosedürünü yönetmek ve verileri merkezi sunucuya aktarmak için kesintisiz ve bağsız bir yöntem gereklidir. Öte yandan, uygun sensörlerin seçilmesi (tür ve özellik), birinci seviye için ikinci önemli husustur.

2. Veriden Bilgiye Dönüştürme: Verilerden anlamlı bilgiler çıkarılmalıdır. Şu anda, veriler için bilgi dönüştürme düzeyine yönelik çeşitli araçlar ve yöntemler mevcuttur. Son yıllarda, bu algoritmaları özellikle hasta belirtileri ve sağlık yönetimi uygulamaları için geliştirmeye yoğun bir şekilde odaklanılmıştır. Sağlık değerini, tahmini kalan faydalı ömrü vb. hesaplama yapılarak, CPS mimarisinin ikinci seviyesi makinelere öz farkındalık getirir.
3. Siber: Siber seviye, bu mimaride merkezi bilgi görevi görür. Makine ağını oluşturmak için her bağlı makineden ona bilgi aktarılıyor. Büyük miktarda bilgi toplandıktan sonra, filo içerisindeki ayrı makinelerin durumu hakkında daha iyi bakış sağlayan ek bilgileri çıkarmak için özel analizler kullanılmalıdır. Bu analizler, tek bir makinenin performansının filo ile karşılaştırılabilmesi ve derecelendirmesi ile makinelere kendi kendini karşılaştırma yeteneği sağlar. Ayrıca makinenin gelecekteki davranışını tahmin etmek için makine performansı ile önceki varlıklar (tarihsel bilgiler) arasındaki benzerlikler ölçülebilir.
4. Biliş Uygulama: Siber fiziksel sistemlerin bu seviyede uygulanması, izlenen sistem hakkında kapsamlı bir bilgi üretir. Edinilen bilgilerin uzman kullanıcılara doğru şekilde sunulması alınacak doğru kararı destekler. Karşılaştırmalı bilgilerin yanı sıra bireysel makine durumu da mevcut olduğundan, bakım sürecini optimize etmek için görevlerin önceliğine karar

[3]MTConnect, üretim alanında veri alışverişi için bir standarttır (B. Lee vd., 2010, s. 1184). "MTConnect" adı, üretim teknolojisi bağlantısı anlamına gelmektedir ve iletişim protokolü, çeşitli üretim kaynakları (atölyelerdeki makineler dahil) ve uygulamalar arasındaki veri iletimini güçlendirmek için tasarlanmıştır (Hu, ve diğerleri, 2018, s. 1194).

verilebilir. Bu seviye için edinilen bilgileri kullanıcılara tamamen aktarmak için uygun bilgi grafikleri gereklidir.

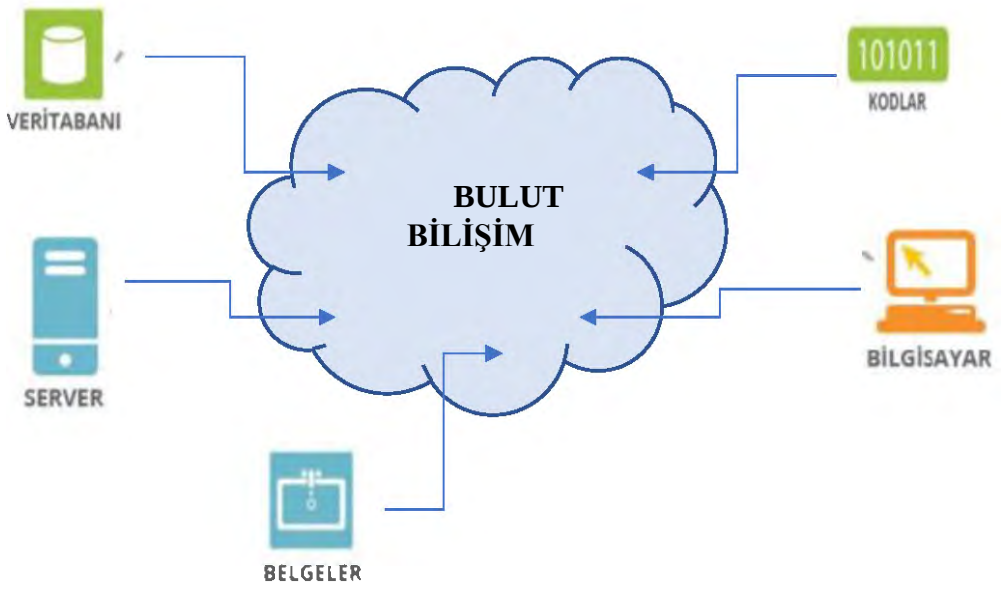
5. Yapılandırma Seviyesi: Yapılandırma düzeyi, siber uzaydan fiziksel alana geri bildirimdir ve makinelerin kendi kendine yapılandırılması ve kendi kendine uyarlanabilir olması için denetim kontrolü görevi görür. Bu aşama, biliş düzeyinde alınan düzeltici ve önleyici kararların izlenen sisteme uygulanması için direnç kontrol sistemi (Resilience Control System-RCS) görevi görür.

Şekil 1. 4. *Üretimde siber fiziksel sistemler için 5C modeli (Lee vd., 2015, s.19)*

2.2.4. Bulut Bilişim

Bulut bilişim, depolama ve hesaplama için bir merkez görevi görerek büyük miktarda veri yüklenerek üretimin kolaylaşmasını sağlamaktadır (Xu, Xu and Li, 2018, s. 2947). Bulut bilişim, minimum yönetim hizmeti gerektiren veya hizmet sağlayıcı etkileşimi ile hızla alınabilen ve verilebilen esnek yapıdaki yapılandırılabilen bilişim kaynaklarının (ağ hizmeti, sunucu hizmeti, depolama hizmeti, uygulamalar ve diğer hizmetler gibi) paylaşıldığı havuza aynı anda her yerde bulunan ve uygun bir şekilde ağ

erişimi sağlayan bir model olarak ifade edilebilir (Mell and Grance, 2011, s. 2) Bulut bilişim ifadesindeki "bulut" kelimesi hizmetlerin internet üzerinden yani gözle görülemeyen bir ağ üzerinden yürütülmesi sebebiyle kullanılmaktadır (Aytekin, Erdoğan ve Kavalcı, 2016, s. 48). Bulut bilişim Şekil 1.5'te gösterildiği üzere bilgisayar, tablet, akıllı mobil cihazlar aracılığıyla herhangi bir yazılım veya depolama birimine ihtiyaç duyulmaksızın internet üzerinden farklı sunuculara bağlanarak hizmet alma şeklidir (Kavzaoğlu ve Şahin, 2012, s. 2).



Şekil 1. 5. *Bulut bilişim bileşenleri (Aytekin, Erdoğan, & Kavalcı, 2016, s. 48)*

Kurumlar tarafından küresel rekabet koşullarında üstünlük sağlamak adına bilişim teknolojileri kapsamında yapılan yatırımlar her geçen gün artığı günümüzde sıkça tekrar edilen bir söylemdir. Diğer taraftan kurumların bilişim teknolojileri kapasitelerini yüksek seviyede kullanmadıklarına dolayısıyla bu kapsamda yapılan yatırım maliyetlerini azaltmak için bu hizmetleri sağlayan merkezi hizmet sağlayıcılardan tedarik edilmesi tercih edilir hale gelmiştir. Bir örnek ile ifade edilecek olunursa; nasıl ki elektrik veya telefon hizmeti alırken bu kapsamda altyapı yatırımı, altyapı bakımı, altyapının nasıl çalıştığı konusunda bilgi sahibi olmak veya ilgili personele ihtiyacı yoktur ve tüm bu sıralanan sorumluluklar hizmet sağlayıcının görevidir. Bulut bilişimde elektrik ve telefon

hizmetleri gibi benzer bir modeli bilişim hizmetleri için sunmaktadır (Seyrek, 2011, s. 702-703).

Bulut bilişim hizmet modellerinin kullanılma biçimleri açısından dört sınıfa ayrılmıştır (Ö. R. Yıldız, 2011, s. 8-9):

- **Genel Bulut (Public Cloud):** Üçüncü taraf hizmet sağlayıcıları tarafından bulut bilişim hizmeti internet üzerinden sunulmaktadır. Dolayısıyla genel kullanıma açık bir yapısı vardır. Kullanıcı birimler Amazon, Google Gogrid vb. web uygulamaları üzerinden erişim sağlamaktadır.
- **Özel Bulut (Private Cloud):** Özel bulut tek bir kuruma hizmet vermesinden kaynaklı bu şekilde ifade edilmiştir. Bulut bilişim hizmeti kurum dışında veya kurum içinde (binasında) verilebilir. Diğer bir nokta ise hizmeti yürütme işlemi kuruma ait olabilir veyahut üçüncü bir taraf işletme tarafından yürütülebilir. Bu haliyle bulut bilişim mimarisinin avantajlarından yararlanmak üzere kuruma özel oluşturulmuş yapılardır ve hizmet kurum içerisinde kurum güvenlik duvarının arkasında kurulup işletilebilir.
- **Topluluk Bulutu (Community Cloud):** Belli bir kurum ve müşterek hareket eden kurumların yani birden fazla kurumun bulut bilişim alt yapısını paylaşma halini ifade etmektedir. Dolayısıyla bu topluluğa dahil kurumların uygulama ve verilere erişim hakkı mevcuttur.
- **Melez Bulut (Hybrid Cloud):** Genel, özel ve topluluk bulutunun bir arada kullanılması melez bulutu oluşturur. Bir kurumun kendine ait özel hizmetlere ek olarak kurum dışından hizmet almayı tercih ettiği durum melez buluta örnektir.

Bulut bilişim kurumların verimliliklerini artırmak adına tercih ettikleri bir teknoloji olmakla birlikte başlıca avantajı *düşük maliyet* sağlamasıdır. Bulut bilişimin düşük maliyet avantajından sonra en önemli avantajı *esnekliktir*. Kurumların bilişim süreçleri dahil tüm iş süreçlerinde meydana gelecek büyüme veya azalma durumunda hızlıca adapte olunması istenmektedir. Bundan dolayı sistemin bu esnekliği sunabilecek şekilde yapılandırılması önemlidir. Kurum tarafından istendiği zaman hizmet kullanılabilmelidir. Kurulum maliyetinin çok düşük olması iş süreçlerindeki değişimlere hızlıca cevap

verebilmesi gibi özellikler bulut bilişim hizmetini sağlayanları daha esnek bir yapıya kavuşturacaktır. Bulut bilişimin diğer faydası ise *kullanılabilirlik ve sürdürülebilirliktir*. Hizmet sağlayıcı kurumlar çok güçlü donanım ve bant genişliği ile iş gereksinimleri karşılamaktadır. Sistemin kaliteli şekilde hizmet sunması için fazladan yollar ve yük dengeleme sistemleriyle bu hizmetin kesintisiz verilmesi amaçlanmaktadır. Fakat teknolojinin doğasından kaynaklı kesinti yaşanması ihtimaline karşılık anlaşma hükümlerinin bu ihtimal göz önünde bulundurulmalıdır. Bulut bilişim tek katkısının depolama olarak düşünülmemelidir. Aynı zamanda olağandışı bir durumun yaşanması sonucu bir kesintinin oluşması durumuna karşılık iş sürekliliğinin sağlanması içinde hizmet vermektedir. Yaşanan kesinti sonrası en son işlenen veriler üzerinden devam edilmesi sağlanacaktır. (Ö. R. Yıldız, 2011, s. 11-12). Tüm bu sağladığı avantajlar yanında bulut bilişim yapısı itibariyle barındırdığı birtakım riskleri söyle sırlanabilir (Seyrek, 2011, s. 706-709):

- Bulut bilişim hizmetinin internet üzerinden sağlanması internet ile ilgili bütün güvenlik sorunlarını bulut bilişim için de güvenlik sorunu haline getirmektedir. Bulut bilişim hizmetinde, birçok kullanıcı hizmet sağlayıcının bilgisayarlarını müşterek kullandığından ve kendi verilerine ve bilişim hizmetlerine internet üzerinden eriştiklerinden, bulut içerisindeki bilgisayarlar saldırganlar için hedef haline gelmektedir.
- Bulut bilişim hizmeti, kullanıcı kurum verilerini hizmet sağlayıcıya emanet etmesi anlamına gelmektedir. Hizmet sağlayıcı sistemi içerisinde tutulan bu verilerin gizliliğinin güvence altına alması oldukça önemlidir. Verilerin gizliliğinin sağlanması, sadece yetkili kişilerin veya uygulamaların bu verilere erişebilmesi demektir. Fakat bulut bilişimde ilgili taraf, uygulama ve cihaz sayısı arttığından bu gizliliğin sağlanması zorlaşmakta ve gizlilikle ilgili riskler artmaktadır.
- Bulut bilişim hizmetlerinin çeşitlenerek yaygınlaşması ve hizmet sağlayıcıların farklı ülkelerden müşterilere hizmet vermesiyle birlikte hizmet verdikleri farklı ülkelerin yasalarına uyma konusunda sorunlar yaşayabilirler.
- Kurumların bulut bilişim tercih etmeleri aldıkları hizmetten memnun kalmaları ile ilişkilidir. Dolayısıyla kurumların bilgi teknoloji

uygulamalarının kesintisiz devam etmesini isterler. Kesintisiz hizmet yanında, verilerin hizmet kalitesi ve performansın yüksek olması önemlidir. Bu bağlamda bulut bilişim hizmeti veren kurumların donanım ve altyapılarının hizmeti verecek şekilde tasarlanmaları önemlidir. Ayrıca hizmet kullanıcılarının verilerinin kesinti halinde verilerinin düzenli şekilde yedeklenmesi ve kayıp olmadan, hızlı şekilde erişime uygun halde olması önemlidir. Tüm bunlar sonucunda hizmet sağlayıcının performansı riskler arasındadır. Bulut bilişim hizmet sağlayıcısının performansının yeterli düzeyde olmaması ilişkili bir diğer riski de beraberinde getirmektedir. Kullanıcının bir bulut bilişim hizmet sağlayıcısından diğerine geçmesi bazı zorlukları (veri ve yazılımların taşınmasında büyük zorluklar gibi) barındırması nedeniyle mevcuttaki bulut bilişim sağlayıcısına bağımlı hale getirmektedir.

2.2.5. Yapay Zeka ve Robotlar

İnsanın akıl yürütme, algılama, kavrama, yargılama ve sonuca varma yeteneği zeka olarak ifade edilmiştir. İnsana ait bu özelliğin makineler tarafından da gerçekleştirilmesi isteğinden yola çıkılarak bilim insanları yapay zeka kapsamında araştırmalar yapmaya başlamıştır (Yıldız ve Yıldırım, 2018, s. 27). Yapay zeka terimini 1955 yılında tanımlayan ilk kişi olan John McCarthy oldu ve yapay zekayı şöyle ifade etti: "yapay zekanın amacı zeki gibi davranan makineler geliştirmektir" (Ertel, 2017, s. 1). Yapay zekanın temel hedeflerinden biri otonom makinelerinin fiziksel dünyada dolaşarak insan ve bilgisayarların karşılıklı şekilde iletişim kurmasına yardımcı olmaktır (Schwab and Davıs, 2019, s. 167).

Yapay zekânın kullanım alanlarından olan robotlar, endüstriyel alanlarda önemli bir rol oynamaktadır. Dördüncü sanayi devrimi geleneksel anlamda yardımcı niteliğinde olan robotları, yardımcılıktan çıkarıp iş birliği ve birlikte üretme şeklinde iş arkadaşı konumunda bir noktaya getirmektedir. Bu iş birliği sürecinde sensörler, kameralar ve yapay zeka içeren öğrenebilir yazılımlar eşlik etmektedir. Akıllı robotlar, otonom (kendini yönetme ve denetleme niteliği) özelliğe sahiptir ve diğer cihazlardan ayıran özelliği yapay zeka içermesidir. Akıllı robotlar, çevresini algılayabilen buna göre hareket edebilen kısa sürelide olsa öngörülebilir bir geleceğe yönelik akla yatkın kararlar üretebilen makinelerdir (Banger, 2018, s. 71-72). Otonom robotlar yalnızca kapalı

alanlardaki basit yapılandırılmış iş akışlarda insanların yerini almakla kalmayacak aynı zamanda robotlar ve insanların görevleri birbirine bağlanacaktır. Robotların görevleri çeşitli işlevleri kapsayacak şekilde genişlemektedir. Üretim, lojistik ve ofis yönetimi (belgeleri dağıtmak için) gelişmeler yaşanmakla birlikte bunlar uzaktan kontrol edilebilmektedir. Uzaktan kontrol edilebilirliği sayesinde gün boyu işletmelerde faaliyetlerin devam ettirilmesi sağlanmaktadır. KUKA tarafından üretilen LBR iiwa, insanlar ile işbirliği içinde çalışarak her zamankinden daha bağımsız ve daha hassas çalışma fırsatı sunmaktadır. LBR iiwa mobildir, esnektir ve son derece çok yönlüdür. Aynı zamanda, hızla değişen üretim gereksinimlerine sorunsuz dijital ağ ve otonom ile uyum sağlar. Akıllı endüstriyel iş asistanı anlamına gelen "iiwa", insan meslektaşlarından öğrenebilir ve buluta bağlıyken kendi çalışmasının sonuçlarını bağımsız olarak kontrol edebilir, optimize edebilir ve belgeleyebilir (Bahrin vd., 2016, s. 139; KUKA, 2017). Otonom robotlar insanların yerine zor, manuel, tekrarlayan ve entelektüel kazanım sağlamayan işleri yürüterek insanların yaşam kalitelerini iyileştirecektir. Ayrıca otonom robotlar verilen görevi belirlenen süre zarfında tamamlayarak güvenlik, esneklik, çok yönlülük ve işbirliğine odaklanabilmektedir (Vaidya, Ambad and Bhosle, 2018, s. 235; Ivanov, 2017, s. 5).

Yapay zekâ yalnızca endüstriyel teknolojileri etkilemekle kalmamış bunun yanında gazetecilik, tıp, muhasebe ve hukuk gibi bilgiye dayalı meslekler üzerinde de etkisini göstermiştir. Yaşanan gelişmeler ilerledikçe avukat ve doktorların yerini tamamen almayacaktır fakat örnek olay çalışmalarını ve tanısal görüntülemeleri analiz edebilen yapay zekâ uygulamaları ile bu mesleklerde değişime sebep olacaktır (Schwab and Davıs, 2019, s. 174). IBM'in Watson isimli robotu akciğer kanseri teşhisi konusunda, bazı testlerde % 50'ye karşılık % 90 oranında tutarlılık göstererek insanlara kıyasla daha kesin bir teşhis yeteneği göstermesi yapay zekanın gelecekte meslekleri etkileme konusundaki resmini çizmektedir (Schwab, 2016, s. 164).

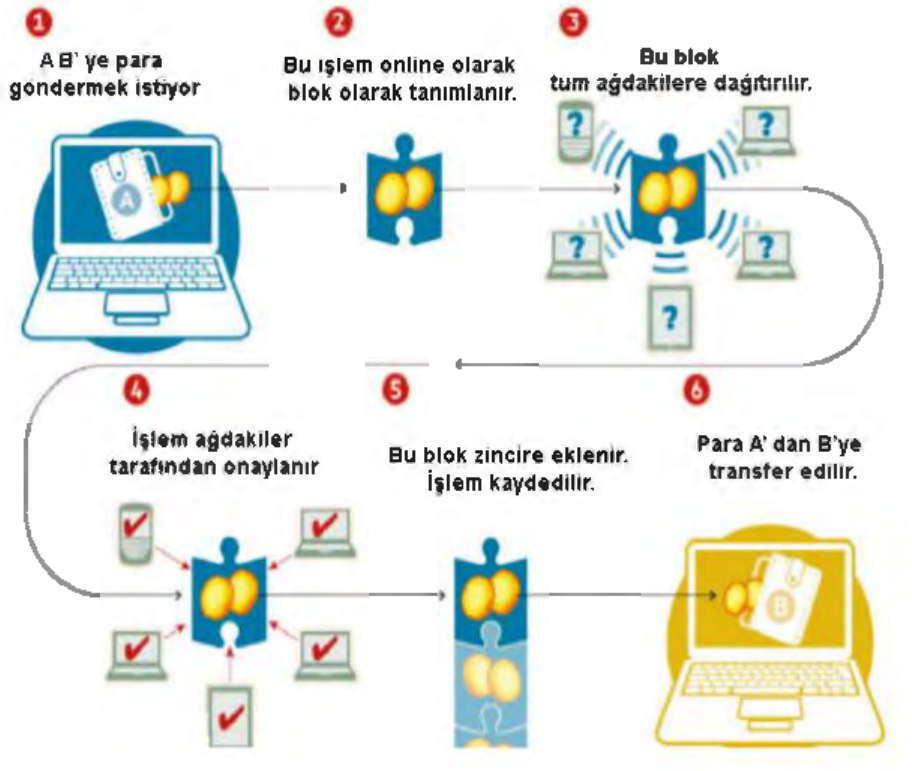
2.2.6. Blokzincir (Blockchain) Teknolojisi

Dijital dünyada daha iyi kararlar almak adına gün geçtikçe yeni teknolojiler gelişmektedir. Bunlardan biri de Türkçe karşılığı blokzincir -blockchain- teknolojisidir. İlk olarak 2008 yılında tanıtılan kripto para birimi ve ödeme sistemi olan Bitcoin, blok zincir teknolojisinin en popüler uygulamalarından biridir (Angraal, Krumholz and Schulz, 2017, s. 1). Fakat blokzincir teknolojisi kripto para birimi temelinden çok daha

fazlasını oluşturmaktadır. Her türlü mal, hizmet veya işlemi değiş tokuş etmek adına güvenli bir yol sunmaktadır (Ahram vd., 2017, s. 137). Beck (2018, s. 55) tarafından blok zinciri, ağdaki çok sayıda düğüm tarafından güvenli ve tutarlı işlemlerin yapılmasını sağlayan bir veri tabanı şeklinde ifade edilmiştir. Reyna vd. (2018, s. 174) ise blokzinciri, işlemlerin güvenirliğinin ağdaki paydaşlar tarafından doğrulandığı dağıtılmış, şeffaf, değiştirilemez ve denetlenebilir bir defter şeklinde tanımlamıştır. Blok zincir teknolojisinin temelinde dağıtık hesap defteri teknolojisi yatmaktadır. Blokzincir teknolojisi ile merkezi ve güvenilir bir tarafa ihtiyaç olmaksızın benzersiz dijital kayıtların yapılması ve takasların gerçekleştirilmesi imkanı bulunmaktadır. Şifreleme ve eşten eşe ağ yöntemi kullanan teknoloji, depolanan ve bir grup insan tarafından paylaşılan enformasyonun hem doğru hem de şeffaf olmasını garanti etmektedir (Schwab and Davıs, 2019, s. 123). Blokzincir aşağıdaki temel özelliklere sahiptir (Zheng vd., 2017, s. 558-559):

- Ademi merkeziyetçilik: Geleneksel merkezileştirilmiş işlem sistemlerinde, her işlemin merkezi güvenilir kurum (örneğin merkez bankası) aracılığıyla doğrulanması gerekir, bu da kaçınılmaz olarak merkezi sunucularda maliyet ve performans darboğazlarına neden olur. Merkezi modun aksine, blok zincirinde artık üçüncü tarafa ihtiyaç yoktur. Blok zincirdeki mutabakat algoritmaları, dağıtılmış ağda veri tutarlılığını korumak için kullanılır.
- Kalıcılık: İşlemler hızlı bir şekilde doğrulanabilir ve geçersiz işlemler dürüst madenciler tarafından kabul edilmez. Blok zincirine dahil edildikten sonra işlemleri silmek veya geri almak neredeyse imkansızdır. Geçersiz işlemler içeren bloklar anında keşfedilebilir.
- Anonimlik: Her kullanıcı, kullanıcının gerçek kimliğini ortaya çıkarmayan, oluşturulmuş bir adresle blokzinciri ile etkileşime girebilir.
- Denetlenebilirlik: Geçerli işlem blok zincirine kaydedildikten sonra işlemler kolayca doğrulanabilir ve izlenebilir.

Blok zincirin çalışma sistemini Şekil 1.6 ile ifade edilmeye çalışılmıştır.



Şekil 1. 6. *Blokzincir teknolojisini kullanan finansal işlemler (Crosby vd., 2016, s. 10)*

Mevcut dijital ekonomi ele alındığında belirli bir güvenilir otoriteye güven duymaya dayanmaktadır. Diğer taraftan kullanılan tüm çevrimiçi işlemler karşıdaki işlemi yürüten otoritenin bize gerçeği söyleyeceği konusunda güven duygusu üzerine kuruludur. Bu durumu somut şekilde ifade edildiğinde; e-postamızın teslim edildiğini bize söyleyen bir e-posta hizmet sağlayıcısı; bize belirli bir dijital sertifikanın güvenilir olduğunu söyleyen bir sertifika yetkilisi; Facebook gibi bir sosyal ağ kişisel paylaşımlarımızın sadece arkadaşlarımızla paylaşıldığını ya da paramızın uzak bir ülkedeki sevdiklerimize güvenilir bir şekilde teslim edildiğini söyleyen bir banka şeklinde listelenen örnekler sıralanabilir. Tüm bu örnekler bireylerin hayatlarının bir noktasında kullanmış dijital varlıklarının güvenliği ve gizliliği için üçüncü bir varlığa güvenerek hayatlarını dijital dünyada güvencesiz bir şekilde sürdürdüğünü göstermektedir. Üçüncü taraf kaynaklar saldırıya uğrayabilir, manipüle edilebilir veya tehlikeye atılabilir. Blok zincir teknolojisi bu noktada devreye girmektedir (Crosby vd., 2016, s. 8).

Blokzincir teknolojisinin ana fikri basit görünmesine rağmen uygulanması çok sayıda zorluk ortaya çıkarmaktadır. Bunlar şöyle sıralanabilir (Reyna vd., 2018, s. 175-179; Meva, 2018, s. 490-491):

- Depolama kapasitesi ve ölçeklenebilirlik, blok zincir teknolojisinde derinlemesine sorgulanmaktadır. Bu teknolojide zincir, Bitcoin'de her 10 dakikada bir blok başına 1MB oranında sürekli büyüyor. Boyut büyüdükçe, düğümler giderek daha fazla kaynağa ihtiyaç duyar ve bu da sistemin kapasite ölçeğini azaltır. Ayrıca, büyük boyutlu bir zincirin performans üzerinde olumsuz etkileri vardır, örneğin yeni kullanıcılar için senkronizasyon süresini artırır.
- Blokzincir teknolojisinin kullanıcıların kimliklerini açıklamama konusunda anonimlik fırsatı sunarken, diğer taraftan yasa dışı ürünlerin satın alınması veya kara para aklama gibi yasa dışı faaliyetlere teşvik etmektedir.
- Güvenlik blokzincir teknolojisindeki bir diğer zorluklardan biridir. Rüşvet yoluyla madencilik gücüne sahip olunmasıdır. İşlemlerdeki sürenin uzunluğu hızlı ödeme beklentisini karşılayamaz ve çift ödemelere önemli güvenlik sorunlarındadır. Güncellemenin tüm düğümlerde yaşanmaması durumunda çatallanmalar yaşanır. Temel olarak iki tür çatal vardır: Sert çatal ve yumuşak çatal. Sistemler yeni sözleşme veya sürümle geldiğinde ve eski sürümle uyumlu değilse, eski düğümler yeni düğümlerin madenciliği ile anlaşamazlar. Bu da bir zinciri ikiye bölüyor. Buna sert çatal denir. Sistemler yeni sözleşme veya sürümle geldiğinde ve eski sürümle uyumlu değilse, yeni düğümler eski düğümlerin madenciliği ile anlaşamaz. Eski düğümler ve yeni düğümler aynı zincir üzerinde çalışmaya devam eder. Buna yumuşak çatal denir. Çatallar, özellikle sert olanlar, topluluğu tamamen farklı iki blok zincirine bölebilir ve bu durum blokzinciri kullanıcıları için bir risk teşkil edebilir.
- Blokzincir uygulamasındaki en büyük zorluk, çeşitli ülkelerin kuralları ve düzenlemeleridir. Bu durum yasal düzenleme sorunlarını getirmektedir. Merkezi olmayan yapı kavramı, ekonomi politikası ve para işlem tutarları açısından merkez bankasının kontrolünü zayıflatacaktır.

- Blokzincir uygulamasında işlemin doğrulanması için yapılan hesaplamalar sırasında bilgisayarlar büyük oranda enerji harcarlar. Enerji kaynakları veya diğer sürdürülebilir iş yapma yöntemleri düşünen birçok kuruluş için bu durum engel teşkil etmektedir.
- Toplumun algısı da diğer bir zorluktur. İnsanların çoğu hala bu teknolojinin varlığından ve kullanımından habersizdir. Bu teknoloji, endüstride devrim niteliğinde değişikliklerdir, ancak bu dağıtılmış defter teknolojisi hakkındaki bilgiler yalnızca bu sürece dahil olanlarla sınırlıdır. Blokzincir hakkında konuştuğumuzda, insanların aklına sadece Bitcoin ve diğer kripto para birimleri gelecektir. Ve insanlar bu para birimini kara para aklama, karaborsa ve diğer yasa dışı görevler olarak düşünüyor. Bu nedenle, insanların Bitcoin ve blokzincir arasındaki farkı ve blokzincir ile ilgili olumsuz imaları anlamaları gerekir.
- Blokzincir teknolojisi henüz teknik olgunluğa ulaşamamıştır. Kapasite, sistem arızası, öngörülemeyen hatalar ve en önemlisi; teknik olarak bilgisiz kullanıcılar tarafından kullanılacaktır.
- Diğer bir önemli zorluk, mevcut sistemi blokzincir tabanlı yeni sistemle değiştirmenin yüksek maliyetidir.

2.2.7. Eklemeli Üretim (Katmanlı Üretim) ve Üç Boyutlu (3D) Yazıcılar

Endüstri 4.0, akıllı otomasyon teknolojisinin son hareketi olup bu yeni çağda modern üretim becerilerinin kullanımı rekabet üstünlüğü elde etmek adına önemli yere sahiptir. Akıllı fabrikaların fiziksel kısmının mevcut üretim sisteminin kapasitesi ile sınırlı olmasından kaynaklı eklemeli üretim Endüstri 4.0 bakış açısında önemli bir yere sahiptir (Dilberoglu vd., 2017, s. 546).

Eklemeli üretim, talaşlı imalat metodolojilerinin aksine, genellikle katman katman 3D model veriden nesneler yapmak için malzemeleri birleştirme süreci olarak ifade edilmektedir. Eklemeli üretim, eklemeli işlemler, eklemeli teknikler, eklemeli katman üretimi, katmanlı üretim ve serbest biçimli üretim şeklinde kullanılabilir (ASTM, 2010, s. 2). Daha büyük bir stoktan veya metal sacdan malzemeleri çıkararak ürünler üreten makineyle işleme ve damgalama gibi geleneksel imalat tekniklerinden farklı olarak, eklemeli imalat, malzeme ekleyerek nihai şekli oluşturur (Huang vd., 2013, s. 1191).

Üç boyutlu yazıcıların çıkışı 1970'lere dayanmakla birlikte hızlı prototipleme olarak tasarımların numunelerini üretmek amaçlanmaktadır. 1980'li yıllara gelindiğinde ise gerçek parça üretimi gündeme gelmiştir. Eklemeli üretim kavramının ortaya çıkışı ise 1990'lı yıllarda metal ve seramikten son kullanım doğrudan fonksiyonel parçaların üretilmesiyle meydana gelmiştir (Özsoy ve Duman, 2017, s. 37). Üç boyutlu yazıcılar ile şimdiye kadar plastik kullanılarak üretim yapılmakla birlikte artık, metal parçaları üretmek amacıyla da kullanılmaktadır. Üç boyutlu yazıcıların kullanım alanları tıp, otomotiv, havacılık endüstrilerinin gelişiminde önemli role sahip olacaktır. Üç boyutlu yazıcıların özellikle karmaşık ve özel parçaların üretiminde maliyeti önemli ölçüde düşürecektir. Ayrıca üç boyutlu yazıcıların daha önceden üretilmesi imkansız olan tasarımların üretilmesini sağlayacaktır. Böylelikle işletmelere hem yeni ürün bazında hem de hızlı üretim konusunda avantaj sağlayacaktır (Kesbiç, 2020, s. 19). Önemli ilerlemeler kaydedildiği ve eklemeli imalat teknolojisinin imalat endüstrisinde devrim yaratabileceği ve genel olarak topluma çeşitli faydalar sağlayabileceği yönünde bir beklenti çeşitli endüstrilere yansımaları görülmektedir. Eklemeli üretimin sağladığı faydalar aşağıdaki şekilde sıralanabilir (Huang vd., 2013, s. 1200-1201):

- Nüfusun refahını önemli ölçüde iyileştirmesi beklenen, bireysel tüketicilerin ihtiyaçlarına göre özelleştirilmiş sağlık ürünleri. Örneğin, eklemeli üretim sağlık sektöründe özelleştirilmiş cerrahi implantlar ve yardımcı cihazlar üretmek için kullanılması.
- Çevresel sürdürülebilirliğe önemli bir katkı olan azaltılmış ham madde kullanımı ve enerji tüketimi. Geleneksel işleme süreçleriyle karşılaştırıldığında eklemeli üretim, işlenmemiş malzeme tüketimi ve su kullanımı açısından daha verimlidir. Soğutucu ve diğer yardımcı işlem girdilerinin kullanımını gerektirmez ve bu nedenle karasal, suyla ilgili ve atmosferik sistemlere daha az kirlilik üretir. Aynı zamanda daha az katı atık depolama sahası gerektirir. Bu nedenle eklemeli üretimin geleceğin sürdürülebilir toplumunda önemli bir üretim teknolojisi olması beklenmektedir.
- Daha az kaynak kullanarak daha ucuz ürünleri tüketicilere daha hızlı ulaştırmak için üretim tedarik zincirini yeniden yapılandırma fırsatı sunan talep üzerine üretimi mümkün kılar. Sonuç olarak, depolama, nakliye ve

paketleme ihtiyacı önemli ölçüde azaltılabilir. Uygun tedarik zinciri yapılandırmasıyla, eklemeli üretim kullanarak müşteriye yanıt verme hızı korunurken maliyet verimliliğini artırmak mümkündür. Kişisel eklemeli üretim makinesinin ortaya çıkmasıyla, müşterilerin arzu ettikleri ürünleri istedikleri zaman ve evlerinden çıkmadan ekonomik bir şekilde elde edebilecekleri imkanı sunar.

2.2.8. Sanal Gerçeklik ve Artırılmış Gerçeklik

Artırılmış gerçeklik sistemi olarak tanınan sistemin geliştirilmesi 1966 yılında bilgisayardaki bilgileri gerçeklikle birleştirmek amacıyla Ivan Sutherland tarafında insanların başlarına taktığı bir ekran icat etmesi sonucu gerçekleşmiştir. Diğer taraftan asıl çıkış noktası olarak II. Dünya Savaşı'nda İngiliz ordusu tarafından geliştirilen bir proje sonucunda savaş uçaklarının ön camlarına yerleştirilen radar bilgilerini gösteren teknolojinin geliştirilmesidir. Bu teknoloji ile pilota diğer şeylerin belirlenmesinin yanı sıra diğer uçakların dost mu yoksa düşman uçakları olup olmadığı konusunda yardımcı olmuştur (Berryman, 2012, s. 213-214). Sonraki yıllarda artırılmış gerçekliğe ilişkin gelişmeler artmıştır ve bugün birçok alanda yer almaktadır.

Artırılmış gerçeklik, kullanıcı deneyimini geliştirmek amacıyla gerçek dünyadaki nesneler veya yerler üzerine dijital bilgiler yerleştiren bir teknolojidir (Berryman, 2012, s. 212). Artırılmış gerçeklik daha genel bir ifade ile internet erişimi ve bazı akıllı cihazlar (akıllı gözlük, akıllı eldiven, bilgisayar vb.) aracılığıyla sanal nesnelerin gerçek görüntülere eklenmesidir. Bazı akıllı cihazlar (bilgisayar, tablet, telefon vb.) tarafından ses, video, grafik, GPS vb. veriler üretilir duyusal/algısal girdi ile artırılması ve gerçek ortamla birleştirilerek yeni bir algısal ortam oluşturulmasıdır (Demirezen, 2019, s. 4). Artırılmış gerçeklik, gerçeklik ile dijital bilgiyi birleştirme yeteneği ile tıpta, pazarlamada, müzelerde, modada ve diğer birçok alanda incelenmekte ve uygulanmaktadır (Berryman, 2012, s. 212).

Sanal gerçeklik, gerçekçi bir ortamı simüle eden gelişmiş bir insan-bilgisayar arayüzüdür. Katılımcılar sanal dünyada hareket edebilirler. Onu farklı açılardan görebilir, içine uzanabilir, kavrayabilir ve yeniden şekillendirebilirler (Zheng, Chan and Gibson, 1998, s. 20). Sanal gerçeklik farklı kaynaklarda, sanal çevre (virtual environment), siberuzay (cyberspace), sanal dünya (virtual world) ve yapay gerçeklik (artificial reality)

olarak adlandırılmaktadır (Ferhat, 2016, s. 725). Sanal gerçeklik, öğrenme için büyük avantajlar sunabilir: fiziksel olarak ulaşamayacağımız nesnelerin ve olayların doğrudan hissedilmesine izin verir, potansiyel gerçek tehlikelerden kaçınarak güvenli bir ortamda eğitimi destekler ve oyun yaklaşımı sayesinde öğrencinin katılımını artırır ve desteklenen öğrenme stilleri yelpazesini genişletirken motive eder (Freina and Ott, 2015, s. 1006). Eğitim alanında etkisinin yanında sanal gerçeklik için sektör bazında kullanım alanları şöyle sıralanabilir (Wohlgenannt, Simons and Stieglitz, 2020, s. 458):

- Perakende: IKEA, yeni çalışanları işe almak için sanal gerçeklikten yararlanıyor, Macy's, müşterilerin alışveriş deneyimini geliştirmek için sanal gerçeklikten yararlanıyor ve Verizon, mağaza görevlilerini rehine ve soygun durumlarıyla başa çıkma konusunda eğitmek için sanal gerçeklikten yararlanıyor.
- Ulaşım: Deutsche Bahn, gerçek trenlerde öğretilemeyen senaryolar (örn. yangınla mücadele) için sanal gerçeklik eğitimleri vermeyi planlıyor, Volkswagen prototipleme için sanal gerçeklik kullanıyor ve Tata Motors, müşterilerinin arabaları sanal gerçeklik yapılandırmasına izin veriyor.
- Enerji: E.ON, trafo merkezi çalışanlarına sanal gerçeklik kullanma talimatı veriyor, Shell derin deniz petrol projelerinde güvenlik eğitimi için sanal gerçeklik kullanıyor ve MHI Vestas, açık deniz rüzgar türbinlerini sergilemek için bir satış aracı olarak sanal gerçeklik teknolojisini kullanıyor.
- Danışmanlık: Accenture, personeli değerlendirmek için sanal gerçeklik kullanıyor, PwC, sanal gerçeklik ile çeşitlilik ve dahil etme eğitimleri yürütüyor ve BDO, personel alımına uygulanabilirliğini test etmeye yönelik sanal gerçekliği kullanmaktadır.
- Sigorta: Farmers Insurance, sanal gerçeklikte çevresiyle uyum becerisi eğitimleri düzenlemeyi planlarken, Cigna sağlık taramaları yapmak ve müşterilere sağlık bilgilerini iletmek için sanal gerçekliği kullanıyor ve PNB MetLife, sanal gerçeklikte müşterileri ile görüşüyor.
- Sağlık Hizmeti: Takeda işe alım için sanal gerçeklik kullanıyor, Columbia Üniversitesi ve Harvard Tıp Okulu cerrahları eğitmek için sanal gerçeklik kullanıyor ve Ivoclar Vivadent, diş tedavileri sırasında hastaların dikkatini dağıtmak için sanal gerçeklik kullanılmasını öneriyor.

- Spor: Dallas Cowboys, oyuncularını sanal gerçeklik kullanarak eğitmeye başladı, Premier Lig takımları futbol yeteneğini belirlemek için sanal gerçeklik kullanıyor ve Ulusal Stok Otomobil Yarışları Birliği (National Association for Stock Car Auto Racing -NASCAR), hayranların yarış etkinliklerini uzaktan deneyimleyebilmesi için sanal gerçeklik kullanıyor.

Artırılmış gerçeklik ve sanal gerçeklik kavramlarının arasındaki farklılığı ortaya koymak önemlidir. Artırılmış gerçeklik sistemleri, sanal gerçeklik sisteminde kullanılan aynı donanım teknolojilerinden bazılarını kullanıyor ancak çok önemli bir fark var: sanal gerçeklik, gerçek dünyayı titizlikle değiştirmeyi hedeflerken, artırılmış gerçeklik, onu iyi bir şekilde desteklemektedir (Feiner, 2002, s. 50). Yakın zamana kadar sanal gerçeklik popüler bir teknoloji iken, kullanıcının çevreyle karşılıklı etkileşime geçmesine imkân sağlaması nedeniyle artırılmış gerçeklik ön plana çıkmaya başlamıştır. Artırılmış gerçekliğin ayrıca elektronik ortamdaki verilerin gerçek hayata eklenebilmesine fırsat sunması, popülaritesinin artmasındaki bir diğer faktördür (Kounavis, Kasimati and Zamani, 2012, s. 2).

2.2.9. Simülasyon

Simülasyon, gerçek dünyada var olan bir fiziksel sisteme ait verilerin sanal bir ortama taşınmasıyla gerçek sisteme ait özelliklerin izlenmesine altyapı oluşturan bir modelleme tekniği şeklinde ifade edilmiştir. Ürünlerin, materyallerin ve üretim süreçlerinde simülasyon teknolojisi kullanılmakla birlikte gelecek kurum faaliyetlerinde kullanımı artacaktır. Simülasyonlar makine, ürün ve insanları kapsayan sanal modellerin gerçek dünyaya yansıtmak için gerçek zamanlı veriyi güçlendirecektir. Simülasyon teknolojisi makine kurulum sürelerini azaltmaya ve kaliteyi artırmaya yardımcı olacaktır. (Rüßmann vd., 2015, s. 56). Bir üretim tesisinin döngü süreleri, enerji tüketimi veya ergonomik yönlerinin simülasyonu için iki boyutlu ve üç boyutlu simülasyonlar oluşturulabilir. Üretim süreçlerinin simülasyonlarının kullanımı sadece devreye alma ve değişiklikler arasındaki kesinti sürelerini kısaltır aynı zamanda başlangıç aşamasındaki üretim hatalarını da azaltır (Simons, Abe and Neser, 2017, s. 83). Ayrıca simülasyon karar alanını netleştirerek hızlı ve kolay senaryoların oluşmasına yardımcı olarak karar verme kalitesini önemli ölçüde geliştirecektir (Schuh vd., 2014, s. 53).

2.2.10. Sistem Entegrasyonu

Sistem entegrasyonu yatay entegrasyon, dikey entegrasyon ve uçtan uca entegrasyon şeklinde sınıflandırılmaktadır. Dikey, yatay ve uçtan uca üretim süreçleri entegrasyonunun ve ürün bağlantısının kurumların daha yüksek endüstriyel performans elde etmelerine yardımcı olabileceği yeni bir endüstriyel aşama olarak kabul edilmektedir (Dalenogare, Benitez and Ayala, 2018, s. 383). Bir kurumda eğer ürün ve süreçler karmaşık hale geliyorsa işbirliği odaklı bir yaklaşım sergilemenin önemi artmaktadır. Yatay entegrasyon sayesinde işbirliği odaklı bir yaklaşımın benimsenmesiyle riskler dengelenir, kaynaklar birleştirilebilir, pazar fırsatları belirlenebilir (Brettel vd., 2014, s. 39). Dikey entegrasyon, geleceğin akıllı fabrikalarındaki ağa bağlı üretim sistemlerini ve montaj hattı üretimi gibi geleneksel sabit üretim süreçlerine alternatif olarak kişiselleştirilmiş özel üretimi kapsamaktadır. Uçtan uca entegrasyon ise özelleştirmeyi en üst düzeye çıkaracak, farklı şirketler arasında entegrasyona sahip dijital bir değer zincirine sahip her terminalin öncülüğünde uygulanan, tüm değer zinciri boyunca tasarlanmış sayısal entegrasyon anlamına gelmektedir (Zhou, Liu and Zhou, 2015, s. 2148).

Endüstri 4.0, her yerde bulunan sensörlerin, gömülü terminal sistemlerinin, akıllı kontrol sistemlerinin ve iletişim tesislerinin CPS içinde akıllı bir ağ oluşturmasını sağlamaktadır. Yatay, dikey ve uçtan uca entegrasyon elde etmek için ara bağlantı insandan insana, insandan makineye, makineden makineye veya hizmetten hizmete olabilir (Zhou, Liu and Zhou, 2015, s. 2148).

2.3. Dijital Dönüşüm ve Getirdiği Riskler

Dördüncü sanayi devrimi, yaşanan teknolojik gelişmeler sayesinde önemli ekonomik faydalar sağlamakla birlikte bazı zorlukların beraberinde getirmiştir. Teknolojide yaşanan bu gelişim insanların gündelik yaşamalarında teknolojiyi hızla kullanıma sevk etmiştir. Dolayısıyla her türlü bilgiyi barındıran bu sanal ortamın getirdiği bazı riskler kaçınılmaz hale gelmiştir (Gürel, 2020, s. 221).Dördüncü sanayi devrimine ilişkin gelişmelerin bir kısmıyla insanoğlunun karşılaşmasına rağmen geleceğe dönük bakıldığında ölçeğinin, kapsamının ve karmaşıklığının ne boyutta olacağı belirlenememektedir. Bu süreç kamu ve özel sektörden, akademik ve sivil topluma kadar tüm paydaşları kapsayacağı ifade edilmektedir (Schwab, 2016, s. 10). Dördüncü sanayi devriminin sağladığı faydanın yanında IIA (2021) tarafından yönetim kurulu üyeleri, üst

düzey yönetim ve denetim müdürlerle (Chief Audit Executive-CAE) yapılan derinlemesine görüşmeler yoluyla 2022'de kurumları etkilemesi muhtemel çok çeşitli riskler on iki başlık altında "OnRisk A Guide To Understaning Aligning And Optimizing Risk 2022" başlıklı raporda sıralanmıştır. Bu risklerin bir kısmı gelişen teknolojinin doğrudan etkisi ile ortaya çıkmakla birlikte diğer kısmı ile teknolojiyle dolaylı etki içerisinde olduğu söylenebilir. Bu anlamda tüm risklerin özet şekilde açıklamalarına aşağıda yer verilmiştir.

- Siber Güvenlik: Artan karmaşıklık ve çeşitlilikteki siber saldırılar, kuruluşların markalarına ve itibarlarına zarar vermeye devam ederek, genellikle büyük oranda mali etkilere neden olmaktadır. Bu risk, kuruluşların kesintiye ve itibar zedelenmesine neden olabilecek siber tehditleri yönetmeye yeterince hazır olup olmadığını incelemektedir (IIA, 2021, s. 5).
- Yetenek Yönetimi: Yetenek yönetimi riski, kuruluşların hedeflerine ulaşmak için doğru yetenekleri belirleme, edinme, geliştirme ve elde tutma konusunda karşılaştıkları zorlukları incelemektedir (IIA, 2021, s. 5). Yetenek yönetimi, iç denetim yöneticileri ve iç denetim profesyonelleri için her zaman bir ilgi alanı ve kaygı sebebidir. Son birkaç yıldır, denetim müdürleri yeni kadroları doldurmak ve yeni ve mevcut riskleri karşılamak için gereken becerilere sahip adaylar bulmaya kafa yormaktadır. İç denetimin artan gereksinimlerini karşılayacak becerilere sahip adaylar havuzunun sınırlı bir havuz olduğu açıktır. Ek olarak, çalışma ortamını, destek ve takdir konusunda daha büyük ve farklı beklentileri bulunan, akıllarında spesifik bir çalışma ortamı bulunan ve daha esnek çalışma programlarını tercih eden Y kuşağı işgücünün kendine özgü özniteliklerine uyarlama zorunluluğu da vardır (IIA, 2018, s. 1). Dolayısıyla değişen dünya karşısında insan gücü kapsamında zorlukların yaşanacağı görülmektedir.
- Organizasyonel Yönetişim: Yönetişim, bir organizasyonun nasıl yönlendirildiğinin ve yönetildiğinin tüm yönlerini (faaliyet gösterdiği kurallar, uygulamalar, süreçler ve kontroller sistemini) kapsamaktadır. Bu risk, işletmelerin yönetişiminin hedeflere ulaşılmasına yardımcı olup

olmadığını veya engelleyip engellemediğini incelemektedir (IIA, 2021, s. 5).

- Veri Gizliliği: Dünyanın dört bir yanındaki yasa düzenleyici otoriteler tarafından giderek artan düzenlemeler, veri gizliliğini giderek daha karmaşık ve dinamik hale getirmektedir. Bu risk, kuruluşların hassas verileri nasıl koruduklarını ve geçerli tüm yasa ve düzenlemelere uyumu nasıl sağladığını incelemektedir (IIA, 2021, s. 5).
- Kültür: Bu risk, kuruluşların istenen davranışı yönlendiren tonu, teşvikleri ve eylemleri anlayıp anlamadığını, izleyip yönetmediğini incelemektedir. (IIA, 2021, s. 5).
- Ekonomik ve Siyasi Dalgalanma: Ulusal seçimler, çok uluslu ticaret anlaşmaları, yeni veya genişletilmiş korumacı tarifeler ve rutin makroekonomik döngülerin zamanlaması konusundaki belirsizlik, kuruluşların faaliyet gösterdiği piyasalarda oynaklık yaratmaktadır. Bu risk, kuruluşların dinamik ve potansiyel olarak değişken bir ekonomik ve politik ortamda karşılaştıkları zorlukları ve belirsizlikleri incelenmektedir (IIA, 2021, s. 5).
- Düzenleyici Ortamda Değişiklikler: Bu risk, kuruluşların dinamik ve belirsiz bir düzenleyici ortamda karşılaştıkları zorlukları incelemektedir (IIA, 2021, s. 5).
- Tedarikçi ve Satıcı Yönetimi: "Tedarikçi ve Satıcı Yönetimi" riski, OnRisk 2021 raporunda "Üçüncü Taraflar" şeklinde ifade edilmiş olup IIA OnRisk 2022 raporunda üçüncü taraf olarak ifade ettiği tarafı daha net şekilde ifade etmiştir. Bir işletmelerin başarılı olması amacıyla dış iş ortakları ve tedarikçiler ile sağlıklı ve verimli ilişkiler sürdürmesi gerekmektedir. Bu risk, işletmelerin üçüncü taraf ilişkilerini seçme ve izleme yeteneklerini incelemektedir (IIA, 2021, s. 5). İşletmeler müşterilerine ürün ve hizmet konusunda beklentilerini karşılamak adına üçüncü taraf tedarikçi ve satıcılara gün geçtikçe bağlı hale gelmektedir. Üçüncü taraflar işletmelere maliyet, zaman tasarrufu şeklinde yarar sağlamanın yanında birbirine bağlı bir iş yapış şeklinden kaynaklı olarak riskleri de beraberinde getirmektedir (EY, 2020, s. 3). Dolayısıyla işletmelerin üçüncü taraf seçimi yaparken net bir stratejiye sahip olmaları risklerin belirlenmesi ve izlenmesi yönünden

önemlidir (KPMG, 2020, s. 4). İşletmeler küresel gelişmeler ve belirsizlikler karşısında üçüncü taraf risklerine ilişkin değerlendirmeleri yaparken yeni risk ve zorlukları dikkate alarak güncelleme yapmaları önemlidir (KPMG, 2020, s. 20). Ayrıca üçüncü taraf ile ilişkilerin seçme ve izleme aşamasını işletmeler etkin şekilde yönetemediği takdirde aşağıda bahsedilecek olan siber saldırılara maruz kalmaktadır. Dolayısıyla hizmet sağlayıcı ve tedarikçi yönetimi işletmenin siber saldırılar sonucu itibarinin zedelenmemesi adına ne kadar önemli olduğu bir kez daha görülmektedir. Tüm bu olumsuzluklar ele alındığında işletmelerin güçlü ve etkin bir üçüncü taraf programına sahip olmaları birbirine bağlılığın artığı bu çağda kritik öneme sahiptir (EY, 2020, s. 3).

- Yıkıcı İnovasyon: Birçok alanda olduğu gibi yıkıcı teknolojilerle beslenen yenilikçi iş modellerinin kullanıldığı bir çağdayız. İşletmeler gelişmekte olan teknolojileri benimsemeye devam ederken bu teknoloji ile ilgili riskleri değerlendirmesi ve bir bakış açısı kazanması zorunluluk haline gelmiştir (Deloitte, 2017a, s. 2). Dolayısıyla bu risk grubu ile inovasyondan işletmelerin yararlanmaya hazır olup olmadığını ve aksamalara uyum sağlayıp sağlayamadıklarını incelenmektedir (IIA, 2021, s. 5). Teknolojiden kaynaklı risklerin önlenmesi veya tespit edilmesi adına uygun kontrollerin uygulandığına ilişkin üst yönetime güvence verme görevi iç denetime düşmektedir. (Deloitte, 2017a, s. 2).
- Sosyal Sürdürülebilirlik: OnRisk 2021 raporuna göre "Sürdürülebilirlik" başlığı altında ele alınan bu risk şöyle ifade edilmiştir. Kurumsal karar alma sürecinde çevresel, sosyal ve yönetişim (Environmental, Social, Governance-ESG) bilinci giderek daha fazla etkiye sahiptir. Bu risk, kuruluşların uzun vadeli sürdürülebilirlik konularını ele almak için stratejiler oluşturma yeteneklerini incelemektir (IIA, 2020c, s. 5). OnRisk 2022 raporunda ise daha çok kurum içi çalışanlar ve toplum üzerindeki etkiye odaklanılarak sürdürülebilirliğin sosyal boyutu ele alınmış ve çevresel boyutu ayrıca bir risk olarak ifade edilmiştir. Kurumların istihdam ettikleri, değer zincirlerinde çalışanlar, ürün ve hizmetlerini tüketen ve toplumlarında yaşayan bireyler üzerinde önemli etkileri olduğu giderek daha fazla kabul görmektedir. Bu risk, kuruluşların eylemlerinin bireyler ve

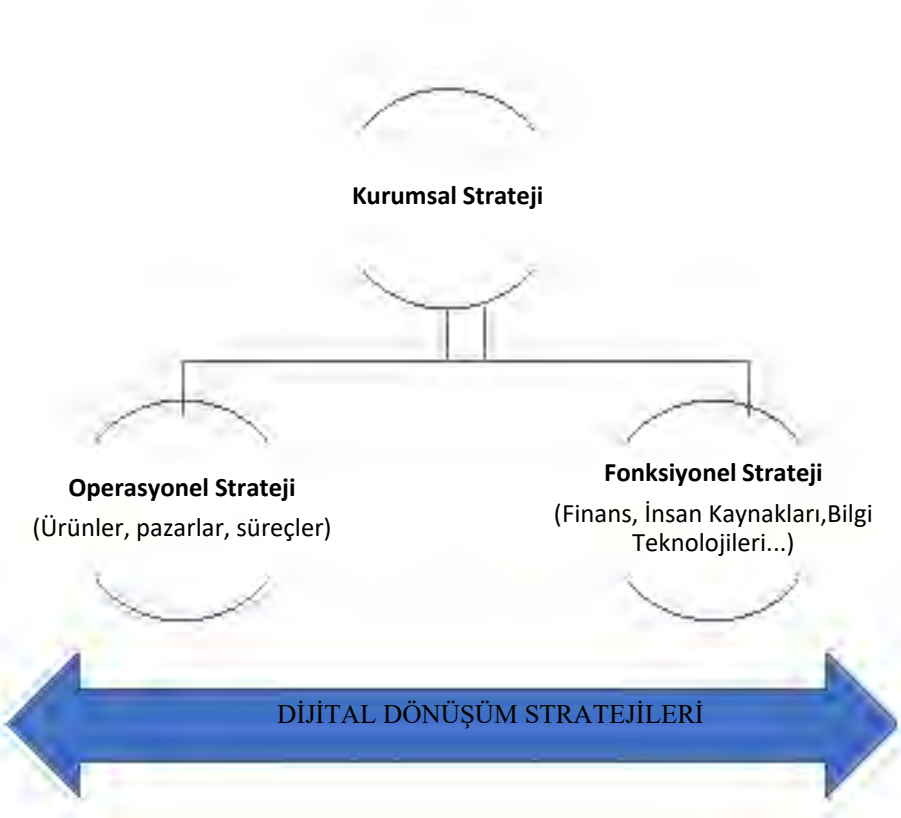
topluluklar üzerindeki doğrudan ve dolaylı etkilerini anlama ve yönetme yeteneğini incelemektedir (IIA, 2021, s. 5).

- Tedarik Zinciri Kesintisi: Tedarik zinciri kesintisi riski OnRisk 2021 raporunda ifade edilmemektedir. Bunun temel sebebi rapor için verilerin pandemi öncesinde toplanmış olması olabilir. 2019 yılı itibariyle dünyada pandeminin etkileri düşünüldüğünde tedarik zinciri kesintisinin riskler arasında sıralanması doğaldır. Kökleri küresel pandemiden kaynaklanan küresel çapta olağan iş operasyonlarının kesintiye uğraması, kuruluşların stratejik hedeflere ulaşmasını desteklemek için tedarik zincirlerinde esnekliğe duyulan ihtiyacın altını çizilmektedir. Bu risk, kuruluşların mevcut ve gelecekteki tedarik zinciri kesintilerine uyum sağlama esnekliğini oluşturup oluşturmadığını incelemektedir (IIA, 2021, s. 5).
- Çevresel sürdürülebilirlik: İşletmeler, faaliyet gösterdikleri çevreyi nasıl etkilediklerini değerlendirmek ve açıklamak konusu hissedarlar, düzenleyiciler, müşteriler ve çalışanlar olmak üzere tüm paydaşlar yönünden ilgi konusudur. Bu risk, kuruluşların çevresel etkilerini güvenilir bir şekilde ölçme, değerlendirme ve doğru bir şekilde raporlama yeteneğini incelemektedir (IIA, 2021, s. 5).

Küresel ve teknolojik yaşanan gelişmeler kurumlar arasında rekabeti artırmanın yanında işlerin daha etkin ve maliyetlerin daha düşük olmasının önemini artırmıştır. Bu rekabet ortamında kurumlarda yaşanan teknolojik gelişmeler ile birlikte iş süreçlerini elektronik ortama aktarmalarından kaynaklı bilgi sistemlerindeki karmaşıklık artmıştır. Bilgi sitemleri rutin işlerin verimli şekilde yürütülmesi, süreçlerin otomatikleştirilmesi, iş süreçlerinin analiz edilmesinden yeniden tasarlanmasına kadar birçok değişimi ve faydayı beraberinde getirmiştir (Sağlam ve Orhan, 2020, s. 191). Diğer taraftan kurumlardaki teknolojik yenilikler birçok riski de beraberinde getirmiştir. Kurumların karşılaştığı risklerin başında siber güvenlik görülmektedir. Siber güvenlik riskinin ardından literatürde en çok dile getirilen risk faktörü ise yetenek yönetimi görülmektedir. Bunun tesadüf olmadığı dijital dönüşümden kaynaklı yaşanan değişimin iş gücü yeteneklerini de değişime ve gelişime zorlamaktadır.

2.4. Kurumlarda Dijital Dönüşüm Süreci ve Kurum Fonksiyonları Üzerinde Etkisi

Dördüncü sanayi devrimi ve bunun altında yatan Endüstri 4.0 olarak bilinen dijital dönüşüm katlanarak ilerliyor (Ghobakhloo, 2020, s. 1). Yapay zeka, nesnelerin interneti, blokzincir, büyük veri, bulut bilişim vb. çeşitli teknolojilerin gelişmesi ve bütünleşmiş çalışabilmesi sonucu kurumlar "Dijital Dönüşüm" olarak ifade edilen dijitalleşme dönemine girmişlerdir (Klein, 2020, s. 1014). Dijital dönüşümün kurumlara verimlilik, kalite, hız vb. konularda avantaj sağlayarak rekabet üstünlüğü kazandırmaktadır. Türkiye dahil birçok ülkede dijital dönüşüm konusunda kendilerine bir yol haritası belirleyerek bu sürecin etkili yönetimi sağlanması amaçlanmıştır (Babaoğlan, 2019). Kurumlar açısından dijital dönüşüm konusu ele alındığında bu konunun kurumsal kaynak planlaması yazılımlarına geçiş veya donanımsal yatırımlar şeklinde yanlış bir algının mevcut olduğu görülmektedir. Oysaki dijital dönüşüm konusu sadece yazılımsal bir yenilik olmaktan öte çok kapsamlı bir konudur. Dolayısıyla bu süreç sadece temel iş süreçlerinin değişmesinden öte, geniş kapsamlı bir konudur. Kurumlar için dijital dönüşüm konusu yeni bir organizasyon ve süreç yönetimi yapısı tasarlamak, yeniden yapılanma modelidir. Bu noktada kurumların dijital dönüşüm anlayarak ve bu süreci planlı şekilde yürütmeleri önemlidir. Dijital dönüşümün sağladığı yararları göz önüne alarak işletmeler stratejik hedeflerine dijital dönüşüm konusuna eğilmelidirler (Kaya, 2018). Dijitalleşmenin potansiyel faydaları çok yönlüdür. Dijitalleşme satış veya üretkenlikteki artışları, değer yaratmadaki yenilikleri ve diğerlerinin yanı sıra müşterilerle yeni etkileşim biçimlerini içermektedir (Matt, Hess and Benlian, 2015, s. 339). Dolayısıyla dijital dönüşüm işletmeleri birçok yönden etkileyen; tedarikçi, müşteri ve çalışan ilişkilerini, iş değer zincirlerini ve tüm iş süreçlerini, aynı zamanda değer sunma ve gelir kazanma şekilleri olan iş modellerini ve ayrıca örgütsel yapıyı, liderlik anlayışını, çalışma şekillerini kapsayacak yönde kapsamlı ve yıkıcı bir dönüşümdür (Klein, 2020, s. 1014). Sonuç olarak, tüm iş modelleri yeniden şekillendirilebilir veya değiştirilebilir. Bu geniş kapsamlı sonuçlara bağlı olarak, dijital dönüşüm stratejileri, dijital dönüşümün birçok bağımsız iş parçacığını koordine etmeye ve önceliklendirmeye çalışır. Şekil 1.7'de de görüldüğü üzere şirkete yayılma özellikleri göz önünde bulundurularak, dijital dönüşüm stratejileri diğer iş stratejilerinin ötesine geçmektedir ve bunlarla uyumlu hale getirilmelidir (Matt, Hess and Benlian, 2015, s. 339).



Şekil 1. 7. *Dijital dönüşüm stratejileri ve diğer kurumsal stratejilerle arasında ilişki (Matt vd., 2015, s.340' dan uyarlanmıştır.)*

Dijital dönüşüm stratejisi, tüm dijital dönüşüm yolculuğunda bir kuruma rehberlik eden kapsamlı ve şirket çapında bir strateji olarak kabul edilir. Bu nedenle, işlevsel düşünceyi aşar ve mümkün kılan dijital teknolojilerle ilişkili fırsatları ve riskleri bütünsel olarak ele almaktadır (Ismail, Khater and Zaki, 2017, s. 14). Kurumların dijital dönüşüm stratejileri farklı bir perspektife sahiptir yani yeni teknolojiler sayesinde ürün, süreç ve yapısal yönlerin dönüşümünü kapsayacak yönde bir bakış açısına sahiptir (Matt, Hess and Benlian, 2015, s. 339). Dijital dönüşüm stratejisi oluşturma aşamasında birtakım adımlar vardır. Bunlar (Albukhitan, 2020, s. 668-671):

- **Dijital dönüşüm vizyon ve hedeflerinin oluşturulması:** Kurumların dijital dönüşüme başlama aşamasında öncelikle vizyon ve hedefler belirlemedirler. Bu noktada kurum uzun vadede hedefler belirleyerek müşteri ve çalışanları ile birlikte sahip olmak istediği deneyimlere odaklanmalıdır. Bu noktada mevcut yapıdaki eksiklikler belirlenerek iyileştirmek için bir yol haritası oluşturulmalıdır. Dijital dönüşüm sürecinde yapılan iki temel hata mevcuttur. Birincisi, kurumdaki dönüşüm süreci inovasyon departmanı veya bilgi teknolojileri departmanı gibi tek bir

departman tarafından onaylanan teknolojiyi kapsayacak şekilde bir yol izlenmesidir. İkinci hata ise kurumların sahip olduğu yetenek veya ekosistem[4] ile başlamayı tercih etmesi veya küresel amaçları olmayan gelişmeler ve özel problemlerden kaynaklı ihtiyaçtan dolayı bir yol izlenmesidir. Bu iki hata sonucu entegre edilmesi ve kurumlara yayılması zor olan izole teknolojilerin oluşmasına neden olmaktadır. Bu nedenle kurumlarda dijital dönüşüm tüm kurum kapsamında entegrasyonun sağlanması adına vizyon ve hedeflerin belirlenmesi ile başlanılmalıdır.

- **Kurumların dijital yeteneğini değerlendirme:** İlk adım ile kurumların dijital dönüşüm ile neyi başarmak istediği belirlenir. Bundan sonraki süreçte kurumların altyapısı değerlendirilmeli, sisteminin, yazılım uygulamalarının ve araçlarının mevcut ve gelecekteki ihtiyaçları karşılamada ne kadar yeterli olduğu araştırılmalıdır. Kurum bu adımıyla dijital dönüşüm stratejisi için gerekli kritik bileşenleri değerlendirerek belirleyecektir. Bu değerlendirme sonucu kurum hangi teknolojileri güncellemesi gerektiği, otomatikleştirme veya optimize edilmesi gereken süreçleri, değiştirilmesi gereken araçları belirlemiş olacaktır. Sonuç olarak kurum dijital dönüşüm stratejisi için görevleri, yatırımları ve girişimleri seçecektir.
- **Kullanıcı/Müşteri ve çalışan deneyimlerini tasarlama:** Kurum vizyonu belirledikten ve dijital yeteneğini değerlendirdikten sonra çalışan ve müşteri için bir tür deneyim geliştirme adımına geçilir. Bu noktada çalışanların işlerini basitleştiren veya yeni uygulamalar, işlevler ve sistemler yoluyla kolaylaştırmasını kapsayacak yönde bir dönüşümün tasarlanması tercih edilmelidir. Aynı şekilde dijital dönüşüm sonucu uygulamaların müşteri beklentilerini karşılayacak ve deneyimlerini iyileştirecek şekilde tasarlanmalıdır.
- **Tedarikçileri (teknoloji sağlayıcısı) ve çözüm yolları inceleme ve seçme:** Geliştirilen hedeflere ulaşmak, beklenen deneyimlerde başarıyı yakalamak mevcut teknolojideki boşlukları doldurmak adına bu adımda tedarikçilerin (teknoloji sağlayıcısı) değerlendirilmesi ve seçimi yapılacaktır.

[4]Ekosistemler, farklı kurumların yeni iş modelleri sunabilmek için gerçekleştirdikleri dijital ortaklıklardır.

Tedarikçinin seçimi aşamasında gerekli yetkinliğe sahip olup olmadığı, ihtiyaç halinde kuruma yanıt verme süresi ve satış sonrası destek kabiliyeti gibi faktörler değerlendirilmelidir.

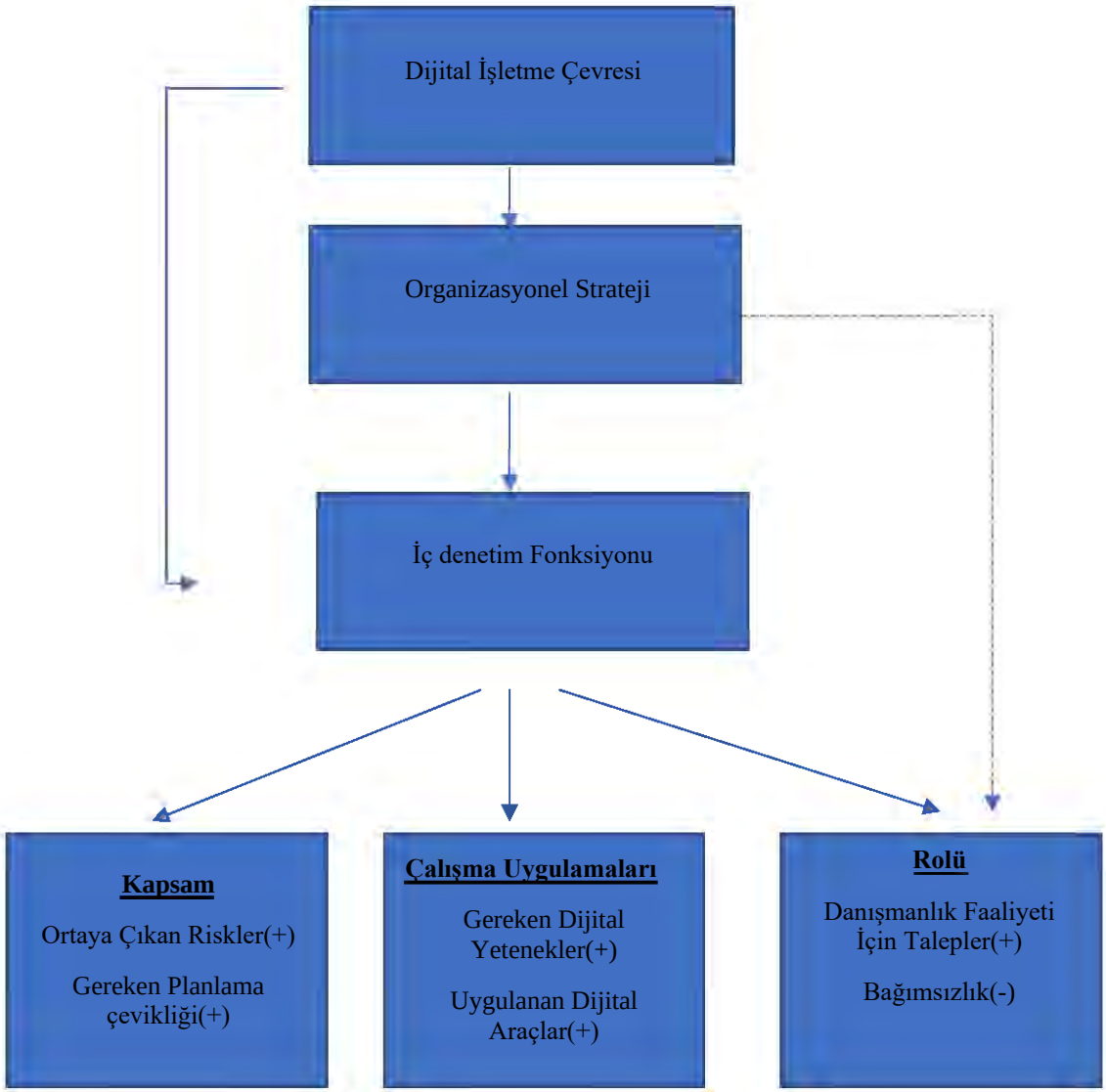
- **Uygulama yol haritasının oluşturulması:** Bu aşama, belirlenen hedefleri, beklenen deneyimleri, mevcut teknolojiyi, potansiyel çözümleri derleyerek bunları eyleme geçirecek bir plan halinde birleştirme kısmıdır. Bu dijital dönüşüm girişimlerinin gerçekleştirilmesi zaman ve kaynak (insan ve sermaye) gerektirmektedir. Dolayısıyla dikkatlice plan yapılması önemlilik arz etmektedir. Kurumdaki birçok uygulamanın sorunsuz yürütülmesindeki gerekli olduğu gibi iş operasyonlarındaki rahatsızlıkları minimize etmek ve dijital dönüşüm girişimlerine gerekli desteği sağlamak adına planlama yapılırken üst yönetimden çalışanına kadar tüm kademeden katılım ile desteklenmelidir.
- **Organizasyon kültürünü ve altyapı adaptasyonu:** Kurumların dijital dönüşüm stratejisini geliştirmesindeki son adım altyapısının hazırlamasıdır. Altyapısının hazırlanması ifadesinden kasıt, kurumların başarılı bir dönüşüm gerçekleştirmesi adına nitelikli uzmanlardan oluşan özel bir ekibin oluşturulmasıdır. Bu ekip işletme içinden ilgili yetkinliğe sahip kişilerden oluşturulacağı gibi dijital dönüşüm stratejisini etkili bir şekilde yürütecek işletme dışından güvenilir bir ekipten de destek alınması şeklinde tercih edilebilir. Bu ekip ile hem kurum içi gelecekteki değişikliklere uyum sağlanması adına yetkinliklerin sağlanması aşamasında hem de yeni işe alım süreçlerinde çok önemlidir. Ayrıca bu aşamada yapılan çalışmalar, dijital dönüşümün kurumların yüksek seviyedeki hedeflerinin önemli bir bölümünü yapmak adına önemlidir.

Kurumlar faaliyetlerini sürdürürken yerine getirmeleri gereken birçok fonksiyon bulunmaktadır. Yukarıda ifade edildiği üzere Endüstri 4.0 teknolojileri ile birlikte dijital dönüşüm sürecinin başta üretim olmak üzere işletmenin tüm fonksiyonları üzerine etkisi kaçınılmazdır. Çalışmanın kapsamı itibariyle iç denetim fonksiyonun ele alınması sebebiyle diğer işletme fonksiyonlarına ilişkin kısaca açıklama yapılarak ağırlıklı olarak bu kısımda dijital dönüşüm ve iç denetim fonksiyonu ele alınacaktır.

Dördüncü sanayi devriminin başlıca etkisi üretim alanındadır. Ağırlıklı olarak otomasyona dayalı ve entegre sistem ile girdilerin ürün ve hizmete dönüştürülmesinde köklü değişiklikleri barındıran etkileri mevcuttur. Bu kapsamda özellikle makine gücünün insanın yerini almasıyla makinelerin kendilerini yönetebildiği ve birbiriyle etkileşime geçtiği akıllı üretim olarak ifade edilen sistemler oluşacaktır. Dijital dönüşüm sonucu üretimde yaşanan bu değişim sonucu olarak bugünkü işletmelerin yerini alacak olan akıllı fabrikalar gelişimini sağlayacaktır. Dolayısıyla kurumlarda yaşanan dijital dönüşüm sonucunda katma değeri yüksek ürünlerin daha düşük maliyette üretilmesi; insan hatasının ortadan kaldırılması ile birlikte daha az fire, yüksek kalite ve verimlilik artışı, üretimde esnekliğin sağlanması, ürünün üretimden pazara sunulmasına kadar olan sürecin kısalması gibi faydalar sağlayacaktır (Bolat, 2019, s. 47-48). Endüstri 4.0 teknolojileri ile yaşanan dijital dönüşüm sürecinden işletmenin bir diğer etkilenen fonksiyonu, pazarlama fonksiyonudur. Teknolojideki değişimler sonucu tüketici tatminini etkileyen yeni uygulamalar ortaya çıkmıştır. Pazarlamadaki yaşanan gelişmeler sonucu bugün pazarlamanın evrilerek Pazarlama 4.0'a dönüştüğü görülmektedir (Büyükkalaycı ve Karaca, 2019, s. 463). Endüstri 4.0 teknolojileri pazarlama alanında birçok konuda avantaj sağlamaktadır. Günümüzde tüketici ürünün bir parçası olmak ve ürün ile etkileşimde olmak istemektedir. Örneğin; yapay zeka pazarlama alanında birçok yönde etkilemektedir. Gelişmiş makine öğrenme algoritmaları pazarlamacıların zorlandığı konularda yardımcı olmaktadır. Büyük miktarda toplanan verilerden tahminler yapılmakta ve ürüne müşterinin ne kadar ödeme yapacağı ya da hangi ürüne daha çok yöneleceği konusunda tahminler yapılmaktadır (Bayuk ve Demir, 2019, s. 787-788). Bunun yanında tüketicinin ürünle etkileşiminin sağlanması nesnelerin interneti ile sağlanacaktır. RFID, NFC ve kare kodlar gibi teknolojiler tüketicinin ürünle etkileşimini sağlayan teknolojiler arasındadır (Büyükkalaycı ve Karaca, 2019, s. 473). Bunlar pazarlanma alanında Endüstri 4.0 teknolojilerinden faydalandığı sadece birkaç örnektir. Özetle müşterilerle etkileşim kurabilme, karar verme sürecinde müşterilerle ilişkilerde devamlılık sağlayabilme, fiyatlandırma, tanıtım ve marka iletişim konularında dijital dönüşümün etkisinin olduğu söylenebilir (Bayuk ve Demir, 2019, s. 796). Muhasebe üzerinde endüstri 4.0'ın etkisine bakıldığında öncelikle bilgi sistemindeki veri akışının otomatik olarak sağlanması sonucu hızlı ve güvenilir bilgiye ulaşma kolaylaşacak ve denetim faaliyetleri daha sağlıklı ve şeffaf şekilde yürütülecektir (Yürekli, Gönen ve Şahiner, 2016, s. 300; Rasgen ve Gönen, 2019, s. 2907). Endüstri 4.0 teknolojilerinin

kullanımı insan hatasını minimize etmeye yardımcı olacaktır. Endüstri 4.0'ın işletmenin fonksiyonlarına etkisi olduğu gibi hem bağımsız denetim hem de iç denetim üzerinde etkisi olacaktır. Dijitalleşme ile birlikte kurumlarda fiziksel olarak bulunmadan denetim gerçekleştirme imkanı olacaktır. Nesnelerin interneti ile denetim sözleşmelerinin bile uzaktan imzalanacak, işletmelerden gelen veriler denetlenecek, denetlenmiş veriler sisteme yüklenecektir. Finansal kayıtlarla ilgili belgelere denetçiler yine aynı sistemlerden ulaşacaktır. Süreçlere ilişkin belgelendirme elektronik yapılacak ve manuel yapılananlar taranarak yüklenecektir. Koordinasyon içinde gerçekleşen anlık olarak denetlenen finansal tablolar her an hazırlanabilecek ve sürekli denetim faaliyeti uygulanabilecektir. Dipnotların üretilmesinde yine Endüstri 4.0 teknolojilerinde nesnelerin interneti kendiliğinden üretilmesini sağlayacaktır (Kablan, 2018, s. 1570). Özellikle bilgi sistemlerinin otomatikleştirilmesi ve yeni teknolojilerin denetim süreçlerinde sağladığı kolaylıklar itibariyle daha kaliteli finansal tabloların hazırlanmasında ve etkin bir denetim gerçekleştirilmesinde katkı sağlayacaktır.

Uluslararası iç denetim standartları 2120.A1'e göre "İç denetim faaliyeti, kurumun stratejik hedeflerine ulaşması ile ilgili olarak kuruluşun yönetişimi, operasyonları ve bilgi sistemleri ile ilgili riskleri değerlendirmek zorundadır." ifadesi iç denetimin kuruma stratejilerinde karşılaşabileceği risklere ilişkin güvence vermesindeki rolünü açıklamaktadır (IIA, 2017a, s. 16). Dolayısıyla işletmelerin stratejilerinde önemle yerini alan dijital dönüşüm konusunda iç denetime de büyük rol düşmektedir. İç denetiminin hizmetlerinden biri olan danışmanlık görevi kapsamında öncelikle yönetim kurulu ve icrai yönetim kademelerinin dijital dönüşüm hakkında bilgilendirilmesi, farkındalık oluşturulması gerekmektedir. Bunun yanında dijital dönüşüm planlarının yapılmasında üst yönetimin ve tüm birimlerin katkısı sunulması aşamasında görevleri mevcuttur. Dijital dönüşüm sürecinde iç denetimin görevini etkin şekilde yerine getirmesi adına bu alanda kendini geliştirmesinin önemi büyüktür (Kaya, 2018). Dijital dönüşüm sonucunda değişen iş çevresi karşısında iç denetimin nasıl etkilediği üzerine Betti ve Sarens (2021, s. 210) tarafından Şekil 1.8'deki model ile özetlenmiştir.



Şekil 1. 8.*İç denetim fonksiyonu üzerinde dijital işletme çevresinin etkisi(Betti ve Sarens, 2021, s.210)*

Bu çalışma kapsamında dijitalleşmenin iç denetim fonksiyonunu üç alanda etkilediğine ulaşılmıştır. Bunlar: iç denetim fonksiyonun kapsamı, iç denetimin rolü ve iç denetimin fonksiyonunun çalışma uygulamaları. Dijitalleşme iç denetimin kapsamını yönelik değişiklik, işletmelerin rekabet avantajı sağlamak amacıyla dijitali stratejilerine eklemeleri sonucu yeni risklerle karşı karşıya kalmasına neden olmaktadır. Bu riskler kullanılan teknolojinin bozulmasından kaynaklı kurum içi riskler olabileceği gibi siber riskler şeklinde kurum dışından kaynaklı olabilirler. Sonuç olarak iç denetim fonksiyonunun kurum ile sınırlı kalmayıp kapsamı genişlemiştir. Bunun yanında bugünün iş ortamının değişken, belirsiz, karmaşık ve muğlak (Volatility, Uncertainty, Complexity, Ambiguity-VUCA) özelliklere sahip olması (Schoemaker, Heaton and Teece, 2018, s. 15) ve yeni ortaya çıkan risklere karşılık verebilmesi adına denetim

planının daha çevik olması gerekmektedir. İkinci olarak dijitalleşme ile birlikte iç denetimin rolünde de değişiklik yaşanacağına ulaşılmıştır. Üst yönetimin bu noktada iç denetim fonksiyonunda dijital dönüşüm ile birlikte sadece güvence faaliyetlerini benimseyen bir kontrolör rolünden ziyade kullanılan teknoloji ile birlikte yaşanmış ya da yaşanması muhtemel zorluklar ile yüzleşmede daha çok danışmanlık faaliyetine ihtiyacı vardır. Aynı zamanda iç denetim fonksiyonunun stratejilerin tanımlanması aşamasında rol almamaları gerektiği ancak dijitalleşmeden kaynaklı kurumların danışmanlık faaliyetine ihtiyacının artması sebebiyle iç denetimin işletme stratejileri üzerinde dolaylı bir şekilde de olsa etkiye sahip olmasına neden olmaktadır. İç denetimin danışmanlık faaliyetine ilişkin artan talep sonucunda bağımsızlık ve danışmanlık faaliyetinin yarattığı katma değer arasında bir bölünmüşlüğün yaşanmasına neden olmaktadır. Üçüncü olarak dijitalleşme iç denetim fonksiyonunun çalışma uygulamalarını etkilemiştir. Bu aşamada dijitalleşme iç denetim çalışmalarının pratikleştirecek araçların kullanımı yönünde etkileyecektir. Kullanılan teknolojinin tüm veri setlerini test etme imkanı vermesi sebebiyle raporlamanın önemli ölçüde doğru olmasını sağlayacaktır. Ayrıca iç denetçilerin analize ayırdığı zamanı da azaltacaktır. İç denetçilerin yeni teknolojileri kullanımı anormalliklerin gelecekte kurumu nasıl etkileyeceğine yönelik derinlemesine ve gelişmiş tahminlere dayalı analizlerin yapılmasına imkan verecektir. Diğer taraftan iç denetimde teknolojinin kullanımı hem kurulum maliyetlerini hem de iç denetçiler için gerekli becerilerin kazandırılmasının maliyetini ortaya çıkarmaktadır. Çünkü dijital dönüşüm ile birlikte dijital beceriler iç denetim departmanları için önemli hale gelmiştir (Betti & Sarens, 2021, s. 202-208). Özetle dijital dönüşüm hem kurumların risk alanlarını genişletip hem de bu risk alanlarına ilişkin danışmanlık faaliyetine daha fazla ihtiyacı artırmıştır. Ayrıca teknolojideki gelişim iç denetim faaliyetlerinin daha etkin yürütülmesi konusunda katkı sağlayacaktır.

İKİNCİ BÖLÜM

İkinci bölümde dijital dönüşüm ile birlikte iç denetim fonksiyonu, yaşanan değişim ve dijital dönüşüm sürecinde kurumların karşılaştığı riskleri doğru yönetmeleri yönünden iç denetimin üstlendiği rol çerçevesinde bilgiler sunulmuştur.

2. DİJİTAL DÖNÜŞÜM SÜRECİNDE İÇ DENETİM ALANINDAKİ GELİŞMELER

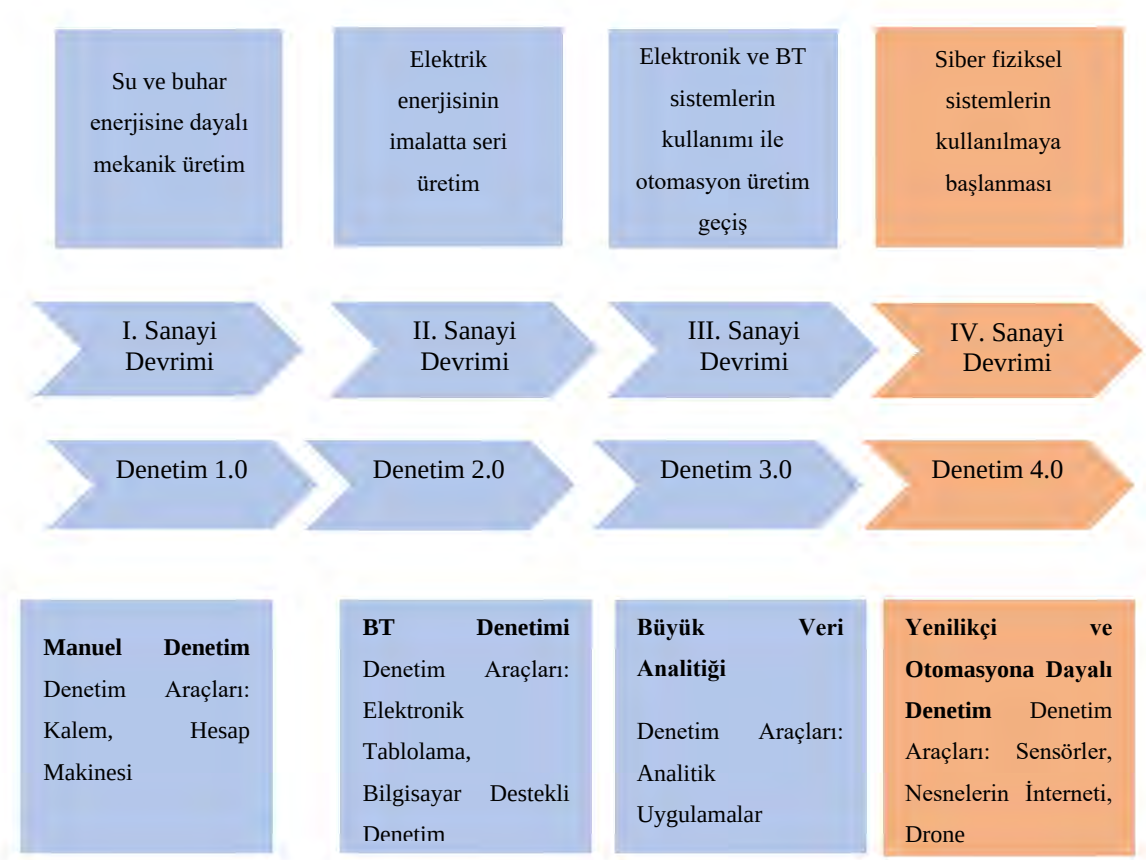
Dünyayı etkisi altına alan yeni teknolojilerin, dijitalleşmenin ve yapay zekânın iş dünyasını çarpıcı biçimde değiştirdiği dördüncü sanayi devriminin hem özel hem kamu sektöründe teknoloji ve inovasyon odaklı, yıkıcı değişimin yaşandığı bir geleceğe doğru sürüklemektedir. Bir taraftan teknolojik gelişmenin yaşanması diğer taraftan COVID-19 salgınının dünyayı etkisi altına alması kurumların teknolojiye adaptasyonunu hızlandırmıştır. Bu teknolojik gelişmelerden kaynaklı kurumların hali hazırda risklerinin yanında yeni stratejik, itibar, operasyonel, finansal, düzenleyici ve teknolojik risklerle karşı karşıya kalmaktadır. Tüm bu yaşanan gelişmeler, iç denetimin güvence ve danışmanlık işlevinin etkili şekilde yürütülmesi için yeni bir vizyon geliştirmesini zorunlu kılmıştır. Dolayısıyla bu yeni süreçte iç denetimin de paydaşların ihtiyaçlarını karşılayacak yönde kendini güncellemesi, yeni özellikleri ve işlevleriyle sürdürülebilir olması, kabul görmesi gerekmektedir (Deloitte, 2018a, s. 2). Bu bağlamda bu bölümde, teknolojinin gelişmesi ve iç denetim bu kapsamda nasıl bir dönüşüm yaşadığı, iç denetimin dijital dönüşüm süreci ile birlikte nasıl bir rol üstlendiği, iç denetçinin taşıması gereken özellikler, kullanılan yeni teknolojiler, uluslararası ve ulusal düzenlemeler konuları ele alınacaktır.

2.1. Denetim 1.0'dan Denetim 4.0'a Yaşanan Gelişmeler ve İç Denetim

Sanayi devrimleri ile yaşanan gelişmelerin birçok konuda üzerinde etkisi olduğu gibi denetim alanında da gelişmelerin yaşanmasında etkili olmuştur. Sanayi devrimleri ve denetim alanındaki gelişmeler incelendiğinde yaşanan teknolojik gelişmelerin denetime yansıdığı Şekil 2.1'de gösterilmiştir. Denetim 1.0 incelendiğinde uzun zaman kullanılan geleneksel manuel denetimleri kapsayan süreçtir. Denetimde bilgi teknolojilerinin benimsendiği dönem Denetim 2.0 olarak ifade edilmektedir. Denetim 2.0 döneminde kullanılan denetim araçları elektronik tablolama, bilgisayar destekli denetim yazılımı örnek gösterilmektedir. İşletmelerin bilgi teknolojilerini benimsemesi denetim ile kıyaslandığında daha hızlı olduğuna ulaşılmıştır. Denetimin bilgi teknolojilerini

benimsemesinde yaşanan gecikmenin temelinde denetim alanındaki profesyonellerin muhafazakarlığı ve teknoloji kullanımındaki katılığı yatmaktadır. 2000'li yıllarla birlikte teknolojideki gelişimin verinin miktarı, çeşiti, hızı ve boyutunda artışın yaşandığı ve mevcut denetim tekniklerinin yetersiz kaldığı bir dönemi ifade etmektedir. Bundan kaynaklı Denetim 3.0 dönemi verideki değişime cevap verecek şekilde mevcut istatistiklerin yanında büyük veri analizlerinim kullanıldığı bir dönemi ifade etmektedir (Dai J. , 2017, s. 32-33; Yıldız ve Ağdeniz, 2019, s. 89).

Denetim 4.0' a gelindiğinde finansal ve operasyonel bilginin yanında ilişkili taraflardan denetimle ilgili verilerin toplanması aşamasında nesnelerin interneti, hizmetlerin interneti, siber fiziksel sistemler vb. teknolojiler kullanılmaktadır. Denetim 4.0 etkili, verimli ve gerçek zamanlı güvence sağlamak amacıyla örnekleri geliştirmek, anormallikleri tanımlamak ve diğer yararlı bilgileri çıkarmak için verileri analiz eder, modeller ve görselleştirir (J. Dai , 2017, s.32). Böylece denetimin sağlamış olduğu güvence hem gerçek zamanlı olmakta hem de artmaktadır. Yıldız ve Ağdeniz (2019, s. 90) tarafından Denetim 4.0'da risk ve risk yönetimi ile danışmanlık faaliyetleri denetçinin temel odak noktası haline geldiği vurgulanmaktadır.



Şekil 2. 1. *Sanayi devrimleri ve denetimin periyodik gelişimi (Dai & Vasarhelyi, 2016, s.2'den uyarlanmıştır.)*

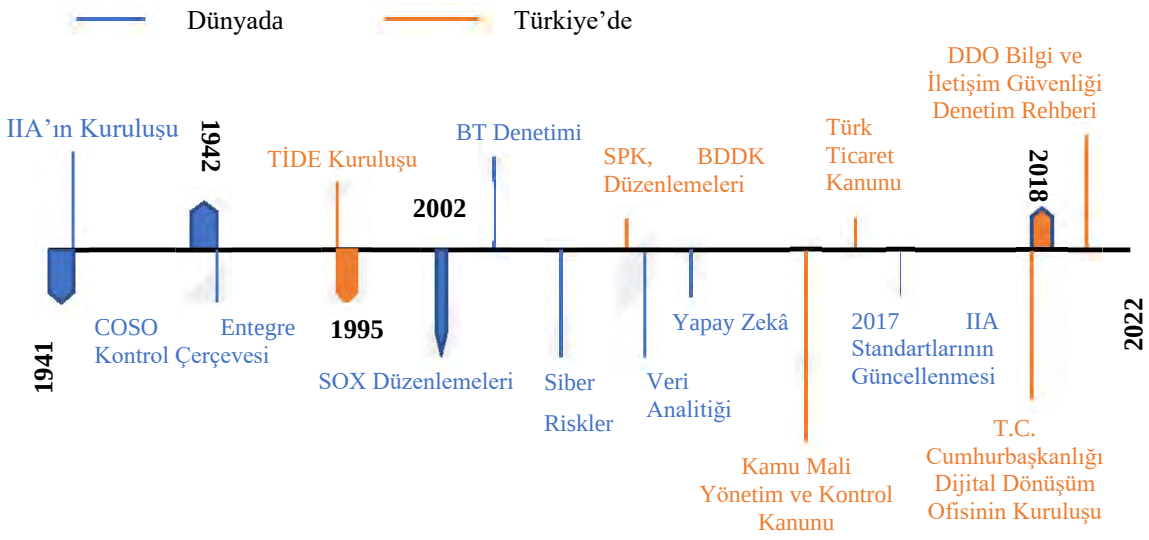
İç denetim özelinde gelişmeler ele alınırsa sanayi devrimleri gibi keskin geçişlerle ayrılmamış ve literatürde ayrıntılı bilgiye yer verilmemiştir. Şekil 2.2'de iç denetimin dünyada ve Türkiye'de periyodik gelişimi sunulmuştur. Buna rağmen modern iç denetimin doğuşuna bakıldığında 1944 yılında Uluslararası İç Denetçiler Enstitüsü'nün (The Institute of Internal Auditor-IIA) kuruluşu İç Denetim 1.0'ın başlangıcı olarak kabul edilir. 2002 yılında Sarbanes Oxley düzenlemeleri muhasebe ve denetim alanındaki etkileri İç Denetim 2.0 olarak ifade edilmektedir.

İç denetimin Türkiye'deki gelişmeleri ele alındığında (Uzun, 2018, s. 70):

- 1995 yılında Türkiye İç Denetçiler Enstitüsü'nün (TİDE) kurulması ile iç denetim mesleğinin gelişiminde atılan bu adım İç Denetim 1.0 olarak ifade edilmektedir. Türkiye'de iç denetim mesleğinin başlangıcı olan bu tarihe bakıldığında bu kapsamda 54 yıllık bir gecikmenin olduğu görülmektedir. TİDE ile birlikte Kurumsal Yönetim, Sermaya Piyasası Kurulu (SPK), Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), Kamu Mali İç

Kontrol Kanunu ve Türk Ticaret Kanunu iç denetimde önemli gelişmeler sağlamıştır.

- İç denetim 2.0 Türkiye boyutu ele alındığında dünyadaki iç denetim gelişmeleri ile birlikte bir gelişme yaşandığı ve İç Denetim 1.0'da yaşanan gecikmenin yaşanmadığı Uzun (2018, s. 70) tarafından ifade edilmiştir. Bankacılık alanındaki gelişmeler, Avrupa Birliği müzakere süreci finans, reel ve kamu sektöründeki kurumsal yönetim ve denetim alanındaki gelişmeler İç Denetim 2.0 olarak ifade edilmektedir.

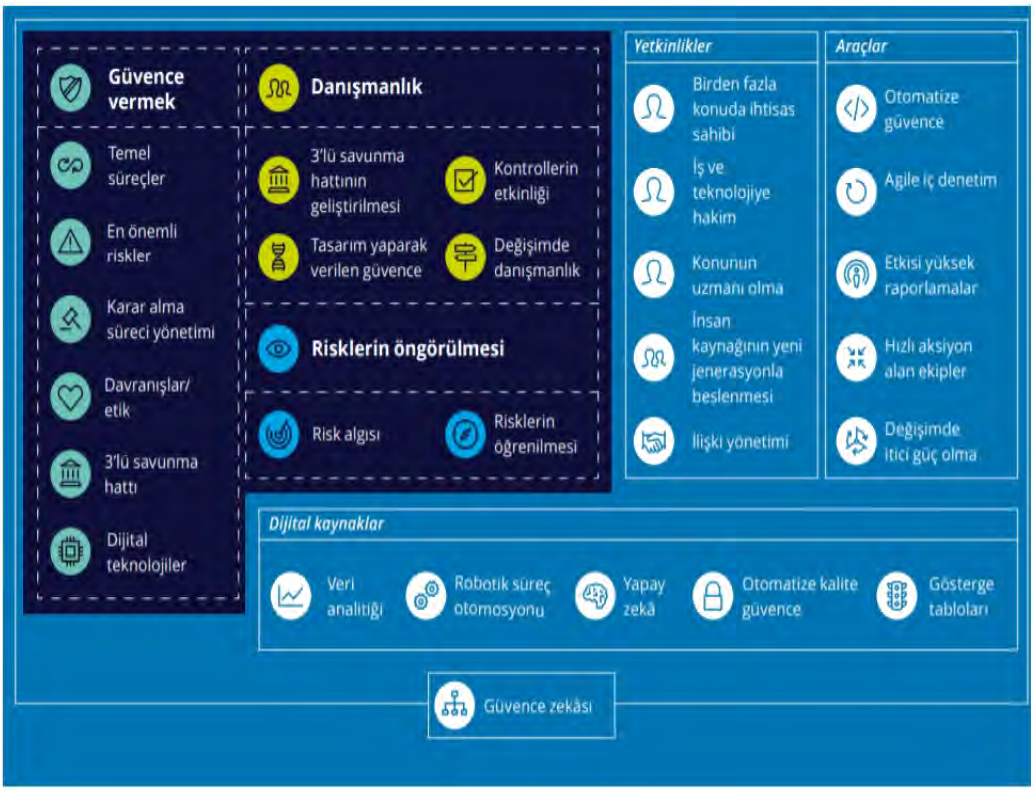


Şekil 2. 2. *İç denetimin gelişimi (Uzun, 2018, s. 70'ten geliştirilmiştir.)*

Kurumlar, giderek artan teknoloji odaklı, inovasyon odaklı, riskli ve yıkıcı bir geleceğe doğru savrulurken iç denetiminde bu noktada paydaşlarının artan ihtiyacını karşılaması gerekliliği ortaya çıkmıştır. Bu gerekliliğin arkasında yatan sebep, yeni yaklaşımlar uygulanmadan, stratejik ve teknolojik gelişmelerin arkasında, paydaşların ihtiyaçlarını karşılayamayan ve ortaya çıkan risklerle başa çıkmak için yeterli donanıma sahip olmayan bir iç denetim fonksiyonunun varlığıdır. Dolayısıyla iç denetimi yeni araç ve teknikleri benimseyen, karşılaşılan zorluklara etkili şekilde yanıt vermesi yönünde gereken yetenekleri sahip olan bir vizyon geliştirmesi önemlidir. Bu yeni vizyona sahip iç denetim, "İç Denetim 3.0" olarak ifade edilmektedir. Kurumlarda ortaya çıkan riskler, teknolojiler, inovasyon ve kesintilerin zorluklarına uyum sağlayan bir fonksiyon;

yönetime, değer yaratma ve sunmanın yeni yöntemlerini takip ederken süreçlerin ve varlıkların korunmasına tam olarak yardımcı olabilecek bir fonksiyondur. İç denetim 3.0 herhangi yararlı sürümde kendini yenileme özelliğine sahip olmakla birlikte geçmiş sürümlerin en iyilerini koruma ve kullanma özelliğine sahiptir. Bu nedenle İç Denetim 3.0, iç denetim mesleğinin ve fonksiyonun hem mevcut hem de ortaya çıkan ihtiyaçları daha iyi karşılamasını sağlayan yenilikçi bir "işletim sistemi" olarak düşünülebilir (Deloitte, 2018b, s. 1).

Teknolojideki yaşanan gelişmeler, dijitalleşmenin ve yapay zekanın iş dünyasını önemli ölçüde değiştirdiği dördüncü sanayi devrimine girilmesiyle birlikte kuruluşlar gelişen stratejik, itibar, operasyonel, finansal, düzenleyici ve teknolojik risklerle karşı karşıyadır. Dördüncü sanayi devrimi ile ilişkili risklerin türleri, karmaşıklıkları ve birbirine bağımlılıkları ve ortaya çıkma hızları yeni bir kavramdır. Bu kapsamda değer yaratması ve sunması için gelişmeye yönelik baskılar yeni olmakla birlikte COVID-19 salgını ile birlikte baskılar artmaktadır. Bunların tamamı iç denetimi, kurumlara etkili güvence ve danışmanlık hizmetleri sağlamadaki ilgisini sürdürmek için rolüne ve görev alanına ilişkin yeni bir vizyon benimsemeye zorlamaktadır. İç denetimin hizmet vurgusu ve sunum modellerinin güncellenmesi gerektiği görüşüne rağmen, güvence vermek ve danışmanlık olan temel amaçları aynıdır (Deloitte, 2018b, s. 2). Bunun yanında Deloitte tarafından 2018 yılında yürütülen çalışmada, en başarılı iç denetim fonksiyonunun sorunları önceden tahmin edecek ve proaktif güvence yoluyla kuruluşların ortaya çıkan risklere ayak uydurmasına ve bunların önüne geçmesine yardımcı olması gerektiği vurgulanmaktadır. Dolayısıyla iç denetimin amaçları güvence vermek, danışmanlık ve tahmin etmek şeklinde ifade edilmektedir. İç Denetim 3.0’ a ilişkin bakış Şekil 2.3’te gösterilmiştir (Deloitte, 2018b, s. 5).



Şekil 2. 3.*İç Denetim 3.0 - Sisteme bakış (Deloitte, 2018b, s. 5)*

Güvence iç denetimin temel rolünü oluşturmaktadır. Zaman içinde güvence altına alınacak faaliyetler, sorunlar ve risklerin yelpazesinin genişlediği görülmektedir. Bu noktada temel süreçler ve önemli riskler konusunda güvence sağlanması esastır. Bunların yanında karar yönetişimi, kurum içinde davranışların uygunluğu, üçlü hat modeli ve dijital teknoloji gözetimi konusunda güvencede önemlidir. İç denetimin diğer biri rolü olan danışmanlık kontrol etkinliği, değişim danışmanlığı, üçlü hat modelinin geliştirilmesi ile ilgili risk yönetiminde iyileştirmeler, iş etkinliği ve verimliliği dahil olmak üzere diğer konular hakkında yönetime danışmanlık yapmak iç denetimin rolü ve paydaşların beklentilerini kapsamaktadır. İç denetimin son rolü olan tahmin etme, riskleri öngörmek ve kurumların karşılaştığı riskleri anlamada ve önleyici kontroller oluşturmada yardımcı olmaktadır. Değişen koşullarla birlikte dış veri kullanımının artması sonucunda iç denetim, kurum hedeflerine ulaşılması kapsamında riski tahmin etme konusunda ideal bir konuma sahiptir. Sorunlar yaşanmadan önce neyin yanlış gittiğine veya neyin yanlış gideceğine ilişkin raporlama yapması itibariyle iç denetim daha proaktif hale gelir ve

güvence ve danışmanlık rolleri aracılığıyla yönetimin riskler gerçekleşmeden önce müdahale edilmesine yardımcı olmaktadır (Deloitte, 2018b, s. 4).

Denetçilerin artık ihtiyaç duydukları araçlara sahip olduğunu ve bu sayede özellikle örneklemden tam kapsamlı denetime ve daha da iyisi, reaktif denetlemeden proaktif denetime geçme konusunda gelişmelerin yaşanacağı görülmektedir. Teknolojideki gelişmeler denetlenen verilerdeki düzensizlikleri bulmada yardımcı olması anormallikler tespit edilecek, otomatik olarak uyarılar oluşturulacak ve bu uyarılar denetimin çalışma paketine eklenen bir çalışma kağıdına atanacaktır. Tüm bu gelişmeler İç Denetim 4.0 olarak ifade edilmektedir. Günümüzde mevcut olan yüksek hacimli veri analizi teknolojisi ile denetim ekiplerinin daha fazlasını uzaktan ve aynı kaynaklarla yapmasını sağlamaktadır. Teknolojik gelişmeler devam edeceği göz önünde bulundurulduğunda iç denetim kapsamında da gelişmelerin devam edeceği ve İç Denetim 5.0 kapsamında denetim sürecini destekleyen sohbet robotları, makine öğrenimi vb. ile yapay zekanın test edildiği şeklinde gelişmelerin yaşanacağı (Frenehard, 2020) yönünde geleceğe dönük tahminler yürütülmektedir.

2.1.1. Denetim 4.0 ilkeleri

Endüstri 4.0 altı ana ilkeden oluşmaktadır. Bu ilkeler: Birlikte çalışabilirlik, Sanallaştırma, Özerk Yönetim, Gerçek Zamanlılık, Hizmet Odaklılık ve Modülerlik. Endüstri 4.0'a benzer şekilde, Denetim 4.0, veri kullanılabilirliğini artırmak, sürekli veri izleme ve doğrulamayı sağlamak ve denetim prosedürlerinin otomasyonunu iyileştirmek için bu altı ilkeye dayanmaktadır. Endüstri 4.0 ilkeleri ve denetim ile ilişkisi aşağıda maddeler halinde açıklanmıştır (J. Dai, 2017, s. 34-40):

- **Birlikte çalışabilirlik:** Birlikte çalışabilirlik ilkesi Endüstri 4.0 teknolojileri sayesinde cihazlar, makinalar, ürünler, kurumlar kısaca değer zincirindeki tüm unsurların birlikte çalışmasını etkileşimli olmasını sağlayan küresel bir ağ aracılığıyla birbirine bağlanacak ve iletişim kuracaktır. Bu yolla gelecekte trafik ışıkları ağa bağlanarak renk ve zaman çizelgeleri konusunda bilgi sağlayacaktır. Otomobiller bu ağlardan bilgi almaları sonucu yakıt tüketimi azaltmak ve emisyonu aza indirmek adına hızlarını ayarlayacaklardır. Ayrıca navigasyon kullanımı da arabaların optimum trafik akışı sağlamasına yardımcı olması adına diğer bir örnektir (Drath and

Horch, 2014, s. 57). Birlikte çalışabilirlik mevcut iş modellerini değiştirdikçe denetimde bundan etkilenecektir. Denetim 4.0 da tedarikçiler müşteriler, bankalar ve diğer ticari kuruluşlar arasında gerçek zamanlı incelemelerin yapılmasına fırsat verecektir (J. Dai, 2017, s. 34-35).

- **Sanallaştırma:** Endüstri 4.0 teknolojileri ile nesneler ağlara bağlı olduklarından konum, koşullar, çevre hakkındaki bilgiler paylaşılabilir ve entegre edilebilir ağda araştırılabilir, keşfedilebilir veya analiz edilebilir hale gelebilir (Drath and Horch, 2014, s. 57). Dolayısıyla bu bilgilerin kullanımı ile iş dünyasında tüm nesnelerin ilişkileri ve faaliyetleri ile temsil eden fiziksel dünyanın sanal bir kopyası oluşturulabilir. Sanallaştırma ile bu dünyada her fiziksel nesnenin bir dijital temsili olup bilgileri sürekli olarak güncellenip ilgili taraflara iletecektir. Sanallaştırma tüm iş süreçleri ve performanslarının ayrıntılı olarak sunulmasıyla değer zinciri boyunca şeffaflık sağlamaktadır. Şeffaflık sağlanması sanallaştırmanın başlıca avantajıdır. Yönetim sanal süreç izleme yoluyla iş akışındaki sorunları gerçek zamanlı olarak tespit edilebilir. Dolayısıyla bu hedefleri etkileyen temel unsurlar hakkında sonuçların çıkarılmasına imkan vermektedir (Schuh vd., 2014, s. 54). Fiziksel dünyanın sanal bir kopyasını oluşturulması için teknolojiler geliştirilmiştir. Bunlardan biri de ayna dünyalar olarak Endüstri 4.0'daki sanallaştırmaya benzer bir teknolojidir. Ayna dünyaların dünyamızı modellemeye yarayan bir teknolojidir ve en bilindik örneği "Google Earth" dür. Ayna dünyalar, fiziksel dünyanın bilgiyle geliştirilmiş sanal modelleri veya yansımaları şeklinde tanımlanmaktadır. Ayna dünyaların yapıları gelişmiş sanal haritalama, modelleme, açıklama araçları, coğrafi mekan, konuma dayalı teknolojileri içermektedir (Smart vd., 2007, s. 9). Denetim açısından ele alındığında ayna dünyalarda kaydedilen bilgiler denetçilerin saha çalışmasında yardımcı olacaktır. Bir iş sürecindeki tüm nesnelerin sanallaştırılması sonucu ayna dünyadaki temsillerinin bulunmasından dolayı denetçiler yerinde incelemelerin çoğunu uzaktan ve sürekli olarak gerçekleştirebilir. Örneğin; ayna dünyalar fiziksel bir envanter kaleminin kuruma giriş ve çıkış zamanını veya zaman içinde konumunu ve koşulunu kaydedebilir. Denetçiler bu bilgileri fiziksel envanter yerine kullanabilir. Aynı zamanda

denetçiler ayna dünyadaki işlemleri kurumsal kaynak planlaması sistemleri ile karşılaştırarak kurumların oluşumu ve tamlığını inceleyebilir. Ayna dünyalar, finansal olmayan süreçleri (örneğin personel, üretim, web tıklamaları) sıralı bütünlük güvencesi sağlayan muhasebe kayıtlarına bağlamak için de kullanılabilir (J. Dai, 2017, s. 37).

- **Özerk Yönetim:** Bu ilke, bugünün üretim sisteminde tüketicilerin kişileştirilmiş taleplerinin artmasını, siparişlere uygun imalat sistemlerinin karmaşık hale gelmesini ve makinelerin merkezi olarak kontrol etmenin zor hale geldiğini ifade etmektedir (Hermann, Pentek and Otto, 2016, s. 12). Diğer bir ifadeyle Endüstri 4.0 daha fazla kişileştirilmiş ürünler, aynı ürünlerin daha fazla değişik biçimde ve daha az miktarda üretimi ifade etmektedir (Schuh vd., 2014, s. 54). Dolayısıyla tüm bunlar iş ortamını daha karmaşık ve dinamik hale getirecektir. İş ortamı daha karmaşık ve dinamik hale geldikçe denetim de etkilenecektir. Bu anlamda muhasebe verilerinin sürekli olarak izlemek ve beklenen limitleri aşan anormallikleri tespit etmek için her bir makine veya cihaza iç kontrol mekanizmaları yerleştirilebilir. Böylece bu mekanizmalar değişen ortama ve denetçilerden gelen girdilere bağlı olarak limitleri kendi başına ayarlayabilecek, hataları ve karmaşık kararları denetçilere sunabilecektir (J. Dai, 2017, s. 38).
- **Gerçek Zamanlılık:** Endüstri 4.0'da sistemdeki hataların belirlenmesi, üretim ayarlamalarının yapılması, karar alınabilmesi için nesnelerin ve üretim faaliyetlerinin sürekli izlenmesi ve gerçek zamanlı karar alınmasını ifade eder. Denetim açısından gerçek zamanlı kontrollerin izlenmesi, işlem verilerini analiz ederek beklenen limitleri ve parametreleri aşan yüksek riskli işlemleri gerçek zamanlı olarak belirlenmesini sağlayacaktır (J. Dai, 2017, s. 38-39).
- **Hizmet Odaklılık:** Hizmet odaklılık, hizmetlerin interneti üzerinden üretim hatları, montaj, depolama, uzman bilgisi vb. konular hakkında hizmetlerin sunulmasını ifade etmektedir. Denetim 4.0 denetçiler ve diğer ilgili hizmet sağlayıcılar arasındaki iş birliğini kolaylaştırmak için hizmet odaklı yapıyı benimseyebilir. Denetim yazılım hizmetleri bulut özellikli hale gelebilir. Veri analitiği denetim tarafından kabul görmüş güçlü ve faydalı bir teknoloji olmasına rağmen kullanımı beklenenin altındadır. Bunun temel sebebi

olarak veri analiz tekniklerinin denetçilerin becerilerinin ötesinde olmasıdır. Dolayısıyla bu noktada denetçiler profesyonel veri analistlerinden yardım alarak iş yüklerini azaltarak önemli kararlara odaklanabilir. Ayrıca hizmet odaklı model ile hem denetim yazılımı ön maliyetleri hem de bakım masrafları azalır (J. Dai, 2017, s. 39).

- **Modülerlik:** Modüler sistemler değişen ortamlara veya gereksinimlere uyum sağlamaları sebebiyle Endüstri 4.0'da öne çıkmaktadır. Değişen koşullara ayak uydurmaları sebebiyle modüler sistemler, mevsimsel dalgalanmalar veya ürün özelliklerinin değişmesi durumunda kolaylıkla ayarlanabilmektedir (Hermann, Pentek and Otto, 2016, s. 13). Denetçiler denetim planına göre uygun denetim uygulamaları seçebilir. Denetçi belirli risklere, iş ortamı, denetçi yetkinliklerine göre her denetim için yeni bir uygulama kullanılabilir (J. Dai, 2017, s. 40).

2.2. Dijital Dönüşüm Çağında İç Denetçi ve Yetenek Yönetimi ile İlişkisi

Kurumların Endüstri 4.0 teknolojilerinden faydalanmaları sonucu yeni ve özel risklerle karşılaşma olasılığı artmaktadır. Kurumlardaki yenilikçilik dürtüsü, iç denetim mesleğini hızlı bir şekilde adapte olmaya ve gelişmeye zorluyor ve birçok denetçinin bu değişikliklere ayak uydurması zorunluluğu ortaya çıkmaktadır. Günümüzün iş ortamında, iç denetçilerin yeteneklerini muhasebe, uyumluluk, hile ve finans gibi geleneksel alanların ötesine genişletmeleri gerekmektedir. Bu noktada bu anlayışa sahip iç denetimin iş ve teknoloji becerilerinin bir karışımına sahip olan, iş bağlamında bilişsel sistemleri anlayan yeni beceri ve yeteneklere sahip olan iç denetçilere ihtiyaç duyulmaktadır. Diğer bir ifadeyle kurumlardaki dijital dönüşümden kaynaklı iş değişimini desteklemek için birçok kurum, veri bilimi, analitik, BT, siber güvenlik ve gizlilik gibi teknik alanlarda uzmanlığa sahip iç denetçilere ihtiyaç duymaktadır. Yaşanan dönüşüm sonucunda iç denetim fonksiyonunun doğru soruları sorabilen, paydaşların ihtiyaçlarını anlayabilen, gerçek riskleri görebilen ve güvence sağlamanın yeni yollarını benimseyen uzmanlar birçok konuda bilgili kişilere ihtiyacı olabilir. Bu sadece birisinin örneğin uygulama geliştirme ve veri erişimiyle ilgili yönetişimi incelemesini sağlamakla ilgili değildir aynı zamanda belirli bir yapay zeka veya robotik süreç otomasyonu (Robotic Process Automation-RPA) uygulamasının doğası gereği ortaya çıkan riskleri ve bunlar hakkında

yapılan varsayımları anlayabilen kişilere sahip olmakla ilgilidir (Deloitte, 2018b, s. 8; DEWAN P.N. CHOPRA & CO., 2020, s. 4).

IIA, iç denetçilerin dijital dönüşümü farkında ve dijital dönüşüm gerekliliklerini taşıyan iç denetçilerin önemini şöyle ifade etmektedir: "Eğer bir iç denetçinin özgeçmişi dijital dönüşüm teknolojileri alanında uzmanlığa sahip ise tebrik ederiz." (IIA, 2019, s. 1) Dolayısıyla bu cümleden hem kurumların dijital dönüşüm çağında hangi özelliklere sahip iç denetçileri bünyelerine katmaları gerektiği hem de iç denetçilerin mesleklerin ne yöne doğru evrildiği görülmektedir. Keza yaşanan dijital dönüşüm sonucu iç denetçilerin ve iç denetim kuruluşlarının teknolojiyi anlamaları ve bunlardan yararlanmaları beklentisi IIA (2017a, s. 7) tarafından Uluslararası İç Denetim Standardı 1210.A3'te iç denetçilerin bilgi teknolojisi riskleri, kontrolleri ve teknoloji tabanlı denetim teknikleri hakkında bilgi sahibi olarak uyum sağlamaları vurgulanmaktadır.

Dijital dönüşüm riskleri değiştirmekle birlikte denetimin yürütülmesinde verimlilik sağlayacak birçok teknoloji sunmaktadır. Risklerin değişmesiyle birlikte iç denetçilerin bilişim konusunda yetkinliğe sahip olması gerektiği dijital dönüşüm çağında bir zorunluluk olmakla birlikte "Teknolojinin gelişimi iç denetim mesleğini acaba yok edecek mi?" sorusunu akıllara getirmektedir. Bu noktada Morgan (2016) tarafından "Yapay Zeka ve Otomatikleşmenin Bizden Alamayacağı Şey" başlıklı yazıda insanların robotlardan ve makinelerden üç konuda ayrıldıkları vurgulanmaktadır: Empati gösterme, İletişime geçme, Bağ Kurma. IIA özellikle iletişim konusuna dikkat çekmiştir. İç denetçilerin geçmişte olduğu gibi bugün de kendi alanları içinde üst yönetim kademelerinden yönetim kuruluna; özel amaçlı denetim açısından kritik öneme sahip uzmanlara kadar birçok kişiyle anlamlı ve verimli bağlantılar kurulması açısından gelecekte de kuvvetli iletişime sahip iç denetçiler rağbet göreceği ifade edilmiştir (IIA, 2019, s. 2-3). Dolayısıyla gelişen teknolojinin iç denetim mesleğinin yok olmasına değil hem geleneksel becerilere sahip hem de teknolojiyi kullanabilen iç denetçilerin kurumlara katkı sağlayacağı söylenebilir.

Kaya (2018) tarafından yaşanan dijital dönüşüm konusuna iç denetçilerin ayrıca eğilmesi gerektiği ve sektörde, ülkede, dünyadaki gelişmeleri yakından takip etmeleri gerektiği vurgulanmaktadır. Ayrıca Endüstri 4.0 teknolojilerinin tüm üretim ve hizmet kurumlarına büyük katkısı olduğu iç denetçilerinde bu teknolojilerin GRC (Governance, Risk, Compliance- Yönetişim, Risk, Uyum) süreçlerine katkıları araştırılabilir,

gelişmeleri raporlayabilir ve öneriler geliştirmelerini ifade etmiştir. Bunların yanında iç denetçiler Endüstri 4.0 bağlamında bulundukları sektörün ne yönde ilerlediği, dijital dönüşüm sürecinde nasıl bir planlama yapılması gerektiği konularında çalışmalar yürütmeleri konusunda kurumlarına katkı sağlamalıdırlar. Dijital dönüşüm sürecinde öncelikle iç denetçilerin BT denetimlerinin yanı sıra insan kaynakları ve yönetim ve organizasyon yapılarının denetiminin yapılması önerilmektedir. Dijital dönüşüm sürecinde iç denetçilerin kurumlara vereceği katkı aşağıdaki şekilde sıralanabilir (Kaya, 2018):

- Kurumda üst yönetimde başlamak üzere tüm kademelerde dijital dönüşüm farkındalığının oluşturulmasında katkı sağlanmalıdır.
- Dijital dönüşüm adına nasıl bir yol izleneceği konusunda eylem planları üst yönetimce, tüm birimlerin katkıları ile oluşturulması sağlanmalıdır.
- Ulusal ve uluslararası sektörde iyi dijital dönüşüm örnekleri, uygulamaları ve kurum içinde uygulama imkanları araştırılmalıdır.
- İç denetçiler kurumun mevcut yönetsel ve organizasyonel yapısının incelemeli, bu inceleme kurum kültürünü anlamaya ve dijital dönüşüm planı çerçevesinin iyileştirilmesine yardımcı olabilirler.
- Şirket iş süreçlerinde dijital dönüşüm planı çerçevesinde iş süreçleri iyileştirme, iş süreçleri yeniden yapılandırma çalışmalarının gerçekleştirilmesinin sağlanması ve bunlara risk/kontrol yapılarını kapsayacak şekilde kurumun dijitalleştirilmesine yönelik gözetim ve destek verilmelidir. Tüm sıralanan konular hakkında iç denetçiler danışmanlık rolünü ön plana çıkarmalıdır ve bu hizmetleri denetim planlarına dahil etmelidirler.

Tüm meslek gruplarında olduğu gibi iç denetçinin de değişen ortama ayak uydurmaması yeni riskleri beraberinde getirmektedir. Yetenek yönetimi IIA ve ECIIA tarafından kurumların karşılaşacağı riskler arasında yer almaktadır. Ayrıca 2021 yılında Deloitte tarafından yürütülen Küresel İnsan Sermayesi Eğilimleri anketinde, yöneticiler çalışanların uyum sağlama, becerilerini güncelleme ve yeni roller üstlenme yeteneklerini gelecekteki iş sürekliliğinin devam ettirilmesi adına kritik konu olarak belirlenmiştir. Ankete cevap veren yöneticilerin %72'si bu konuyu ilk iki sırada seçtiği konular arasındadır (Deloitte, 2021, s. 20). Yetenek yönetimi kurumların yapay zeka gibi

teknolojilerin uygulaması sonucu iç denetimin karşı karşıya olduğu önemli bir risktir, çünkü teknolojik yeteneklere sahip kişiler makine öğrenimi üzerindeki algoritmaları yöneten, büyük verileri kullanan, toplayan ve modelleyen kişilerdir ancak risk analizi ve yönetişim konusunda yetenekli değillerdir. İç denetim adaylarının gelecekteki risklerle mücadele etme becerilerine, eleştirel düşünmeye, iyi iletişime, yaratıcılık ve yenilik becerilerine, veri analizi becerilerine ve sürekli büyüme arzusuna sahip olması bu nedenle gerekmektedir (Alina, Cerasela and Gabriela, 2018, s. 444). Özetle Denetim 4.0 olarak adlandırdığımız yeni denetim sürecinde denetçilerin veri analizi ve risk analizi gibi konular üzerine odaklanmaları gerektiği ve dolayısıyla yeni süreçte denetçilerin yeni donanımlarla kendilerini yetiştirmeleri gerekmektedir. Yıldız ve Ağdeniz (2019, s. 99) çalışmalarında Denetim 4.0 sürecinde denetçilerin birer "denetim mühendisi" olarak adlandırılabileceği ifade edilmektedir. Ayrıca öğrencilerin daha iyi bir veri bilimcisi olmaları adına muhasebe ve ilgili programlar çerçevesinde kendilerini güncellemesi (Earley, 2015, s. 499) geleceğin denetçilerini yaşanan dijital dönüşüm çerçevesinde yeteneklerini geliştirmeleri konusunda yararlı olacağı düşünülmektedir.

Yetenek yönetimi konusunda ele alınan diğer konu, risk değişmesidir. Risklerin değişmesinden kaynaklı olarak kurumların iç denetim birimlerine bu risklere ilişkin yeterli güvenceyi vermeleri için ihtiyaç duyulan yeteneği bulma konusunda zorluklar yaşamasıdır. Siber güvenlik riskleri sektör ayrımı yapılmaksızın yöneticiler tarafından kurumlara en yüksek tehdit oluşturan risk olarak ifade edilmektedir (IIA, 2019, s. 4). Dolayısıyla hem özel hem de kamu sektörünün siber güvenliğe duyarlılığı artıkça iç denetimin bu süreçte kuruluşa siber güvenlik kontrollerinin değerlendirilmesi, uygulamaya konulması açısından yönetime yardımcı olacak iç denetçiyi kendine nasıl çekeceği ve bu yeteneğin gelişimini nasıl sağlayacağı konusunda yeni sorular ortaya çıkmaktadır. Bu noktada kurumlar iki yolu seçebilir. Birincisi siber güvenlik risklerini yönetmek için uzman veya hizmet sağlayıcı yoluna başvurabilir; ikincisi ise kurum elindeki kaynağı kullanarak sahip olduğu iç denetçi niteliği ile sınırlandırabilir. Bu iki seçenek başka riskleri beraberinde getirmektedir. Bu nedenle iç denetçiler dijital dönüşüm çağının getirdiği siber riskler konusunda kuruma güvence ve danışmanlık faaliyetlerini yürütürken yetkinlik alanlarının yeterli olması şeklinde bir sorumluluğu vardır (IIA, 2019, s. 5-6). İç denetçilerin bakış açısına göre, güvenilir bir siber güvenlik danışmanı olmak, siber güvenlik risklerinin temel kavramlarını bilmekle sınırlı

kalmamalı, siber güvenlik uzmanlığı sağlamak için BT personeli ile işbirliği yapmalıdır. İç denetçiler, proaktif içgörüler sağlamak için kendi BT denetim yeteneklerini genişletmelidir ve bu şekilde yönetime katma değerli önerilerde bulunabilirler. İç denetçiler, ilgili düzenlemelerde yapılacak değişiklikler, yeni gereksinimler ve diğer sektör eğilimleri hakkında güçlü bir çalışma bilgisine sahip olmalıdır (Kahyaoglu and Caliyurt, 2018, s. 372).

İç denetçinin sahip olması gereken niteliklerin yanında kurumların bu niteliğe sahip iş gücünü istihdam etmesi, kurum içinde geliştirmesi, elde tutması ve motive etmesi yetenek yönetiminin kapsayan diğer bir konudur. Tüm bunların sağlanmasında kurumlar bir stratejiye sahip olmaları gerekmektedir. Kurum dışından yeterli yetkinliğe sahip iş gücünü istihdam etme bir tercih iken iç denetim birimini güçlendirmenin başka yolları da vardır (IIA, 2019, s. 9). IIA "Yıkıcı Dönüşüm Çağında İç Denetim" başlıklı çalışmasında, iç denetimin dijital dönüşüm sonucu kurumlar üzerindeki etkilerini yönetmek adına birtakım önerilerde bulunmuştur. Bunlardan biri kurumların dijital dönüşüm eğitimlerine yatırım yapmalarıdır. Kurumlar tarafından benimsenen teknolojilerin beraberinde getirdiği riskler hakkında daha fazla bilgi edinmek adına eğitimlerin sürekli takip edilmesi gerektiği vurgulanmaktadır. Bu süreçte iç denetim yöneticileri süreci etkili yönetmek adına teknolojiyi anlama ve geliştirme kapsayacak şekilde niteliğe sahip uyarlanabilen, esnek ve inovatif bir personel dağılım modeli oluşturmalıdır (IIA, 2018b, s. 6). Kurum içinde eğitimin verilmesi vasıflı adayların beraberinde getirdikleri yüksek ücret etkilerinden kaçınmalara yardımcı olmaktadır. Ayrıca kurumların iyi bir eğitim programına sahip olmaları rekabetçi piyasada tecrübesiz fakat öğrenmeye istekli adayların değerlendirilmesine imkan vermektedir. Diğer bir strateji ise eğitim kurumları ile ortak projeler yürütülerek hem iç denetim birimleri yetenek istihdamı, yetenek eğitimi ve yeteneği elde tutmak için faydalanabilecekleri bir kaynağa ulaşırken öğrenciler deneyime sahip olacaktır. Bir diğer stratejik seçenek ise BT, BT güvenliği, muhasebe alanlarında tecrübeli olup emekli yaşı gelmiş veya emekli olmuş kişilerin tam veya yarı zamanlı işe alarak kuruma değer katmalarını sağlamaya dayanmaktadır (IIA, 2019, s. 11-12).

Yetenek yönetiminde nitelikli iş gücünü (nitelikli iç denetçiyi) elde tutma ve motive etme diğer önemli bir konudur. Kurumların vasıflı bir iç denetçiyi istihdam etme yolunu seçmeleri veya iç denetçinin gelişimine yönelik kaynak ayırma da gönüllü olmalarına

rağmen nitelikli iç denetçinin kurumlara bağlılığını sağlayamayabilirler. Dolayısıyla kurumların nitelikli iç denetçiyi elde tutma stratejileri bulunmalıdır. Maslow'un ihtiyaçlar hiyerarşisi piramidi, yetenek yönetiminin nitelikli iç denetçinin elde tutulması aşamasında kuruma katılan kişi ne kadar "kendini gerçekleştirme" (Maslow'un hiyerarşi piramidinin üst basamağı) aşamasına ulaşırsa o kişi kurumda kalmaya o denli inanacaktır. Buradan yola çıkarak maaş ve ücret kişilerin işe alım sürecinde motive edici bir faktör olmakla birlikte kurumlara bağlılığını sürdürmek için yeterli değildir. Bu sebeple daha güçlü bir motive edici faktöre ihtiyaç vardır. Bu faktör kurum kültürüdür. Yetenekler (nitelikli iç denetçi) yaptığın işin kuruma değer kattığını görmeyi, yönetimden geri bildirim almayı, kurum içinde yükselme olanaklarının tanımlanmış olmasını, mesleki istikrar kazandıracak ortamda çalışmayı ve ofis dışı hayat sürdürme imkan tanıyacak şartlara sahip olmayı istemektedirler. Bunların tamamı kurum kültüründe barınmasıyla yeteneğin motivasyonu ve kuruma bağlılığı artacaktır. İç denetimin nitelikli yetenekleri istihdam etmesi, elde tutması ve bağlılığı sağlayabilmesi için hem iç denetim birimi bazında hem de kurumun tamamını kapsayacak şekilde yetenek yönetim stratejisinde bu yeni konuyu gerektiği ölçüde ele alınmalıdır (IIA, 2019, s. 15-16).

İlerleyen yıllarda küresel ekonominin büyük çoğunluğu Y kuşağından meydana gelecek olup bu kuşağın mesleklerini çekici hale getirmek görevleri arasındadır. Y kuşağının gözünde iç denetim mesleğini de çekici hale getirmek gerekmektedir. Y kuşağının birçok riske maruz kaldığı düşünüldüğünde risk konusu bu neslin dikkatini çekecektir. Diğer taraftan bu nesil, teknoloji kullanma konusunda muhafazakâr bir tavır sergilemektedir. KPMG'nin raporunda bu durum gözler önüne serilmektedir. Bu raporda iç denetimin kurumlara yönelik en önemli teknolojik risklere yönelik güvence sağlama konusunda yeterli yetkinliğe sahip olup olmadığı incelenmiş ve denetçilerin denetledikleri birçok alanda yetenek eksikliği ile karşı karşıya olduklarına ulaşılmıştır. Bu alanların başında siber güvenlik, veri analitiği ve gizliliktir (KPMG, 2017, s. 11). Oysaki kurumlardaki üstendikleri misyonu itibariyle paydaşların yararına yürüttüğü güvence verme ve danışmanlık görevini yerine getirmeleri için yeniliklere açık bir tavır sergilemede lider pozisyon almalıdırlar. Bu anlayış kurumun geneline yayılarak lider pozisyona gelmesi Y kuşağının ilgisini çekecektir (IIA, 2019, s. 16-17).

Yetenek yönetimi kavramı incelendiğinde birçok konunun ele alındığına ulaşılmıştır. Hem denetçinin dijital dönüşüm çağında taşıması gereken yeni nitelikler hem

de kurumda istihdam edilmesinden elde tutulmasına, motive edilmesine, teknolojiyi benimsemede gelecek nesli teşvik etmek adına üstlendiği rolle kadar birçok yönden yetenek yönetimi iç denetçiler yönünden bakıldığında da her zaman ilgi alanı ve endişe sebepleri arasındadır (IIA, 2018a, s. 1).

2.3. İç Denetim Kapsamında Kullanılan Teknolojiler ve Denetim Sürecine Etkileri

Bu başlık altında Endüstri 4.0 teknolojilerinin iç denetim sürecinde kullanım alanları ve etkilerine yer verilmiştir.

2.3.1. Nesnelerin interneti

Nesnelerin internetinin temel fikri, fiziksel öğelerin gömülü elektroniklerle (RFID etiketleri, sensörler vb.) zenginleştirildiği ve internete bağlandığı bir sistemdir (Shrouf, Ordieres and Miragliotta, 2014, s. 697). Nesnelerin interneti altyapısı, değer zinciri aracılığıyla bilgi toplar, paylaşır ve gerçek zamanlı karar vermeyi ve iş otomasyonunu daha da kolaylaştırır. Denetçiler gerçek zamanlı, kapsamlı güvence sağlamak için nesnelerin interneti altyapısını kullanabilir. Literatür tarandığında Endüstri 4.0 teknolojilerinin işlem bilgilerinin izlenmesi ve denetlenmesi sırasında geleneksel olarak tanımlanmış muhasebe verilerinden çok daha geniş bir veri kapsamına yani büyük veri kullanılmasını imkan verdiğine ulaşılmaktadır. Bu teknoloji aracılığıyla sosyal medya, bloglar vb. çok çeşitli alanlar bilgi toplanmasına kolaylık sağlanmasından kaynaklı finansal bilgilerin sürekli izlenmesinde entegre edilebilmektedir (O'Leary, 2013, s. 61). Denetçiler, çok çeşitli kaynaklardan yüksek hacimli, farklı bilgi yapılarını gerçek zamanlı olarak yakalamak için nesnelerin interneti teknolojisine güvenebilirler. Ayrıca nesnelerin interneti, iş süreçlerinin maliyet ve performansının gerçek zamanlı denetimini kolaylaştırabilir. Örneğin, nesnelerin internetinin yardımıyla gerçek zamanlı olarak (örneğin makine, üretim hattı ve tesis düzeyinde) enerji tüketimi verilerinin toplanmasını sağlanabilir (Shrouf, Ordieres and Miragliotta, 2014, s. 700). İç denetçiler, üretim planlarını ve gerçek zamanlı enerji tüketimini karşılaştırarak boşa harcanan enerji kullanımını tespit edebilirler (Dai and Vasarhelyi, 2016, s. 6). Nesnelerin interneti teknolojisi ile bir makinenin ne kadar zamandır çalıştığı, musluktan ne kadar su aktığı, bir lokasyondan kaç kişinin ve kimlerin geçtiği, prizdeki elektrik akım miktarı, konum, sıcaklık, ses, görüntü, stok düzeyi şeklinde veriler elde edilerek denetim kanıtları elde edilebilir (Yıldız ve Ağdeniz, 2019, s. 94).

Nesnelerin interneti teknolojisi geleneksel denetimden farklı olarak birçok avantajı bulunmaktadır. Denetçi denetim faaliyetini yürütürken sadece denetimin yapıldığı döneme bağlı kalmayarak her zaman kurumdaki faaliyetler hakkında bilgi sahibi olma imkanı vardır. Bu sayede denetçi faaliyetler sonlandırıldıktan sonra değil, faaliyetler sürdürülürken bilgi sahibi olma, yönetimi ve hatta gerekirse bağlı olduğu üst kurumları bilgilendirme fırsatı bulabilmektedir. Tüm bunların gerçekleşmesi için kurum faaliyetleri ve denetim faaliyetlerinin ortak veri ağına sahip olması gerekmektedir (Erturan ve Ergin, 2017, s. 21). Nesnelerin internetinin iç denetim kapsamında sağlayacağı diğer bir yarar ise iç kontrol tasarımına ilişkindir. Endüstriyel gelişmeler sonucu fabrika tasarım ve üretim süreçleri değişmektedir. Dolayısıyla bu değişiklik iç kontrol tasarımında da değişiklik yaratacaktır. Örneğin nesnelerin internetiyle denetçi, büyük veri tabanından istediği bilgilere istediği zaman ulaşarak gerçek zamanlı bilgi elde etme imkanı bulacaktır. Bu teknoloji sürekli denetim ihtiyacını artıracaktır. Bu sistem sayesinde risklere proaktif şekilde cevap verilmesini ve yönetim ile gerçek zamanlı etkileşim sağlanması yönünde fayda sağlayacaktır (Erturan ve Ergin, 2018, s. 822).

Görsel olarak işletmeyi denetlemek isteyen denetçi, kameralar, nesnelerin interneti ve robotlar sayesinde dijital ortamda denetim faaliyetini gerçekleştirebilecektir. İşletmenin stok, depo, üretim hattı, satış, sevkiyat gibi süreçleri görsel olarak istenildiği zaman, işletmeye haber verilmeden kontrol edilebilecektir. Denetçi şirketteki kamera sistemine erişim sağlayarak istediği zaman dilimlerinde, çalışanların denetlendiğini hissetmeyecek şekilde denetim yapabilecektir (Erturan ve Ergin, 2017, s. 22). Bu durum özellikle COVID-19 etkisiyle uzaktan denetim kavramında da çokça telaffuz edilen bir yöntemdir.

2.3.2.Yapay zeka

Yapay zeka, Denetim 4.0 için önemli olan ve tam ve sürekli güvencenin sağlanması aşamasında kullanılacak bir teknolojik araçtır. Denetimde yapay zeka uygulamalarının artığına ilişkin en büyük kanıt dört büyük denetim firmasının faaliyetlerinde yapay zeka kullanımına ilişkin örneklerde görülmektedir. Dört büyük denetim firmasının yapay zeka uygulamalarına ilişkin birkaç örnek şöyledir: Deloitte'un Argus (Deloitte, 2018c) adlı yapay zeka uygulaması ile işletmelerin bankalar ile düzenlediği kredi sözleşmeleri, denetlenen firmaların müşterileri ile imzaladığı satış sözleşmeleri, alım yaptığı firmalar ile imzaladığı alım sözleşmeleri taranmaktadır. Bu tarama sonucu oluşan bilgiler,

denetçinin programa girdiği anahtar veriler ile analiz edilmektedir ve çalışma sonucunda program uygulama tarafından denetçiye raporlanmaktadır. Ernst & Young (EY) tarafından, daha fazla denetim kanıtı elde etmek için yapılandırılmamış verilerden verileri analiz etmek ve çıkarmak; hileden kaynaklanan önemli yanlışlık risklerini değerlendirmek için büyük veri kümelerini analiz etmek için makine öğrenimi teknikleri kullanılır. Makine öğrenimi uygulamaları, artan doğruluk ve hızın yanı sıra analiz edilen belge sayısını da artırır EY tarafından Canvas uygulaması denetim uzmanlarını müşterileriyle buluşturan ve boyut, konum veya karmaşıklık ne olursa olsun tutarlı denetim koordinasyonu ve yönetimi sağlayan ilk çevrimiçi platform olarak nitelendirilmektedir. Canvas, denetçilerin risklere ve risklere verdikleri tepkilere odaklanmasına yardımcı olmak amacıyla geliştirilmiştir. Temel olarak, denetçilerin bir denetimin en önemli alanlarına daha fazla zaman ayırmasına yardımcı olmaktadır. KPMG tarafından geliştirilen Clara, verileri analiz etmek, anlamlı modeller sağlamak ve riskleri ve anormallikleri belirlemek için en son makine öğrenimi ve yapay zeka çözümlerini benimseyen akıllı bir denetim platformudur (Ucoglu, 2020, s. 3-4). PWC (2018b) tarafından "GL.ai" yapay zeka teknolojisi geliştirilmiştir. Bu teknoloji ile üst düzey denetçilerin bilgi ve deneyiminin bir araya gelmesiyle bir şirketin defteri kebirindeki anormallikleri tespit edilmektedir. Gl. ai görselleştirmeler yaparak hem denetçinin hem de müşterinin sorunu tam olarak anlamasını ve etkin bir şekilde çözebilmesini sağlayarak tanımlanan her sorun için anlayış ve bakış açısı sağlamaktadır.

İşletmelerin yapay zekayı kullanma aşamasında karşılarına ilk çıkan soru yapay zekayı anlamaya yöneliktir. Yapay zeka insan beyni gibi davranabilen donanım ve yazılım olmasıdır: öğrenme, akıl yürütme, uyarlama, analiz etme, karar verme ve karmaşık ve yargılama odaklı görevleri yerine getirme özelliğine sahiptir. Bu özellikleri bugün üretilen muazzam miktarda veriyle birleştirdiğinizde, yapay zeka destekli makinelerin üretkenliği nasıl artırabileceğini ve sıradan görevleri devralarak hayatı nasıl kolaylaştırabileceğini görmek kolaydır. Dolayısıyla bu denli özelliğe sahip bir teknolojinin iç denetime de etkisi olacağı açıktır (IIA, 2017b, s. 1). Yapay zeka denetimde ilgili bilgileri arama, belgelerden çıkarma ve bunları kullanılabilir formata dönüştürme konusunda zaman alan görevlerin yükünü azaltarak denetçilere yardımcı olacaktır. Yapay zekanın veri toplama konusunda yardımları sonucunda denetçilerin karar alma süreçlerine daha fazla zaman ayırmalarını sağlayacaktır (Brennan, Flynn and Baccala,

2017). Yapay zeka kurumlara birçok fayda sağlaması ile birlikte iç denetimin de genel kalitesine olumlu yönde etkisi mevcuttur. Bu etkiler şöyle sıralanabilir (Ghanoum and Alaba, 2020, s. 59):

- Yapay zeka denetim sürecine dahil olması sonucunda adımların etkin şekilde yürütülmesi ve etkinliği artırılmasına yardımcı olmaktadır.
- Denetçilerin denetim sürecinde tekrar ettiği hataların azaltılmasını sağlamaktadır.
- Yapay zeka finansal kayıtları toplayabilir ve inceleyebilir. Yapay zeka sayesinde sınıflandırma ve karşılaştırma süresinin azaltılmasında yardımcı olmaktadır. Manuel yöntemler kullanan denetçiler bu işlemlerde daha fazla vakit harcarlar.
- Yapay zekanın hata, manipülasyon veya ihmal riskinin artmasına neden olan insan hatasını azalttığına ulaşılmıştır.
- Yapay zeka kullanımının uluslararası standartlara uyumu ve profesyonelliği artırdığına ulaşılmıştır.
- Yapay zeka risklerin nerede olduğunu gösterir ve odaklanılacak alanının belirlenmesinde yardımcı olur. Manuel denetimde, analiz için rastgele örnekleme kullanılmasından kaynaklı daha az etkilidir.

2.3.3. Büyük Veri, Veri Analitiği/Analizi

Büyük veri, karar almak için uygun maliyetli, yenilikçi bilgi işleme biçimleri talep eden yüksek hacimli, yüksek hızlı ve yüksek çeşitlilikteki bilgi varlıkları olarak tanımlanmaktadır. Büyük veri, veri miktarını ifade etmek için kullanılmanın yanında büyük verinin analiziyle ilgilidir. Veri analizleri işletme içinde çeşitli amaçlar için kullanılmaktadır. Teknolojinin gelişimi ile birlikte veri analitiği araçları, iç denetim departmanlarının öncelikli olarak odaklanmaya başladıkları araçlar olarak arasında yer almaktadır (Betti and Sarens, 2021, s. 209). İç denetimin işletme genelinde etkili ve verimli faaliyetlerin sürdürülmesi sorumluluğu göz önüne alındığında veri analitiği kullanılması yararlı olacaktır (Tang, Norman and Vendrzyk, 2017, s. 1127). İç denetim, veri analitiğini kullanarak müşteri ödeme davranışını analiz edebilir, müşteri kredi notunu değerlendirebilir, müşteri kredi riskini tahmin edebilir, kredi limitinin gelir üzerindeki etkisini tahmin edebilir. Ayrıca, veri analitiği yoluyla büyük miktarlarda yapılandırılmamış ve yarı yapılandırılmış veriler elde edilebilir ve veri tabanının

zamanında güncellenmesiyle iç denetimin doğruluğunu ve uygunluğunu artırmaya yardımcı olmaktadır (Xie, 2020, s. 186). Veri analitiği iç denetimin etkin olmayan kontrol alanlarını belirlenmesini, farkına varılmayan risklerin belirlenmesine yardımcı olmaktadır. Ayrıca veri analitiğinin kullanımı denetçilerin çalışmalarının riskli iş alanlarına göre sıralayarak öncelik vermesinde imkan sunacaktır. Denetim esnasında veri analitiğinin kullanımı, farklı sistemlerdeki yüklü miktardaki verinin denetimi ayrıca dış veri kaynaklarının kullanımını yeni öngörülerde bulunulmasına imkan tanımaktadır (PWC, 2015, s. 4). Veri analitiğinin iç denetim fonksiyonun denetim komitesine rapor sunmasında, denetim yöneticisinin işletme yönetimi ile olumlu iletişim kurmasına, iç denetim fonksiyonun hile tespiti, risk yönetim güvencesi ve bilgi teknolojisi risk denetim faaliyetlerine katılımı konularında pozitif etkisi vardır (Rakipi, Santis and D'Onza, 2021, s. 2).

PWC (2015, s. 3) iç denetim ve kurumlar için veri analitiği kullanımı geleceğe dönük tahminleri daha doğru yapılması, uygunluk yönünden gelişmiş bir iç denetim, yaratıcılığın gelişimi, üretkenliğin artışı, yüksek hacimlerle çalışma imkanı, geniş ölçekte düşünme yeteneği, iç denetim becerilerinin gelişimi, düzensiz verilerin düzenlenmesi, çapraz analiz imkanı, karmaşıklığı sadeleştirme becerisi, geleceğe yönelik tahminler konusunda açık iletişim sağlanması şeklinde faydaları sıralamaktadır. Dolayısıyla veri analitiği hem veri analizleri hem denetim becerileri ve geleceğine yönelik tahminlerde fayda sağladığı görülmektedir.

2.4. Dijital Dönüşümün Yarattığı Riskler Karşısında Uluslararası ve Ulusal Düzenlemeler

Bu başlık altında uluslararası ve ulusal camiada öncü kuruluşlar tarafından yayımlanan yasal düzenlemelere ilişkin bilgiler detaylı şekilde sunulmuştur.

2.4.1. Uluslararası Düzenlemeler/Kılavuzlar

Uluslararası düzenlemelerde ISO 27000 serisi, COBIT, ITIL, NIST Siber Güvenlik çerçevesi ve AICPA dikkat çekmektedir. Bu düzenlemelere ilişkin açıklamalar sırasıyla bu başlık altında ele alınmıştır.

2.4.1.1. ISO 27000 serisi

ISO 27000 ailesi bilgi teknolojileri, bilgi güvenliği ve siber güvenlik konularını içeren uluslararası kabul görmüş bir çerçevedir. 27000'den başlayarak 27999 arası

standartlar bilgi güvenliği standartlarına ayrılmıştır. Bu bölümde ISO 27000 standart ailesi içerisinde yer alan önemli standartlar açıklanacaktır. ISO/IEC 27000 ailesindeki yer alan bazı standartlar daha yaygın olarak referans almakta ve bunlara ilişkin kısaca açıklamalar aşağıda sıralanmıştır:

- **ISO/IEC 27001 Bilgi Teknolojisi-Siber Güvenlik ve Gizlilik Koruması-Bilgi Güvenliği Yönetim Sistemleri-Gereklilikler:** Bir bilgi güvenliği yönetim sisteminin (BGYS) benimsenmesi, bir kuruluş için stratejik bir karardır. Bir kuruluşun bilgi güvenliği yönetim sisteminin kurulması ve uygulanması, kuruluşun ihtiyaç ve hedeflerinden, güvenlik gereksinimlerinden, kullanılan kurumsal süreçlerden ve kuruluşun büyüklüğünden ve yapısından etkilenir. Bilgi güvenliği yönetim sistemi, bir risk yönetimi süreci uygulayarak bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini korur ve ilgili taraflara risklerin yeterince yönetildiğine dair güven verir. Bilgi güvenliği yönetim sisteminin, kuruluşun süreçlerinin ve genel yönetim yapısının bir parçası olması ve bunlarla entegre olması ve süreçlerin, bilgi sistemlerinin ve kontrollerin tasarımında bilgi güvenliğinin dikkate alınması önemlidir. ISO/IEC 27001, kuruluş bağlamında bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gereksinimleri belirtmektedir. Ayrıca, kuruluşun ihtiyaçlarına göre uyarlanmış bilgi güvenliği risklerinin değerlendirilmesi ve iyileştirilmesi için gereksinimleri de kapsamaktadır. ISO/IEC 27001 belirtilen gereksinimler geneldir ve türü, boyutu veya yapısı ne olursa olsun tüm kuruluşlara uygulanabilir olması amaçlanmıştır (International Organization for Standardization, 2022a).
- **ISO/IEC 27002 Bilgi Teknolojisi-Siber Güvenlik ve Gizlilik Koruması-Bilgi Güvenliği Kontrolleri:** Bu standart, uygulama kılavuzu da dahil olmak üzere bir genel bilgi güvenliği kontrolleri referans seti sağlamaktadır. Ayrıca kuruluşlar tarafından ISO/IEC27001'e dayalı bir bilgi güvenliği yönetim sistemi (BGYS) bağlamında; uluslararası kabul görmüş en iyi uygulamalara dayalı bilgi güvenliği kontrollerini uygulamak için; kuruluşa özel bilgi güvenliği yönetim kılavuzlarının geliştirilmesi için kullanılmak

üzere tasarlanmıştır (International Organization for Standardization, 2022b).

- **ISO/IEC 27003 Bilgi teknolojisi-Güvenlik Teknikleri -Bilgi Güvenliği Yönetim Sistemi-Rehber:** ISO/IEC 27001'de belirtildiği gibi bir BGYS için gereklilikler, bunu yanında gerekliliklerle ilgili tavsiyeler, olasılıklar ve izinler hakkında rehberlik sağlamaktadır (International Organization for Standardization, 2017)
- **ISO/IEC 27005 Bilgi Güvenliği, Siber Güvenlik ve Gizlilik Koruması - Bilgi Güvenliği Risk Yönetimi-Rehberlik:** ISO/IEC 27001'de belirtildiği gibi bir BGYS için gereklilikleri ve bilgi güvenliği risk değerlendirmesi ve iyileştirilmesinin gerçekleştirilmesinde rehberlik sağlamaktadır. ISO/IEC 27005, kuruluşun bilgi güvenliğini tehlikeye atabilecek riskleri yönetmeyi amaçlayan her boyutta, sektörde ve her tür kuruluş (örneğin ticari işletmeler, devlet kurumları, kar amacı gütmeyen kuruluşlar) için geçerlidir (International Organization for Standardization, 2022c).
- **ISO/IEC 27007 Bilgi Güvenliği, Siber Güvenlik ve Gizlilik Koruması-Bilgi Güvenliği Yönetim Sistemleri Denetimi İçin Rehber:** Bu standart, ISO 19011'de (Yönetim Sistemleri Denetim Standardı) yer alan kılavuza ek olarak, bir bilgi güvenliği yönetim sistemi (BGYS) denetim programının yönetilmesi, denetimlerin yürütülmesi ve BGYS denetçilerinin yeterliliği hakkında rehberlik sağlar. Bu belge, bir BGYS'nin iç ve dış denetimlerini anlaması veya yürütmesi veya bir BGYS denetim programını yönetmesi gerekenler için geçerlidir (International Organization for Standardization, 2020).
- **ISO/IEC 27032 Bilgi teknolojisi-Güvenlik Teknikleri-Siber Güvenlik İçin Kılavuz:** ISO/IEC 27032, Siber Güvenlik durumunu iyileştirmek için rehberlik sağlamaktadır. Siber güvenlik faaliyetinin benzersiz yönlerini ve özellikle bilgi güvenliği, ağ güvenliği, internet güvenliği ve kritik bilgi altyapısı koruması gibi diğer güvenlik alanlarına bağımlılıklarını ortaya çıkarır. Bu uluslararası standart siber güvenliğe genel bir bakış, siber güvenlik ile diğer güvenlik türleri arasındaki ilişkinin açıklaması, paydaşların tanımı ve siber güvenlikteki rollerinin tanımı, ortak siber güvenlik sorunlarına yönelik rehberlik ve siber güvenlik sorunlarını çözmek

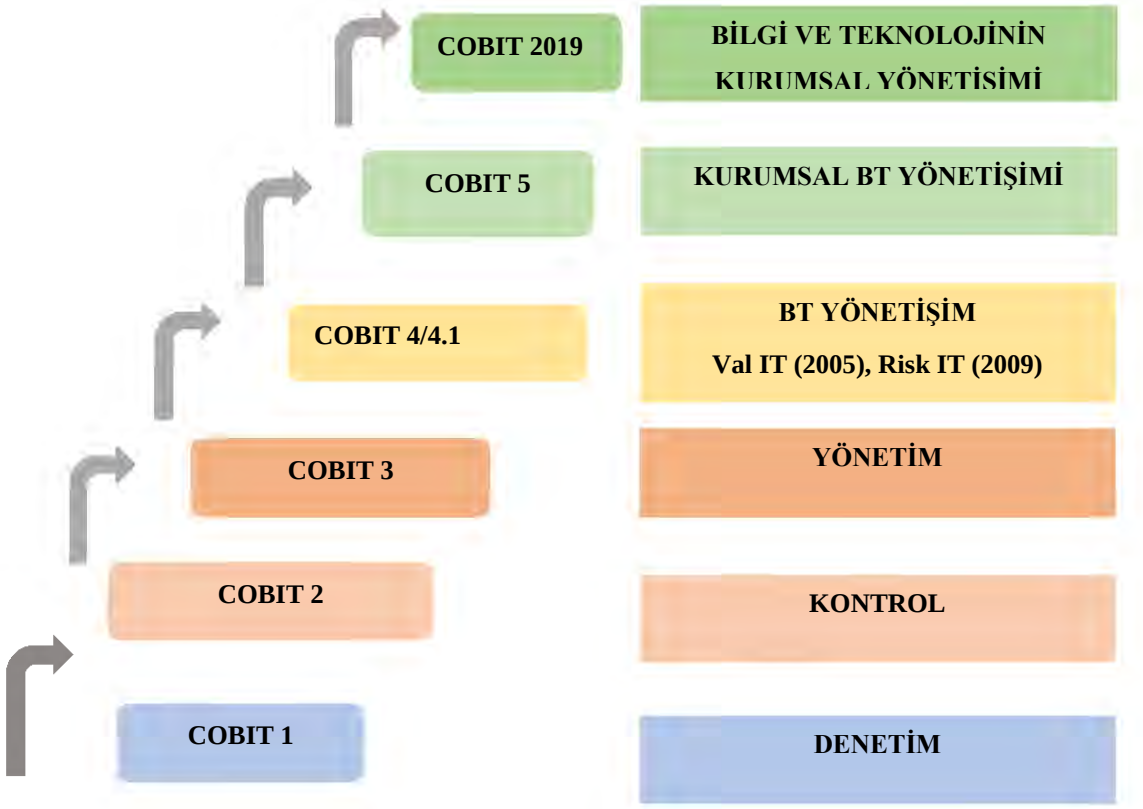
için iş birliği yapmaları için paydaşlarına imkân sunan bir kılavuzdur (International Organization for Standardization, 2012).

2.4.1.2. COBIT

COBIT (Control Objectives for Information and related Technology- Bilgi ve İlgili Teknoloji İçin Kontrol Hedefleri), ISACA (Information Systems Audit and Control Association-Bilgi Sistemleri Denetim ve Kontrol Derneği) ve ITGI (Information Technology Governance Institute-BT Yönetişim Enstitüsü) tarafından oluşturulan bilgi teknolojisi yönetimi için geliştirilmiştir (Sahibudin, Sharifi and Ayat, 2008, s. 751).

COBIT'in misyonu, kurum yöneticileri ve denetçiler tarafından günlük kullanım için yetkili, güncel, uluslararası genel kabul görmüş bilgi teknolojisi kontrol hedeflerini araştırmak, geliştirmek, tanıtmak ve teşvik etmektir. COBIT, yöneticilere, denetçilere ve BT kullanıcılarına, bilgi teknolojisinin kullanımı yoluyla elde edilen faydaları en üst düzeye çıkarma ve bir şirkette uygun BT yönetişimi ve kontrolünü geliştirme konusunda onlara yardımcı olmak için bir dizi genel kabul görmüş ölçü, gösterge, süreç ve en iyi uygulama sağlamaktadır. Yöneticiler, denetçiler ve kullanıcılar, BT sistemlerini anlamalarına ve bir BT yönetişim modelinin geliştirilmesi yoluyla şirketlerinin varlıklarını korumak için gerekli olan güvenlik ve kontrol düzeyine karar vermelerine yardımcı olduğu için COBIT'in geliştirilmesinden yararlanırlar (Sahibudin, Sharifi and Ayat, 2008, s. 751). COBIT ilk baskısı yayımlandıktan sonra yaşanan değişim ile çeşitli güncel versiyonları yayınlanmıştır. ISACA, 1996 yılında BT denetim görevlerini yürütmek için bir çerçeve olarak COBIT'in ilk baskısını yayınlamıştır. COBIT ilk versiyonu denetim ile sınırlandırılmıştır. Bu ilk baskının ardından, 1998 yılında BT süreçleri için kapsamlı bir dizi kontrol hedefi etrafında inşa edilen ikinci baskı oluşturulmuştur. Böylece COBIT'in ikinci versiyonunda "kontrol" kavramı ortaya konulmuştur (KPMG, 2013, s. 37). BT'nin kurumlar için artan önemini ve BT'nin etkili kontrole yönelik artan ihtiyacını fark eden ISACA, 1998'de BT yönetişimi için bir düşünce kuruluşu olarak ITGI kurulmuştur. ITGI aracılığıyla toplanan görüşler, COBIT'in BT yönetimi için iyi bir uygulama çerçevesine doğru evrimine büyük ölçüde katkıda bulunmuştur (Haes vd., 2020, s. 125). COBIT çerçevesinin üçüncü versiyonu 2000 yılında yayınlandı ve yönetim yönergelerini (ölçüler, kritik başarı faktörleri ve BT süreçleri için olgunluk modelleri dahil) içermektedir. Böylece COBIT üçüncü versiyonu ile BT yönetim çerçevesi haline gelmiştir (KPMG, 2013, s. 37). 2005 yılında ISACA iş

ve BT hedeflerinin sıralanması ve destekleyici BT süreçleriyle ilişkileri, BT süreçleri bağlamında roller ve sorumluluklar, BT süreçleri arasındaki karşılıklı ilişkiler şeklinde birçok yeni yönetim ve yönetişim kavramlarını tanıtan COBIT 4.0 yayımlamıştır. COBIT dördüncü baskının amacı COBIT'i BT yönetişimi için genel kabul görmüş bir çerçeve haline getirmektir. ITGI tarafından değer sunumu ve risk yönetiminin BT yönetişiminin temel sonuç alanları olduğu konusundaki görüşler sunulmuştur. Bu görüşlerin sonucunda, BT ile ilişkili olan iş süreçleri ve sorumluluklarının katma değer oluşturmada "Val IT" (2008 yılında) ve risklerin yönetilmesini "Risk IT" (2009 yılında) çerçeveleri yayınlanmıştır. Bu iki çerçeve COBIT 4.0 ve COBIT 4.1'ın (yayınlanma yılı 2007) tamamlayıcısı niteliğindedir. (Haes vd., 2020, s. 126). COBIT 5.0 ise "Kurumsal BT Yönetişimi" öne çıkaran bir çerçeve olup 2012 yılında yayınlanmıştır (KPMG, 2013, s. 37). 2019 yılında COBIT çerçevesinin en son güncellemesi, yani COBIT 2019, esnek ve uyarlanmış bir EGIT (Enterprise Governance Of Information And Technology- Bilgi ve Teknolojinin Kurumsal Yönetişimi) tasarımı ve uygulamasını kolaylaştırmayı amaçlamaktadır (Haes vd., 2020, s. 126). Yıllar itibariyle COBIT gelişimi Şekil 2.4'te sunulmuştur.



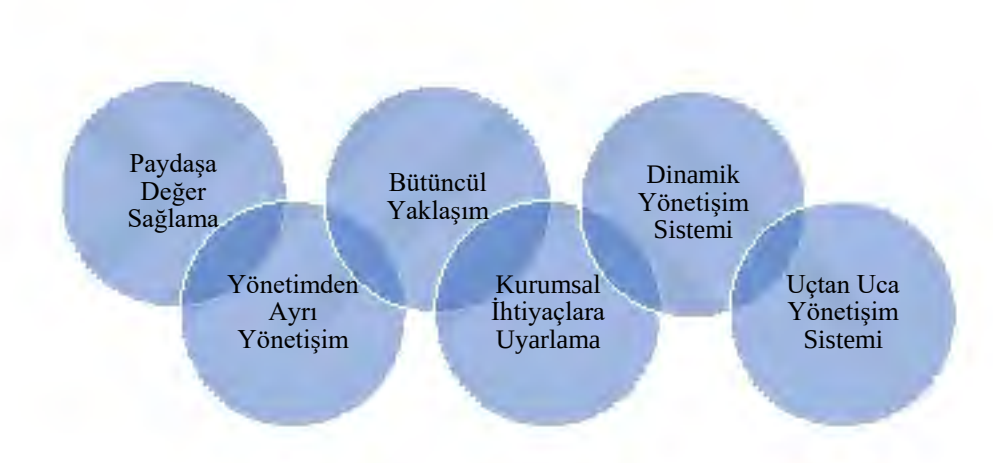
Şekil 2. 4. *COBIT gelişimi (Yazar tarafından hazırlanmıştır.)*

COBIT 2019 çerçevesi, bir EGIT sisteminin temel gereksinimlerini tanımlayan altı ilkeyi sunar (Şekil 2.5'te görselleştirilmiştir). Bu ilkelerin her biri aşağıda kısaca açıklanmıştır (ISACA, 2019, s. 17).

1. **Paydaşa Değer Sağlama:** ISACA'ya göre, bir EGIT sisteminin amacı, paydaş ihtiyaçlarını karşılamak ve bilgi ve teknoloji kullanımından değer yaratmak ve korumaktır. Değer; faydalar, risk ve kaynaklar arasındaki dengeyi yansıtmaktadır. Bu değeri kurumlar uygulanabilir bir strateji ve yönetişim sistemiyle sağlayabilir.
2. **Bütüncül Yaklaşım:** Etkili bir EGIT sisteminin bütünsel bir şekilde birlikte çalışan bir dizi bileşenden (yani süreçler ve diğer ilgili bileşenler) oluşmaktadır. Bu konu daha çok kurumun iş yapmak için bir araya geldiği insanlarla alakalıdır.
3. **Dinamik Yönetişim Sistemi:** Bu ilke, tasarım etkenlerinden herhangi biri veya birkaçının farklılaşması halinde (örneğin, strateji veya teknolojideki bir değişiklik), bu farklılaşmaların EGIT sistemi üzerindeki etkisinin göz önünde bulundurulmasını ifade etmektedir. Dolayısıyla yönetişim sistemi dinamik

olmalıdır. EGIT'in dinamik bir görünümü, geleceğe yönelik uygulanabilir bir EGIT sistemine yol açacaktır.

4. **Yönetimden Ayrı Yönetişim:** Bir yönetişim sistemi, yönetişim ve yönetim faaliyetleri ile yapıları arasında açıkça ayrım yapmalıdır.
5. **Kurumsal İhtiyaçlara Uyarlama:** Bir yönetişim sistemi, yönetişim sistemi bileşenlerini özelleştirmek ve önceliklendirmek için parametre olarak bir dizi tasarım etkeni kullanarak kurumların ihtiyaçlarına göre uyarlanmalıdır.
6. **Uçtan Uça Yönetişim Sistemi:** Bir yönetişim sistemi, sadece BT birimine değil, aynı zamanda yapılan işlemin kurumda bulunduğu yere bakılmaksızın, kurumun amaçlarına ulaşmak için koyduğu tüm teknoloji ve bilgilere odaklanarak, kurumların uçtan uca kapsamasını sağlamalıdır.



Şekil 2. 5. *COBIT 2019 yönetişim sistemi ilkeleri (ISACA, 2019, s.17)*

Bilgi ve Teknolojinin Kurumsal Yönetişimi (EGIT) dijital dönüşümden değer sağlama ve dijital dönüşümden kaynaklı iş risklerini azaltmaya odaklanmaktadır. ISACA tarafından bilgi ve teknolojinin kurumsal yönetişiminin yararları üç başlık altında toplanmıştır. Bunlar (ISACA, 2019, s. 11-12):

- **Fayda Gerçekleştirimi:** Fayda gerçekleştirimi, bilgi ve teknoloji ile işletmeye değer yaratmayı, işletmelerin sahip oldukları bilgi ve teknolojinin değer yaratmasının sürdürülmesi ve artırılması ayrıca işletmeye değer yaratmayan BT yatırım ve varlıklarının ortadan kaldırılması anlamına gelmektedir.
- **Risk Optimizasyonu:** Bir kurumda bilgi ve teknolojinin kullanımıyla alakalı iş riskinin ele alınmasını ifade etmektedir. Bilgi ve teknolojiye ilişkin

iş riski, işi etkileme potansiyeline sahip bilgi ve teknolojiye ilişkin olaylardan kaynaklanmaktadır. Risk yönetimi değer korumaya odaklı olması sebebiyle kurumun bilgi ve teknolojiye ilişkin risk yönetimi, kurumsal risk yönetimi yaklaşımına entegre edilmelidir. Ayrıca, bilgi ve teknolojiye ilişkin iş riski optimizasyonunun değerin korunmasına yönelik nasıl bir etki ve katkı sağladığı ölçülmelidir.

- **Kaynak Optimizasyonu:** Kaynak optimizasyonu stratejik planı yürütmek amacıyla kurumun yeterli kaynağa sahip olup olmadığını incelemesi ve emin olunması gerektiğini ifade eder. Kaynak optimizasyonu için uygun yeteneklerin mevcut ve yeterli, uygun ve etkin kaynakların sağlandığına emin olmaktır. Kaynak optimizasyonu, bütünleşik ve ekonomik bir BT altyapısının oluşturulmasını, işin gerektirdiği şekilde yeni teknolojilere başvurulmasını ve güncel olmayan sistemlerin güncellenmesi veya değiştirilmesini sağlamaktadır. Sadece donanım ve yazılım şeklinde düşünülmemelidir. Aynı zamanda insan sermayesinin önemini vurgulamaktadır. Kişilerin eğitiminden, kurumda devamlılığına ve yetkinliğinin sağlanmasına şeklinde konulara odaklanır. Kaynak optimizasyonunda diğer önemli bir konu en iyi değeri elde etmek için veri ve bilginin kullanmanın önemidir.

Bilgi teknolojisi, işletmelerin desteklenmesi, sürdürülebilirliği ve büyümesinde çok önemli hale gelmiştir. Önceden yönetim kurulları ve üst düzey yöneticiler, kararların çoğunu fonksiyonel yönetime bırakarak BT yönetimine katılımlarını en aza indirebiliyordu. Çoğu sektör ve endüstride işletmeler hayatta kalmak ve büyümek için giderek daha fazla BT'ye bağımlı hale geldiğinden bu tür tutumlar artık imkansızdır. Bu kuruluşlar ayrıca suistimal/kötüye kullanım, siber suçlar, hileler, hatalar ve eksiklikler dahil olmak üzere BT'den kaynaklanan geniş bir dış tehdit yelpazesiyle karşı karşıyadır (DeHaes, Grembergen and Debreceny, 2013, s. 307). Dolayısıyla COBIT, yöneticilere, denetçilere ve BT kullanıcılarına, bir şirkette bilgi teknolojisi kullanımı yoluyla elde edilen faydaları en üst düzeye çıkarmaya yardımcı olmaktadır. Ayrıca COBIT, BT yönetişimi ve kontrolünü geliştirmede işletmelerde ilgili kişilere (yöneticilere, denetçilere ve BT kullanıcıları) yardımcı olmak için bir dizi genel kabul görmüş ölçü, gösterge, süreç ve en iyi uygulama şekli olarak ifade edilmektedir (Sahibudin, Sharifi and Ayat, 2008, s.

751). Yıllar itibariyle güncellenmesi ile BT denetiminden BT kurumsal yönetişimine evrildiği söylenebilir.

2.4.1.3. ITIL

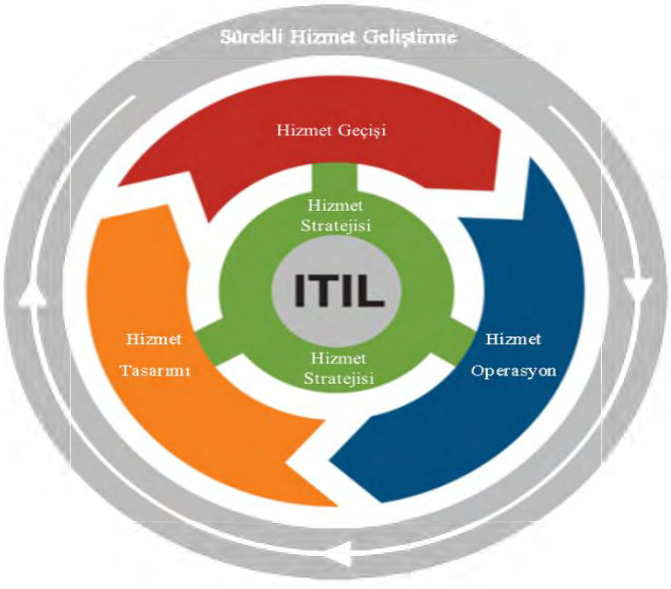
ITIL (Information Technology Infrastructure Library- Bilgi Teknolojisi Altyapı Kütüphanesi), BT hizmet yönetimindeki en iyi uygulama şeklinde tanımlanan genel bir çerçevedir. BT yönetişimi ve BT hizmetlerinin yönetimi ve kontrolü için bir çerçeve sağlamaktadır. Hem iş hem de müşteri açısından sunulan BT hizmetinin kalitesinin sürekli ölçülmesine ve iyileştirilmesine odaklanmaktadır. Bu odaklanma, ITIL'ın dünya çapındaki başarısında önemli bir faktör olarak görülmektedir. Bunun yanında ITIL'ın verimli kullanımına ve kurum genelinde teknikleri ve süreçleri uygulayan kurumların elde ettiği temel faydalara katkıda bulunmuştur. Bu avantajlardan bazıları aşağıda sıralanmıştır (Cartlidge vd., 2012, s. 6):

- BT hizmetlerinde artan kullanıcı ve müşteri memnuniyeti,
- Doğrudan iş kârı ve gelirinde artışa yol açan iyileştirilmiş hizmet kullanılabilirliği,
- Yeniden çalışma veya kayıp sürenin azalması, iyileştirilmiş kaynak yönetimi ve kullanımından kaynaklanan finansal tasarruf,
- Yeni ürün ve hizmetlerin piyasaya sürülme süresinde iyileştirmenin artması,
- Karar almada iyileştirme ve riskin azaltılmasıdır.

ITIL kapsamında gelişmeler, İngiltere Ticaret Bakanlığı tarafından CCTA'ya (Central Computer and Telecommunications Agency- Merkezi Bilgisayar ve Telekomünikasyon Kurumu) BT servislerindeki kalitenin iyileştirilmesi için bir çerçeve geliştirme görevi verilmesi ile adım atılmıştır. Avrupa'da kamu kurumları başta olmak üzere BT yönetimindeki kargaşaların sona ermesi amacıyla 1989 yılında ITIL V1 yayımlanmıştır. 2000'li yıllara kadar ITIL çerçevesi üzerinde çalışmalar sürdürülür ve 2001 yılında ITIL V2 oluşturulmuştur. ITIL V2 sekiz kitap (Service Support, Service Delivery, Business Perspective, Planning to Implement ITSM, Infrastructure Management, Application Management, Software Asset Management, Security Management) şeklinde yayınlanmış ve kütüphaneye dönüştürülmüştür. 2005 yılına gelindiğinde ISO (International Standart Organization) tarafından ISO 20000 BT Yönetim Sistemi geliştirilmiştir. ISO 20000 konuya farklı bir bakış açısı getirmesi ile süreç bazlı

bir çalışma olan ITIL V2 bir yönetim sistemi zemini haline getirilmiştir. 2007 yılında yaşam döngüsü (Planla, Uygula, Kontrol Et, Önlem Al) yaklaşımını içeren ITIL V3 yayımlanmıştır. 2011 yılında ITIL V3 versiyonunda bazı güncellemeler yapılmıştır. 2019 yılına gelindiğinde ITIL'ın son versiyonu olan ITIL V4 yayımlanmıştır (Ak, 2020).

ITIL V4 bir önceki versiyonun (ITIL V3) yükseltilmiş şekli olarak yayımlanmıştır ve BT hizmet yönetiminin kurum gerekliliklerileyle daha fazla adaptasyonu sağlayan gelişmiş stratejik unsurları kapsamaktadır. ITIL V4 bilgi teknolojilerine uygun etkin ürün ve hizmetlerin oluşturulması, sunulması ve sürekli iyileştirilmesi için bir işletim modeli sunmaktadır. ITIL V4 etkin bir BT Hizmet Yönetimi süreci oluşturulmasına yardımcı olmuştur. Bunun yanında ITIL V4, kurumların yeni hizmet yönetimi zorluklarıyla başa çıkması için yol göstericidir (Güngör, 2021, s. 147). ITIL, BT hizmet yönetimi için beş aşamalı hizmet yaşam döngüsüne dayanan bir çerçevedir. Şekil 2.6'da ITIL hizmet yaşam döngüsü görselleştirilmiştir.



Şekil 2. 6. *ITIL hizmet yaşam döngüsü (Ak,2020)*

ITIL hizmet yaşam döngüsüne ilişkin aşamalar aşağıda kısaca ifade edilmiştir (Cartlidge vd., 2012, s. 12-57):

- **Hizmet Stratejisi:** ITIL Hizmet Stratejisi, ITIL yaşam döngüsünün merkezinde yer almaktadır. Tüm BT hizmet sağlayıcılarına ve müşterilerine, net bir hizmet stratejisi oluşturarak uzun vadede çalışmalarına ve gelişmelerine yardımcı olmak için kılavuzluk sağlamaktadır. Hizmet stratejisinin kılavuzluk kapsamı hangi hizmetlerin sunulacağı, kimlere sunulacağı, paydaşların değeri nasıl algılayacakları, hizmet varlıklarına ve hizmet yönetimi yeteneklerine stratejik yatırımı güvence altına almak için sağlam iş senaryolarının nasıl oluşturulacağı vb. birçok konudadır.
- **Hizmet Tasarımı:** Hizmet tasarımının amacı, yeni veya değişen hizmetlerin kurumların değişen gereksinimlerini karşılayacak şekilde tasarlanmasını sağlamaktır. Hizmet tasarımı, hizmet stratejisinden yeni bir gereksinimi iş hedeflerini gerçekleştirmek için bir tasarıma dönüştüren yaşam döngüsündeki aşamadır. Yaşam döngüsünün bu aşamasındaki temel faaliyetler olarak tasarım faaliyetlerin planlanması ve koordinasyonu, tutarlı hizmet tasarımlarının sağlanması, hizmet yönetim bilgi sistemleri, mimariler, teknoloji, süreçler, bilgi ve ölçümler, hizmet tasarım paketlerinin üretimi, arayüzlerin yönetimi, hizmet tasarım etkinliklerinin ve süreçlerinin iyileştirilmesi yer almaktadır. ITIL hizmet tasarımı, hizmetlerin ve hizmet yönetimi uygulamalarının tasarımı ve geliştirilmesi için rehberlik; stratejik hedefleri bir hizmet ve hizmet varlıkları portföyüne dönüştürmek için tasarım ilkeleri ve yöntemleri sağlamaktadır.
- **Hizmet Geçişi-Devreye Alma:** Hizmet geçişinin amacı yeni, değiştirilmiş veya kullanımdan kaldırılan hizmetlerin, hizmet yaşam döngüsünün hizmet stratejisi ve hizmet tasarımı aşamalarında belgelendiği şekilde kurumun beklentilerini karşılamasını sağlamaktır. Hizmet yaşam döngüsünün bu aşamasındaki temel faaliyetler arasında değişikliklerin ve sürümlerin planlanması ve yönetilmesi, risklerin yönetilmesi, bilgi aktarımı, beklentilerin belirlenmesi ve beklenen iş değerinin sağlanması yer almaktadır. Hizmet geçişi/devreye alma, hizmetin tüm yönlerini uygulamaya, yeni veya değişen hizmetin müşteri beklentilerini karşılamasını ve hizmet sağlayıcı tarafından yönetilebilmesini sağlamaya odaklanmaktadır.

- **Hizmet Operasyonu:** Hizmet operasyonunun amacı kullanıcılara ve müşterilere kararlaştırılan düzeyde hizmet sunmak ve hizmetlerin sunulmasını destekleyen uygulamaları, teknolojiyi ve altyapıyı yönetmektir. Yaşam döngüsünün, kurumlara hizmetlerin gerçekten değer kattığı aşamasıdır. Hizmet stratejisi değeri tanımlar, hizmet tasarımı bu değeri sağlayacak hizmetleri tasarlar, hizmet geçişi bu tasarımı canlı bir hizmete getirir ve ardından hizmetin diğer bir ifadeyle değerin sunulmasını/teslim edilmesini sağlamak hizmet operasyon personelinin sorumluluğundadır. Hizmet operasyonu, yaşam döngüsünün neredeyse tamamen kullanıcılarla ilgilenen aşamasıdır.
- **Sürekli Hizmet İyileştirme:** Bu aşama hizmet kalitesinin ve hizmet yaşam döngüsünün ve temel süreçlerin genel olgunluğunun sürekli değerlendirilmesi ve iyileştirilmesi yoluyla müşteriler için değerin korunmasıyla ilgilidir. Birçok kurum için sürekli hizmet iyileştirmesi bir şey başarısız olduğunda ve iş ciddi şekilde etkilediğinde proje haline gelirken, sorun çözüme ulaştığı zaman bir sonraki başarısızlığa kadar bu kavram unutulur. Fakat kurumların başarılarının sürekli olması için, sürekli hizmet iyileştirmesi kurum kültürüne yerleştirilmeli ve rutin bir faaliyet haline gelmelidir. Çünkü sürekli hizmet iyileştirmesi mevcut hizmetleri, süreçleri ve ilgili faaliyetleri ve teknolojinin yanında hizmet yaşam döngüsünün her aşamasını geliştirmeye çalışan; kalite yönetimi, değişiklik yönetimi ve yetenek geliştirme ilkelerini, uygulamalarını ve yöntemlerini birleştirir.

2.4.1.4.NIST Siber Güvenlik Çerçevesi

Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology- NIST) ABD'de bir kurumdur. NIST CSF (Cyber Security Framework- Siber Güvenlik Çerçevesi), ABD Ulusal Standartlar ve Teknoloji Enstitüsü tarafından siber güvenlik ekosisteminde endüstriler 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 alarak "Framework for Improving Critical Infrastructure Cybersecurity - Kritik Altyapı Siber Güvenliğini Geliştirme Çerçevesi" başlığı ile Versiyon 1.0 şeklinde 2014 yılı Şubat ayında yayımlanmıştır. Bu çerçeve; siber güvenlik riskini daha iyi yönetmek ve azaltmak için mevcut standartlara, kılavuzlara ve uygulamalara dayalı

gönüllü rehberlik etmek hem iç hem de dış kurumsal paydaşlar arasında risk ve siber güvenlik yönetimi iletişimini teşvik etmek için tasarlanmıştır (Çolak, 2020). 2017 ve 2018 yıllarında çerçevede güncelleme yapılmış olup Versiyon 1.1 2018 yılında yayımlanmıştır (NIST, 2018).

NIST CSF siber güvenlik riskini yönetmeye yönelik risk tabanlı bir yaklaşım olup üç bölümden oluşmaktadır. Birinci bölüm; arzu edilen, hedeflenen güvenliğin ne olduğunun tanımlandığı çekirdek bölümdür. CSF Çekirdeği, belirli bir siber güvenlik sonuçlarını elde etmek için bir dizi etkinlik sağlayan 5 temel işlevden oluşmaktadır. Bunlar (NIST, 2018, s. 7-8):

- **Tanımla:** Çerçevenin etkin kullanımı için tanımlama aşaması yapılmalıdır. Sistemlere, insanlara, varlıklara, verilere ve yeteneklere yönelik siber güvenlik riskini yönetmek için kurumsal bir anlayış geliştirilmesine yardımcı olmaktadır. Kurum ortamını, siber riskleri anlamak, kurumun risk yönetimi stratejisi ve kurum ihtiyaçlarında nelere odaklanması gerektiğini belirlenmesinde yardımcı olur.
- **Koru:** Kritik hizmetlerin korunmasını sağlamak ve potansiyel bir siber güvenlik olayının etkisini sınırlamak için uygun önlemlerin alınmasını kapsamaktadır.
- **Tespit Et/Algıla:** Siber güvenlik olaylarının zamanında keşfedilmesini sağlamak için uygun faaliyetler geliştirilmesini ve uygulanmasını içermektedir.
- **Yanıt Ver:** Tespit edilen bir siber güvenlik olayına karşı müdahale etmek için uygun faaliyetleri kapsamaktadır.
- **Kurtar/İyileştir:** Esneklik planlarını sürdürmek ve bir siber güvenlik olayı nedeniyle bozulan yetenekleri veya hizmetleri geri yüklemek için uygun faaliyetleri geliştirme ve uygulama işlevidir.

İkinci bölüm; belirli bir uygulama senaryosunda standartların, kılavuzların ve uygulamaların çerçeve çekirdeği bölümünde bulunan işlevler ile uygun hale getirilmesi olarak tanımlandığı profil bölümüdür. Güncel Profil (Current Profile) ve Hedef Profil (Target Profile) olarak iki başlık altında incelenmektedir. Güncel profilin tanımlanması, kurumların siber güvenlik programlarının CSF yönünden objektif bir inceleme

yapmalarını ve mevcut güvenlik durumlarının ne olduğunu tam olarak bilmelerini sağlar. Hedef Profil, istenen siber güvenlik risk yönetimi hedeflerine ulaşmak için gereken sonuçları belirtir. Üçüncü bölüm ise; kurumun siber güvenlik risklerini nasıl yönettiğini gösteren uygulama katmanları bölümüdür (NIST, 2018, s. 3-4). Katmanlar siber güvenlik risk yönetimi uygulamalarında artan derecede dikkati ve karmaşıklığı tanımlamaktadır. Katmanlar siber güvenlik risk yönetiminin iş ihtiyaçları tarafından ne ölçüde bilgilendirildiğini ve bir kurumun genel risk yönetimi uygulamalarına entegre edildiğini belirlemeye yardımcı olurlar. (NIST, 2018, s. 8).

NIST siber güvenlik çerçevesine göre bir siber güvenlik programının oluşturulması 7 adımdan oluşmaktadır. Aşağıdaki adımlar, bir kuruluşun yeni bir siber güvenlik programı oluşturmak veya mevcut bir programı geliştirmek için çerçeveyi nasıl kullanabileceğini göstermektedir. Siber güvenliği sürekli iyileştirmek için bu adımlar gerektiği kadar tekrarlanmalıdır. Bu adımlar aşağıda sırasıyla kısaca açıklanmıştır (NIST, 2018, s. 14-15):

1. Önceliklendirme ve Kapsam: Kurumlar bu aşamada iş/misyon hedeflerini ve üst düzey organizasyonel önceliklerini tanımlamalıdır. Bu bilgilerle kurum, siber güvenlik uygulamalarıyla ilgili stratejik kararlar alır ve seçilen iş kolunu veya süreci destekleyen sistem ve varlıkların kapsamını belirleyebilirler.
2. Konumlanma: Bir iş kolu veya süreç için siber güvenlik programının kapsamı belirlendikten sonra, kurum ile ilgili sistemleri ve varlıkları, yasal gereklilikleri ve genel risk yaklaşımını belirlenmelidir. Kurum daha sonra bu sistemler ve varlıklar için geçerli olan tehditleri ve güvenlik açıklarını belirlemek için kaynaklara danışmalıdır.
3. Güncel Profil Oluşturma: Kurum birinci bölümden (Çekirdek Bölüm) hangi kategori ve alt kategori sonuçlarının elde edildiğini belirterek bir Güncel Profil geliştirmelidir. Bunun yapılması sonraki adımların desteklenmesine yardımcı olacaktır.
4. Risk Değerlendirmesi Yürütme: Kurumlar bir siber güvenlik olayının olasılığını ve olayın kurum üzerindeki etkisini ayırt etmek için operasyonel ortamı analiz ettiği adımdır. Kurumların ortaya çıkan riskleri belirlemesi ve

siber güvenlik olaylarının olasılığını ve etkisini daha iyi anlamak için iç ve dış kaynaklardan gelen siber tehdit bilgilerini kullanmaları önemlidir.

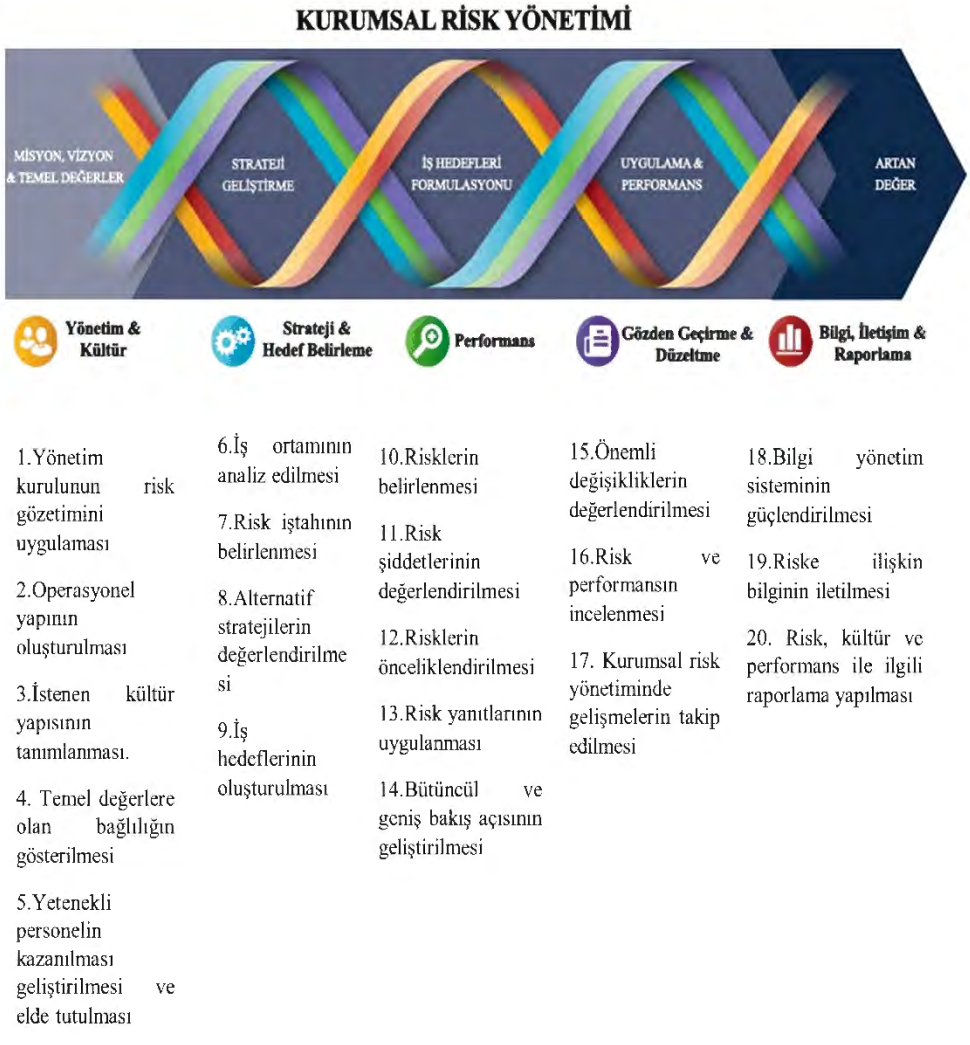
5. Hedef Profil Oluşturma: Kurum, istenen siber güvenlik sonuçlarını tanımlayan kategorileri, kurum hedeflerini ve yasal uyumluluk ile ilgili gereklilikleri dikkate alarak değerlendirir ve Hedef Profil oluşturur. Kurum, bir Hedef Profili oluştururken sektör kuruluşları, müşteriler ve iş ortakları gibi dış paydaşların etkilerini ve gereksinimlerini de dikkate alabilir.
6. Fark Belirleme, Analiz Etme ve Önceliklendirme: Kurum; Güncel Profil ile Hedef Profil'i karşılaştırarak farkları belirlemelidir, Hedef Profil'e ulaşmak için farklara yönelik eylem planı hazırlamalıdır. Daha sonra kurum, farkları gidermek için gerekli finansman ve işgücü dahil kaynakları belirlemelidir. Profilleri bu şekilde kullanmak, kurumun siber güvenlik faaliyetleri hakkında doğru kararlar almasına yardımcı olacaktır.
7. Eylem Planını Uygulama: Kurum, önceki adımda belirtilen farkları gidermek için hangi önlemlerin alınacağını belirler ve daha sonra Hedef Profil'e ulaşmak için mevcut siber güvenlik uygulamalarını ayarlamalıdır.

2.4.1.5. Siber Riskler ve COSO Kurumsal Risk Yönetimi- Riskin Strateji ve Performansla Uyumlaştırılması

Kurumlar birbirine giderek teknolojik bağlantılı olması ve dijital hale gelmesi sonucunda daha fazla ve karmaşık siber tehditler ve saldırılar ile karşı karşıya kalmaktadır, her geçen gün siber tehditlerin sayısı artmaya devam etmektedir. Kuzey Amerika'da dijital dönüşüm ile ilgilenen kuruluşların yüzde doksanının risk profilinin genişlediği ve siber riskleri yönetmenin karar vericiler için en önemli risk hedefi olduğu ifade edilmektedir. Özetle kurumlar yapay zeka, blockchain, bulut bilişim, makine öğrenme vb. yeni teknolojiler gelişmeye devam ettikçe faaliyetlerini devam ettirmek adına dış taraflar ile bağlantısı olması sebebiyle siber saldırganlar bilgi sistemleri ve kontrollerinin izin verdiği ölçüde güvenlik açıklarından faydalanacaklardır (COSO, 2019, s. 3).

Kurumlar çeşitli siber tehdit senaryoları ile hem kurum içi hem kurum dışı siber saldırılara maruz kalabilirler. Kurumlar, siber tehditlerden korunmak adına stratejisi, süreci ve teknolojisini nasıl geliştirmesi gerektiğini göz önünde bulundurması aşamasında tüm verilerini koruyamayacağını göz ardı etmemelidir.

Siber güvenliğin sağlanması adına birçok düzenleme bulunmakla birlikte iç denetim kavramı denilince risk yönetimi konusunda COSO tarafından yayımlanan çerçeveler başta gelmektedir. 2017 yılında yenilenen COSO KRY çerçevesi kullanıcılara 5 ana bileşen ve 20 alt bileşen ile daha detaylı ve bütüncül bir kurumsal risk yönetim yapısı sunmaktadır. COSO KRY çerçevesi bileşenleri Şekil 2.7'de sunulmuştur.



Şekil 2. 7.*COSO Kurumsal risk yönetim bileşenleri (COSO,2017, s.6' den uyarlanmıştır.)*

İşletmeler ve teknoloji geliştikçe, 2017 yılında güncellenen ve Kurumsal Risk Yönetimi-Strateji ve Performansla Bütünleşme "ERM Çerçevesi" başlıklı COSO

Kurumsal Risk Yönetimi (ERM) Çerçevesi de değişmiştir. ERM Çerçevesinin güncellenmesinin arkasındaki temel itici güçler, siber çağda risk yönetiminin evrimini ele alma ihtiyacı ve kuruluşların gelişen iş ortamının taleplerini karşılamak için siber riski yönetme yaklaşımlarını iyileştirme yatmaktadır. ERM Çerçevesi hem strateji belirleme sürecinde hem de performansı yönlendirmede riskin dikkate alınmasının önemini vurgulamak için birçok yönden geliştirilmiştir (COSO, 2019, s. 2). Bu noktada kurumların başlıca görevi tüm güvenlik açıklarının ele alınıp alınmadığından emin olmalarıdır. Bu noktada COSO tarafından kurumların siber risk profillerini ortaya koymak amacıyla "Kurumsal Risk Yönetimi- Riskin Strateji ve Performansla Uyumlaştırılması" çerçevesi uyarınca risk yönetim bileşenleri aracılığıyla ele alınmıştır. Beş ana bileşen ve yirmi alt bileşen çerçevesinde siber risklerin yönetimi aşağıda sırasıyla açıklanmıştır (COSO, 2019, s. 5-17).

2.4.1.5.1. Yönetişim ve kültür -Siber riskler

Yönetişim ve kültür bileşeni KRY çerçevesinin ilk bileşeni olup, tüm risk yönetim bileşenlerinin temelini oluşturmaktadır. Bu bileşende görüldüğü üzere yönetişim ve kültür olmak üzere iki kavram ön plana çıkmaktadır. Yönetişim, kurumun kendine özgü bir yönetişim anlayışını tasarlayarak benimsenmesini ifade etmektedir. Yönetişim birçok aktörü barındıran kararların alındığı fikir alışverişinin yapıldığı bir anlayıştır (Aydın ve Durgun, 2017, s. 25). G. Karakaya (2018, s. 18) tarafından yönetim ve yönetişim kavramı arasındaki fark ortaya konularak COSO'nun bu ifadeyi kullanma amacı şöyle açıklanmıştır; yönetim (goverment) kavramı ayrı ayrı bütünler şeklinde yöneten ve yönetilen tarafları ifade ederken; yönetişim(governance) kavramı iş birliği çerçevesinde birlikte yönetme isteğinden doğmaktadır. Kültür ise etik değerler, istenen davranışları ve risk anlayışı ile doğrudan bağlantılıdır (COSO, 2017, s. 6).

Yönetişim ve kültür, siber riski yönetmek için temel bir bileşendir ve iş sorumlulukları ve sistem erişiminde görevlerin ayrılmasını ve kuruluş genelinde birden çok savunma hattını içeren bir iş stratejisinin yürütülmesini sağlamaktadır. Yönetişim ve kültür bileşeni beş alt bileşenden oluşmaktadır. Bu beş alt bileşeni siber risklerin yönetimini kapsayacak şekilde aşağıda sırasıyla açıklanmıştır (COSO, 2019, s. 5-9):

1) **Yönetim Kurulunun Risk Gözetimini Uygulaması:** kurumların siber riskle karşı karşıya kalmasıyla veri kaybı, faaliyetlerin kesintiye uğraması,

marka ve itibar kaybı veya yasal yaptırımların uygulanması şeklinde sonuçlar doğurabilir. Bu aşamada yönetim kurulu siber riskleri kurumsal riskin bir parçası olarak göz önünde bulundurmalı ve siber riskleri sadece BT meselesi olarak algılamamalıdır. Dolayısıyla yönetim kurulunun siber güvenlik uzmanları veya ilgili uzmanlığa sahip danışmanları kurum bünyelerine katmaları zorunluluk haline gelmiştir. Siber risklere maruz kalmanın gün geçtikçe artmasından kaynaklı olarak yönetim kurumlarının siber riskleri anlamaları, siber programları ve girişimleri değerlendirmesi ve kurumun karşı karşıya kaldığı siber riskleri ne ölçüde ele aldığını değerlendirmek için siber güvenlik yetkinliğine sahip uzmanlar kurumlar için önemlidir.

2) **Operasyonel Yapının Oluşturulması:** kurumların strateji ve iş hedeflerini takip eden operasyonel yapılarının oluşturulduğu aşamadır (COSO, 2017, s. 10). Siber riskin yaygın doğasından kaynaklı siber güvenliğe KRY bakış açısıyla yaklaşmak önemlidir. Dolayısıyla bu bakış açısının sağlanması yani siber risklerle başa çıkmak adına bilgi işlem sorumlusu veya bilgi güvenliği yöneticisi, mali işler sorumlusu, risk yönetim sorumlusu, genel danışman ve kurum sorumlusunu kapsayan bir siber risk ekibi oluşturulmalıdır. Siber risk ekibi, kurum çapında bir siber risk çerçevesini baz alarak değerlendiren, siber tehdit risklerini değerlendiren, kurum çapında bir siber güvenlik planı tasarlayan ve siber riskleri azaltmak için bir bütçe geliştiren departmanlar ve fonksiyonlar arası bir temsil görevi üstlenmelidir. Siber risk yönetimi ekibi, siber tehditlerin kuruma etkisi ve bu risklerin yönetimi adına alınan aksiyonlar hakkında yönetim kuruluna rapor vermelidir. Siber risk yönetim ekibinde kurumun iç denetim yöneticisi ekibin bir parçası veya ekibin bağımsız danışmanı olmalıdır. Özetle KRY' de etkin bir yönetişim ve kültür bileşeni yaratmak adına süreçlerin işleyişinden, yetkilerin dağıtımına kadar temel operasyonel konuların belirlendiği aşamadır (G. Karakaya, 2018, s. 18).
3) **İstenen Kültür Yapısının Tanımlanması:** kurum içinde oluşturulmak istenen kültürün sağlanması için sergilenmesi istenilen davranışların belirlenmesidir (COSO, 2017, s. 10). Siber güvenlik kültürü, kurum kültüründen ayrı düşünülmemeli; kurum kültürüne gömülü olmalıdır. Bir

kurumun siber güvenlik kültürü, güvenlik bilinci ve buna bağlı olarak istenen çalışan davranışı tüm çalışanları kapsayacak şekilde üst yönetimden (yönetim kurulu ve yöneticiler) başlamalıdır. Siber güvenlik bilinci, eğitim ve veri kaybını önlemeye odaklanan güçlü bir kültüre sahip kurumlar, siber risklere karşı duyarlılığını (etki seviyesini) azaltabilir. Etkili siber kültüre sahip kurumların yaratmak istedikleri kültürü ve istenen davranışların çalışan tarafından sergilenmesi aşamasında temel sahip olduğu bileşen üst düzey yönetimin katılımı ve desteğidir. Bu aşamada siber güvenliğin sağlanmasında çalışanlara eğitimlerin verilmesi, çalışanların siber risk konusundaki görüşlerinin sürekli alınması aracılığıyla çalışanların siber güvenlik rolleri kapsamında farkındalıkları artırılır ve siber güvenlik programında ana hatlarıyla belirtilen çalışan davranış ve alışkanlıkları geliştirilir. Siber güvenlik eğitimlerinde çalışanlara olası bir siber tehditle karşı karşıya kalmaları halinde bunun sorumlu kişiye bildirilmesi konusunda eğitim verilmesi gerektiği COSO tarafından vurgulanmaktadır.

4) **Temel Değerlere Olan Bağlılığın Gösterilmesi:** kurumun temel değerlerine üst yönetim dahil olmak üzere tüm çalışanların bağlılığını ifade etmektedir (COSO, 2017, s. 10). Bir kurumun siber risk yönetimi programının, yönetim kurulu ve üst düzey yönetim tarafından belirlenen kuruluşun temel değerleriyle tutarlı olması gerekmektedir. Programın politikaları, standartları, çalışan beklentileri, hesap verebilirliği ve ilgili tüm iletişimleri, kurumun temel değerlerini desteklediğini göstermelidir. Örneğin, yönetim, istenen davranışları zorlamak yerine, çalışanlarına siber risklere karşı dikkatli olmanın önemini kabul etmelerini sağlayan güveni oluşturmaya çalışmalıdır. Üst düzey liderlik, doğru uyumu belirlemek için istenen siber davranış ve alışkanlıkları da sergilemelidir.
5) **Yetenekli Personelin Kazanılması, Geliştirilmesi ve Elde Tutulması:** kurum, strateji ve hedeflerini devam ettirmek adına uygun beşerî sermayeye sahip olmalıdır (COSO, 2017, s. 10). Her geçen gün siber tehditler artmakta, karmaşık hale gelmekte ve saldırganlar yeni sistem açıklarını bulma girişimindedirler. Dolayısıyla bu denli hızlı gelişen risk karşısında kurumların nitelikli siber risk profesyonellerine sahip olmaları, bir kurumun siber riskleri etkin bir şekilde değerlendirmesi, riskleri azaltması ve siber

güvenlik programının etkinliğini izlemesi için kritik öneme sahiptir. Kurumların bazıları siber güvenliğin sağlanması adına nitelikli iş gücüne sahipken, diğerleri siber güvenliğin sağlanması için dışarıdan uzmanlara ihtiyaç duyabilir. Bunun yanında kurum bünyesine kattığı yeni teknolojinden kaynaklı riskleri yönetmek için eğitim verilmesi veya gelişmiş yeteneklere sahip profesyoneller ile çalışılması gereklidir. Bunların yanında kurumlar, siber risklere ilişkin değerlendirilmelerin yapılması, önlemlerin alınması ve siber güvenlik programının etkinliğinin periyodik olarak değerlendirilmesine yardımcı olmak için bir dış firmadan hizmet alınma yolu tercih edebilir. Ayrıca bir kurum önemli bir siber güvenlik olayı veya ihlali yaşarsa, adli veya soruşturma çalışması yapmak için dışarıdan uzman yardımına ihtiyaç duyulabilir.

2.4.1.5.2. Strateji ve hedefleri belirleme - Siber riskler

Kurumsal risk yönetimi, strateji ve hedef belirleme, stratejik planlama sürecinde birlikte çalışır. Bir risk iştahı oluşturulur ve strateji ile uyumlu hale getirilir; iş hedefleri, stratejiyi uygulamaya koyarken; riski belirleme, değerlendirme ve riske yanıt verme için bir temel oluşturur (COSO, 2017, s. 6).

Siber risk yönetimi, strateji ve iş hedefleri belirleme süreci aracılığıyla kurumun stratejik planına entegre edilmelidir. İş ortamının anlaşılmasıyla kurum, iç ve dış faktörler ve bunların risk üzerindeki etkileri hakkında fikir edinilmektedir. Bir kurum siber risk iştahını strateji oluşturulması ile birlikte belirlemektedir. İş hedefleri, stratejinin uygulamaya konmasına ve kurumun günlük operasyonlarını ve önceliklerini şekillendirmesine izin vermektedir (COSO, 2019, s. 4).

Strateji ve hedefleri belirleme bileşeni dört alt bileşenden oluşmaktadır ve bu bileşenler siber risklerin yönetimi açısından aşağıda sırasıyla açıklanmıştır (COSO, 2019, s. 8-9):

1) **İş Ortamının Analiz Edilmesi:** İş ortamı, bir kuruluşun mevcut ve gelecekteki stratejisini ve iş hedeflerini etkileyen eğilimleri, ilişkileri ve diğer faktörleri ifade etmektedir. Dolayısıyla gün geçtikte teknoloji ile birlikte kurumların ortamındaki değişiklik sonucunda değişime ayak uydurmaları için mevcut siber ortamın anlaşılması zorunluluk haline

gelmiştir. Bundan dolayı kurumların strateji ve iş hedeflerinin periyodik olarak gözden geçirerek hem mevcut hem de gelecekteki durumda kurumların iş hedeflerine ulaşması için kritik öneme sahip olan bilgi ve teknolojiyi dikkate almalıdır. Siber güvenlik, kurumların sürekli değişen çalışma ortamında iş ortamı geliştikçe düşünülmelidir. Kurumlar siber alandaki mevcut riskleri, trendleri ve etkileyicileri farkında olmaları gerekmektedir.

2) **Risk İştahının Tanımlanması/Belirlenmesi:** COSO KRY 2017 düzenlemesi, kurumların risk iştahını tanımlarken/belirlerken; değer oluşturma, mevcut değeri koruma bağlamında değerlendirmektedir (COSO, 2017, s. 10). Risk iştahını ve siber risk bedeli arasındaki uygun dengeyi tanımlamak, her kuruluşun dikkate alması gereken bir şeydir. Dijital girişimler için giderek daha önemli hale gelen risk iştahının bir yönü, ileri teknolojiyi benimsememenin veya teknik yetenekleri genişletmemenin maliyet-faydasıdır. Kurumlar daha hızlı hareket etmek, daha gelişmiş teknolojiler kullanmak zorunda olduklarını görüyorlar ve bu nedenle risk iştahlarının, belirli durumlarda kuruluşun mevcut ticari operasyonlarda geleneksel olarak kabul ettiğinin ötesinde ayarlanması gerekebilir. Kurumlar mevcut siber ortamı değerlendirmeye çalışırken, yönetimin siber programlarını ne ölçüde dağıtmayı planladıklarını değerlendirmesi gerekmektedir. Bu sürecin bir parçası olarak, kurumların kritik varlıkların envanterini çıkarması, riski belirlemesi ve siber güvenlik açıklarının nerede olduğunu belirlemelidir.

3) **Alternatif Stratejilerin Değerlendirilmesi:** Risk iştahı belirlendikten sonra kurumlar, riskin olası etkilerini de göz önüne alarak alternatif stratejileri değerlendirmektedir (COSO, 2017, s. 10). Bu bileşende önemli nokta; iş ortamındaki değişikliklere bağlı olarak risklerde de değişim yaşanacak, dolayısıyla kurum bu değişimi göz önünde bulundurarak stratejilerinin uygunluğunu değerlendirmesi gerekmektedir (Karakaya G. , 2018, s. 20). Siber güvenlik risk iştahı tanımlandıktan sonra yönetim, siber risk yönetimi programını yönetmeye yardımcı olacak bir güvenlik modeli belirlemelidir. Yönetimin hangi siber güvenlik modeli uygulayacağını belirlerken, kurum için doğru siber stratejinin belirlenmesi ile birlikte

sermaye, kaynaklar ve teknoloji gibi faktörleri dikkate alarak değerlendirme yapmalıdır.

4) **İş Hedeflerinin Oluşturulması:** Kurumlar, stratejiyi uyumlu hale getiren ve destekleyen çeşitli seviyelerde iş hedeflerini oluştururken riski göz önünde bulundurmalıdır (COSO, 2017, s. 10). Bu ifadeden yola çıkılarak siber uzaydaki sürekli değişimden kaynaklı olarak, siber güvenlik programının yeniden değerlendirilmesi önemlilik arz etmektedir. Değerlendirme sonucunda hedeflere ulaşılamaması ve belirlenen toleransların aşılması durumunda siber güvenlik risk iştahının veya siber yönetişim modelinin yeniden gözden geçirilmesi gerekmektedir.

2.4.1.5.3. Performans - Siber riskler

Kurumlar hedefleri ile doğrudan ilgili risklerini belirler ve değerlendirir. Bu değerlendirme sonucunda riskleri önem derecesine göre sıralar ve risk yanıtlarını seçerek risk portföyünü oluşturmalıdır (COSO, 2017, s. 6). Bu anlayıştan dolayı kurumlar, stratejileri ve iş hedeflerini gerçekleştirmesini etkileyecek siber risklerini belirleyerek, değerlendirmelidirler. Siber riskleri önem derecesine göre ve kurumun siber risk iştahını dikkate alarak önceliklendirmelidirler. Kurum belirlediği siber risklere karşı yanıtlarını seçerek değişim için performansını izlemelidir. Bu sayede siber riskler dahil olmak üzere kurumun stratejisi ve kurum düzeyindeki iş hedefleri çerçevesinde kurumun üstlendiği risk miktarının görünümü ortaya konulacaktır (COSO, 2019, s. 4).

COSO KRY Çerçevesi'nde "Performans" bileşeni beş alt bileşenden oluşmaktadır. Bu bileşenler siber risklerin yönetimi kapsamında aşağıda kısaca açıklanmıştır (COSO, 2019, s. 10-12):

1) **Risklerin Belirlenmesi:** Kurumun strateji ve iş hedeflerini etkileyen risklerin belirlenmesi aşamasıdır (COSO, 2017, s. 10). Kurumlar kendi bünyesinde ve kurum dışında olmak üzere birçok siber riskle karşı karşıya kalmaktadır. Dolayısıyla bu aşamada kurumun belirlediği siber risk haritaları sayesinde hem siber risk iştahlarının belirlenmesi hem de iş ortamına ilişkin siber risk güncellemelerinin yapılmasında hem de iş hedeflerinin sürdürülmesinde bir siber risk veri tabanın oluşturmasına imkan verecektir (G. Karakaya, 2018, s. 20).

2) **Risk Şiddetlerinin Değerlendirilmesi:** kurumların risklerinin şiddetini değerlendirdiği aşama olup risklerin tanımlanması ve risklerin derecelendirilmesi arasındaki süreçte riskler değerlendirilmektedir (G. Karakaya, 2018, s. 20; COSO, 2017, s. 10). Riskleri derecelendirmeden önce kurumun stratejileri, hedefleri üzerinde olası etkileri değerlendirilmektedir. Bu değerlendirme aşamasında çeşitli yöntemler kullanılmaktadır. Bir kurumun siber riskini değerlendirmeye ise hangi bilgi sistemlerinin değerli olduğunun değerlendirilmesi ile başlanılmalıdır. Diğer taraftan siber risk değerlendirmesi, kurumun hedeflerini desteklemede bilgi sistemlerine yönelik nasıl risk yanıtlarının geliştirilmesi konusunda yönetim kararlarını bilgilendirdiğinden dolayı tüm paydaşlara kurumun amaçları ile uyumlu olarak nelerin korunması gerektiğini belirlemede yardımcı olmaktadır. Siber risk değerlendirmesi, kurum için hangi bilgi sistemlerinin önemli olduğu veya neleri tam olarak koruyacaklarını bilmelerine veya bilgilerin nerede, nasıl saklandığını kolay şekilde anlama noktasında yardımcı olmaktadır. Tabii bu aşamada belirli bilgi sistemlerinin aşırı derece korunmasına, diğerlerinin yetersiz şekilde korunmasına neden olabilir. Bu durumun yaşanmaması adına kabul edilebilir bir risk toleransının belirlenmesi ve kurumun kritik öneme sahip bilgi sistemlerini korumaya yönelik girişimlerde bulunması önemlidir.
3) **Risklerin Önceliklendirilmesi/ Derecelendirilmesi:** Risklerin önceliklendirilmesi, kuruma risklerin etkilerini sıralamak amacıyla yapılmakta ve risk derecelendirme sonucu risklere verilecek yanıtlara ilişkin ipuçlarını bulmaya yardımcı olmaktadır (E. Karakaya & G. Karakaya, 2017, s. 301; COSO, 2017, s. 10). Kurum siber risk olaylarının ve sonuçlarının şiddeti ve olasılığı ile ilgili riskleri değerlendirip önceliklendirdikçe risk değerlendirmesi daha derinlemesine incelenmiş olur. Bu aşamada kurum siber risklere sadece kurum içinden geniş açıdan bakmakla kalmayıp sektör bazlı siber riskleri incelemesi gereklidir. Çünkü siber riskler, saldırıyı gerçekleştiren aktöre ve sektöre göre değişiklik göstermektedir. Örneğin, bir perakende işletmesinin karına yönelik (kredi kartı verilerinin çalınması) siber saldırılara maruz kalırken, petrol ve gaz endüstrisi gelecekteki arama

sahaları hakkında stratejik verileri çalmak amacıyla bir siber saldırıya maruz kalabilir.

4) **Risk Yanıtlarının Uygulanması:** Bu aşama, kurumlar risklere yanıtlarını belirmesi ve seçmesinden oluşmaktadır (COSO, 2017, s. 10). Risklere farklı şekilde yanıtlar verilebilir. Kurum riskin sonuçlarını kabul edebilir; riskleri daha etkin veya verimli bir şekilde yönetebildiği zamana devredebilir veya risklerin etkisini hafifletmek veya azaltmak için bir aksiyon alabilir. Risklere karşı cevap vermeye karar verildiği zaman kurumlar kontrol faaliyetlerini devreye sokmaktadır[5]. Kurumlar siber riske hem kurum içinden hem kurum dışından maruz kalma olasılığına karşılık hem önleyici hem de tespit edici kontrol uygulamaları gerekmektedir. Önleyici kontroller, kurum içi BT çevresine karşı izinsiz bir giriş sağlanmaması ve bilgi sistemlerinin güvende kalmasını sağlayarak siber saldırıları engellemektedir. Diğer taraftan tespit edici kontroller, kurumun siber saldırıya maruz kalması halinde tespit edilmesine ve yönetimin düzeltici eylemlerde bulunmasına, olası zararın en kısa sürede düzeltilmesine imkân vermektedir. Siber riskler kaçınılmaz olmakla birlikte bu risklere karşı yanıtlar dikkatli şekilde tasarlanıp, uygulandığı takdirde yönetilebilir. Performans bileşenin alt aşamaları düşünüldüğünde siber risklere yanıt verme aşamasına gelene kadar siber risklerin belirlenmesi, değerlendirilmesi siber saldırıların kurumun hedefleri üzerindeki olası etkilerini en aza indirecek şekilde önlemler alınmasına yardımcı olacaktır. Önemli bir diğer konu siber risklere maruz kalma olasılığına karşı etkin ve güçlü bir kurtarma süreci kritik öneme sahiptir. Bu süreç siber saldırının türüne ve maruz kalma düzeyine göre değişiklik göstermektedir. Örneğin bir kurumun bilgi varlığına ilişkin düzenlenen bir fidye saldırıya karşılık kurtarma işlemi yüksek kayıplara neden olacağı için burada kurtarma süreci büyük öneme sahiptir. Fakat kötü amaçlı yazılımın, çalışanın dizüstü bilgisayarına yüklendiği ve diğer cihazları etkilemeden önce kuruluşun

[5]Kontrol faaliyetleri, hedeflere ulaşılmasına yönelik riskleri azaltmak için yönetimin direktiflerinin takip edilmesini sağlamaya yardımcı olan kurum içindeki bireyler tarafından gerçekleştirilen eylemlerdir.

ağından kaldırıldığı bir olayda kurtarma işlemi o kadar kritik öneme sahip değildir.

5) **Bütüncül ve Geniş Bir Bakış Açısının Geliştirilmesi:** siber risklerin belirlenmesi, değerlendirilmesi ve siber risklere yanıt verilmesi sonucunda kurum siber riske ilişkin bütüncül bir bakış açısı geliştirecek ve değerlendirecektir.

2.4.1.5.4. İnceleme ve gözden geçirme- Siber riskler

İnceleme ve gözden geçirme aşaması, kurum performansını gözden geçirmesi ve zaman içerisinde kurumsal risk yönetim bileşenlerinin nasıl çalıştığını ve revizyon ihtiyacının olup olmadığı yönünde tespitin yapılmasını sağlamaktadır (COSO, 2017, s. 6). İnceleme ve gözden geçirme bileşeni kurumların siber dünyadaki değişiklikler karşısında siber risklerin yönetiminde değişiklik veya iyileştirme ihtiyacına yönelik tespitlerin yapılması aşamasında önemli rol oynamaktadır (COSO, 2019, s. 4).

KRY çerçevesinin dördüncü bileşeni olan inceleme ve gözden geçirme, üç alt bileşenden oluşmaktadır. Bu bileşenler sırasıyla aşağıda siber risklerin yönetimi kapsamında açıklanmıştır (COSO, 2019, s. 13-14):

1) **Önemli Değişikliklerin Değerlendirilmesi:** Kurumların strateji ve iş hedeflerini etkileyecek değişikliklerin belirlemesini ve değerlendirmesini ifade etmektedir (COSO, 2017, s. 10). Kurumların içinde ve dışında değişikliğin yaşanması kaçınılmaz olduğu göz önünde bulundurulduğunda siber risk değerlendirme süreçleri bu değişikliklerle birlikte yinelenmelidir. Bu aşamadaki temel amaç, yaşanan değişikliğin kurum üzerinde nasıl bir etki yarattığı ve siber riskin en iyi nasıl yönetileceğini belirlemektir.
2) **Risk ve Performansın Gözden Geçirilmesi:** bu aşama kurumların performanslarının gözden geçirilerek mevcut ya da potansiyel risklerin tanımlanıp değerlendirilmesidir (COSO, 2017, s. 10). Bu aşamada kurumlar potansiyel siber risk saldırılarını ve tehditlerini belirlemek ve azaltmak için siber güvenlik risk değerlendirme girişimleri sürekli şekilde gözden geçirilmelidir. Yeni teknolojileri kullanmayı tercih eden kurumların riskten kaçınmaları etkili bir strateji olmayacaktır. Bu noktada teknolojideki değişim, iş hedeflerindeki değişiklikler yeni siber riskler ile karşı karşıya

kalmalarına neden olabilir. Bundan ötürü risk değerlendirme süreçlerinde iyileştirme ihtiyacı doğabilir.

3) **KRY ile İlgili Gelişmelerin/Değişiklerin Takip Edilmesi:** Kurumsal risk yönetimin gelişiminin/değişiminin kurumlar tarafından takip edilmesidir (COSO, 2017, s. 10). Kurumlar, siber risk profillerini değiştirebilecek potansiyel gelişmeleri/değişiklikleri yakalamak ve değerlendirmek için yönetişim süreçlerini faaliyete geçirmelidir. Bu değişikleri takip etme sürecine yeni ve değişen ürün ve hizmetler, bilgi teknolojisi ve gelişen dijital stratejileri, iş süreçlerini, işletme birleşmeleri, satın almaları, yeniden düzenlemeler, yasa ve düzenlemelerdeki değişiklikler dahil edilmelidir. Tüm bu öğeler siber risk yönetim programına dahil olan nitelikli kilit paydaşlar tarafından değerlendirilmelidir.

2.4.1.5.5. Bilgi, İletişim ve Raporlama- Siber Risk

COSO Kurumsal Risk Yönetimi- Riskin Strateji ve Performansla Uyumlaştırılması çerçevesinin son bileşeni bilgi, iletişim ve raporlamadır. Bu bileşen kurumların hem yatay hem dikey olarak; içerden ve dışardan bilginin elde edilmesi, paylaşılması ve raporlanması için sürekli bir KRY yapısının oluşturulmasını ifade etmektedir (COSO, 2017, s. 6). Dolayısıyla böyle bir yapı içerisinde yönetim siber risk yönetimini etkin şekilde yürütmek amacıyla hem iç hem de dış kaynaklardan elde edilen bilgiyi kullanmaktadır. Kurumlar bilgi sistemlerinden yararlanarak bilgi ve iletişim elde eder, işler ve yönetmektedir (COSO, 2019, s. 4).

COSO KRY son bileşeni üç alt bileşenden oluşmaktadır. Bu üç alt bileşen siber risk yönetim çerçevesinde aşağıda sırasıyla açıklanmaktadır (COSO, 2019, s. 15-17):

1) **Bilgi Yönetim Sisteminin Güçlendirilmesi:** Bu alt bileşen kurumların kurumsal risk yönetim sistemlerini desteklemeleri amacıyla bilgi ve teknoloji sistemlerini güçlendirmeleri gerektiğini ifade eder (COSO, 2017, s. 10). Bu süreç özellikle siber saldırıların zamanında tespit edilmemesi olasılığına karşılık güvenli, tam, doğru ve ilgili bilginin sağlanmasında kritik öneme sahiptir. Çünkü bilgi, yönetimin karar almasını etkilemektedir. Diğer bir konu ise yönetimin kararlarının gerçek zamanlı olarak alması için bilgi sistemleri sadece bilginin güvenliği için değil aynı zamanda bilginin

raporlanma ve kullanılma hızı için de önemlidir. Burada temel olarak vurgulanan konu, kurumların siber saldırılara karşı gerekli ekipman veya verileri korumak için ihtiyaç duyulan kaynağa sahip olmadıkları takdirde savunmasız olacaklarıdır. Sınırlı BT kaynağına ve aracına sahip olan kurumlar, siber güvenliğin izlenmesi ve raporlanması aşamasında dışarıdan hizmet almayı tercih edebilir. Bu noktada kurum, hizmet sağlayıcı ile düzenli iletişim kurmalı, değişimle birlikte yeni siber tehditleri değerlendirmeli, ani gelişen olaylar karşısında güçlü iletişim kanallarına sahip olmalıdır.

2) **Riske İlişkin Bilginin İletilmesi/Paylaşılması:** Kurumların kurumsal risk yönetimini desteklemek amacıyla iletişim kanalları kurmasını ifade etmektedir (COSO, 2017, s. 10). Kurumlar için temel zorunluluklardan biri, siber riskle ilgili konularda hem iç hem de dış iletişim kurma yeteneğini geliştirmesidir. Çünkü iletişim kurma becerisi; siber risklere karşı çevik olmayı, kuruma karşı ortaya çıkacak tehditleri en kısa sürede fark edilmesini ve önemli siber saldırıların önlenmesinde veya azaltılmasında yardımcı olacaktır. Bir kurumun içinde güçlü iletişim kanallarına sahip olması ne kadar önemli ise hizmet sağlayıcılar ile açık bir iletişim kanalına sahip olması eşit derecede önemlidir.
3) **Risk, Kültür ve Performans ile İlgili Raporlama Yapılması:** Kurumun tüm seviyesini kapsayacak şekilde risk, kültür ve performansı hakkında raporlama yapılması gerektiğini ifade eden alt bileşendir (COSO, 2017, s. 10). KRY yapısının, kurumun siber risklerini etkin şekilde yönetebilmesi adına ilgili ve zamanında raporlama süreçlerini net şekilde tanımlanması gerekmektedir. Siber saldırıları olayı ve konuyla alakalı raporlamanın detayını ilgili taraflara (bilgi güvenliği ekibi, siber risk yönetimi ekibi, üst düzey yönetim, yönetim kurulu) göre değişiklik göstereceğinden ilgili tarafa göre düzenlenmelidir. Kuruma etkisi düşük siber saldırlar ve daha ayrıntılı siber saldırılar, bilgi güvenliği ekibine veya siber risk yönetimi ekibine raporlanmalı ve düzenli olarak güvenlik açıkları giderilmelidir. Fakat kurumun varlıklarının kaybına veya sistemin kesintiye uğraması şeklinde ciddi olaylar üst yönetime hatta bazı durumlarda yönetim kuruluna raporlanmalıdır.

Kurumlar siber risk ile mücadelede yapılandırılmış bir yaklaşımı benimsemeleri zorunluluk haline gelmiştir. COSO KRY çerçevesi siber risklerin belirlenmesi ve yönetilmesi konusunda kurumlara beş bileşeni ve yirmi ilkesinden nasıl yararlanmaları konusunda bakış açısı sunmuştur. COSO KRY çerçevesini kurumlar temel alarak ve diğer açıklanan siber risk konusundaki düzenlemeleri (COBIT,ISO, NIST CSF, ITIL, AICPA) benimseyerek dijital dönüşüm çağında etkin bir siber risk yönetimine hazırlanabilir. Yönetim kurulu, denetim komitesi, şirket yöneticileri güçlü bir tavır sergileyerek kurumun her seviyesinde siber güvenlik bilinci oluşturulmalıdır (COSO, 2019, s. 18). Bir kurumda siber güvenliğin sağlanması aşamasında tüm çalışanların sorumluluğu vardır. Dolayısıyla iç denetçinin bu noktada rolü KRY yapısının oluşturulması aşamasında güvence ve danışmalık hizmeti vermekle rol almaktadır (Can ve Çetin, 2019, s. 165; COSO, 2017, s. 18).

2.4.1.6. AICPA Siber Güvenlik Risk Yönetimi Raporlama Çerçevesi

AICPA (Association of International Certified Professional Accountants), siber güvenlik risk yönetimi programlarının etkinliği hakkında ilgili ve faydalı bilgileri iletirken kuruluşlara yardımcı olan bir siber güvenlik risk yönetimi raporlama çerçevesi geliştirmiştir. Çerçeve, Serbest Muhasebeci Mali Müşavir (Certified Public Accountant-CPA) tarafından bir kurumun siber güvenlik risk yönetimi programı hakkında rapor verdiği siber güvenlik yükümlülükleri için Sistem ve Organizasyon Kontrollerinin (System and Organization Controls- SOC) önemli bir bileşenidir. Bu bilgiler üst yönetimin, yönetim kurullarının, analistlerin, yatırımcıların ve iş ortaklarının kurumların çabalarını daha iyi anlamalarına yardımcı olabilir (COSO, 2019).

2.4.2. Bilgi Sistemleri ile İlgili Ulusal Düzenlemeler

Ulusal düzenlemeler incelendiğinde bu alandaki düzenlemelerin SPK, BDDK ve T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayımlandığına ulaşılmıştır. SPK **"**Bilgi Sistemleri Bağımsız Denetim Tebliği" ve "Bilgi Sistemleri Yönetimi Tebliği" başlıkları halinde tebliğ yayımlarken; BDDK "Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Hakkında Yönetmelik" şeklinde yayımlamıştır. Bu üç kurum tarafından yayımlanan düzenlemelere ilişkin bilgiler aşağıda sırasıyla açıklanmıştır.

2.4.2.1.Bilgi Sistemleri Yönetimi Tebliği ve Bilgi Sistemleri Bağımsız Denetim Tebliği

Ulusal kapsamda yayımlanan düzenlemelerin başında Sermaye Piyasası Kurulu (SPK) tarafından 05.01.2018 tarihinde "Bilgi Sistemleri Bağımsız Denetim Tebliği" ve "Bilgi Sistemleri Yönetimi Tebliği" iki tebliğ yer almaktadır. Bu iki tebliğ çok sayıda kurumu kapsayacak şekilde düzenlenmiştir. Bu kuruluşlar aşağıda sıralanmıştır (SPK, 2018):

- Borsa İstanbul A.Ş.
- Borsalar ve piyasa işleticileri ile teşkilatlanmış diğer pazar yerleri,
- Emeklilik yatırım fonları
- İstanbul Takas ve Saklama Bankası A.Ş.
- Merkezi Kayıt Kuruluşu A.Ş.
- Portföy saklayıcısı kuruluşlar
- Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.
- Sermaye piyasası kurumları
- Halka açık ortaklıklar
- Türkiye Sermaye Piyasaları Birliği
- Türkiye Değerleme Uzmanları Birliği

"Bilgi Sistemleri Yönetimi Tebliği" ile bilgi sistemlerinin yönetimine ilişkin usul ve esaslar belirlenmiş olup "Bilgi Sistemleri Bağımsız Denetim Tebliği" ile bilgi sistemleri bağımsız denetimi faaliyetlerinin genel esasları, denetim metodolojisi, denetim sonuçlarının raporlanması, bilgi sistemleri bağımsız denetimini yürütecek kuruluşların yetkilendirilmesi, yönetici ve çalışanlarının lisanslanmasına ilişkin usul ve esaslar belirlenmiştir (PWC, 2018a, s. 2).

Bu tebliğlerin yürürlüğe girmesiyle öne çıkan başlıca hususlar şöyle sıralanabilir (Deloitte, 2018d, s. 61-62):

- Bilgi sistemi denetçilerinin CISA (Certified Information Systems Auditor-Sertifikalı Bilgi Sistemleri Denetçisi) sertifikası alma zorunluluğu gelmiştir. Bu durum sektörde sertifikalı bilgi sistemleri denetçi sayısını artmıştır.
- Bilgi sistemlerinin iç kontrolleri hakkında yönetim beyanı hazırlama zorunluluğu iç kontrol ve iç denetim ekibinin aksiyonlarını ön plana çıkarmıştır.

- Tebliğler kapsamında yukarıda sıralanan kurumların periyodik zamanlarda bilgi sistemleri denetim ve bilgi sistemleri yönetim tebliğlerine uyum zorunluluğu getirilmiştir.

Bilgi Sistemleri Bağımsız Denetim Tebliği kapsamında denetime tabi olan kuruluşların denetime başlama tarihleri ve periyodlarına ilişkin bilgiler Tablo 2.1'de sunulmuştur.

Tablo 2. 1.*SPK- Bilgi sistemleri bağımsız denetimine ilişkin bilgiler (KPMG, 2018, s. 3; SPK, 2018)*

Kurum, Kuruluş ve Ortaklıklar	Denetim Periyodu	Denetim Başlangıç Tarihi
Borsa İstanbul A.Ş., İstanbul Takas ve Saklama Bankası A.Ş., Merkezi Kayıt Kuruluşu A.Ş., borsalar ve piyasa işleticileri, teşkilatlanmış diğer pazar yerleri, merkezi takas kuruluşları, merkezi saklama kuruluşları ve veri depolama kuruluşları	Her Yıl	2018
Kısmî ve Geniş Yetkili Aracı Kurumlar, asgari özsermaye yükümlülüğü 5 Milyon TL'den fazla olan portföy yönetim şirketleri	İki Yılda Bir	2019
Asgari özsermaye yükümlülüğü 5 Milyon TL ve az olan portföy yönetim şirketleri ve Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.	Üç Yılda Bir	2020
Dar yetkili aracı kurumlar, varlık kiralama şirketleri, ipotek finansmanı kuruluşları, Türkiye Sermaye Piyasaları Birliği, Türkiye Değerleme Uzmanları Birliği, bağımsız denetim, derecelendirme ve değerleme kuruluşları, halka açık ortaklıklar, varlık finansmanı fonları, kolektif yatırım kuruluşları, emeklilik yatırım fonları, konut finansmanı fonları	Periyodik denetim zorunluluğu bulunmamaktadır.	

2.4.2.2.Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Hakkında Yönetmelik

Ulusal çerçevede bir diğer düzenleme ise BDDK (Bankacılık Düzenleme ve Denetleme Kurumu) tarafından 31.12.2021 tarihinde yayımlanmıştır. Bu düzenleme "Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Hakkında Yönetmelik" kurum

gözetimi ve denetimi altındaki kuruluşların bilgi sistemleri ile iş süreçlerinin, bu düzenleme kapsamında yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesine yönelik usul ve esasları düzenlemek amacı ile yayımlanmıştır. (BDDK, 2021). BBDK (2021) yayımlanan yönetmeliğin içeriğine ilişkin önemli görülen bilgiler maddeler şeklinde aşağıda sıralanmıştır.

- Bilgi sistemleri bağımsız denetimi, bilgi sistemlerinin genel kontrollerini kapsarken; iş süreçlerine ilişkin bağımsız denetim ise denetlenen kurumun tabi olduğu kanuni düzenlemeler dikkate alınarak iş süreçleri ve bu süreçler üzerindeki iç kontrolleri kapsamaktadır.
- Bankaların iş süreçlerine ilişkin bağımsız denetimi mevduat süreci, bireysel ve kurumsal kredi süreçleri, muhasebe süreci, banka ve kredi kartları süreci, finansal raporlama süreci, ödeme sistemleri süreçleri, hazine/menkul kıymet ve fon yönetimi sürecinden oluşmaktadır.
- Bankalar, Risk Merkezi ve bilgi alışverişi kuruluşlarında iş süreçleri bağımsız denetimi her yıl, bilgi sistemleri bağımsız denetimi ise iki yılda bir kez yapılır. Diğer finansal kuruluşlarda bilgi sistemleri bağımsız denetimi üç yılda bir yapılır. Denetlenen herhangi bir kurum veya tüm denetlenenlere ilişkin sürelere yönelik değişiklik BDDK bağlıdır.
- Denetçinin taşıması gereken özellikler göze çarpmaktadır. Bilgi sistemleri bağımsız denetçisinin 1 yılı fiilen bilgi sistemleri bağımsız denetimi alanında olmak üzere 3 yıllık mesleki tecrübeye sahip olması; bilgi sistemleri bağımsız kıdemli denetçisinin 2 yılı fiilen bilgi sistemleri bağımsız denetimi alanında olmak üzere 6 yıllık mesleki tecrübeye sahip olması; bilgi sistemleri bağımsız baş denetçisinin 3 yılı fiilen bilgi sistemleri bağımsız denetimi alanında olmak üzere 10 yıllık mesleki tecrübeye sahip olması gerekmektedir.
- Denetçi, iç kontrol ve iç denetim kapsamında yürüttüğü çalışmalar bilgi sistemleri genel kontrolleri ve iş süreçleri ile sınırlıdır.
- Denetçi dilerse denetim yapılmayan yıllara ilişkin bulgularını denetim kapsamına almakla birlikte süreçlerin kapsama eklenme nedenlerini raporda yer vermelidir.

- Bilgi sistemleri bağımsız denetimi ile bağımsız denetimin ilişkisi ele alındığında birbirlerinin kapsam ve sonucunu etkileyecek hususlar içinde barındırmaları sebebiyle etkileşimli bir yaklaşım içinde planlanır ve uygulanır. Ayrıca bilgi sistemleri ve bankalarda iş süreçlerine ilişkin şartlı, olumsuz veya görüşten kaçınma şeklinde görüş oluşması halinde bu görüşün oluşmasına neden olan tespitler yazılı olarak bağımsız denetçiye iletilir.

2.4.2.3.Bilgi ve İletişim Güvenliği Denetim Rehberi

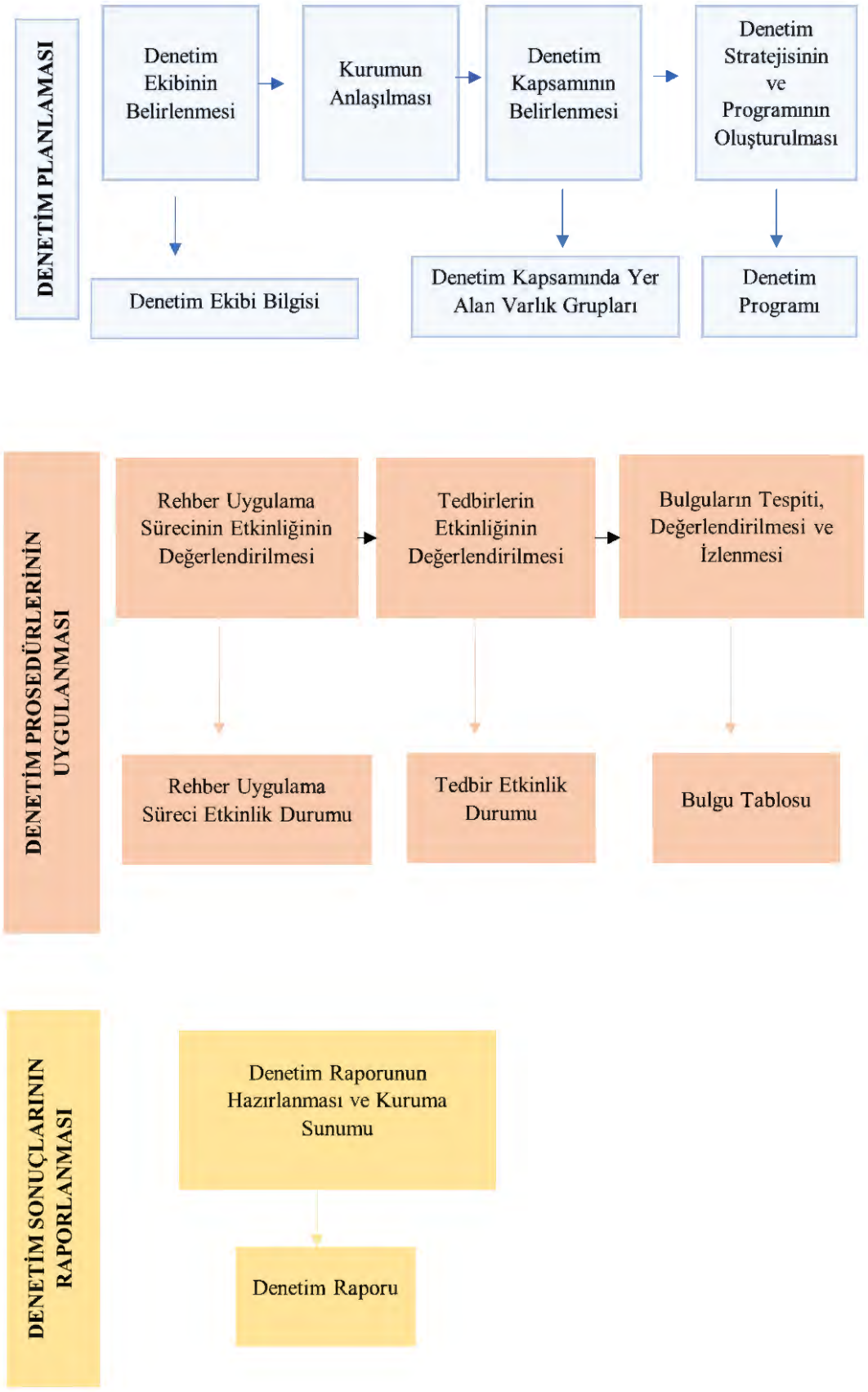
Kamu kurum ve kuruluşları tarafından bilgi sistemlerinde karşılaşılan riskleri yönetmek adına uyulması gereken hususlara ilişkin ilk referans belge özelliğini taşıyan "Bilgi ve İletişim Güvenliği Rehberi" Cumhurbaşkanlığı Genelgesi ile 6 Temmuz 2019 tarihinde ve 30823 sayılı Resmî Gazete 'de yayımlanmıştır. Bu rehberde belirtilen faaliyetlerin kamu kurum ve kuruluşları tarafından kararlaştırılan süre dahilinde tamamlamaları beklenmektedir. Kamu kurum ve kuruluşları tarafından yürütülen ve alınan faaliyetler sonucunda yılda en az bir kez denetim yapmaları beklenmektedir. Denetim faaliyetlerinde kamu kuruluşlarına yol gösterici olması amacıyla "Bilgi ve İletişim Güvenliği Denetim Rehberi" 2021 Ekim ayında T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO) tarafından yayımlanmıştır (DDO, 2021).

Rehber dört bölümden oluşmaktadır. Bunlar:

1. Giriş: rehberin Amacı ve yapısına yönelik açıklamalar mevcuttur.
2. Denetim Çalışmalarına Hazırlık: Rehberin yayımlanmasından itibaren uygulanmasına kadar yapılması gereken hazırlık sürecine ilişkin açıklamalar yer almaktadır.
3. Bilgi ve İletişim Güvenliği Denetim Metodolojisi: Denetimin planlanması ve denetimin prosedürlerinin uygulanması ve denetim sonuçlarının raporlanmasına ilişkin bilgi verilmiştir.
4. Denetim Sonuçlarının Dijital Ofise Gönderilmesi: Denetim sonucunda uygulanan düzeltici ve önleyici faaliyetler, rehberde belirtilen usul ve esaslara göre rapor şeklinde Dijital Dönüşüm Ofisine gönderileceğine ilişkin açıklamalar yer almaktadır.

Rehberle ilgili başlıca konulardan biri denetim faaliyetinin öncelikle iç denetim birimlerinde görev alan ve bilgi teknolojisi alanında görevlendirilen iç denetçiler tarafından yapılması gerektiği üzerinedir. Kurumda iç denetim birimi yoksa veya yeterlik ve yetkinlikte denetçi bulunmadığı durumda diğer kurumlardan veya kurum içinden destek alınarak denetim gerçekleştirileceği belirtilmiştir. Diğer taraftan kurumlar denetim için dışardan hizmet alımı yapabilmektedir. Hizmet alımına ilişkin kurum ve firma/denetçi yükümlülükleri rehberde ayrıntılı şekilde ifade edilmiştir (DDO, 2021, s. 11-14).

Denetim metodolojisine ilişkin açıklamalar incelendiğinde rehberin temel iki hedefi olduğu belirtilmiştir. Birincisi, uygulama sürecinin etkinliği; ikincisi varlık gruplarına uygulanan tedbirlerin etkinliği denetimin temel hedefleri olarak belirlenmiştir. Denetim süreci Şekil 2.8'te ifade edilmiştir (DDO, 2021, s. 17-31).



Şekil 2. 8.*Denetimin ana ve alt süreçleri (DDO, 2021, s.17)*

Denetimin planlanması aşamasında denetimin temel hedeflerine ulaşması sebebiyle takip edilmesi gereken adımları kapsamaktadır. Denetimin verimli şekilde yürütülmesi adına yol haritası niteliğindedir. Denetim planlanması kısmında denetim ekibinin belirlenmesi, kurumun anlaşılması, denetim kapsamının belirlenmesi, denetim stratejisi ve denetim programının hazırlanması şeklinde dört başlık yer almaktadır. Denetim ekibinin belirlenmesi aşamasında bir konuya dikkat çekmekte yarar vardır. Denetim ekibi oluşturulurken yetkinliği yönünden belli kıstaslar belirlenmiştir. Denetçi ya ISO/IEC 27001 Baş denetçi sertifikasına sahip olması veya CISA sertifikasına sahip olması ya da belgelendirme programı kapsamında yetkilendirilmiş denetçi veya baş denetçi olması gerekmektedir. Bu üç şarttan birini taşıyan en az iki kişiden oluşan bir denetim ekibi oluşturulma zorunluluğu bulunmaktadır. Kurumun anlaşılması kısmında kurumun organizasyon yapısından üçüncü taraflara, iş süreçlerinden önceki dönem raporlarına, mevzuattan kaynaklı yükümlülüklerden kurumun varlık gruplarına kadar birçok konuda denetim ekibi kurumu incelemelidir. Denetim kapsamı belirlenirken rehbere uyum kapsamında hangi varlık gruplarının denetim kapsamına dahil edileceği belirlenir. Bu noktada risk tabanlı denetim yaklaşımı ve önemlilik kriteri temel alınmalıdır. Tüm bu aşamalardan sonra denetim ekibinin kurumun etkinliğini nasıl değerlendireceği konusunda bir denetim stratejisi ve programı oluşturulmalıdır (DDO, 2021, s. 18-23).

Denetim prosedürlerinin uygulanma aşaması varlık gruplarının güvenliğini sağlama amacıyla alınan tedbirlerin etkinliğini değerlendirme sırasında hangi denetim yöntemlerinin kullanılacağını, denetim görüşünün oluşturulması denetim kanıtının nasıl toplanacağını, elde edilen bulguların değerlendirilmesini ve sınıflandırma yöntemlerini kapsamaktadır (DDO, 2021, s. 23-30).

Denetim ekibinin, kurumun faaliyetlerini rehbere uyumlu şekilde yürütüp yürütmediğine ilişkin kanaatini denetim raporunda beyan etmektedir. Eğer denetim ekibi görüşünü oluşturmak için ihtiyacı olan yeterli seviyede dokümana ulaşması konusunda kurum tarafından bir engellenme veya dokümanın sağlanmadığı durumlarda, kurumun ilgili birimlerine konu hakkında yazılı bilgi sunmalıdır. Denetim raporu denetim ekibi tarafından elektronik imza ile imzalanır. Denetim raporu gizlilik niteliğinde bilgi olması sebebiyle denetim raporu herhangi bir yerde yayımlanmamaktadır. Ayrıca denetim ekibi kurum dışından bir uygulama, cihaz vb. araç kullandığı takdirde denetim çalışması

tamamlandıktan sonra bu araçlardaki bilgiler geri döndürülemeyecek şekilde silinmesi hatta imha edilmesi gerektiği rehberde belirtilmiştir (DDO, 2021, s. 31-32).

Son aşamada denetim raporunun tamamlanmasının akabinde denetim sonuçlarının dijital dönüşüm ofisine gönderilmesi aşamasına geçilmektedir. Denetim raporunun tamamlanma tarihinden itibaren en geç iki ay içinde denetim ekibi, varlık grubu ve denetim kapsamı, rehber uygulama süreci etkinlik durumu, tedbir etkinlik durumu, denetim görüşü hakkındaki bilgilerin yer aldığı rapor ofise iletilmelidir. Ayrıca denetimin gerçekleşmediği kurumların üst yöneticileri sebebini dijital dönüşüm ofisine bildirmelidir (DDO, 2021, s. 35).

2.5. Siber Risklerin Yönetimi ve İç Denetim Fonksiyonu

Dijital dönüşümden kaynaklı riskleri yönetmek adına iç denetim fonksiyonun üstlendiği görev kapsamında aşağıda açıklama yapılmıştır. Dijitalleşme denilince başlıca risk olarak siber risk ifade edilmesi sebebiyle bu kapsamda özellikle siber riskler karşısında iç denetimin fonksiyonunun rolü ve önemi ele alınmıştır.

2.5.1.Üçlü hat modeli

Teknolojide yaşanan hızlı gelişmeler, ekonomik eşitsizlikte artış, küreselleşme, iklim değişikliği, yaşanan sağlık krizleri şeklinde konular belirsizliğin artışına bununla birlikte risklerin çeşitlenerek stratejik, itibar, operasyonel, finansal, yasal ve siber risklerin önem kazanmasına neden olmaktadır. Dolayısıyla tüm bu risklerin kurumlar tarafından yönetimi ve izlenmesi zorluğu sebebiyle IIA tarafından 2013 yılı Ocak ayı itibariyle resmi olarak uygulanmasını önerdiği ilk ismiyle "Etkili Risk Yönetimi ve Kontrolünde Üçlü Savunma Hattı" (The Three Lines Of Defence In Efecttive Risk Management and Control) başlığı ile kısaca "Üçlü Savunma Hattı" modelini tasarlamıştır. Yaşanan gelişmeler ve değişim sebebiyle modelin üzerinde güncelleme yapılacağı IIA tarafından 2019 yılında üyeleri ve ilgili paydaşları ile paylaşılarak güncelleme konusunda görüş alma süreci başlatılmıştır (Özbilger, 2021, s. 41; IIA, 2020a, s. 2; Burca, 2020).

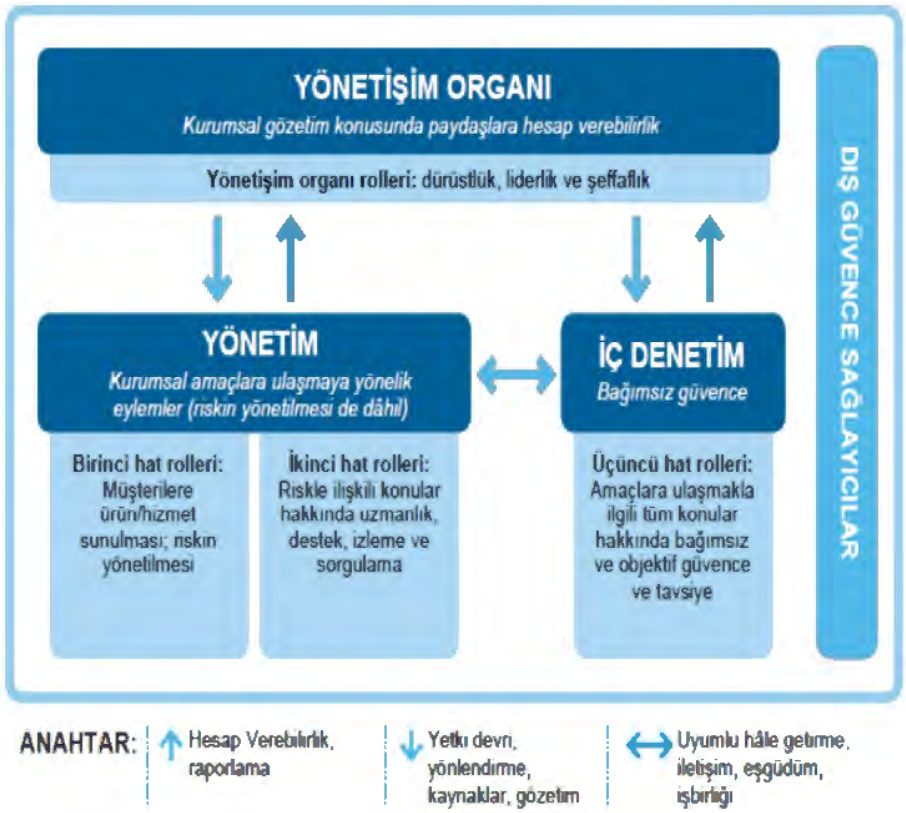
Üçlü Savunma Hattı'nın güncellenmiş yeni modeli 20 Temmuz 2020 tarihinde IIA tarafından "Üçlü Hat Modeli" başlığı ile yayımlanmıştır. Güncellenme sonucunda üçlü hat modelinin kurumların amaçlarına ulaşmalarını en iyi şekilde sağlayacak güçlü yönetişim ve risk yönetimi yapı ve süreçlerinin belirlenmesine ve tasarlanması

konusunda yardımcı olacağı ifade edilmektedir. Güncellenen yeni model yönetişim organı, yönetim ve iç denetim olmak üzere üç önemli aktörü vurgulamaktadır (IIA, 2020a, s. 2). Güncellenen yeni model Şekil 2.9'da sunulmuştur. Modelin güncellenmesinde temel sebep, iç denetimin üçüncü savunma hattı olarak ifade edilmesinin yeni koşullara uyum sağlamaması gösterilmektedir. Bu ifade Uluslararası Mesleki Uygulama Çerçevesi'nde (UMUÇ) yer alan iç denetim misyonunu; "risk bazlı objektif güvence sağlayarak, tavsiye ve iç görülerle kurumsal değeri korumak ve geliştirmek" karşılamamasıdır. Güncelleme sonucunda temel değişiklikler şöyledir (Özbilger, 2021, s. 44-45; IIA, 2020b, s. 9; Chambers, 2020):

- Eski modelde bir şeye karşı müdahale etme anlamında kullanılan "savunma" kelimesinin yeni güncelleme ile yer almadığı görülmektedir. Bu değişimle risk yönetiminin sadece risk almama ve riski minimize etmeden ibaret olmadığı; bunun yerine riskin proaktif bir şekilde yönetilmesi üzerine kurulu bir yapının olması gerektiği vurgulamak amaçlanmaktadır.
- Modelde diğer bir değişiklik ise altı temel ilkeden oluşan ilkesel bir modellemeye dönüştüğü görülmektedir. Bu altı ilke aşağıda kısaca açıklanmıştır:
  - ❖ Yönetişim: Yönetişim ile bir kurumun yönetimi hesap verebilirlik, eyleme geçmek ve güvence sağlayan uygun yapılar ve süreçler gerektiren üçlü saç ayağından oluşması ifade edilmiştir.
  - ❖ Yönetişim organının rolleri: yönetişim organı kurumun hedeflerine ulaşmasında etkili yönetişim için uygun yapı ve süreçlerin uygulanmasında paydaş çıkarının gözetildiği; yasal, düzenleyici ve etik beklentilerin karşılanmasını temin etmenin yanında kurum hedeflerine ulaşmasında yönetime sorumluluk devrettiği; kurum hedefleri gerçekleştirilirken bağımsız, tarafsız ve yetkin bir iç denetim fonksiyonu kurulmasında rolleri vardır.
  - ❖ Yönetim, birinci ve ikinci hat modeli: kurumların amaçlarına ulaşma sürecinde hem birinci hat hem de ikinci hat rollerini kapsamaktadır. Diğer bir ifadeyle birinci ve ikinci karşılıklı etkileşim halinde olabilir veya ayrılabilir.
  - ❖ Üçüncü hattın rolleri: iç denetim fonksiyonunun ifade edildiği ilkedir.

- ❖ Üçüncü hattın bağımsızlığı: İç denetimin bağımsızlığı, objektifliği konularında vurgu yapılmaktadır.
- ❖ Değer katma ve koruma: altıncı ilke olan değer katma ve koruma kapsamında paydaşların çıkarları gözetildiğinde değer yaratılması ve korunmasında yönetişim organı birinci, ikinci ve üçüncü hat rolleri hep birlikte katkı sağladığı ele alınmıştır.

- İlk modelden farklı olarak "Üçlü Hat Modeli" düzenleyici kurumlar ve dış güvence sağlayıcıları tek başlık altında ele alınmıştır.
- Eski modelden farklı olarak yeni modelde sadece üst yönetime ilişkin dikey bir iletişim yerine kurum içinde hem yatay hem dikey olmak üzere her yöne doğru iletişim benimsenmiştir. Eski modelden farklı olarak birimler yerine rol, sorumluluk ve roller arası ilişki net bir şekilde tanımlanmıştır. İlk modele göre modele daha fazla dâhil edilen, dürüstlük, şeffaflık ve liderlik rollerini yönetişim organına; ürün ve hizmetlerin sunulması ve risklerin yönetilmesi (birinci role), uzmanlık, destek, sorgulama ve izleme (ikinci role) rollerini birinci ve ikinci hatların birleşimi şeklinde oluşturulan yönetim organına; kurumsal amaç ve hedeflere taşıyacak faaliyetler hakkında bağımsız ve objektif bir şekilde güvence ve danışmanlık sağlayıcı rolü iç denetim organına (üçüncü role) verilmiştir.



Şekil 2. 9. *Üçlü savunma hattının modernize edilmiş versiyonu olarak üçlü hat modeli (IIA, 2020, s.9)*

Güncellenen modelde en önemli konu yönetişim unsuru kapsamında kontrolleri içerecek şekilde risklere yanıt verme sürecinin etkinliği ve yeterliliği konusunda güvence ihtiyacını güçlendirmektir. Bu güvence, iç denetim tarafından sağlanabilir (IIA, 2020a, s. 5).

2.5.1.1.Birinci hat rolü

Birinci hattı, risklere ve kontrollere sahip olan ve bunları yöneten ve süreç ve kontrol eksikliklerini gidermek için düzeltici eylemler uygulayan operasyon yöneticilerinden oluşmaktadır. Siber güvenliğin sağlanması adına kurumlar birden fazla düzeltici eylem pozisyonu oluşturabilir. Kurumlarda teknoloji yöneticisi (CTO- Chief Technology Officer), kurumun misyonunu devam ettirmek maksadıyla mevcut teknolojilerle ilgili bilgi ve yönlendirme sağlamaktan sorumlu kişidir. Teknoloji yöneticisi genel itibariyle kurumun fikri mülkiyetini koruma sorumluluğuna sahiptir. Ayrıca teknoloji yöneticisinin görevleri arasında; kurumun rekabet avantajı sağlaması, stratejik değişim ve inovasyonu mümkün kılacak teknolojik gelişimin sonraki

aşamalarına hazırlanmasını sağlamaktır. Kurum, siber güvenliğinin sağlanması için teknoloji yöneticisinin (CTO) yanında güvenlik görevlisi (CSO- Chief Security Officer), bilgi güvenliği yöneticisi (CISO- Chief Information Security Officer) veya bilgi teknolojisi (BT) güvenliğinden sorumlu başka bir kişiyi görevlendirebilir. Siber tehditleri belirleme ve anlamada ana aktör olarak CSO veya CISO siber güvenlik strateji oluşturma ve geliştirme, güvenlik politika ve prosedür güçlendirmede rol üstlenirler. Rol üstlendikleri bir diğer konu ise kurumun varlıklarını ve paydaş verilerini uygun şekilde korunmasını sağlamada gözetim programları geliştirme aşamasıdır. Sorumlu bu kişilerin yanında diğer bir sorumlu kişi bilgi yöneticisidir (CIO- Chief Information Officer). Bilgi yöneticisi, kuruluşun rekabet avantajı elde etmesi ve strateji değiştirmede sorumluluğa sahiptir. Bu noktada CIO siber güvenlik programlarının geliştirilmesi, siber güvenlik eğitim programlarının oluşturulması ve uygulanması, siber güvenlik politikalarının oluşturulması aşamasında rol oynamaktadır. Tüm bu aşamaya kadar bahsedilen sorumlu kişiler (CTO, CSO, CISO ve CIO) siber saldırılar ve siber suçlar ile mücadelede üst düzey yönetim ile iletişim halinde olmalıdır. Kurum içinde her bir bölüm eğer kendi sorumluluğunu almışsa, bu durum işletme içindeki diğer risk değerlendirme faaliyetleri ile koordineli olarak teknolojilerini ve verilerini güvence altına almak için uygun kontrollerin tasarlanması ve uygulama sorumluluğunu üstlenmektedir. Yukarıda bahsedilen sorumluluklar yerine getirilmediği takdirde siber güvenlik riskine cevap vermek yetkili bir birimin oluşturulması veya BT yöneticileri ile sağlanabilir (IIA, 2016a, s. 6-9).

Birinci hat rolünde yaygın şekilde yürütülen faaliyetler şöyle sıralanmıştır (IIA, 2016a, s. 7):

- Siber güvenliğe ilişkin prosedürlerin, eğitimlerin ve testlerin yönetilmesi,
- Güvenli cihaz yapılandırmalarının, güncel yazılımların ve güvenlik yamalarının yapılması,
- Saldırı tespit sistemini etkin kullanmak ve sızma testlerinin yürütülmesi,
- Network trafiği akışını uygun şekilde yönetmek ve korumak için güvenli bir şekilde network yapılandırması,
- 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 saldırıların amacı, sistemleri çökertmek veya verileri elde etmek olduğundan genellikle önemli verilerin toplandığı her yerde (veri merkezleri, iç ağlar, dış ortak çevre, iş sürekliliği platformalar) siber saldırıların gerçekleşme olasılığı vardır. Siber saldırıların nereden geldiğinden ziyade saldırı sonucu kuruma verdiği zarar önemlidir. Siber saldırılar sonucunda kurumlar mevzuat ihlali, para cezaları, itibar ve gelir kaybı şeklinde olumsuz etkilerle karşı karşıya kalabilirler (IIA, 2016a, s. 8).

Kurumlar için önemli olan veriler kurum içinde, kurum dışında veya her iki yöntemin birlikte kullanılması tercih edilerek depolanabilir. Kurum içinde saklanması tercih edilmesi halinde kurumlar birinci hat rolü olarak güvenli yapılandırmalar, güvenlik duvarları ve erişim kontrolleri gibi teknolojilere güvenmektedir. Bu önlemlerin mutlak güvenlik sağlaması beklenmemeli çünkü güvenlik duvarını aşmak için yapılan özel bir saldırının gerçekleşmesi halinde istenmeyen erişim sağlanabilir veya yetkisiz bir işlem gerçekleştirilebilir. Dolayısıyla bu tür siber saldırılara karşı güvenlik duvarını aşma riskini azaltmak için birinci hat, ağın çevresinde önleyici tedbirler almaktadır. Bu aşama yetkisiz iş yapma ve sınırlı erişimi içeren zorlu bir süreci kapsamaktadır. Yazılım ürünleri ve kötü amaçlı web siteleri hakkında elde edilen bilgiye dayalı olarak bilinen güvenlik açıklarını izlemek amacıyla tespit edici kontroller kurulmalıdır. Birçok kurum ağ trafiğinden kaynaklı olarak bir beyaz liste ve blok konulan kara liste oluşturmaktadır. Bu listeler, aktif izleme ve ağ trafiğinin dinamik bir yapıya sahip olması nedeniyle sürekli güncellenmesi tavsiye edilmektedir (IIA, 2016a, s. 8). Ayrıca kurumlarda veri güvenliğine ilişkin tek sorumluluk bilişim uzmanlarına ait değil, kurumda herkesin sorumluluğu vardır. Veri güvenliğinin sağlanması noktasında teknik önlemleri almanın yanında insan faktörü de göz önünde bulundurulmalıdır. Kurumlar veri güvenliğini sağlamak için sadece dış etkenlere odaklanmak yerine kurum içi insan doğası, davranışları, ilişkilerini odaklanan hem veri güvenliği hem de örgüt kültürünü birleştiren strateji benimsemelidir (Chang and Lin, 2007, s. 452).

Bulut depolama veri sahiplerinin (kurumların) verilerini yerel bilgi işlem sistemlerinden buluta taşımasına olanak tanıyan önemli bir bulut bilişim hizmetidir. Veri sahipleri giderek daha fazla, verilerini buluta taşımayı tercih ediyor. Bunun ana nedeni özellikle küçük ve orta ölçekli kurumlar için geçerli olan maliyet etkinliğidir. Veri sahipleri, verilerini buluta taşıyarak, pahalı altyapı kurulumunun, büyük ekipmanların ve günlük bakım maliyetlerinin ilk yatırımını önleyebilmektedir (Yang and Jia, 2012, s. 410). Bahsedilen yararların yanında verilerin kurum dışında depolandığı durumda hizmet sağlayıcısının riskleri en aza indirgemesi ve risklerden korunması göz ardı edilmemelidir. Kurumların verilerini dışarıda depolamayı tercih etmeleri halinde birinci hat rolü için en önemli adım olarak aşağıda sıralananları barındıran güçlü sözleşmeler oluşturulması gösterilmektedir (IIA, 2016a, s. 8):

- Hizmet kuruluşu kontrol (SOC-Service Organization Control) raporları,
- Denetim hakkı şartları
- Hizmet seviyesi anlaşmaları (SLA-Service Level Agreements)
- Siber güvenlik inceleme yükümlülükleri

Sözleşmeye yönelik anlaşma yapıldıktan sonra yönetim, hizmet seviyesi anlaşmalarına uygunluğun sağlanması amacıyla önemli metrikler üzerinde izleme ve raporlama yoluyla hizmet sağlayıcıyı denetlemelidir. Hizmet sağlayıcı sözleşme gerekliliğini yerine getirmemesi halinde işletme yönetimi sorunların zamanında çözümünü talep edebilir, cezaları güçlendirebilir ve eğer gerekli görürse alternatif bir hizmet sağlayıcı aramayı düşünebilir.

Kurum yönetiminin bir diğer dikkat etmesi gereken konu ise en zorlu siber güvenlik tehditlerinden biri olarak ortaya çıkan sosyal mühendisliktir (Aldawood and Skinner, 2018, s. 62). Sosyal mühendislik saldırıları e-dolandırıcılık/ kimlik avı e-postaları ve kötü amaçlı telefon aramalar şeklinde saldırılar olup manipülasyon yoluyla insan zayıflıklarından yararlanma uygulamasıdır (IIA, 2016a, s. 8; Aldawood and Skinner, 2018, s. 62). Bu tür saldırılar bilgi veya eylem ihtiyacı olan meşru bir kuruluşu veya kişiyi taklit etmesi sonucu yetkili kişilerden hassas verilerin paylaşımı, sistem kimlik bilgilerine ulaşım izni, sahte web sitelere yönlendirilerek tıklanma veya hedef kişinin bilgisayarına kötü amaçlı yazılımların yüklenmesi şeklinde olumsuz eylemlere ikna edilmesiyle gerçekleştirilir. Kötü amaçlı yazılım yüklendikten sonra, kurumun ağında çoğalabilir,

sistem performansını ve kullanılabilirliğini bozabilir, verileri çalabilir ve saldırganların dolandırıcılık girişimlerinin ilerletebilmesine sebep olabilir (IIA, 2016a, s. 9).

Kurumlar giderek bilgi işlemeye büyük ölçüde bağımlı hale gelmektedir. Sonuç olarak, kurumlar bilgi güvenliğine yönelik tehditleri azaltmak için teknik önlemler uygulamaktadır. Ancak, çalışanlar potansiyel güvenlik risklerinin farkında olmadığı sürece teknik önlemler yetersiz kalacaktır (Lebek vd., 2013, s. 2978). Kurumsal önceliklerin gerçekleştirilmesi için hayati önem taşıyan siber güvenlik güvence sürecinin iş birimleri genelinde farkındalığının sağlanması önemlidir. Günlük çalışma ortamında iş birimleri ve ilgili personel arasında stratejik iş birliğini ve bilgi alışverişini desteklemek ve kolaylaştırmak için siber güvenlik güvencesinin kurumsal politikalarla koordinasyonu ve uyumuna ihtiyaç vardır (Kahyaoglu and Caliyurt, 2018, s. 366). Kötü amaçlı yazılımlar, farkındalık eksikliğinden yararlanılarak geliştirilir. Bu nedenle, kişilere (kurum çalışanlarına) şüpheli veya olağandışı e-postalar, daha önce karşılaşılmamış istekler, telefon görüşmeleri veya sistem etkinliğine karşı tetikte olmalarını sık sık hatırlatmak önemlidir. Eğitim bu tür siber saldırılara karşı bireylerin hayali iletişimleri tanımasına ve bu tür saldırıları araştırma, iletme ve çözüm için hızlı bir şekilde raporlamasına yardımcı olacaktır. Sektördeki meslektaşlardan öğrenilen dersler ve edinilen bilgiler eğitim, farkındalık ve ek önleyici tedbirlerin benimsenmesi adına etkili olacaktır (IIA, 2016a, s. 9).

2.5.1.2.İkinci hat rolü

İkinci hat rolünde BT risk yönetimi ve BT uyumluluk işlevlerinden oluşmaktadır. Kurumlar giderek daha fazla teknolojiye bağımlı hale geldiğinden, BT tehditlerine karşı daha savunmasız hale geliyorlar. Bu nedenle kurumların risk analizlerini doğru yapmaları, risk düzeylerini belirlemeleri ve buna göre önlem almaları gerekmektedir (Bandyopadhyay, Mykytyn and Mykytyn, 1999, s. 443). Bir kurumun güvenlik durumu ve program tasarımında ikinci hat rolü önemli görev üstlenmektedir. İkinci hat rolü sorumlulukları şöyle sıralanmıştır (IIA, 2016a, s. 9):

- Siber güvenlikle ilgili riskleri değerlendirmek ve bunların kurumun risk iştahıyla uyumlu olup olmadığını belirlemek.
- Mevcut ve ortaya çıkan riskleri, yasa ve yönetmeliklerdeki değişiklikleri izlemek.

- Uygun kontrol tasarımını sağlamak için birinci hat rolü ile iş birliği yapmak.

Siber riskler, iş beklentilerine yönelik tehditler listesinin en üstüne çıkmıştır. Harvard "Business Review Analytic Services" tarafından PWC sponsorluğunda 168 ABD'li yöneticinin katıldığı 2020 anketinde, ankete katılanların %74'ü siber riski şirketlerinin karşı karşıya olduğu en büyük üç riskten biri olarak nitelendirmektedir (HBR, 2020, s. 1). Siber güvenlik riskleri, çoğu geleneksel riskten belirgin şekilde daha dinamiktir ve zamanında müdahale gerektirmektedir. Riskler ve kurumların bunlara maruz kalması değiştikçe ikinci hat rolü, gelişen tehdit ortamına cevap verebilmesi için kurumu hazırlamak ve güvence almak için yönetişim ve gözetimi yönlendirmede kritik role sahiptir. Güvenlik ihlali, bir kurumun risk iştahının yanında devlet yönetiminin konu hakkında düzenlemelerinde de değişikliklere sebep olabilir (IIA, 2016a, s. 9).

İkinci hat rolleri risk yönetim uygulamalarına odaklanmaktadır. Bu risk yönetim uygulamalarının odak noktasında kanuni düzenlemeler, etik davranışlar, iç kontroller, sürdürülebilirlik, kalite güvencesi şeklinde konuların yanı sıra bilgi ve teknolojide yer almaktadır. Üçlü hat modelinin ikinci hattının temel ilkelerinden biri risk yönetiminin etkinliğine yönelik analizlerin yapılması ve rapor sunulmasıdır. (IIA, 2020b, s. 6). İkinci hat rolü yönetim kurulu veya yönetim organları arasında etkili bir farkındalık yaratmak ve siber güvenlik riskleri ve kontrolleri hakkında raporlamanın yeterli ve güncel olmasını sağlamak için birinci hat rolleri ve üçüncü hat rolleri ile iş birliği içinde çalışmalıdır. İkinci hat rolü risk değerlendirmelerini gerçekleştirip raporlarken, siber güvenliği bir öncelik olarak tutmaya devam etmelidir. Ayrıca, sektöre ve kurum türüne bağlı olarak özel bir siber güvenlik risk değerlendirmesi ile desteklenmelidir. İkinci hat rolünde siber riskler açık şekilde belirlenmelidir (IIA, 2016a, s. 10).

Kurumlar kritik iş süreçlerinde kilit satıcılardan ve tedarikçilerden faydalanırken ve pandeminin ardından ekonomik iyileşme hız kazanırken, üçüncü taraf risk yönetimi her zamankinden daha önemli hale gelmiştir. KPMG (2022, s. 4) tarafından dünya çapında 16 ülkede, altı sektörde ve 1.263 kıdemli üçüncü taraf risk yönetimi uzmanıyla yapılan ankette kurumların yüzde 85'i için üçüncü taraf risk yönetiminin stratejik bir öncelik olduğu ortaya konulmuştur. İkinci hat rolü, hizmet sağlayıcılarının kurum ağına doğrudan bağlantısı veya veri aktarımı yöntemleriyle hassas sınıflandırılmış verilere erişimi olabileceğinden, siber güvenlik riski açısından bu üçüncü taraf hizmet sağlayıcılarla olan ilişkileri değerlendirilmesi gerekebilmektedir. Bu noktada teknik ve sözleşmeye dayalı

kontrol hükümleri gözden geçirilmelidir. Bunun yanında hizmet sağlayıcısının anlaşmaya varılan siber güvenlik kontrolleri hakkında yeterli raporlama ile düzenli aralıklarla güvence sağlamaları önemlilik arz etmektedir. Özetle ikinci hat rolü, verilerin kurum dışında depolanması tercih edilmesi durumunda yönetimin siber güvenlik riskiyle ilgili hizmet sağlayıcısının yönetişimini sağlamaktan sorumludur. Bu tür bir yönetişim hizmet sağlayıcısı beklentilere veya SLA'lara uymadığında, kontrol raporlarının alınmasını ve gözden geçirilmesini, kontrol faaliyetlerinin izlenmesini ve hizmet sağlayıcısı risk komitesi gibi kuruluş içindeki yönetim organlarına risklerin uygun şekilde iletilmesini içermektedir (IIA, 2016a, s. 10).

İkinci hat rolünde siber güvenliğe yönelik yaygın şekilde yürütülen faaliyetler şöyle sıralanmıştır (IIA, 2016a, s. 9):

- Siber güvenlik politikalarının, eğitimlerin ve testlerin tasarlaması,
- Siber risk değerlendirmelerinin yapılması,
- Siber tehditte ilişkin bilgilerin toplanması,
- Verileri sınıflandırılması ve kısıtlı erişim rollerinin tasarlanması,
- Olayların, temel risk göstergelerinin izlenmesi ve iyileştirilmesi,
- Sertifikalı BT risk personelinin işe alınması ve devamlılığının sağlanması,
- Üçüncü taraflar, tedarikçiler ve hizmet sağlayıcılarla ilişkilerin değerlendirilmesi,
- İş sürekliliğinin planlanması/test edilmesi ve olağanüstü durumların iyileştirilmesi ve testlerine katılım.

2.5.1.3.Üçüncü hat rolü

Uluslararası İç Denetçiler Standardında iç denetim fonksiyonun teknoloji karşısında sorumluluğu Standart 2110.A2'de "İç denetim faaliyeti, kurumun bilgi teknolojileri yönetişiminin kurumun strateji ve amaçlarını destekleyip desteklemediğini değerlendirmek zorundadır" şeklinde ifade edilmektedir (IIA, 2017a). İç denetim faaliyetlerini kapsayan üçüncü hat rolü, özellikle siber güvenlik sağlanmasında ikinci hat rolü ile koordinasyonda önemli bir rol üstlenmektedir. İç denetim birimi siber güvenlik konusunda şu konular hakkında kurumlara danışmanlık yapabilir (IIA, 2016a, s. 11-12):

- Siber güvenlik ve kurumsal risk arasındaki ilişki kurmak,

- Siber risklere karşı verilecek yanıtlar ve kontrol faaliyetlerine öncelik vermek,
- Kurumun tüm ilgili yönlerinde siber güvenlik riskinin azaltılması için denetim yapmak; örneğin imtiyazlı erişim, ağ tasarımı, hizmet sağlayıcı yönetimi, izleme vb.
- İyileştirme faaliyetlerinde güvence sağlamak,
- Birinci ve ikinci hat rolleri yeterli seviyede olgunlaşmamış kurumlarda risk farkındalığını artırmak ve siber güvenlik risk yönetimi ile koordinasyon sağlamak,
- Siber güvenlik hükümlerinin kurumun iş sürekliliği planlarına ve olağanüstü durum iyileştirme test çalışmalarına dahil edilip edilmediğini doğrulamak.

IIA Standardı 2120: Risk Yönetimi kapsamında gerekli olan risk yönetimi sürecinin etkinliğini değerlendirmenin bir parçası olarak, iç denetim faaliyetinin rolü, kurumun risk yönetim süreçlerine uyumu sağlamak için siber güvenlik risklerini ve kontrollerini bağımsız olarak değerlendirmektir. Dolayısıyla bu risk değerlendirme aşamasında ikinci hat rolünde belirlenen çerçeveler, standartlar, risk değerlendirme ve yönetişim ile ilgili yeterliliğin gözden geçirilmesini kapsamaktadır. Ayrıca iç denetim faaliyetleri birinci hat rolündeki kontrollerin etkinliğini de değerlendirmektedir. Siber güvenlik risklerini azaltmak için BT genel kontrolleri önemli olmakla birlikte siber riskler için tamamen çözüm sağlamamaktadır. Dolayısıyla siber riskin karmaşıklığından kaynaklı ek kontrollere ihtiyaç vardır. Geleneksel anlayışa dayalı güvence faaliyetleri siber güvenlik riskini karşılamadığından yenilikçi bir güvence stratejisine ihtiyaç vardır. Bu noktada güvence yapılandırmalarındaki değişiklikleri, ortaya çıkan risk aykırı değerler ve eğilimler, yanıt süreleri ve iyileştirme alternatifleri değerlendirmek için sürekli denetim teknikleri gereklidir (IIA, 2016a, s. 12). İç denetim fonksiyonunun, dijital öncelikli bir ortamda eski metodolojileri kullanmaya devam edemeyeceği ve iç denetim fonksiyonunun başarılı olabilmesi için bütünsel bir dijital dönüşümden geçmesi gerektiği Nair (2022) tarafından da vurgulanmaktadır. Ayrıca bu dönüşümün yalnızca iç denetçilerin iç denetim görevlerini yerine getirmek için teknolojik araçları kullanmasıyla eksik olacağı aynı zamanda bir zihniyet değişikliği ve beceri seti uyarlaması gerektiğine dikkat çekmektedir.

Siber güvenlik konusu sadece siber güvenlik uzman sorumluluğu olan kişileri ilgilendiren bir konu değildir. Çünkü kurumlar bir siber güvenlik başarısızlığı sonucu birçok yönden (fikri mülkiyet kaybı, itibar kaybı vb.) zarara uğramaktadır. Dolayısıyla siber güvenliğin bir teknoloji riskinden daha öteye taşındığı ve iş riski haline geldiği göz önüne alındığında iç denetçiler siber güvenliğin sağlanmasında önemli role sahiplerdir. Siber güvenlik konusunda iç denetim yöneticilerinin benimsediği yaklaşımlar önemli olduğu kadar yönetim kurulu, denetim komitesi ve üst yönetimde önem vermesi gerekmektedir. Eskiye oranla siber güvenliğin sağlanamamasının sonuçlarının kurumlara etkileri daha fazla bilindiğinden yönetim kurulunun siber güvenliğe ilgisi artmıştır. İç denetim biriminin yönetim kurulu, denetim komitesi ve üst yönetime erişim kolaylığı düşünüldüğünde siber güvenlik konusunu bu üç grubun gündeminde yer almasında etkisi olduğu söylenebilir. İç denetim yöneticileri bu gruplara ilgili raporlama yapmaları sonucu siber güvenlik konusuna ilgilerini çekebilir, ilgili çalışmaların ve güncellemelerin yapılmasını sağlayabilir. İç denetim yöneticileri kurumların sahip olduğu siber güvenlik projelerinin etkinliği, bu projelere aktarılan kaynağın verimli kullanılıp kullanılmadığı ve olası saldırılara karşı yeterli seviyede olup olmadığı konusunda tavsiyeler sunmalıdır (IIA, 2016b, s. 3-6). Bir iç denetçi yöneticisi, kurumun siber güvenlikle ilgili yönetişimi değerlendirirken dikkate alması gereken 10 soru aşağıda belirtilmiştir (IIA, 2016a, s. 13-14):

1. Üst yönetim ve yönetim organı (denetim komitesi, yönetim kurulu, vb.) siber güvenlikle ilgili temel risklerin farkında mı? Siber güvenlik girişimleri yeterli destek ve öncelik veriliyor mu?
2. Yönetim, siber tehditlere veya güvenlik ihlallerine hassas varlıkları belirlemek için bir risk değerlendirmesi yaptı mı ve potansiyel etki (finansal ve finansal olmayan) değerlendirildi mi?
3. Birinci ve ikinci hat rolleri, siber güvenlikle ilgili yeni/ortaya çıkan riskler, yaygın zayıflıklar ve siber güvenlik ihlalleri konusunda güncel kalmak için sektördeki meslektaşlarıyla konferanslar, ağ forumları ve web yayınları şeklinde iş birliği yapıyor mu?
4. Siber güvenlik politikaları ve prosedürleri yürürlükte mi ve çalışanlar ve yükleniciler/hizmet sağlayıcıları düzenli aralıklarla siber güvenlik farkındalığı eğitimi alıyor mu?

5. BT süreçleri siber tehditleri tespit etmek için tasarlanmış mı ve çalışıyor mu? Yönetimin yerinde yeterli izleme kontrolleri var mı?
6. Üst yönetime ve yönetim kuruluna kurumun siber güvenlik programlarının durumu hakkında bilgi vermek için geri bildirim mekanizmaları çalışıyor mu?
7. Yönetim, bir siber saldırı veya tehdit durumunda etkin bir yardım hattına veya acil durum prosedürüne sahip mi? Bunlar çalışanlara, yüklenicilere ve hizmet sağlayıcılarına iletildi mi?
8. İç denetim faaliyeti, siber tehditleri azaltmak için süreçleri ve kontrolleri değerlendirme yeteneğine sahip mi aksi durumda iç denetçi yöneticisinin siber güvenlik uzmanlığına sahip ek kaynakları dikkate alması gerekiyor mu?
9. Kurum verileri kurum dışında depolanması (örneğin; BT sağlayıcıları, bulut depolama sağlayıcıları, ödeme işlemcileri) halinde sistem erişimi olan üçüncü taraf hizmet sağlayıcılarının bir listesi kurum tarafından tutuluyor mu? Hizmet kuruluşunun siber güvenlik risk yönetimi programının bir parçası olarak kontrollerinin etkinliğini değerlendirmek için bağımsız bir siber güvenlik incelemesi yapılıyor mu?
10. İç denetim, kurumun karşı karşıya olduğu yaygın siber tehditleri (örneğin, ulus- devlet, siber suçlular, bilgisayar korsanları, ağ bağlantılı sistemler, bulut sağlayıcılar, tedarikçiler, sosyal medya sistemleri, kötü amaçlı yazılımlar) belirlemiş mi? Ayrıca bu tehditleri iç denetim risk değerlendirmesi ve planlama sürecine dahil etmiş mi?

Yukarıdaki sorular incelendiğinde siber güvenliğin sağlanmasında sadece üst yönetimin değil güçlü bir yönetişime duyulan ihtiyaç vurgulandığı görülmektedir. Keza üçlü hat modeli, ilk modelden ayıran özellikleri düşünüldüğünde yönetişime duyulan ihtiyacın artması doğaldır. Dolayısıyla bu sorulardan alınan cevaplardan yola çıkarak iç denetim yöneticisi siber güvenlikle ilgili olumsuz noktaları belirleyebilir. Bu sorulara verilen cevapları yorumlama ve risk temelli yaklaşıma göre siber güvenlik riski altında bulunan alanları belirleme sürecini başlatma görevi iç denetçi yöneticisine aittir. İç denetçi yöneticileri bu sorularla, birinci hat rolünün riskleri belirleyip, risklere cevap

verip vermediğini, zamanında düzeltici önlemler alınıp alınmadığı; ikinci hat rolünün ise stratejik şekilde hareket edip etmediğini değerlendirebilir (IIA, 2016a, s. 14).

Üçüncü hat olarak iç denetim birimi, kurumun siber güvenlik risklerini tespit etme ve azaltma kabiliyetlerini geliştirmek amacına yönelik siber güvenlik stratejileri ve politikaları geliştirme çabalarında yönetimle ve yönetim kuruluyla birlikte çalışmalı; denetim komitesiyle ve yönetim kuruluyla ilişkileri güçlendirmeli ve onların bağlılıklarından emin olmalı ve siber güvenlik risk planı uygulamak için gereken becerilerle (kurum içi veya ortak kaynak kullanımı yoluyla) plana resmen entegre edilmesini temin etmelidir. Gelişmekte olan teknolojiler ve trendler bir kurumun siber güvenlik risk profilini etkiler; bu sebeple, iç denetim birimi gelişen teknolojilerden de haberdar kalmalı ve kurumun kırılganlık seviyesini değerlendirmeli ve kurumun risk faaliyetlerini tercih edilen siber güvenlik planına kıyasla gözden geçirmelidir (IIA, 2018a, s. 8). İç denetim, siber güvenlik riskinin yönetiminin başarıya ulaşmasında sistematik ve teknik yaklaşımları kullanarak, güvenlik mekanizmasında liderlik rolünü üstlenmektedir (Selimoğlu & Saldı, 2019, s. 17).

2.5.2. İç denetim için önerilen siber güvenlik çerçeveleri

Kurumların siber güvenliğe ilişkin etkinliğini değerlendirmek adına çeşitli kurumlar tarafından çeşitli çerçeveler sunulmuştur. Bu kapsamda IIA'ın ve Deloitte tarafından sunulan çerçeveler ele alınmıştır.

IIA (2016a) tarafından yönetimin siber güvenlik kontrollerinin ve yönetişiminin tasarımını ve işletim/çalıştırma etkinliğini değerlendirmek için Şekil 2.10'da gösterildiği üzere altı bileşenden oluşan bir çerçeve sunulmuştur. Bu bileşenlerin birinin etkin olmaması siber güvenliğin genel etkinliğini etkileyeceğinden, her birinin nasıl tasarlandığını ve diğerleriyle birlikte nasıl çalıştığını değerlendirmek, iç denetim

yöneticilerine kurumun siber güvenlik risklerini ele almak için ne kadar iyi hazırlanmış olduğunu belirlemesi amacıyla temel bir bakış açısı sağlamaktadır.

Şekil 2. 10. *Siber güvenlik riski değerlendirme çerçevesi (IIA,2016a, s.17)*

Siber güvenlik riski değerlendirme çerçevesinin bileşenlerine ilişkin açıklamalar aşağıda özet şekilde sunulmuştur (IIA, 2016a, s.16-22).

- **Siber Güvenlik Yönetişimi:** İç denetim faaliyeti, kurumun siber güvenlik uygulamalarına, süreçlerine ve yönetişimine hâkim olmalıdır. 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.
- **Bilgi Varlığı Envanteri:** Tüm bilgi varlıklarının envanteri BT departmanı tarafından tutulmalı ve kurum hedefleri baz alınarak önceliklendirilmelidir. Kurumların stratejik hedefleri ve girişimleri tarafından beklenti karşılanması amacıyla geleneksel BT genel kontrolleri ve düzenli aralıklarla yapılan değerlendirmelerden daha fazlasına ihtiyaç vardır. Örneğin

varlıkları korumak amacıyla önleyici ve tespit edici kontrollerin yanı sıra sürekli izleme ile etkinlik takip edilmelidir.

- **Standart Güvenlik Yapılandırmaları:** Cihazlar, işletim sistemleri ve uygulama yazılımları için temel oluşturmak ve sürdürmek için merkezileştirilmiş, otomatik yapılandırma yönetim yazılımı kullanılabilir. Yönetim yazılımını kullanmak, sistemleri manuel olarak veya standart dışı bir şekilde yönetmekten daha etkilidir. Bilgi güvenliği ve iç denetim faaliyeti, riske dayalı ortamların doğru bir şekilde değerlendirilmesini sağlamak için temelleri gözden geçirmelidir (örneğin, dışarıya dönük web ortamları ek koruma gerektirebilir). Sektörde yeni tehdit bilgileri ortaya çıktıkça güvenli yapılandırmaların güncel kalmasını sağlamak için yazılım ve donanım güncellemelerinin yanı sıra gerekli yamaları uygulama süreçlerine de ihtiyaç vardır.
- **Bilgi Erişim Yönetimi:** Kurum yönetimi, iş rollerine göre kullanıcılara erişim izni vermek ve onaylamak için bir sürece ve önleyici kontrollere sahip olmalıdır. Bunu yanında çalışanların kurumda bulunma zaman aralıkları gözetilerek oluşturulan süreç kullanıcı erişimim ayarlanmasına yardımcı olur. İç denetim faaliyeti, önemli verilere ve sitemlere erişimleri inceleyerek erişim düzeylerinin mevcut roller için düzenlenip düzenlenmediğini doğrulayabilir. Ayrıcalıklı erişim bir diğer önemli konudur. Bu nedenle erişim izni vermek ve iptal etmek için önleyici kontrol faaliyetlerinin doğrulanması ve ayrıcalıklı erişime sahip kullanıcıların duyarlılıklarının ve davranışlarının değerlendirilmesi, kurumun siber güvenlik programının etkinliğinin önde gelen bir ölçüsüdür.
- **Hızlı Yanıt Verme ve İyileştirme:** Kurumun riskleri anında iletme ve iyileştirme yeteneği, programın etkinliğini ve olgunluk seviyesini göstermektedir. Olgun programlar, yönetimin yanıt verme süresini sürekli olarak kısaltabilir.

  • **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.

Sektörlerde bulunan siber güvenlik risklerinin yanı sıra benzer kurumlar tarafından yaşanan olaylar siber riskin kurumların devam eden izleme stratejilerini zaman içinde güncellemelerini gerektirmektedir.

Siber güvenliğin sağlanmasında iç denetçiye önemli ölçüde görev düşmektedir. İç denetim yöneticisi siber güvenlik çerçevesinde uzmanlığı ile doğru zamanda doğru kişiye sorular sorarak kurumun siber güvenlik konusundaki felsefesini, kurumun politika ve prosedürleri siber güvenlik felsefesini destekleyip desteklemediğini ve sektör ile kıyaslandığında kurumun ne seviyede olduğunu anlamalıdır (IIA, 2016b, s. 8).

Diğer bir çerçeve ise Big Four olarak adlandırılan denetim şirketlerinden biri olan Deloitte tarafından sunulmuştur. Bu çerçeve iç denetimin, siber güvenliğe kapsamlı bir bakış sunması ve yalnızca hedefe yönelik denetimler yaparak yanlış bir güvenlik algısı oluşturmaması için geniş bir yaklaşım benimsenmesi üzerinedir. Birçok iç denetim fonksiyonu, kurumun siber güvenlik hazırlığının bileşenlerini değerlendirmeye yönelik prosedürler uygulamıştır. Saldırı ve sızma prosedürleri gibi bu hedefe yönelik denetimler değerlidir, ancak siber güvenlik riskleri yelpazesinde güvence sağlamamaktadır. Bu çerçeve Tablo 2.2'de üç temaya (Güven-İhtiyatlı-Dirençli/Secure-Vigilant-Resilient) dayalı bir siber güvenlik değerlendirme çerçevesini göstermektedir. Gösterildiği gibi birden çok güvenlik alanı, üç temanın her birini desteklemektedir. Siber güvenlik hazırlığını değerlendirirken iç denetim, 12 alanın her birinin içindeki yetenekleri, bunların bugün nasıl ele alındığını ve kurum içinde mevcut olabilecek boşlukları anlamaktan yararlanabilir (Deloitte, 2017b, s. 2).

Kurumlar, siber risk değerlendirmesine başlarken; kimler tarafından saldırıya uğrayabilecekleri, saldırganların amaçları kuruma hangi yönde zarar vermek ve hangi taktikleri kullanacakları yönünde sorularını sormalıdırlar. Güvenli, ihtiyatlı ve dirençli bir kurum bağlamında yukarıda sorulan kim, ne ve nasıl sorularının araştırılması, kurumun siber savunma girişimlerinin ayrılmaz bir parçası olacak geniş bir iç denetim siber güvenlik değerlendirme çerçevesi için temel sağlayacaktır (Deloitte, 2017b, s. 2).

Tablo 2. 2. *Siber güvenlik açığı güçleri (Deloitte, 2017b, s. 3)*

GÜVEN	Siber güvenlik riski ve uyumluluk yönetimi	Güvenli geliştirme yaşam döngüsü	Güvenlik programı ve yetenek yönetimi
	Uyumluluk izleme Sorun ve düzeltici eylem planlaması Düzenleyici ve sınav yönetimi Risk ve uygunluk değerlendirmesi ve yönetimi Entegre gereksinimler ve kontrol çerçevesi	Güvenli yapı ve test Güvenli kodlama yönergeleri Uygulama rolü tasarımı/erişim Güvenlik tasarımı/mimarisi Güvenlik/risk gereksinimleri	Güvenlik yönü ve stratejisi Güvenlik bütçesi ve finans yönetimi Politika ve standart yönetimi Sıra dışı durum yönetimi Yetenek stratejisi
	Üçüncü Taraf Yönetimi	Bilgi ve Varlık Yönetimi	Kimlik ve Erişim Yönetimi
	Değerlendirme ve seçim Kontrast ve hizmet başlatma Sürekli izleme Hizmet sınırlama	Bilgi ve varlık sınıflandırması ve envanter Bilgi kayıtları yönetimi Fiziksel ve çevresel güvenlik kontrolleri Fiziksel ortam işleme	Hesap yetkilendirme Ayrıcalıklı kullanıcı yönetimi Erişim sertifikası Erişim yönetimi ve yönetişim
UYANIK/İHTİYATLI	Tehdit ve güvenlik açığı yönetimi	Veri yönetimi ve koruma	Risk Analizi
	Olaylara müdahale ve hukuki Uygulama güvenlik testi Tehdit modelleme ve istihbarat Güvenlik olayı izleme ve günlüğe kaydetme Penetrasyon testi Güvenlik açığı yönetimi	Veri sınıflandırma ve envanter İhlal bildirimi ve yönetimi Veri kaybı önleme Veri güvenliği stratejisi Veri şifreleme ve gizleme Kayıtlar ve mobil cihaz yönetimi	Aşağıdakiler etrafında bilgi toplama ve analiz etme: -Kullanıcı, hesap, varlık -Vakalar -Hile ve kara para aklamanın önlenmesi -Operasyonel kayıp
DAYANIKLI/DİRENÇLİ	Kriz yönetimi ve dayanıklılık	Güvenlik operasyonları	Güvenlik bilinci ve eğitimi
	Strateji, plan ve prosedürleri kurtarma/iyileştirme Test ve egzersiz İş etki analizi İş sürekliliği planlaması (BCP-Business Contuniuty Plans) Olağanüstü durum kurtarma planlaması (DRP-Disaster Recovery Plans)	Değişim Yönetimi Konfigürasyon/yapılandırma yönetimi Ağ savunması Güvenlik operasyonları yönetimi Güvenlik mimarisi	Güvenlik eğitimi Güvenlik farkındalığı Üçüncü taraf sorumlulukları
SOX (yalnızca finansal olarak ilgili sistemler)		Sızma ve güvenlik açığı testi	BCP/DRP testi

Çerçeve incelendiğinde roller ve sorumluluklar BT organizasyonuyla sınırlı değildir, tüm kurumu kapsamaktadır. Çerçevedeki renk vurguları, Sarbanes-Oxley testinin, sızma ve güvenlik açığı testinin ve iş sürekliliği ve olağanüstü durum kurtarma testlerinin her birinin çerçevenin belirli öğelerini ele aldığını göstermektedir.

Siber riskler sıklık ve çeşitlilik yönünden kurumlara, ticaret ortaklarına ve müşterilerine verebilecekleri olası zararlar açısından büyümeye her geçen gün devam etmektedir. Çoğu kurum bu riskleri ciddiye alır, ancak hem tehlikelerle mücadele etmek hem de kurum liderlerini siber güvenlik hazırlığı konusunda bilgilendirmek için daha

fazlası yapılmalıdır. İç denetim hem mevcut ve ihtiyaç duyulan kontrollerin bağımsız bir değerlendirmesini sağlayarak hem de denetim komitesinin ve yönetim kurulunun dijital dünyanın çeşitli risklerini anlamasına ve ele almasına yardımcı olarak, devam eden siber tehditleri yönetme savaşında kurumlara yardımcı olmada kritik bir role sahiptir. (Deloitte, 2017b, s. 6). İç denetim uzmanları bir siber güvenlik değerlendirmesini, değerlendirip yürütürken birkaç faktör dikkate değerdir. İlk olarak, gerekli deneyim ve becerilere sahip insanları dahil etmek hayati önem taşımaktadır. İç denetim, değerlendirmeleri yapacak bilgi birikimine sahip olmakla birlikte, BT departmanının mı yoksa CISO'nun güçlü bir tehdit modelleme işi yapıp yapmadığını anlamak, sorulacak etkili soruları bilen konu uzmanlarını gerektirebilir. Siber dünyada deneyimli, teknoloji odaklı bir denetim uzmanı vazgeçilmez bir kaynaktır. Son olarak, ilk değerlendirme geniş bir değerlendirme olmalıdır. Kapsamlı testler gerektiren ayrıntılı bir analiz olması amaçlanmamalıdır. Bunun yerine ilk değerlendirme, ek risk tabanlı siber güvenlik derinlemesine incelemelere yönlendirmelidir. (Deloitte, 2017b, s. 4).

ÜÇÜNCÜ BÖLÜM

Son bölüm olan üçüncü bölümde ise çalışmanın uygulama kısmı yer almaktadır.

3. TÜRKİYE'DE DİJİTAL DÖNÜŞÜMÜN İÇ KONTROL SİSTEMİNDE YARATTIĞI RİSKLER VE BU RİSKLERİN YÖNETİMİNDE İÇ DENETİM FONKSİYONU KAPSAMINDA FARKINDALIĞIN ARAŞTIRILMASI

Bu bölümde Türkiye'de faaliyet gösteren dijital dönüşümün yarattığı riskler ve iç denetim çerçevesinde uzman kişilerden alınan bilgiler doğrultusunda farkındalık değerlendirilmesi yapılmıştır.

3.1.Problem

Teknolojide yaşanan gelişmeler ve getirdiği riskler kurum ve bireyler açısından giderek yıkıcı etkiye sahip olması nedeniyle önemli hale gelmiştir. Yaşanan COVID-19 salgın süreci iş yapış şekillerinde değişiklik yaratması nedeniyle dijital dönüşümden kaynaklı risklere maruz kalma oranını ve farkındalığını artmıştır. Bu anlamda kurumların güvence ve danışmanlık rolünü üstlenen iç denetim fonksiyonunun geleneksel yöntemlerle bu sürecin yönetiminde etkili olamayacağı vurgulanmaktadır. Dijital dönüşümün kurumların iç kontrol sistemlerinde yarattığı riskleri iç denetim fonksiyonunun etkili nasıl yönetecekleri ve değişen rolünün önemi artmıştır.

Bu tez çalışmasının problemi, dijital dönüşüm ile birlikte ortaya çıkan ve değişen riskler karşısında iç denetiminin nasıl dönüşüme uğraması gerektiği üzerinedir. Bu çerçevede iç denetimin yeni sürece ayak uydurması adına geleneksel yöntemlerden sıyrılıp neleri dikkate alması gerektiği belirlemeye çalışarak farkındalık oluşturmak amaçlanmıştır.

3.2.İlgili Araştırmalar

Dijital dönüşüm ile birlikte karşılaşılan riskler ve iç denetim ilişkisini, rolünü ele alan akademik çalışmaları belirlemek amacıyla literatür taraması yapılmıştır. Bu kapsamda çalışmanın temel olarak ele aldığı dijital dönüşüm, siber güvenlik ve iç denetim kapsamında ele alınan çalışmalar incelenmiştir. Yapılan çalışmalar Türkiye'de yapılan ve yurtdışında yapılan çalışmalar olarak iki başlık halinde incelenmiştir.

3.2.1. Türkiye'de Yapılan Çalışmalar

Dijital dönüşüm, Endüstri 4.0 teknolojileri, bilgi teknolojileri konularının muhasebe uygulamaları ve muhasebe mesleğine etkileri Türkiye literatüründe yoğun şekilde incelenirken, dijital dönüşüm, Endüstri 4.0 teknolojileri, bilgi teknolojileri kavramlarını denetim ile ilişkilendiren çalışmalara ulaşılmıştır. Özellikle gelişen teknoloji ve değişen koşullar sebebiyle uzaktan denetim, kamu ve özel sektörde denetçinin edinmesi gereken özellikler, Denetim 4.0 kavramı, iç denetim faaliyetlerinin rolü, iç denetimin değişen yapısı konularına ilişkin araştırmalara ulaşılmıştır.

Yıldız ve Ağdeniz (2019) çalışmalarında teknolojik altyapının dijital çağın bir sonuncu olarak denetimin Denetim 4.0'a doğru evrilmesine imkan verdiği vurgulanmıştır. Bu çerçevede Denetim 4.0'ın teknolojik alt yapıları hakkında bilgi sunulmuştur.

Ağdeniz (2021) tarafından yürütülen çalışmada kamu iç denetçilerinin bilgi ve iletişim güvenliği denetimi konusu ele alınmıştır. Bu kapsamda İDDK (İç Denetim Koordinasyon Kurulu) tarafından yayımlanan Kamu İç Denetim Genel raporları içerik analizi kullanılarak analiz edilmiştir. Çalışma sonucunda kamu iç denetiminde BT denetimi konusunda farkındalığın son beş yılda arttığına ulaşılmıştır.

Ağdeniz ve Çetin (2021) araştırmalarında, uzaktan çalışma sürecinde denetim çalışma faaliyetinin ne şekilde yürütüleceği, nasıl risklerle karşılaşılacağı ve sınırlılıkların neler olduğunu tespit etmek adına 63 devlet üniversitelerinin iç denetim birimiyle görüşme yapmışlardır. Çalışma sonucunda Türkiye'de devlet üniversiteleri tarafından uzaktan denetimin etkin bir şekilde gerçekleştirildiğine ulaşılmıştır.

Akbaş ve Çarıkçı (2022) araştırmalarında Endüstri 4.0 ile yaşanan dijitalleşmenin denetim mesleğine, bağımsız denetçilere ve denetim uygulamalarına etkileri dört büyük denetim firmasında, bin bağımsız denetçiye anket göndermişlerdir. Çalışma sonucunda Endüstri 4.0'ın bağımsız denetçilerin etkinliğini artırdığına ulaşılmıştır.

Akçakanat, Özdemir ve Mazak (2021) tarafından yürütülen çalışmada kurumların siber risklerini ortaya koyarak bu riskleri yönetme hakkında bilgi verilmektedir. Bu kapsamda aktif büyüklüğüne göre ilk on bankanın faaliyet ve entegre raporlarında siber güvenlik çerçevesinde sunulmuş bilgiler ve bilgi sistemleri incelenmiştir. Çalışma sonucunda bankaların ulusal ve uluslararası düzenlemelere uygun yapıya sahip oldukları,

iç denetimin ilgili denetim faaliyetlerini yürüttükleri ve bu kapsamda ilgili eğitimlerin verildiği, veri güvenliği için teknolojinin takip edildiğine ulaşılmıştır.

Akmeşe (2020) tarafından kamu kurumlarında yaşanan dijital dönüşüm çerçevesinde iç denetim faaliyetlerinin rolü değerlendirilmiştir. Bu çalışma sonucunda iç denetimin kuruma siber güvenlik stratejileri konusunda güvence ve danışmanlık hizmeti vermesi sonucunda etkin bir dijital risk yönetim mekanizması geliştirileceği vurgulanmıştır.

Bircan (2020) çalışmasında iç denetçilerin iç denetimde yapısal değişim ve dönüşüm süreci çerçevesinde farkındalıklarını ölçmeyi amaçlanmıştır. Bu çalışma çerçevesinde 51 iç denetçiden anket yöntemiyle veri toplanmıştır. Çalışma sonucunda iç denetçilerde zihinsel olarak değişim ve dönüşüme yönelik farkındalığa sahip oldukları fakat iç denetim uygulamaları aşamasında eksikliklerin var olduğuna ulaşılmıştır.

Demirkol ve İkvan (2020) çalışmalarında Endüstri 4.0 sistemleri denetim çerçevesinde incelenmiştir. Sistemin sunduğu imkanlar ve denetim sürecine etkileri ele alınmıştır.

Erdoğan (2019) tarafından yürütülen çalışmada denetimin Endüstri 4.0 felsefesine uygun olarak Denetim 4.0 şeklinde ele alınması gerektiği ve bu çerçevede muhasebe ve denetim süreçlerindeki değişim ve dönüşüm ele alınmıştır.

Güler (2018) araştırmasında, dördüncü sanayi devrimi teknolojilerinin muhasebe ve denetime etkileri ele alınmıştır.

Kablan (2018) çalışmasında nesnelerin interneti kavramı, bu kavramın denetim anlayışı üzerindeki etkisi ve nesnelerin internetinden faydalanılması halinde ne gibi yararları olduğu üzerine yoğunlaşılmıştır.

Güler ve Arkın (2019) çalışmalarında iç denetimin rolü siber güvenlik ve siber hijyen çerçevesinde değerlendirilmiştir. İç denetimin siber güvenliğin sağlanması aşamasında güçlü potansiyele sahip olduğu ve her geçen gün iç denetimin siber sorumluluğunun artığı ele alınmıştır.

Karahan ve Tüfekçi (2019) araştırmalarında, blokzincir teknolojisinden bahsederek denetim mesleğine etkilerini ele almışlardır. Çalışmada iç denetim standartlarında yetkinlik kısmına vurgu yaparak iç denetçilerin blokzincir teknolojisi konusunda

eğitimler alması gerektiği vurgulanmıştır. Alınan eğitim neticesinde yeterli yetkinliğe erişen iç denetçilerin bu teknolojiyi kuruma entegre edebilecekleri belirtilmektedir.

Köse ve Polat (2021) çalışmalarında dijital dönüşümün denetim üzerindeki olumlu olumsuz etkileri ve gelecekteki denetimin nasıl şekil alacağına ilişkin inceleme yapılmışlardır.

Kurt ve Uysal (2015) çalışmalarında kurumların siber risklerini nasıl yönetmeleri ve nasıl iç kontrol sistemi geliştirilmesi gerektiği üzerine inceleme yapılmıştır. Yazarlar siber risklerin yönetiminde COSO İç Kontrol Bütünleşik Çerçevesinin yanında siber odaklı diğer çerçevelerin kurumlara yardımcı olacağını belirtmişlerdir.

Mollaoğulları ve Özdoğan (2018) araştırmalarında bilgi teknolojilerinin getirdiği riskler, iç denetimin riskleri nasıl yönetmesi gerektiği, yeni teknolojilere iç denetimin adaptasyonu ve kullanımı üzerine inceleme yapmışlardır.

Öztürk (2018) tarafından yürütülen çalışmada, siber güvenlik denetimi için denetimin planlanmasından raporlanmasına kadar bir model önerilmiş ve bu model akış şemaları ile sunulmuştur.

Sabuncu (2018) tarafından yürütülen çalışmada, iç denetimin iç denetimin tarihsel gelişimi ele alınarak bulut bilişim, yapay zeka, blokzincir gibi teknolojiler aracılığıyla dijital iç denetimin geleneksel iç denetim uygulamalarının yerini alacağı yönünde sonucuna varılmıştır.

Selimoğlu ve Altunel (2019) çalışmalarında siber risklerden korunma aşamasında iç denetimin rolü ele alınmıştır. IIA tarafından siber güvenliğin sağlanmasına yönelik sistematik bakış açısı sunan üçlü savunma hattına vurgu yapılmıştır.

Selimoğlu ve Saldı (2019) araştırmalarında kurumların karşılaştığı riskleri analiz, haritalama ve değerlendirmesinde kullanılan uygulamaları ve iç denetimin üstlendiği rolü ele almışlardır.

Selimoğlu ve Saldı (2022) çalışmalarında siber güvenlik yönetişimde iç denetim faaliyetinin konumu belirlenmiştir. Delphi tekniği kullanılarak uzman kişilerden görüşler toplanmıştır. Bankacılık sektöründe yürütülen çalışma "Sorumluluk", "Etik İlkeler", "Yetkinlik", "Gizlilik, Bütünlük ve Erişilebilirlik", "Yönetişim", "Kurumsal Yönetim

İlkeleri", "Yasal ve Uluslararası Politika Çerçevesi" başlıkları hakkında sonuçlara ulaşmıştır.

Şentürk (2021) tarafından yürütülen çalışmada, denetim ve dijital dönüşüm konularına yoğunlaşılmakla birlikte kamu kurumlarında dijital dönüşüm konusu ele alınmıştır.

Soğuksu (2020) araştırmasında, muhasebe denetiminde kullanılan denetim yazılımlarını incelemiş, karşılaştırmış ve eksikleri tespit etmiştir. Çalışmada anket tekniği ve görüşme yöntemi kullanılmıştır. Bu çalışma sonucunda Türkiye'de en çok CAP bağımsız denetim yazılımı, ardından LUCA ve MicroKom bağımsız denetim yazılım programının kullanıldığına ulaşılmıştır. Bağımsız denetim kuruluşlarının genel itibariyle paket yazılım programlarını kullandıklarına ulaşmıştır. Fakat bazı kuruluşlar ihtiyaçlarını karşılamak adına kendilerinin bilgisayar tabanlı bağımsız denetim yazılım programı geliştirdiğine ulaşmıştır. Denetçiler paket programları kullanmadaki temel zayıflık olarak profesyonel olmadıklarını ve mevzuata uyumda gecikmelere sebebiyet verdiğini belirtmişlerdir.

Ağdeniz (2020) tarafından yürütülen çalışma, gelişen teknolojiden iç denetim mesleğinin de yararlanması gerektiği üzerinedir. Çalışmanın sonucunda iç denetime duyulan ihtiyaç vurgulanmakta ve iç denetimin güvence sağlama konusunda iç denetçilerin karşılaştığı birtakım sorunlara karşı makine öğrenmesinin sunduğu çözümler ortaya konulmuştur.

Yalçın (2020) araştırmasında, yaşanan teknolojik gelişmeler sonucunda kurumsal risk yönetiminin, iç kontrol sisteminin, yönetişimin yeni fırsatları ve riskleri değerlendirmeleri gerektiğini vurgulamaktadır. Diğer taraftan kurumlar tarafından istihdam edilmek istenen iç denetçi profili değişmektedir. Bundan dolayı iç denetçinin sahip olması gereken yeni yetkinlik ve becerilerin neler olması gerektiği konusu ele alınmıştır.

Dijital dönüşüm ve iç denetim hakkında yayınların yanında iç denetim çerçevesinde siber güvenlik, siber risk ve bilgi teknolojileri üzerine Türkiye'de tez çalışması olarak yayımlanan araştırmalar (Zaralı, 2022; Tok, 2019; İşgüden, 2012; Ocak, 2021; Güngör, 2021; Turan, 2020; Bilgin, 2016; Saldı, 2022) Tablo 3.1'de sunulmuştur.

Tablo 3. 1. *İç denetim çerçevesinde dijital dönüşüm, siber güvenlik, bilgi teknolojileri üzerine Türkiye'deki tezler*

Yazar Adı (Yayın Yılı-Tez Türü)	**Araştırmanın Amacı**	**Araştırmanın Yöntemi**	**Araştırma Bulguları/Sonuçları**
Zaralı-2022 (Yüksek Lisans)	Kurumlarda yapılan dijital dönüşüm projelerinin siber güvenlik mahremiyetini ve güvenliğini etkileyip etkilemediğini incelemenin yanında bu projelerin güvenlik ve mahremiyet konularını risk altına atıp atmadığı incelenmiştir.	Araştırma 44 CEO/Genel Müdür, CIO / BT Direktörü / BT Müdürü yöneticilerine anket çalışması uygulanmıştır.	Çalışma sonucunda üst düzey yöneticilerin dijital dönüşümün siber güvenlik ve mahremiyet konuları hakkında farkındalık düzeylerinin yüksek olduğu ve projelerini güncel tehdit konularını takip ederek planladıklarına ulaşılmıştır. Ayrıca üst düzey yöneticilerin başlıca endişesinin üçüncü taraflar ile entegrasyon olduğuna ulaşılmıştır. Bunun yanında kurum verilerinin çalınması diğer endişe konusudur.
Saldı- 2022 (Doktora)	İç denetçilerin bilgi teknolojileri kontrollerindeki operasyonları ile etkileşim halinde olan siber güvenlik yönetimi süreçlerini gözlemlemek ve sektör uzmanlarına, akademisyenlere geleceğe yönelik çözümler sunmak amaçlanmıştır.	Delphi tekniği kullanılarak denetçiler, bilgi güvenliği uzmanları, akademisyenler ve yasal düzenleyicilerden veri toplanmıştır.	Çalışma sonucunda yetkilendirme siber güvenlik yönetişimindeki risk kontrolleri için en kritik parça yetkilendirme olduğuna ulaşılmıştır. Ayrıca blokzincir teknolojisine dikkat çekilmiş ve siber uzaydaki faaliyetlerin sürekli izleme yöntemlerinin otomatikleştirilmesi ve iyileştirilmesi önerilmiştir.
Ocak- 2021 (Yüksek Lisans)	Artan siber saldırılar karşısında kurumların siber saldırılara karşı zararın nasıl aza indirileceğine ilişkin önlemlerin ifade edilmesi amaçlanmıştır.	Araştırmada yaşanan Oltalama (Phishing) saldırısı sonucu bir kurumun nasıl harekete geçtiğine ilişkin örnek bir işletme incelenmiştir.	Çalışma sonucunda, siber güvenliğe ilişkin kurum çalışanlarına eğitim verilmediği, siber saldırılara karşı sigorta yapılmadığı, zafiyet tespiti için sızma testi daha önce yapılmadığı, gizli dosyalara ilişkin şifreleme politikası uygulanmadığı, beklenmeyen durumda bir aksiyon planının mevcut olmadığı, log kayıtlarının tutulduğu, yedekleme yapıldığı, flash bellek kullanımına ilişkin bir yasaklama politikasının bulunmadığı ve uzaktan erişim güvenliği için dışarıdan hizmet alınmadığına ulaşılmıştır. Türkiye'deki kurum yöneticilerinin siber güvenlik konusunu, saldırı gerçekleşene kadar önemsemediği ve iç denetçilerin bu konuda vakıf olmadığı belirtilmiştir.

Tablo 3. 1. (Devamı) *İç denetim çerçevesinde dijital dönüşüm, siber güvenlik, bilgi teknolojileri üzerine Türkiye'deki tezler*

Güngör-2021 (Doktora)	Çalışmanın üç amacı vardır; birincisi Türkiye'de halka açık işletmelerin siber güvenlik faaliyetini tespit etmek; ikincisi iç denetim faaliyetlerinin siber güvenlik faaliyet etkinliğini tespit etmek ve bu etkinliğin işletmelere göre farklılaşıp farklılaşmadığını belirlemektir. Üçüncüsü, işletmelerin siber güvenlik faaliyet düzeyi ile iç denetimin siber güvenlik faaliyet etkinliği ile ilişkisi olup olmadığını tespit etmektir.	Çalışmanın amacı doğrultusunda Borsa İstanbul'a kote halka açık işletmelerin bünyesinde çalışan 222 iç denetçiye anket çalışması uygulanmıştır.	Yapılan çalışma sonucunda işletmelerin türüne göre siber güvenlik seviyelerinin farklılaştığına, iç denetimin siber güvenlik faaliyet etkinliğinin işletme türlerine göre değiştiği, siber güvenlik faaliyet düzeyi ile iç denetim biriminin siber güvenlik faaliyet etkinliği arasında güçlü bir ilişki olduğuna ulaşılmıştır.
Turan -2020 (Yüksek Lisans)	Türkiye'deki bankacılık sektöründe dijital dönüşümün iç denetim süreç mekanizmaları üzerindeki etkisini belirleyerek gelecek iç denetim süreç mekanizmaları için öneriler sunmaktır.	Çalışmada Türkiye'de faaliyet gösteren orta ölçekli bir banka üzerinden vaka analizi yapılmıştır.	Çalışma sonucunda incelenen bankanın iç denetim biriminin denetim süreçlerini dijital dönüşüm kaynaklarını kullanarak yeniden şekillendirdiklerine ulaşılmıştır. İlerleyen dönemde iç denetim biriminin dijital dönüşüm kaynaklarını kullanarak uçtan uca yeni bir dijital denetim kuracak yönde yapılanmaya başladıklarına ulaşılmıştır.
TOK-2019 (Yüksek Lisans)	Araştırmanın amacı, bilgi teknolojilerin denetim faaliyetlerinde ne tür etkisi olduğu ve denetim kalitesini artırmak için hangi çalışmaların yapılması gerektiği üzerine öngörüler oluşturmaktır.	Kayseri'de bağımsız denetçi unvanına sahip 36 denetçi örneklem olarak belirlenip, anket çalışması uygulanmıştır.	Çalışma sonucunda bilgi teknolojileri konusunda yeterli düzeyde yasal düzenleme ve sertifikasyonun olmadığına ve bu durumun diğer ülkelerle kıyaslandığında Türkiye adına olumsuzluk yaratacağına ulaşılmıştır. Bunun yanında bilgi teknolojisi kullanan denetçiler ile kullanmayan denetçiler arasında bilgi teknolojisinin önemi konusunda tutum farklılığının olmadığına ulaşılmış. Bunun temel sebebinin BT araçlarının bilinçli şekilde kullanılmadığından kaynaklı olduğu sonucuna varılmıştır.

Tablo 3. 1. (Devamı) *İç denetim çerçevesinde dijital dönüşüm, siber güvenlik, bilgi teknolojileri üzerine Türkiye'deki tezler*

Bilgin -2016 (Yüksek Lisans)	Araştırmanın amacı, bilgi teknolojileri kontrollerini (genel kontroller ve uygulama kontrollerinin) incelenerek belirlenmesi amaçlanmıştır.	Araştırmanın amacı doğrultusunda örnek bir kurumda BT risk değerlemesi yapılmıştır ve kapsaması gereken kontrol alanları tespit edilmiştir.	Çalışma sonucunda, bilgi teknolojileri denetim sonuçları elde edilmiştir. BT denetimi sonucunda örnek kurumun yazılım şirketi ile olan sözleşmesine ilişkin tedarikçi performans izlemesi yapmadığı, tarafların aralarında hizmet alım sözleşme olmasına rağmen tedarikçi performansını değerlendirmeye yönelik prosedürlerin var olmadığına ulaşılmıştır. Bunun yanında iş süreklilik planı prosedürleri ve felaket kurtarma planın düzenli şekilde test edilmediğine ulaşılmıştır.
İşgüden-2012 (Doktora)	Kurumlardaki bilgi teknolojisine ilişkin değişimlerin sonucu iç denetimde yarattığı değişimi incelemek ve iç denetim taraflarının bu değişimlere adaptasyonunu irdeleyerek, değişimleri nasıl değerlendirdiklerini ortaya koymaktır.	İMKB-100'de işlem gören 71 işletme örneklemi oluşturmaktadır. Veri toplama tekniği olarak anket tekniği kullanılmış olup anketlere 71 işletmenin genel müdür yardımcısı, mali işler koordinatörü, muhasebe müdürü, denetim koordinatörü, iç kontrol koordinatörü, iç kontrol koordinatör yardımcılığı gibi birim bazında müdürlük, koordinatörlük ve koordinatör yardımcılığı görevlerindeki kişiler cevaplamıştır.	Çalışma sonucunda BT denetimin etkinliğinin iç denetim gelişmişliği ve çalışan personelin yetkinliğinden etkilendiğine ulaşılmıştır. İşletme yönetimi iç denetim birimi ile bilgi işlem biriminin birbirinden bağımsız şekilde BT denetim yapmasından yana olduğu sonucuna varılmıştır. Diğer bir sonuç ise BT denetiminin 5 yıldan kısa sürede gerçekleştiren birimler bilgi işlemden bağımsız şekilde birim bazında denetim yaparken, 5 yıldan uzun sürede gerçekleştirilen denetimlerde bilgi işlemden yardım istendiğine ulaşılmıştır. Son olarak çalışma sonucunda bilgi teknolojilerindeki gelişmelerin iç denetim faaliyetlerini etkilediğini, iç denetimin danışmanlık ve güvence rolünü yerini getirmelerini, iç denetimin faaliyet alanlarının gelişmesini ve yeni yaklaşımları benimsemelerini sağladığına ulaşılmıştır.

Sonuç olarak, Türkiye'deki alan yazın incelendiğinde araştırmaların bilgi teknolojileri ile iç denetim ilişkisinin yoğunlaştığına ulaşılmaktadır. Bunun yanında dijital dönüşümden kaynaklı riskler olarak son dönemde siber güvenlik konusuna odaklanıldığı ve denetçinin yeni teknolojilere uyum sağlaması konusunun ele alındığı

tespit edilmiştir. Diğer taraftan COVID-19 salgının etkisi uzaktan denetim konusuna yoğunlaşılmasına neden olduğu görülmektedir.

3.2.2. Yurtdışında Yapılan Çalışmalar

Dijital dönüşüm ve iç denetim çerçevesinde çalışmalar incelendiğinde iç denetimin dijital dönüşüm çağında nasıl geliştiği ve iç denetim uygulamalarında nasıl değişiklik yaşandığı, iç denetçinin yetkinliğinin değişmesi gerekliliği, dijitalleşme sonucunda artan riskler karşısında iç denetimin yaşadığı zorlukları, siber güvenlik konusu ve iç denetim ilişkisinin önemi, İç denetim 4.0'ın kurumun geleneksel anlamda sahip olduğu iç denetimin katma değerine etkisi, denetim uygulamalarındaki değişiklikler konularının ele alındığı göze çarpmaktadır. Uluslararası literatürde bu konular çerçevesinde yapılan araştırmaların detayları aşağıda açıklanmıştır.

Betti ve Sarens (2021) tarafından yürütülen araştırmada, dijitalleşen iş ortamında iç denetimin nasıl geliştiğine dair araştırma yapılmıştır. Nitel araştırma yöntemi olan görüşme tekniği kullanılmıştır. Denetim komitesi üyesi, iç denetim müdürü ve iç denetçi olmak üzere yirmi dokuz kişiyle görüşme yapılmıştır. Çalışma sonucunda dijitalleşen iş ortamının iç denetim fonksiyonunu üç açıdan etkilediğine ulaşılmıştır. Birincisi, iç denetimin kapsamının genişlediğidir. İç denetim planlamasının çevikliği ve gerekli dijital bilgi birikiminin artması ve özellikle siber güvenlik tehditleri olmak üzere bilgi teknolojisi risklerinin önem kazandığı vurgulanmıştır. İkincisi, iç denetçiler tarafından gerçekleştirilen danışmanlık faaliyetlerine olan talep daha yüksektir. Üçüncüsü ise dijitalleşme iç denetçilerin günlük görevlerinde çalışma uygulamalarını değiştirdiğini ve veri analitiği araçları gibi yeni teknolojiler, iç denetim departmanlarında aşamalı olarak uygulanmakta ve dijital beceriler kritik bir varlık olarak kabul edilmektedir.

Betti, Sarens ve Poncin (2021) araştırmalarında iç denetim fonksiyonunun kurumların dijitalleşmesiyle ilgili faaliyetlerini ve uygulamalarını nasıl değiştirdiğini araştırmayı amaçlamaktadır. Bu araştırmada özellikle veri analitiğinin kullanımını ve iç denetçiler tarafından danışmanlık faaliyetlerinin performansını incelenmiştir. ABD'de iç denetçiler enstitüsünde iç denetçilere anket tekniği uygulanmış ve seksen iki katılımcıdan dönüş sağlanmıştır. Çalışma sonucunda iş ortamının dijitalleştirilmesinin iç denetçiler için veri analitiği kullanımıyla olumlu bir şekilde ilişkili olduğuna ve iç denetim fonksiyonunun veri analitiği teknolojilerini kullanmalarından kaynaklı kurumların

dijitalleşme düzeyinin danışmanlık faaliyetlerinin performansını olumlu yönde etkilediğine ulaşılmıştır.

Rosa vd. (2021) çalışmalarında, sanayi devrimleriyle birlikte teknolojinin denetimdeki yansımalarını ele almışlardır. Denetim 4.0 kavramı, ilkeleri ve teknolojilerine ilişkin açıklamalar yapılmıştır. Bu açıklamalar doğrultusunda devlet yönetimi iç denetim araçlarında denetim faaliyetlerinin Endüstri 4.0 etkisine uyum sağlaması gerektiği vurgulamışlardır. Bu çerçevede yazarlar yeni teknolojilerin kullanımı ve iç denetim profesyonellerinin yenilikçi olmalarını belirtmişlerdir.

Kahyaoğlu ve Aksoy (2021) çalışmalarında, dijital çalışma ortamlarına bağlı olarak dijitalleşme, büyük veri analizi ve yapay zeka uygulamaları nedeniyle iç denetim ve risk değerlendirmesinin karşılaştığı zorluklara ve fırsatlara odaklanmaktadır.

Kahyaoğlu ve Çalıyurt (2018) tarafından yürütülen çalışmada, iç denetim ve risk yönetimi perspektifinde temel konuları ve zayıflıkları belirlemek için siber güvenlik güvence yaklaşımları ele alınmıştır. Bu çerçevede siber güvenlik tanımlanmış ve ilgili literatüre dayalı olarak siber güvenlik güvence modeli yazarlar tarafından açıklanmıştır.

Kupec (2017) araştırmasında, kurum yönetiminin önemli bir bölümünü oluşturan pazarlama alanında iç denetimin dijital potansiyelinin etkinliğini doğrulaması üzerinedir. Delphi tekniğinden faydalanılarak bilgi riski, stratejik risk, verimlilik riski ve mevzuat riski analiz edilmiştir. Çalışma sonucunda pazarlama etkinliğinin iç denetimde dijital tekniklerin uygulanmasıyla sağlanabileceğine ulaşılmıştır.

Lois vd. (2021) araştırmalarında, siber güvenliği etkileyen ve iç denetimle ilgili olan değişkenleri incelemeyi amaçlamışlardır. Bu amaç doğrultusunda Atina Menkul Kıymetler Borsası'nda işlem gören şirketlerdeki iç denetçilere anket tekniği uygulanarak veri toplanmıştır. Çalışma sonucunda BT personeli ile denetçiler arasındaki iş birliğinin derecesi ve niteliği ve bilgi teknolojisine ilişkin eğitim dahil olmak üzere siber güvenliği etkileyen temel faktörler olarak belirlenmiştir. Bu araştırma, dijitalleştirilmiş denetimde etkinliğin başarıya ulaşması için denetim ve denetçilerin siber güvenlik konusundaki bilgilerini genişletmeleri gerekliliğini vurgulamaktadır.

Mervelito vd. (2021) tarafından yürütülen çalışmada, kuruma katma değer sağlama konusunda Endüstri 4.0 çağında iç denetimde geleneksel iç denetim yaklaşımının

değişimini analiz etmeyi amaçlamaktadır. Çalışmada Endonezya'daki devlet kurumlarından, devlete ait şirketlerden ve özel şirketlerden anket tekniği ile veri toplanmıştır. Çalışma sonucunda İç Denetim 4.0, kurumun geleneksel iç denetim katma değerine yönelik etkisinde olumlu ve önemli ölçüde aracılık ettiğine ulaşılmıştır. Bunun yanında ulaşılan sonuçlarda, İç Denetim 4.0 yaklaşımı kurumların denetim performansına katkıda bulunacağı ve bu durum kurumların katma değerini artırabileceği fakat geleneksel iç denetimin katma değerini tamamen ortadan kaldırmayacağı vurgulanmıştır.

Pop (2020) araştırmasında, teorik araştırma metodolojisini tercih etmiştir. Bu çerçevede iç denetçiler enstitüsü tarafından yayımlanan CBOK (Global Internal Audit Common Body of Knowledge- Küresel İç Denetim Genel Bilgi Tabanı) raporu; KPMG, Deloitte ve Potriviti tarafından yürütülen çalışmalar incelenmiştir. İç denetim fonksiyonları, iç denetimi paydaşlarla bağlantılarını iyileştirecek ve geleneksel düşünce, yaklaşım ve zihniyetleri değiştirecek şekilde konumlandırmak için yeni becerilere ve yeteneklere ihtiyaç duyduğu, yeni nesil iç denetim ortaya çıkan riskler, teknolojiler ve aksamaların getirdiği zorluklara uyum sağlayan bir fonksiyon olacağı sonucuna varmıştır.

Tiberius ve Hirth (2019) çalışmalarında, Alman denetim profesyonellerinin önümüzdeki beş ila on yıl içinde denetim uygulamalarında beklediği değişiklikleri incelemişlerdir. Çalışmada Delphi tekniği ile veri toplanmıştır. Çalışma denetim algısına, denetçi-müşteri ilişkisine, düzenlemelere, denetim firmaları için yapısal ve prosedürel değişikliklere ve denetim mesleğinin profiline değinmektedir. Çalışma sonucunda belirlenen zaman diliminde geniş kapsamlı değişikliklerin beklenmediğine, yıllık denetim giderek sürekli bir denetim yaklaşımına doğru evrileceğine ulaşılmıştır. Ağırlıklı olarak belirsiz görüşlere rağmen uzmanlar, yeni teknolojilerin denetçinin yerini almayacağına bunun yerine yardım ve destek sağlayacağına, işin gereklilikleri meslekte kalmayı zorlaştırsa da yakın gelecekte denetçilerin iş yerlerinde yıkıcı etkiler beklenmediği belirlenmiştir.

Xie (2020) çalışmasında, iç denetim tanımının risk önleme ve kontrol yönüne doğru değişimini ve çeşitli risk yönetimi dernekleri tarafından iç denetimin risk yönetiminin rolünü, dijital riskin tanımını ve özelliklerini analiz etmiş ve dijital riskin işletmelerde evrensellik, karmaşıklık ve şiddetli yıkıcılığını ele almıştır. Ayrıca dijital ekonomide önemli bir risk önleme ve kontrol aracı olarak iç denetimin teknolojik yenilik, büyük veri

kullanımı, dijital gelişimi ve denetçi kalitesini geliştirmesi açısından iyileştirilmesi gerektiğini ortaya koymuştur.

Furtuna ve Cıucıoı (2019) çalışmalarında kurumlar tarafından iç denetim alanında belirlenen önceliklere genel bir bakış sunmayı ve iç denetim departmanlarının faaliyetlerinin etkinliğini ve verimliliğini artırma fırsatlarını göstermeyi amaçlamışlardır. Bu amaç doğrultusunda Romanya'daki kurumların iç denetim başkanlarına anket tekniği uygulanarak veri toplanmıştır. Çalışma sonucunda kurumlarda iç denetim fonksiyonun kilit rol oynadığına ve bu durumun gelecekte de devam edeceğine ulaşılmıştır. Çalışmanın yazarları iç denetim departmanlarının karşılaştığı en büyük zorluklar, çalışanların becerilerinin mevcudiyeti, inovasyonu teşvik etmek için verileri kullanma becerisi, kurumsal yönetişimi ve stratejik süreçleri geliştirme ihtiyacı ile ilgili olduğu sonucuna varmıştır. Bunun yanında iç denetçilerin %42'sinin siber güvenlik risk yönetiminin şirketlerin karşılaştığı ana zorluklardan biri olduğunu ifade etmişlerdir.

Islam vd. (2018) çalışmalarında kurumların iç denetim fonksiyonu tarafından güvenlik/siber güvenlik denetiminin kapsamı ile ilgili faktörleri araştırmayı amaçlamışlardır. Çalışmanın sonucunda, iç denetim fonksiyonu tarafından gerçekleştirilen güvenlik/siber güvenlik denetiminin kapsamının yönetişim, risk ve kontrol ile ilgili iç denetim fonksiyonu yeterliliği ile önemli ölçüde ve olumlu bir şekilde ilişkili olduğunu ulaşmışlardır.

Lois vd. (2020) araştırmalarında dijital çağda sürekli denetimi denetim firması çalışanlarının bakış açısıyla incelemiştir. Ayrıca sürekli denetimi etkileyen çağdaş faktörleri ve bunun uygulanması için kullanılabilecek teknikleri araştırmışlardır. Çalışma sonucunda başlıca olarak iç denetimin karşılaması gereken üç ana hedefi vurgulamışlardır. Bunlar kişisel verilerin korunması, siber saldırıların önlenmesi ve uzman personelin eğitimi şeklindedir. Ayrıca etkin bir dijital denetim sisteminin kurulması için teknolojik gelişmeler takip etmenin gerekliliği, siber saldırılara karşı veri koruma önlemlerinin yanı sıra çalışanların becerileri ve eğitiminin etkisinin önemli olduğu ve sanal denetim ekiplerinin hazırlanmasına ve oluşturulmasına önem verilmesi gerekliliği sonucuna varmışlardır.

3.3.Araştırmanın Amacı

Bu çalışmada dijital dönüşüm çağında risk yönetiminde iç denetim fonksiyonunun ne yönde olduğu ve bu yeni dönemde daha etkin bir iç denetim için iç denetçilerin kendilerini bu çağa nasıl adapte ettikleri veya etmeleri gerektiği incelenmiştir. Bu anlamda dijital dönüşüm sürecinde karşılaşılan riskleri yönetmek için iç denetim fonksiyonunun nasıl bir yol izlediği/izleyeceği yönünde Türkiye'de farkındalık araştırması yapılması ve bu araştırma sonucunda önerilerin sunulması amaçlanmaktadır.

3.4.Araştırmanın Önemi

Teknolojide yaşanan gelişmeler birçok alanda etkisini göstermekle birlikte muhasebe ve denetim üzerinde de etkisi bulunmaktadır. Bu anlamda yapılan incelemeler doğrultusunda 2011 yılında ortaya atılan Endüstri 4.0 gibi yeni bir olgunun denetim alanını ne şekilde etkilediği konusunda COVID-19 salgının etkilerinden kaynaklı yoğunlaşılmış olmasına rağmen sınırlı sayıda araştırma bulunduğuna ulaşılmıştır. Ayrıca bu çalışmaların büyük çoğunluğu kavramsal açıklamalara yer vermiştir. Bu nedenle çalışmanın literatürdeki boşluğu doldurması hem kurumlara hem de iç denetim mesleğine rehberlik etmesi açısından oldukça önemlidir. Çalışma özellikle dijital dönüşümden kaynaklı risklerin yönetimi açısından denetçilerin kendilerini ne yönde geliştirmesi gerektiği, meslek örgütlerin bu alandaki ihtiyaca yönelik farkındalığının oluşturulması, kamu ve özel sektörde dijital dönüşümden kaynaklı risklerin yönetiminde iç denetim fonksiyonun önemi ve rolünün vurgulanması açısında önem arz etmektedir.

3.5. Sayıltılar

Bu araştırmada,

- Verileri toplama sürecinde tercih edilen Delphi tekniğinin çalışmanın amacına ve konusuna uygun olduğu,
- Çalışmanın örneklemini oluşturan, görüşlerine başvurulan uzmanların yeterli olduğu,
- Çalışmaya katılım sağlayan uzmanların iç denetim ve dijital dönüşüm çerçevesinde bilgi ve deneyime sahip oldukları,
- Çalışmaya katılım sağlayan uzmanların Delphi turlarına istekli bir şekilde katıldıkları ve kendilerine yöneltilen sorulara samimi bir şekilde yanıtladıkları bu haliyle gönüllülük esasının sağlandığı varsayılmaktadır.

3.6. Sınırlılıklar

Bu araştırma,

- Dijital dönüşüm, dijital dönüşümden kaynaklı riskler ve iç denetim çerçevesinde bilgi ve deneyime sahip olan, bu konular özelinde yayın yapan ve araştırmaya katılmayı kabul eden akademisyenlerle,
- Dijital dönüşüm, dijital dönüşümden kaynaklı riskler ve iç denetime ilişkin bilgi ve deneyime sahip olan, kamuda veya denetim şirketlerinde profesyonel yaşamlarını sürdüren ve araştırmaya katılmayı kabul eden iç denetçilerle,
- İç denetim çerçevesinde mesleki kuruluşlarda görev alan ve araştırmayı kabul eden iç denetçilerle,
- Kullanılan veriler açısından katılımcılardan toplanan görüşler ve ölçme aracında yer alan ifadelerle,
- Delphi tekniği kullanılarak yapılan nitel ve nicel veri analizleriyle,
- Mayıs 2022-Kasım 2022 arasında toplanan veriler ile sınırlıdır.

3.7.Yöntem

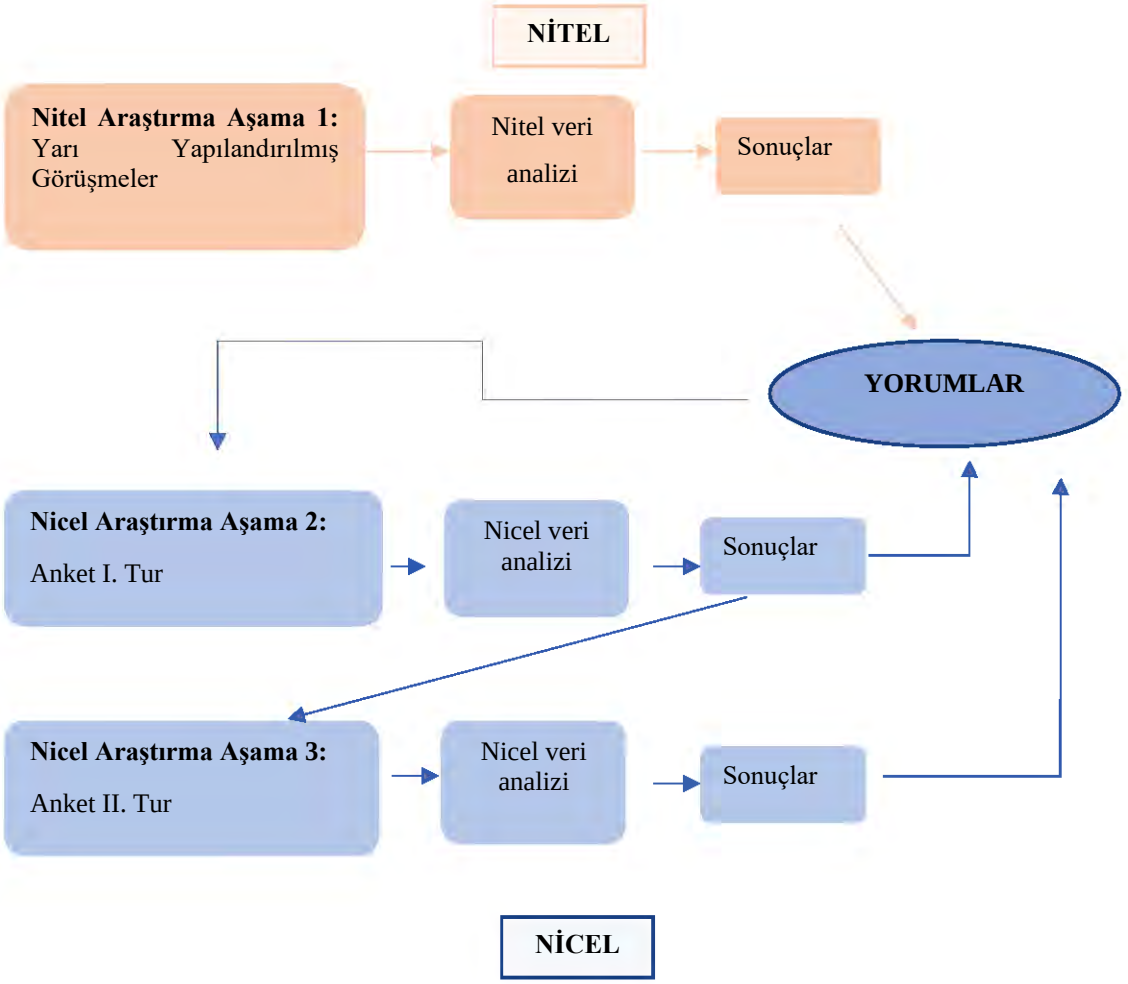
Yöntem kısmında araştırma deseni, Delphi tekniği, evren ve örneklem, veri toplama araçları ve analizi hakkında açıklamalar yapılmıştır.

3.7.1.Araştırma deseni (Karma yöntem araştırmaları tasarımı)

Türkiye'de dijital dönüşümün iç kontrol sisteminde yarattığı riskler ve bu risklerin yönetiminde iç denetim fonksiyonunun farkındalığı üzerine yapılan bu çalışmada Delphi tekniği kullanılmıştır. Çalışma, kullanılan yöntem itibariyle karma modelde tasarlanmıştır.

Karma yöntem araştırması, araştırmacının tek bir çalışmada hem nitel hem de nicel veri toplama ve analiz yöntemlerini birleştirdiği bir çalışmadır (Creswell, 1999, s. 455). Delphi tekniği kapsamında bu çalışmanın nitel kısmında katılımcılarla öncelikle yarı yapılandırılmış görüşme yöntemi kullanılmıştır. Yapılan teorik açıklamalar çerçevesinde öncelikle görüşme soruları hazırlanmıştır. Akabinde katılımcılar ile görüşme yapılarak dijital dönüşüm ile birlikte gelen riskler, bu riskler karşısında iç denetim fonksiyonunun rolü, iç denetçinin niteliği ve yasal düzenlemeler üzerine değerlendirme yapılmıştır. Katılımcılarla yapılan görüşme sonrası elde edilen veriler nitel çözümleme yöntemi ile

analiz edilerek, Delphi tekniğinin ikinci turu için anket formu hazırlanarak katılımcılara iletilmiştir. Bu kısım yöntemin nicel kısmını oluşturmaktadır. Üçüncü tur için katılımcıların uzlaşı sağladıkları ifadelerden oluşan anket formu katılımcılara tekrar iletilerek katılımcıların görüşleri alınmıştır. Şekil 3.1'de karma modelde tasarlanan çalışma süreci sunulmuştur.



Şekil 3. 1. *Çalışmanın karma yöntemde desenlenmesi (Opoku & Ahmed, 2013, s. 135; Keser, 2018, s. 44; Yeşilçelebi, 2019, s. 148)*

3.7.2.Delphi tekniği

Bu çalışmada veriler Delphi tekniği uygulanarak toplanmıştır. Delphi tekniği, bir grup iletişim sürecini yapılandırmak için bir yöntemdir. Böylece süreç, aranan bilgilerin öznel olduğu ve katılımcıların fiziksel mesafeyle ayrıldığı belirli bir konuda uzmanlığa sahip bir grup birey arasında fikir birliği elde etmede etkilidir (Khayun, Ractham and Firpo, 2012, s. 34). Macmillan (1971, s. 1) tarafından Delphi tekniği, grup yargılarını

ortaya çıkarma ve iyileştirme yöntemi olarak ifade edilmektedir. Yöntem, bilgili ve uzman katılımcıların sorulara bireysel olarak yanıt vermesini ve sonuçları merkezi bir araştırmacıya iletmesini gerektirmektedir. Araştırmacı, merkezi ve aşırı eğilimleri ve bunların gerekçelerini arayarak katkıları belirler ve sonuçlar yanıtlayanlara geri gönderilir. Daha sonra, araştırmacı tarafından sağlanan girdilerin yardımıyla yanıt verenlerden görüşlerini yeniden sunmaları istenir. Bu süreç, araştırmacı bir fikir birliğinin oluştuğunu görene kadar devam etmektedir. Teknik, farklı uzman gruplarının bir araya gelmesiyle ortaya çıkan yanlılığı ortadan kaldırmayı amaçlamaktadır. Delphi tekniğinde uzmanlar süreç boyunca diğer uzmanların kim olduğunu bilmezler (Grisham, 2009, s. 114).

Delphi tekniğinin temel amacı araştırmaya katılan katılımcıların görüş birliği sağlamasıdır. Bu nedenle katılımcıların likert tipi ölçeğe verdikleri yanıtlarda uzlaşmanın sağlanması için bazı ölçütlerin (uzlaşma düzeyi) belirlenmesi gerekmektedir. Bu ölçütlere ilişkin çeşitli görüşler bulunmaktadır. Kurubacak (2011, s. 154) çalışmasında ortalama ve frekans değerlerini ölçüt olarak kullanırken, Gracht ve Darkow (2010, s. 53) çalışmasında ortalama, çeyrekler arası fark, standart sapma değerlerini kullanmaktadır. Bu çalışmada ölçütler medyan değeri, çeyrekler arası fark ve uzlaşı yüzdesidir (üçlü likert ölçeğinde "katılıyorum" cevabını verenler). Bu ölçütlere ilişkin açıklamalar kısaca şöyledir:

- Medyan, verilen yanıtları küçükten büyüğe doğru sıralanmış istatistiksel bir seriyi iki eşit parçaya bölen, ortadaki değerdir.
- Çeyrekler arası fark (ÇAF): Yanıtların %25'ini soluna, %75'ini sağına alan noktaya birinci çeyrek (Ç1) denir. Yanıtların %25'ini sağına, %75'ini de soluna alan noktaya üçüncü çeyrek (Ç3) adı verilir. Çeyrekler arası fark (IQR, Interquartile range), birinci çeyrek ve üçüncü çeyrek arasındaki farktır. Bu farkın 1'e eşit veya daha küçük olması (ÇAF $\leq$ 1) uzlaşma derecesinin yüksek olduğunu ifade eder. Çeyrekler arası aralık ne kadar küçükse, elde edilen uzlaşma derecesi o kadar yüksek olur (Galloway, 1999, s. 49).
- Uzlaşma (uzlaşı) yüzdesi: İkinci ve üçüncü turda, 5'li likert ölçeğinde "kesinlikle katılıyorum ve katılıyorum "yanıtını verenlerin yüzdeleri toplamıdır (Bahar & Demir, 2021, s. 45). Bu çalışmada üçlü likert ölçeği kullanılması sebebiyle "katılıyorum" yanıtını verenlerin yüzdesini ifade

etmektedir. Uzlaşı, önceden belirlenmiş bir katılımcı yüzdesinin çalışılan konular üzerinde anlaşmaya varmasını ifade etmektedir (Nworie, 2011, s. 26). Diğer bir ifadeyle yanıtların önceden belirlenen yüzde aralığına denk gelmesi halinde uzlaşı sağlandığı kabul edilir (Bahar & Demir, 2021, s. 45). Uzlaşı yüzde aralığı net olmamakla birlikte bu aralık Hasson vd. (2000, s. 1011) tarafından yürütülen çalışmada farklı öneriler sunulmuş ve %51 (Loughlin and Moore, 1979, s. 103) ila %80 (Green vd., 1999, s. 202) olarak belirlendiğine ulaşılmıştır.

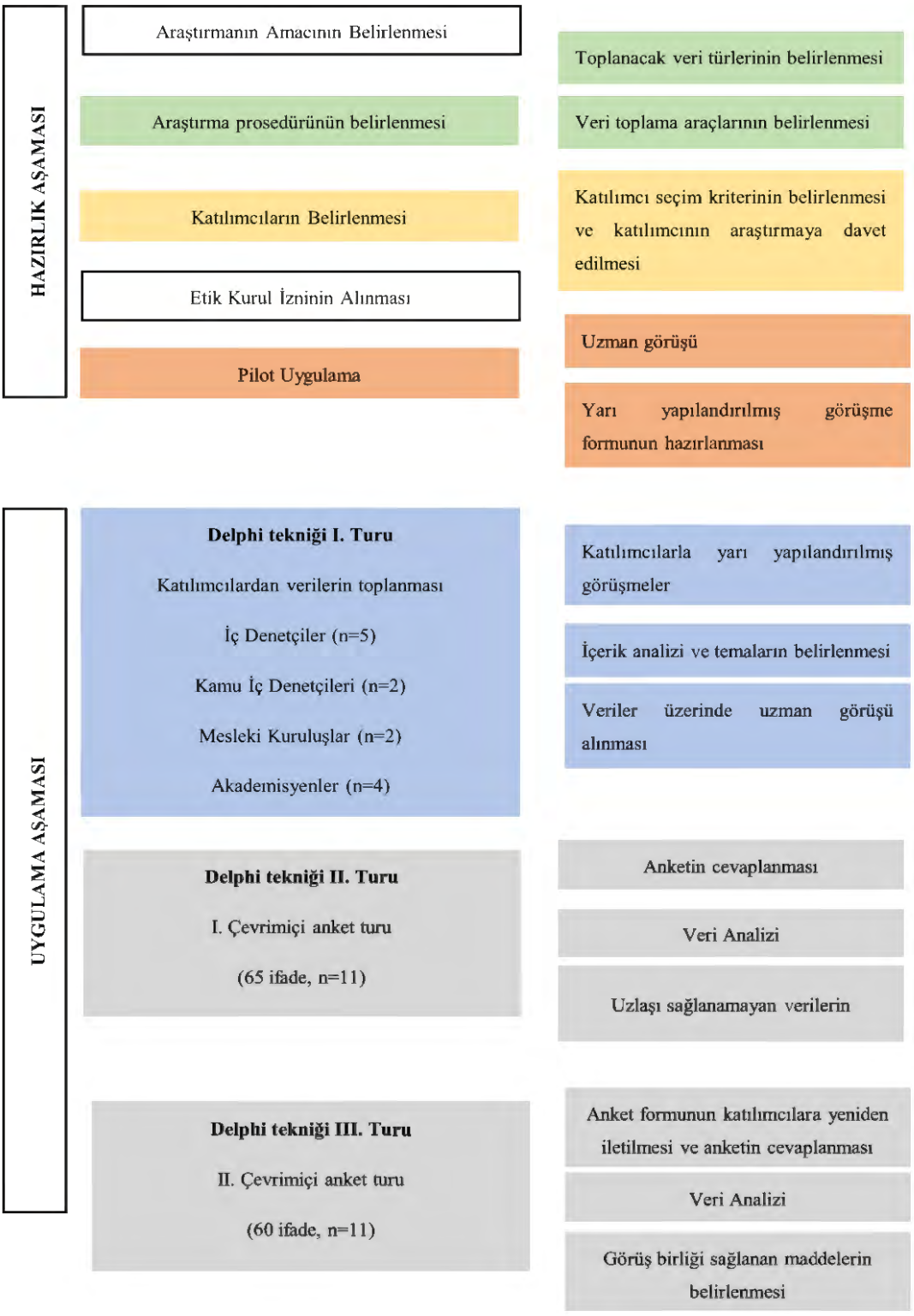
Bu çalışmada görüş birliğinin sağlanabilmesi için ulusal ve uluslararası literatüre dayandırılarak aşağıdaki üç ölçütün aynı anda sağlanması esas alınmıştır:

- Medyan değeri = 1
- Çeyrekler arası fark (ÇAF) ≤ 1
- 1 frekans değer yüzdesi ≥ %75

Bu üç ölçüt aynı anda sağlandığında katılımcılar arasında görüş birliği sağlandığı kabul edilmiştir.

Delphi tekniği genel itibariyle iki aşamadan oluşmaktadır. İlk olarak tekniğin uygulanması için detaylı bir hazırlık süreci mevcuttur. İkincisi uygulama aşaması olup, süreç tamamlanmaktadır. Bu çalışmanın hazırlık aşamasında öncelikle literatür taraması, yöntemin tasarlanması, katılımcıların belirlenmesi, etik kurul izni ve pilot uygulama yer almaktadır. Bu çalışma için veri toplama araçlarına ilişkin alınan etik kurul izni Ek-3'te sunulmuştur. İkinci aşama olan uygulama aşamasında öncelikle katılımcılarla yarı yapılandırılmış görüşmeler gerçekleştirilmiştir. Akabinde 65 ifadeden oluşan 3'lü likert tipi Delphi II. tur anketi uygulanmıştır. Sağlanan dönüşlerden elde edilen analiz sonucunda uzlaşı sağlanamayan ifadeler çıkarılarak 60 ifadeden oluşan Delphi III. tur anketi hazırlanarak, katılımcılara iletilmiştir. Delphi tekniğinde kaç tur yapılacağına ilişkin Rowe ve Wright (2001, s. 125) genellikle iki veya üç turun yeterli olduğu belirtmiştir.

Araştırma süreci Şekil 3.2'de ayrıntılı şekilde sunulmuştur.



Şekil 3. 2. *Araştırma Süreci (Yeşilçelebi, 2019, s.151'den uyarlanmıştır.)*

3.7.3.Evren ve örneklem

Çalışmanın örneklem seçiminde amaçlı örneklem yöntemi benimsenmiştir. Amaçlı örnekleme tekniği araştırmacının, çalışmanın amacına başarılı şekilde ulaşmak için en iyi bilgiyi kimin sağlayacağına dair yargısına dayanır. Araştırmayı yürüten kişinin gerekli bilgilere sahip olan ve paylaşmaya istekli kişilere odaklanması gerekir (Etikan and Abubakar, 2017, s. 1). Bundan kaynaklı örneklem seçiminde çalışmada amaca uygun hareket edilmiştir. Bu bağlamda çalışma evreninde bağımsız denetim kurumları (E&Y, KPMG, PWC, Deloitte, Mazars Denge), mesleki kuruluşlar (ISACA, TİDE, ICI, İDKK, KIDDER), kamu kurumunda iç denetçi görevinde çalışan ve çalışmanın konusu çerçevesinde bilgi sahibi akademisyenler yer almaktadır. Çalışmanın evrenine ilişkin bilgiler Şekil 3.8'de verilmiştir. Görüşme yapılan kişiler çalışmanın evrenini oluşturan ve çalışmaya katılım çağrısını kabul eden kişilerden seçilmiştir. Katılımcıların çalışmaya katılmaları için konu ve yöntem hakkında özet bilgi sunan bir davet e-postası gönderilmiştir. Davet e-postası Ek 1'de sunulmuştur.

Şekil 3. 3. *Çalışmanın katılımcıları*

Katılımcıların seçiminde birtakım özellikler göz önünde bulundurulmuştur. Katılımcılar nitelikleri itibariyle şöyledir: bağımsız denetim şirketlerinde iç denetçi olarak mesleğini icra eden ve danışmanlık hizmeti sunan kişiler; mesleki kuruluşlarda görev alan ve iç denetçi mesleğini icra eden kişiler; kamu kurumunda kamu iç denetçisi olarak görev alan kişiler; akademisyenler eserleri itibariyle iç denetim ve bilgi

teknolojileri, dijital riskler, siber riskler, Endüstri 4.0 teknolojileri vb. konularını çalışan kişilerdir. Tablo 3.2'de örnekleme ilişkin bilgiler sunulmuştur.

Tablo 3. 2. *Araştırmada yer alan katılımcıların özellikleri*

Akademisyenler					
Kod	**Unvan**	**Cinsiyet**	**Öğrenim Durumu**	**Mesleki Deneyim (Yıl)**	**Çalıştığı Kurum**
K1	Doç. Dr.	Erkek	Doktora	20 yıl ve üstü	Devlet Üniversitesi
K2	Doç. Dr.	Kadın	Doktora	15-19	Devlet Üniversitesi
K5	Doç. Dr.	Kadın	Doktora	20 yıl ve üstü	Vakıf Üniversitesi
K9	Doç. Dr.	Erkek	Doktora	15-19	Vakıf Üniversitesi
İç Denetçi					
K3	İç Denetçi	Erkek	Yüksek Lisans	10-14	Uluslararası Denetim Firması
K4	İç denetçi	Kadın	Lisans	5-9	Dört Büyük Denetim Firması
K7	Şirket Ortağı/İç Denetçi	Erkek	-[6]	-	Dört Büyük Denetim Firması
K8	İç Denetçi	Kadın	-	-	Dört Büyük Denetim Firması
K13	İç Denetçi	Erkek	Yüksek Lisans	15-19	Dört Büyük Denetim Firması
Kamu İç Denetçisi					
K6	Kamu İç Denetçisi	Erkek	Lisans	20 yıl ve üstü	Kamu Kurumu
K10	Kamu İç Denetçisi	Erkek	Doktora	20 yıl ve üstü	Kamu Kurumu
Mesleki Kuruluşlar					
K11	İç Denetçi	Erkek	Yüksek Lisans	20 yıl ve üstü	ISACA
K12	İç Denetçi	Erkek	Yüksek Lisans	15-19	ISACA

Delphi tekniği kullanılan çalışmalarda ideal katılımcı sayısına ilişkin farklı görüşler bulunmaktadır. Rowe ve Wright (2001, s. 125) 5 ila 20 arası katılımcının yeterli olduğunu

[6]Bu alandaki bilgiler demografik bilgiler olup Delphi II. tur anketinden elde edilen sonuçlar doğrultusunda oluşturulmaktadır. K7 ve K8 Delphi II. tur anketine katılmadıkları için eğitim durumları ve mesleki deneyimleri hakkında bilgi alınamamıştır.

ifade ederken; Okoli ve Pawlowski (2004, s. 18) tarafından 10-18 arasında katılımcının olması tavsiye edilmektedir. A. E. Şahin (2001, s. 217) tarafından ise akademik çalışmalarda Delphi tekniği kullanılırken büyük ya da küçük uzman grupları ile çalışmanın mümkün olduğu ve en az 7 katılımcıdan oluşan uzman grubun yeterli olduğu belirtilmektedir. Literatürde Delphi tekniği için önerilen katılımcı sayıları göz önüne alınınca bu çalışmanın katılımcı sayısının yeterli olduğu söylenebilir.

3.7.4.Veri toplama araçları ve analizi

Bu çalışmada veri toplama aracı olarak yarı yapılandırılmış görüşme tekniği ve anket kullanılmıştır. Yarı yapılandırılmış görüşme tekniği yapılandırılmış görüşme tekniğine kıyasen daha esnektir. Bu teknikte araştırmacı önceden soruları hazırlamasına rağmen katılımcı ile görüşme esnasında akışa bağlı olarak katılımcının yanıtlarını ayrıntılayabilir (Türnüklü, 2000, s. 547). Katılımcıların belli bir konu hakkındaki tutum, düşünce ve davranışlarını öğrenmek amacıyla belli sırada ve yapıda oluşturulmuş sorulara dayalı olarak paylaşmasına imkan tanıyan veri toplama aracına anket denir (Gürbüz & Şahin, 2018, s. 175).

Bu çalışmada hem nitel hem nicel veriler kullanılmış olup, nitel verileri oluşturan görüşme sorularının ve nicel verileri oluşturan anket formunun hazırlanması ve analizine ilişkin aşağıda detaylı açıklama yapılmıştır.

3.7.4.1.Görüşme formu

Delphi tekniği uygulama aşamasının ilk kısmında görüşme tekniği kullanılmıştır. Araştırmacı tarafından görüşme soruları hazırlandıktan sonra alanında uzman iki kişiyle görüşülerek hem çalışmanın amacına uygunluğu hem de soruların anlaşılırlığı gözden geçirilmiştir. Bu incelemeler sonucu uzmanlar tarafından görüşme sorularının geçerliliği saptanmış ve çalışmanın amacı için yeterliliği onaylanmıştır. Delphi tekniğinin birinci turunda açık uçlu olarak hazırlanan sorular yarı yapılandırılmış görüşme tekniği ile 13 katılımcıya sorulmuştur. Yüz yüze veya video konferans araçları ile yapılan görüşmeler katılımcılardan alınan izin doğrultusunda kayıt altına alınmıştır. Tamamlanan görüşmeler daha sonra kâğıda aktarılmıştır.

Görüşme soruları iki bölümden oluşmaktadır. İlk bölüm katılımcıyı tanımaya yönelik soruyu kapsamaktadır. İkinci bölüm ise dijital dönüşümün yarattığı riskler karşısında iç denetim fonksiyonunun hangi rolüyle ön plana çıktığı, dijital dönüşüm

sürecinde iç denetçi rolü ve yetkinliği, dijital dönüşümden kaynaklı riskler karşısında uluslararası ve ulusal yasal düzenlemeleri anlamaya yönelik soruları kapsamaktadır. İkinci bölümdeki sorular ilgili literatür araştırması sonucunda oluşturulmuştur. Araştırmada kullanılan görüşme formu Ek 2'de sunulmuştur.

Bölüm A: Kişisel Bilgiler

Amaç: Katılımcı hakkında bilgi edinmek

1. Kurumdaki göreviniz nedir ve bu görevinizde ne zamandan beri çalışıyorsunuz?

Bölüm B: Dijital dönüşümün yarattığı riskler karşısında iç denetim fonksiyonunun rolü

Amaç: Dijital dönüşümün yarattığı riskler karşısında iç denetim fonksiyonunun hangi rolüyle ön plana çıktığı, dijital dönüşüm sürecinde iç denetçi rolü ve yetkinliği, dijital dönüşümden kaynaklı riskler karşısında uluslararası ve ulusal yasal düzenlemeleri anlamak

2. Dördüncü Sanayi Devrimi, Dördüncü Sanayi Devrimi teknolojileri, dijital dönüşüm, sizde ne çağrıştırıyor? Dijital dönüşümün kurumunuza yansımaları nelerdir?
3. Kurumlar göz önüne alındığında yaşanan dijital dönüşümün getireceği başlıca riskler olarak neleri görüyorsunuz?
4. Dijital dönüşüm ile beraber karşılaşılan riskler karşısında iç denetim fonksiyonunun rolü nedir?
5. Dijital dönüşüm çerçevesinde iç denetimin güvence sağlama ve danışmanlık rolünü nasıl değerlendirirsiniz?
6. Üçlü hat modelinin, üçüncü hat rolünde yer alan iç denetimi dijital riskler çerçevesinde nasıl değerlendirirsiniz?
7. Kurumları dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde nasıl değişiklikler yapmalıdır? Bu noktada iç denetimin rolü nedir?
8. Sizce dijital dönüşüm süreci ile birlikte iç denetçilerin taşıması gereken yeni özellikler nelerdir? Bu süreçte iç denetçilerin odak noktası ne olmalıdır?

9. Denetçinin sürecin doğru yönetilmesi adına hangi eğitimleri/sertifikaları alması gerekir? Bu dönüşüm çağının gerektirdiği yetkinlikte iç denetçilerin yetiştirilmesi adına neler yapılmalıdır?
10. Dijital dönüşüm ile birlikte gelen riskler karşısında iç denetim faaliyeti yürütülürken başlıca hangi düzenlemeler/kılavuzlar kullanılmalıdır? Bu kılavuzların içeriğini nasıl değerlendirirsiniz?
11. Türkiye'de dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeleri nasıl değerlendirirsiniz?

3.7.4.2. Anket formu

Katılımcılar ile yapılan görüşme sonucu elde edilen yanıtların çözümlenmesi ile anket formu oluşturulmuştur. Anketin geçerliliğini sağlamak amacı ile alanında uzman kişiden görüş alınmıştır. Katılımcıların verdiği yanıtlar dikkate alınarak yedi tema 65 ifadeden oluşan 3'lü Likert ölçeğinde (1= Katılıyorum; 2= Katılmıyorum, 3= Uygun Değil) anket formu hazırlanmıştır. Delphi tekniğinin ikinci turunda hazırlanan anket formu tek tek katılımcılara iletilerek, anket formundaki ifadelere ilişkin görüşlerini beyan etmeleri istenmiştir. Delphi tekniği ikinci tur anketi Ek 4'te sunulmuştur. Delphi tekniğinin nicel verilerini analiz etmek için SPSS Versiyon 26 programı kullanılmıştır. Katılımcılardan gelen yanıtlar sonucunda istatistiki analizler yapılarak katılımcıların uzlaşı sağladığı ve sağlamadığı ifadeler belirlenmiştir. Delphi tekniğinin son turunda bazı çalışmalarda sadece uzlaşı sağlanan maddeler katılımcılara tekrar iletilirken (Karacaoğlu, 2009, s. 15; Osborne vd., 2003, s. 705) bazı çalışmalarda ise uzlaşı sağlanamayan ifadelere iletilmiştir (Gracht & Darkow, 2010, s. 52). Çalışmanın üçüncü turu için uzlaşı sağlanamayan maddeler çıkarılarak yeni bir anket formu hazırlanmıştır. Delphi tekniği üçüncü tur anketi Ek 5'te sunulmuştur. Üçüncü tur için hazırlanan anket formunda yer alan ifadeler üzerinde katılımcıların görüş ve düşüncelerinde farklılık olup olmadığı belirlemek adına tekrar tek tek katılımcılara anket formu iletilmiştir. Katılımcıların yaptığı dönütler sonucunda görüş birliği sağlanan ve sağlanmayan ifadeler belirlenerek çalışma sonlandırılmıştır.

3.8. Araştırmanın İnanırlığı

Bu çalışmanın inanırlığının sağlanması için uygulanan maddeler aşağıda sırlanmıştır:

- Çalışma literatür dikkate alınarak yapılandırılmıştır ve çalışmanın tüm aşamaları sürecin gerekliliği dikkate alınarak yürütülmüştür.
- Çalışmada farklı veri toplama araçları kullanılmıştır.
- Çalışmada yönteme ilişkin adımlardan detaylı şekilde bahsedilmiştir.
- Çalışmanın yöntemi itibariyle hazırlanan görüşme soruları ve anket formundaki ifadeler üzerine uzman görüşüne başvurulmuştur ve uzmanlar tarafından incelenmiştir.
- Çalışmada toplanan veriler kayıt altına alınmıştır.
- Çalışmaya katılım sağlayan katılımcılar, çalışmanın konusu ve amacına göre tecrübeye sahip uzman kişilerdir.
- Çalışmaya katılım sağlayan katılımcılar gönüllülük esasına dayalı olarak çalışmada yer almışlardır.

3.9.Bulgular ve Yorumlar

3.9.1.Delphi I. turu

Çalışmanın birinci turunda katılımcılara açık uçlu olarak hazırlanan yarı yapılandırılmış on bir soru sorulmuştur. İlk soru katılımcıların demografik özelliklerine ilişkin olduğundan bu kısımda bu soruya ilişkin yanıtlara yer verilmemiştir. İkinci olarak katılımcılara "Dördüncü Sanayi Devrimi, Dördüncü Sanayi Devrimi teknolojileri, dijital dönüşüm, sizde ne çağrıştırıyor? Dijital dönüşümün kurumunuza yansımaları nelerdir?" soruları sorulmuştur. Katılımcıların bu sorulara verdikleri cevaplar aşağıdaki gibidir:

K3- *Dördüncü sanayi devrimi, özellikle 5G teknolojisi ile beraber iş ve özel hayatımızda kullandığımız makinelerin internete bağlanarak onları uzaktan kontrol edebilmemizi, makine ve robotik teknolojilerin gelişimi, özellikle rutin işler için insan emeğinin azaltılarak makine ve robotların üretim süreçlerine daha fazla entegre edilmesini çağrıştırmaktadır. Denetim ve danışmanlık firması olarak dijital dönüşümün kurumumuza yansımaları, üretim, hizmet, perakende gibi reel sektörlere kıyasla daha dolaylı olmuştur.*

K4- "*Dördüncü sanayi denildiğinde aslında bütün iş dünyasının dijitalleşmesi yani sadece bir üretim hattının ya da faaliyetinin değil tüm süreçlerin dijitalleşmesi olarak düşünüyorum. Özellikle bazı trend olan teknolojiler var, bunlar: akıllı süreç otomasyonu, nesnelerin interneti, yapay zeka, sosyal medya ve platformları, büyük veri ve bulut*

sistemleri, robot ve dronların geleceğe yön vermesi beklenen yeni teknolojiler olduğunu görüyoruz. Bu süreçlerin iş dünyasına adaptasyonu benim için dördüncü sanayi devrimi."

Dijital dönüşümün kurumuma yansımalarına baktığımızda bizim kurumumuz ana hizmetlerinden biri dijital teknolojilerin kamu kurumlarına adaptasyonu ve kamu politikalarının veri ve kanıta dayalı geliştirilmesi ve inovasyonu. İç denetim ve iç kontrol süreçlerinin gerçek zamanlı izlenebilmesi ve yönetilebilmesi. Dolayısıyla bizi de doğrudan ilgilendiren bir konu olduğu için bizim de iş yapış şekillerimizden tutun da çözümlerimize kadar şirket stratejilerine kadar önemli bir konudur.

K5- "*Bu konuda en önemlisi internet, yapay zeka uygulamaları ve robotik uygulamalar ile ortaya çıkan iş modelindeki değişim çağrıştırmaktadır. Kurumunuzda bu yönde akıllı üniversite çalışması ve kurulan merkezlerimiz ile teknolojik gelişmeler desteklenmektedir. Stratejik planımızdan başlayarak tüm iş süreçlerimizde önemli olmaktadır."*

K7- "*Birkaç anlam ifade ediyor. Birincisi dijital dönüşüm ile birlikte bir otomasyonun hızlanması ve otomasyonun hızlanması ile birlikte makinelerin iş hayatında dijital iş gücü olarak yer alması anlam ifade ediyor. IoT sistemlerin birbiriyle konuşmasıyla farklı karar mercilerinin destek mekanizması olarak hayata geçirilmesinde bir süreç var karşımızda ve bu devamlı gelişiyor. Özellikle üretim sektöründe, otomotiv sektöründe fazla görülmeye başladı bu çalışmalar. Tabii ki entegre bir sistem alt yapısına ihtiyaç var entegre sistem çözümüne ihtiyaç var ve bizim için, danışmanlık tarafı için ise bu sistemlerin kurulumu ve bu sistemlerden alınacak verilerin işlenmesi ve takibi, üçüncüsü ise bu sistemlerin güvenliği; cybersecurity(siber güvenlik) anlamında güvenliğidir. Çünkü herhangi bir olumsuz durumda, örneğin enerji hatlarındaki kesintiler, örneğin üretim bandında yaşanacak kesintilerin önüne geçilebilmesi açısından tabii ki burada siber güvenlik hizmetleri bizim için kritik ve önemli oluyor."*

K9- "*Dijital dönüşüm daha çok endüstri 4.0'ı çağrıştırıyor. Çağdaş otomasyon sistemleri, veri alış-verişleri, üretim teknolojilerinin kolektif çalışmasını, IoT, siber fiziksel sistemler bunların oluşturduğu bir küme diyebiliriz. Bu uygulamaları özel sektörde biraz daha fazla görüyorum, önde gibi. Üniversitelerde daha çok teorik kısımlarda duruluyor. Kendi işimizden bahsedersek, denetim ile ilgili yeni yazılımlar, iş*

kontrolü ile ilgili yeni yazılımlar bunlar birbirine entegre çalışıyor, kendi içlerinde birbirlerine veri akışı sağlıyorlar. Bir yerin muhasebesini tutuyorsak aynı zamanda bir denetim yazılımına aktarılıyor. Eskiden sadece muhasebe yazılımları stok yazılımları ile birlikte çalışıyordu, şimdi artık iç kontrol, iç denetim yazılımları da geliştirildiği için bunlarda birbiriyle entegre çalışıyor yani birbiriyle veri trafiği hatta veri analizi bütünleşik olarak gerçekleşmesi söz konusu oluyor. Muhasebe, denetim, iç kontrol, stok yönetimi birçok şey birlikte yürütülüyor."

K12- "*Teknoloji iş süreçlerinin işleyiş biçimini temelden değiştirdi. Artık iş süreçlerinde gerçekleştirilen tüm fonksiyonlara yönelik teknolojiler kullanıma alınmış durumda, üstelik bu teknolojiler birbirleriyle sorunsuz denilebilecek bir etkileşim içinde çalışabiliyor. Bu dijital dönüşüm denen kavramın aslında hedeflediği noktaya doğru götürüyor bizi. İnsanın tabi olduğu zaman, mekân ve diğer fiziki zorunluluklardan en az etkilenen iş süreçlerinin, paydaşlara vadedilen değeri yukarılara doğru taşıma, sunulan hizmetlerin kalite ve hızını azamiye çıkarma açısından tarihte eşi görülmemiş fırsatlar sunuyor. Hiçbir şirket dijital dönüşümden kaçamaz, bir zaman bir şekilde kendisi de bundan etkilenmek zorunda. İçinde olduğum firma, bir blockchain(blokzincir) teknoloji firması olması nedeniyle, dijital teknolojileri hem kullanmakta hem de bunları iyileştirme, dönüştürme veya devrimci bir yaklaşımla alışılmış olanı yıkıp yenisini inşa etme konusunda çok agresif. Ve beni bu firmaya çeken de zaten buydu."*

K13-" Kurumların dijitalleşmesi, çoğu makinaların birbiriyle konuşarak, veriyle entegre bir şekilde çalışması diye düşünüyorum. Tabii bunun kuruma yansımaları olabildiğince sistemleri otomatize etmek, olabildiğince insan müdahalesini, insanın harcadığı zamanı azaltmak ve daha efektif daha kolay, dünyanın her yerinden ulaşılabilir, dünyanın her yerinden internete bağlı olduğunuz sürece çalışılabilir, bu pandemi ile birlikte sistemleri yaratmanın ne kadar önemli olduğunu bir kez daha görmüş olduk aslında. İster istemez dijital dönüşüm de bizim gibi kurumlara yansıyor, çalıştığım şirketleri değerlendirdiğim de ikisi de dört büyük denetim şirketleriydi, bu gibi şirketler bu pandemiye en hazır yakalanan şirketler. Bu şirketler uzaktan sistemlere erişim mevcut ve işte Teams , Zoom, Sype Business gibi programlar zaten halihazır da kullanılıyordu. Sadece burada bizimki gibi şirketleri zorlayan şey müşteri alışkanlıkları oldu. Çünkü işte dokümanların kağıt şeklinde verilmesi ve basılı evrakların dijital ortama aktarılmamış oluşu, siz ne kadar dijital dönüşümü sağlarsanız sağlayın, siz beraber çalıştığınız

müşterilerin buna bir uyumu yoksa biraz havada kalıyor. Ama en azından önceki çalıştığım ve şu anki kurumumun dijital dönüşüm konusunda rakiplerine göre daha önde olduğunu söyleyebilirim."

Katılımcılar tarafından dijital dönüşüm ve Endüstri 4.0 kavramlarına ilişkin alan yazında yer alan teknolojilere vurgu yapılmış olup, denetim açısından teknoloji sayesinde gerçek zamanlı izleme fırsatından bahsedilmiş, dijital dönüşüm tüm sektörleri etkilediği ve dijital dönüşümün Endüstri 4.0 çağrıştırdığı ifade edilmiştir. Diğer taraftan bağımsız denetim kurumlarının pandemi öncesinde dijital teknoloji yönünde halihazırda gelişmelerinin mevcut olduğunun fakat müşteri işletmelerin sürece uyum konusunda direnç gösterip, alışkanlıklarından vazgeçmemesi dijital dönüşüm sürecini bir bütün şekillinde ilerlemesini olumsuz yönde etkilemektedir.

Katılımcılara üçüncü soru olarak "Kurumlar göz önüne alındığında yaşanan dijital dönüşümün getireceği başlıca riskler olarak neleri görüyorsunuz?" yöneltilmiştir. Katılımcıların bu soruya verdikleri cevaplar aşağıdaki gibidir:

K1- "*Dijitalleşmenin iş yapış şekillerini değiştirmesinden kaynaklı yeni riskler ortaya çıkacağı gibi riskin önem derecesi de değişebilmektedir.*

- *Daha önceki sanayi devrimlerine kıyasla çok daha kısa sürede uyum sağlama ihtiyacının doğurabileceği yanlış kararlar ve bunlardan kaynaklı katlanılan yüksek maliyetler*
- *Yeterli düzeyde araştırma-geliştirme ve testlerin yapılmamasından kaynaklı kayıplar (zaman, iş gücü, bütçe vb.)*
- *Veri bütünlüğü ve güvenilirliğinin sağlanamaması*
- *Yıkıcı teknolojilerden gelebilecek potansiyel tehditler"*

K2- *"Dijital dönüşüm ile birlikte yaşanacak en önemli risklerin kişisel verilerin korunması ve siber güvenlik riskleri olduğunu düşünüyorum."*

K3- *"İş yapış şekillerinde gerçekleşecek önemli değişiklikler, insan emeği yerine makine ve robotik süreçlerin artması bazı iş kollarını son verecek ancak yeni iş kolları yaratacaktır. Bu sebeple bu süreçlere entegre olamayan ve kendini yenileyemeyen kişiler ve toplumlar için işsizlik önemli bir sorun gibi gözükmektedir. Artan makine ve robotlaşmanın sonucu olarak, en ince ayrıntısına kadar düşünülüp kurgulanmayan*

süreçlerde hata oranları ve bu hataları tespit için gereken süreler artacaktır. Dijital ortamlarda bilgi ve belge üretmenin daha kolay ve bunları doğrulamanın daha zor olması sebebiyle suistimal risklerinin artma ihtimali bulunmaktadır. Dijitalleşme sebebiyle çeşitli siber saldırılar artmakta ve firmalarda bilgi güvenliği riski oluşmaktadır."

K4- "*Dijital dönüşümden kaynaklı en büyük risk veri alanındadır. Burada sadece veri kaybı olarak düşünülmesin verinin bütüncül ve anlamlı şekilde tutulması/tutulamaması yani verinin doğru anlamlandırılamaması büyük bir risktir. Çünkü bu veri önemli karar destek mekanizmalarını da bir girdi oluşturuyor. Dolayısıyla o verinin anlamlı, tam doğru şekilde tutulamaması da önemli bir risktir."*

İkinci olarak risk de siber güvenlik riskidir. Özellikle uzaktan çalışma süreciyle birlikte daha da ön plana çıktı.

Üçüncü bir konu da otomasyondan en çok etkilenen süreçler arasında örneğin finans sektöründe satış, müşteri hizmetleri gibi süreçler var. Dolayısıyla work force'da (iş gücünde) bir dönüşüm gerekiyor. Özellikle kamu sektöründe yetkinliklerin yeniden tanımlanması, alt fikir dediğimiz yetkinliklerin ihtiyaca göre yeniden dönüştürülmesi gerekiyor, insan kaynakları kısmında bu riskten bahsedebilirim. Yetenek yönetimi önemli riskler arasında işverenler 2023'e kadar iş gücünün %54'ünün önemli yeni yetkinlikler kazandırma ve var olan yetkinliklerini geliştirme gerektireceğini ifade ediyor. Bu çok önemli bir oran gerçekten. OECD göre mevcut işlerin %14'ü otomatize olacak ve yüzde 32'sinde köklü değişikliklere bu durumda doğrudan işsizlik oranlarının artacağı sorunlarını doğurabilir. Dolayısıyla yeni yetkinlik ve beceri setlerinin kazandırılması ve var olanların geliştirilmesi ve dönüştürülmesi ile yeni işlerin ortaya çıkması ya da mevcut işlerin dönüştürülmesi büyük bir önem kazanıyor."

K7- "*Siber güvenlik riskini önemsiyorum. Hem üretilen verilerin dışarı çıkması hem de o verilere ya da sistemlere dışardan saldırıların olabilmesi ve sistemin süreli ya da uzun bir zaman kesintiye uğrayabilmesi en büyük risklerden bir tanesi. İkincisi dijital iş gücü akla gelebilir. Verimlilik artırılması için olması gereken süreç bu şekilde ilerlemelidir. Bunu riskten ziyade insanların iş yapış şekillerin değişmesi gerektiği üzerine bir çıkarımla söylemek daha doğru olacaktır."*

K11- "*Dijital dönüşümün ilk büyük riski "uyum". Zira görece eski teknoloji ve iş yapış tarzı ile ilerlemeye alışmış bir işyeri, bu değişime uyum sağlamak için öncelikli*

olarak sağlam bir vizyona sahip olmalıdır. Tabii ki bu vizyonu destekleyecek yöneticilere, bunları uygulayacak çalışanlara ve bu ortamı oluşturacak yatırım gücüne sahip olmalıdır. Bu anlamda bazı şirketler değişim kültürüne ve risk alma vizyonuna sahip ise daha hızlı yol alacaklardır ve uyum süreçleri daha az sancılı olacaktır.

Dijital dönüşüm bazı iş kalıplarından çıkmayı, yeni iş modellerine (uzaktan çalışma, bulut teknolojileri, vb,) ve yeni yıkıcı (disruptive) teknolojilere yaklaşmayı zorunlu kılmaktadır. Bu kapsamda da bir diğer risk, "bilgi güvenliği"dir. Zira, dijital çağda en değerli kurumsal/kişisel varlık artık "bilgi"dir. Bilgiyi oluşturmak, kullanmak, ondan yararlanmak, işlemek, saklamak, değeri oranında korumak yeni ve daha büyük bir iş yükü haline gelmiştir. Kişisel veri mahremiyetinden kurumsal gizli bilgilere; ticari sırlardan pazardaki yeniliklere kadar pek çok boyutta bilgi işleme kolaylaştığı kadar onu korumak ve uygun şartlarda kullanmak da o derece zorlaşmıştır.

Son olarak da dijital dönüşümün getirdiği yeni yaklaşımlar ve özellikle de Z kuşağının bu alanda önderliği alarak ilerlemesi, oyunun kurallarının artık değiştiğinin göstergesidir. COVID-19 pandemisinin yarattığı etkileri de değerlendirdiğimizde şirket yöneticilerine bu yeni kurallara göre insan kaynaklarının yönetimi anlamında kendi vizyon ve dönüşümlerini tekrar değerlendirmeleri mecburiyeti gelmiştir. Yoksa, oyun dışında kalmak işten bile değildir."

Katılımcılar dijital dönüşüm ile birlikte başlıca riskler olarak bilgi güvenliği ve siber güvenlik riskini, verinin bütünlüğü, anlamlandırılması ve güvenilirliği riski, kurumların uyum sağlama sürecinde karşılaşılan riskler, insan gücünün adapte olamamasından kaynaklı bazı mesleklerin kaybolma riski konularını ele almışlardır.

Dördüncü soru olarak katılımcılara "Dijital dönüşüm ile beraber karşılaşılan riskler karşısında iç denetim fonksiyonunun rolü nedir?" sorusu yöneltilmiştir. Katılımcıların bu soruya verdikleri cevaplar aşağıdaki gibidir:

K2- *"İç denetimin tanımında da verildiği üzere iç denetim birimi içinde bulunduğu kurumda kurmay bir rol üstlenmektedir. Bu anlamda dijital dönüşümün getireceği riskler ve bu risklerin yönetiminde vereceği hem güvence hem de danışmanlık faaliyeti ile kuruma önemli katkılar sağlayabilecektir."*

K5- *"İç denetim fonksiyonu uluslararası standartlara uygun çalıştığında çok katkı sağlayabilir. Ancak bunun için henüz gerekli koşullar yoktur."*

K7- "*Yetkinlikler değişmesi gerekiyor. Denetimi yapacak olan denetçinin yetkinliği değişiyor. Dijital anlamda kendimizin değişmesi gerekiyor. Geleneksel yöntemler güzel, örneklem seçilmesi, testlerin yapılması gibi. Dijitalleşen platformda hem işin süreç kısmını bilen hem de teknoloji kısmını bilen ve bunları anlamlandıran her ikisini çakıştıran yetkinliklere ihtiyacımız oluyor. Bu anlamda bazen bunu yaparken farklı farklı ekipler bir araya gelerek yapıyoruz. Bazen tek kişiden bu multidisipliner alanları bekliyoruz ve beklemeye devam edeceğiz gibi gözüküyor. Şu anda gelişme alanlarından bir tanesi geleneksel yapılanma yöntemlerin aslında biraz daha teknolojik yetkinliklerle birlikte değişip ilerlemesi gerektiğine ilişkin bir görüş var. Bu tabii personel açısından ve bir yandan da süreçler otomatize oldukça onun kendi içerisinde getirdiği risklerde tabii ki önceden karşılaştığımız risklerin yanında yeni riskleri beraberinde getiriyor. Dolayısıyla bunlara ilişkin de bir bilgi birikimi geliştirmek çok önemli. Dediğim gibi önceden çok basit anlamda yaşanan bir kesinti belki o kadar önemli olmasa da otomatize edilmiş dijital iş gücüne aktarılmış alanlarda, açıkçası bu risklerin bertaraf edilmesi için teknolojik risklerin yönetimine ilişkin bir çalışma faaliyeti, organizasyonda yer verilmesi gerekiyor. Bizde iş yapış şekilleri devamlı değişiyor, değişecektir. Bu anlamda hem data analizi (veri analizi) hem sistem içerisinde bilgi sistem güvenliği hem operasyonel süreçlerin bilgi birikiminin bir arada yürümesi gereken bir sürece doğru evriliyor ve evrilecek dolayısıyla bu bizim için en büyük risklerden ya da en büyük değişimlerden biri şeklinde bahsedebilirim."*

K8- *"İç denetim öncelikle kurumu risk konusunda bilgilendirmesi gerekiyor. Aslında ben iç denetimi sadece bir denetçi olarak değil bir danışmanlık şapkasının da olduğunu düşünüyorum. İşi en iyi bilenler süreç sahipleridir. Ama iç denetçi çok güzel riskleri tespit edebilir, bu konuda kurumu yönlendirebilir, risklerin bertaraf edilmesi ya da minimize edilmesine yönelik aksiyon planları sunabilir. Dolayısıyla iki şapkasını da kullanması gerektiği şeklinde özetleyebilirim."*

K10- *"Burada öncelikle iç denetçinin bir dönüşüm sağlaması lazım, proaktif olması lazım, COVID döneminde bizler proaktif davranıp denetim programı aldık. Dijital üniversite konseptinde yeni normale bir uyum sürecinde bir süreç belirledik. Bunu denetledik mesela birkaç büyük fakültelerde. Bakalım nasıl gidiyor hem idare hem eğitim*

açısından nasıl gidiyor diye baktık. Öncelikle denetçinin proaktif olması lazım. Denetçinin bu sürece ayak uydurması lazım, böyle bir şeye inanması lazım ve donanımı olması lazım. İkincisi de kurumuna bu konuda yön göstermesi lazım. Kurumda icracı birimler yoğunluğundan kaynaklı bu konulara çok fazla vakit ayıramayabilirler. Ama iç denetim biriminin görevi danışmanlık ve denetim, başka bir görevi yok. Bu anlamda bu konularda daha açık olması lazım ve kurumu ile paylaşması lazım. Biz dijital dönüşüme geçerken neler yapılması gerektiği, hangi aksiyonlar alınması gerektiği konusunda yönetime rapor sunduk."

K12- **"***İç denetim fonksiyonları öncelikle yeni teknolojilerin beraberinde getirdiği fırsat ve tehditler konusunda derinlemesine analizler gerçekleştirip, bu konularda üst yönetimi iyi yönlendirmesi gerekiyor. Genellikle güvence fonksiyonu üzerinden değerlendirilen iç denetim birimlerinin, danışmanlık kasları bu açıdan çok değerli. Ayrıca güvence faaliyetleri aracılığıyla görünmeyen veya ilk başta anlaşılamayan sorunların ortaya çıkarılması ve bu konularda ilgili paydaşların dikkatinin çekilmesi çok kritik. Örnek olarak bir şirket, bulut hizmetlerinden yararlanmayı isteyebilir. Bu parasını verip, iki günde çözülecek bir konu değil. Topyekûn bir kültür değişimi gerektiriyor. Ayrıca çok önemli riskler barındırıyor. En basitinden bir veri göçü sorunu var. Eminim veri taşıma konusundaki hayati kritik noktaları birçok üst yönetici farkında değildir. İşte bu iç denetimin en önemli başlıklarından birisi olmalı. Yeni teknolojilerinin iyi analiz edilip anlaşıldığından emin olunmalı."*

Beşinci soru olarak katılımcılara "Dijital dönüşüm çerçevesinde iç denetimin güvence sağlama ve danışmanlık rolünü nasıl değerlendirirsiniz?" sorusu yöneltilmiştir. Katılımcıların bu soruya verdikleri cevaplar aşağıdaki gibidir:

K1- *"Dijital dönüşüm sürecine ilişkin fayda maliyet analizlerinin yapılması; ABD, Almanya, Çin gibi ülke örneklerinin değerlendirilmesi; dijitalleşmenin getirebileceği risk ve ilgili kontroller, kurumun yapısı ve uyum sağlama durumu, kurum insan kaynağının yeterliliği vb. konularda danışmanlık hizmeti verilebilir."*

K3- *"Dijital dönüşüm çerçevesinde iç denetimin temel faaliyeti olan güvence ve danışmanlık görevi daha önemli bir seviyeye evrilecek olup görevin icrası konusunda süreç daha zor bir hale evrilecektir."*

K5- *"İlk etapta danışmanlık önemli katkı sağlayabilir. Kurumsal olgunluk düzeyi arttıkça güvence faaliyetlerine yer verilebilir."*

K6- *"Güvence sağlamayı bilgi ve iletişim denetimi ile yapacağız. Bu noktada saha çalışması sonucu rapor üretiyoruz. O raporu birimle paylaşıyoruz, alınması gereken tedbirler ne ise bunları paylaşıyoruz, onların da görüşlerini aldıktan sonra üst yöneticiye sunuyoruz. Cumhurbaşkanlığı istediği için bazı bilgileri onlara da göndereceğiz. Elimizde bir standart/kılavuz olmadığı bir dönemde bu konuda başka bir kamu kurumundayken yapmıştık. Denetim, danışmanlığa göre daha sert oluyor. Bu noktada daha çok değer katma, iyileştirmeye yönelikti. Kurumumuzda yetişmiş bir kadro var. Hem hizmet alımı yapılmış hem de dışardan sözleşmeli personel alınmış, standartlara uyum konusunda sürekli çalışmaları var. İç denetim birimi olarak danışmanlık verecek pozisyonda değiliz çünkü yetişmiş elemanımız yok, ama daha ileri de olabilir. Bizim kendi faaliyetlerimiz rehbere uygun olduğundan özellikle kamu iç denetim rehberinde risk denetimi konusunda iç denetçinin üstlenmesi ve üstlenmemesi gereken roller var. Biz sistemin konusunda rol göstericiyiz, sorumluluk idaredir."*

K7- *"Biz iç denetim olarak danışmanlık fonksiyonu altında çalışıyoruz. Biz finansal denetim ya da teknoloji denetimi yapan ekiplerden farklıyız. İç denetim olarak zaten danışmanlık şapkamız zaten var. Bu çerçevede hem yetkinliklerin gelişmesi hem de süreçlerin iyileştirilmesine ilişkin fikir beyanında bulunacağımız için. Mevcut süreçler içindeki eksikleri tespit etmenin yanında bizim temel fonksiyonlarımızdan birisi iyileştirici öneriler sunmasıdır. Dolayısıyla danışmanlık rolüne ihtiyaç yüksektir. Departmanın konumu gereği de bunu söyleyebilirim. Ben danışmanlık ekibiyle çalışıyorum ama danışmanlığa olan ihtiyacın artığı yönde bir değişiklik söz konusu olduğunu söyleyebilirim."*

K8- *"Öncelikle biraz önce sadece siber güvenlikten bahsettik ama genelde ITGC (IT General Control) dediğimiz IT genel kontrolleri olabilir. Fiziki olarak dediğimiz donanımların kontrolü olabilir ya da başka alt yapısal yeterlilikleri ölçen denetimler olabilir, proje bazlı denetim olabilir. Yani denetimi çeşitlenmesi aslında iç denetçilerin elinde. Yani kurumu bu şekilde yönlendirmesi gerekiyor. Sadece IT denetimini yaparken denetçinin olmasından ziyade farklı yetkinliklerden de yararlanabilinir diye düşünüyorum. Örneğin bir SAP denetleniyorsa bir ABAP kodu yazan birisinden ya da bir dış taraf denetleniyorsa o konuyla ilgili bir hukukçudan destek alınabilir. Yani bir*

denetçinin aslında tek başına bir denetimi alıp yürütmesi de bence çok yeterli gibi gözükmüyor. Farklı yetkinlikte bir arada birleşip denetim yapılması gerekiyor diye düşünüyorum. Çünkü bir denetçi çok uzman olsa bile, uluslararası sertifikaları olsa bile ya da bizim gibi böyle Big Four'da sürekli farklı şirketler görüyoruz, farklı projeler yapıyoruz, tecrübemiz çok olsa bile her şeyi bilmemiz tabii ki mümkün değil, dolayısıyla özellikle dijitalleşme konusunda bu kadar gelişmeler hızlı şekilde olurken dışardan hizmetler alınması yani yetkin kişilerin denetime dahil edilmesi gerektiğini düşünüyorum.

Danışmanlık konusunda da bilgi işlem alt yapısının yeterli olup olmadığı ya da hangi modül alınacak ya da kaç kişinin sahip olması gerekiyor, yani bu iş yükü analizi de olabilir, sistem yeterliliği testi de olabilir. Aslında danışmanlık anlamında iç denetçilerin yapabileceği çok şey var.

Dijital dönüşüm ile birlikte danışmanlık rolüne ihtiyacın artmasının denetçinin bağımsızlık ve tarafsızlığını koruma anlamında bir olumsuzluk yaşatmadı. Eğer bunu yaşayan şirketler varsa da üç hat dediğimiz modele uymadıklarını düşünüyorum. Eski adıyla üçlü savunma hattı. Danışmanlık verirken bir işi bizzat yapmıyor olması gerekiyor. Bizzat yaptığınız şeyi denetleyemezsiniz. Danışmanlık bir opsiyonların ilgili kişilere verilmesi ilgili literatür araştırmaların yapılması ve önerilerin hazırlanmasıdır. Bu önerilerin yapılıp yapılmayacağı tabii ki başka birimlerin sorumluluğundadır. Ama iç denetçi ya da şirketlerdeki bazı yöneticiler iç denetçilerden hakikaten çok fazla şey bekliyor. İşi kalkıp kendileri yaparsa tabii ki denetlenemez ve bağımsız olmayan bir süreç haline düşer. Ama kesinlikle bu üçlü hat modeline uygun olduğu sürece denetçinin danışmanlık vermesinde hiçbir sakınca görmüyorum. Hatta pandemiyle birlikte iki senedir denetçiden beklenen kısım biraz daha danışmanlık şapkasına önem vermesidir."

K9- *"İç denetim mutlaka kurulmalı, Türkiye'de bu konuda bizler geç de kaldık. Benzer şekilde dijital dönüşüme de geç kaldık. İç denetime de dijital dönüşüme de entegrasyon en kısa sürede gerçekleştirilmesi gerekiyor. Ama tabii ki iç denetim olan firmalarda da hiçbir zaman %100 güvence sağlanamadı. Şunu demek istiyorum. Bir şirkette iç denetim varsa %100 riskler sıfırlanır ya da güvence sağlanır diye bir şey yok. Ama önemli bir kısmı hal oluyor. Dijital dönüşüm çerçevesinde iç denetimin %100 güvence sağlayamama konusu devam edecek hatta güvence sağlayamama durumu daha da artabilir. Ama diğer taftan danışmanlık rolü daha belirgin olacak. Hatta danışmanlık rolünün daha kritik hale geleceğini düşünüyorum."*

Katılımcılar dijital dönüşümle birlikte iç denetim fonksiyonuna hem güvence hem danışmanlık rolü kapsamında ihtiyaç duyulduğu, denetçinin yetkinliğine vurgu yapıldığı, iç denetçilerin kurumlarını dijital dönüşümün etkileri -fırsatlar ve riskler- konusunda farkındalık yaratılması şeklindeki rolünü ifade etmişlerdir. Diğer taraftan katılımcılar danışmanlık rolüne dijital dönüşüm ile birlikte ihtiyacın artığı fakat bu durumun iç denetçinin bağımsızlık ve tarafsızlığı konusunda olumsuz etki yaratmadığı vurgulanmıştır. Üçlü hat modeline uygun hareket edilmesi halinde dijital dönüşüm sürecinde denetçilerin bağımsızlık ve tarafsız şekilde faaliyetlerine devam edebilecekleri ifade edilmiştir. Ayrıca COVID-19 salgının danışmanlık rolüne ihtiyaç konusunda artış şeklinde etkilediği katılımcılar tarafından belirtilmiştir.

Altıncı soru olarak katılımcılara "Üçlü hat modelinin, üçüncü hat rolünde yer alan iç denetimi dijital riskler çerçevesinde nasıl değerlendirirsiniz?" sorusu yöneltilmiştir. Katılımcıların bu soruya verdikleri cevaplar aşağıdaki gibidir:

K1- *"Bu modelde iç denetim, amaçlara ulaşmakla ilgili tüm konular hakkında bağımsız ve objektif güvence ve tavsiye verme sorumluluğuna sahiptir. Bu doğrultuda;*

- *Dijitalleşme sürecinde kurumun amaçlarına ulaşmasını desteklemek ve sürekli gelişme ve iyileşmeyi teşvik etmek ve kolaylaştırmak amaçlarıyla, yönetişimin ve risk yönetiminin (iç kontrol de dâhil) yeterliliği ve etkililiği ile ilgili olarak yönetime bağımsız ve objektif güvence ve tavsiye sunmak konusunda kilit bir role sahiptir.*

İç denetim, dijital dönüşüm sürecinin yönetişim, risk yönetimi ve iç kontrol sisteminde yaratacağı değişime ilişkin tavsiyelerde bulunmak, bu konularda kuruma ve yönetime danışmanlık yapmak ve destek sunmak gibi önemli rollere sahiptir. Yeni sistemin yeterliği ve etkililiğinin değerlendirmesi de rolleri arasında yer almaktadır. Dönüşüm sürecinde kurumda en doğru yapının oluşturulması ve kurumun buna uyum sağlaması noktasında iç denetim önemli katkılar sunabilir."

K2- *"Revize edilen üçlü hat modelinde iç denetimin önemi daha ön plana çıkarılmış ve iç denetimden olan beklentilerde artmıştır. Söz konusu bu durumda değişen ve dijitalleşen yeni dünyada dijitalleşme kaynaklı riskler iç denetim faaliyetini daha da gerekli kılmaktadır."*

K6- *"Bakanlıkta üçlü hat tam olarak kuramsal olarak uygulanmasa da uygulamada yer alan bir konudur. Kurumlar özellikle uygulamada veri yönetimi, bakanlıkta bilgi teknolojileri genel müdürlüğü, muhasebe hizmeti veren muhasebat genel müdürlüğü bilgi işlemi birinci hattı uyguluyorlar. Risk yönetimi konusu bir model olarak hareket etmiyor. Dijital dönüşüm konusunda risklerin olması konusunda yönetim açısından bir farkındalık var. Biz daha çok kurumsal risk yönetim konusunda odaklanıyoruz. Raporda riskleri bertaraf etmeye yönelik öneriler bulunuyor. Risk yönetimi bir yönetim şekli olarak uygulanmıyor. Bizim çalışmamız tamamen bu modele yönelik, risk yönetim modeline yöneliktir. Bu noktada faaliyetlerimizi planlayarak yürütmek, dokümantasyon oluşturmak. Bu dokümantasyondan iç denetim olarak bizde faydalanıyoruz. Mesela yeni biriyle iç denetime başladığımızda dokümantasyonumuzun ne olduğunu gösteriyoruz ki nasıl bir faaliyet yürüteceğini görsün diye. İç denetim için bize ilk denilen şey, dokümantasyon bizim kırmızı çizgimizdir. Rapor var ama raporun altında çalışma kağıtları var, çalışma kağıtları sizi sonuca götürüyor.*"

K4- *"Üçlü hat modeli bir risk çerçevesidir ve risklerden bir kurum içerinde nasıl daha iyi korunur. Birinci hat rolünde risk sahipleri riskleri elimine etsin, riskleri indirgesin; ikinci hatta biraz daha iç kontrol, risk fonksiyonları işin içinde daha olsun; üçüncü hatta bağımsız bir göz olarak, bağımsız bir fonksiyon olarak iç denetim bu güvenceyi sağlasın şeklinde bir yapılanma var. Dijital dönüşüm çerçevesinde aslında bizim de gündemimizde dijital riskler var. Dediğim gibi sistem üzerinden de iç denetim yapmaya geçmek üzereyiz. Big Four kurumu olarak da kendi toolumuz (aracımız) var bununla ilgili, iç denetim araçlarımız. Globalden bazı araçları ve sistemleri müşterilerimize entegre etmeye çalışıyoruz. İç denetim artık kendi risk denetimi yaparken, risk değerlendirmesi yaparken, planı oluşturmadan önce artık bir veri üzerinden değil de gerçek zamanlı riskler üzerinden özellikle bizim araçlarımız advance analtics marker(gelişmiş analitik işaretler) olarak içinde dolayısıyla advance analiticse uygun olarak real time monitoring (gerçek zamanlı izleme) yapabilecekleri control effectiveness (kontrol etkinliği) anlık olarak takip edebilecekleri, authorisation'ları (yetkilendirmeleri) üst yönetimin anlık takip edebileceği alanların oluşturulduğu önemli araçlar, dolayısıyla iç denetim artık biraz hem planlamasını oluştururken risk denetim faaliyetlerinde hem iç denetim faaliyetlerini gerçekleştirirken hem de raporlama kısmında böyle 30 sayfalık*

rapor vermek yerine daha farklı interaktif raporlama mekanizması tasarlamaya başladık. İç denetim artık riskleri daha proaktif bir yönettiği döneme geliyor."

K7- *"Birinci hat süreci gerçekleştirenlerin yaptığı kontrolü ikinci hat genelde iç kontrol, üçüncü hatta aslında teftiş kolu gibi denetimlerin yapıldığı bir fonksiyon şeklinde düşünürsek; dijitalleşme ile birlikte tüm popülasyonları bir arada değerlendirip riskli alanlara odaklanılması söz konusu olabiliyor. Geçtiğimiz zaman içerisinde tabii ki üçüncü hat kontrolleri geçmişe dönük yapıldığı için bir sampling(örneklem) seçilerek yapıldığı için bazen olası bir riskli alan kaçırılabiliyor. Dijitalleşme ile birlikte aslında iç denetçilerin üçüncü seviye kontrollerin sadece tüm popülasyonların taranıp sadece normal dışına odaklanması söz konusu olabilir ki, bence zaten sektörde bu yöne doğru gidiyor. Dolayısıyla orda nokta atışı söz konusu oluyor ve olacaktır diye düşünüyorum.*

K9- *"Önümüzdeki dönemlerde iç denetçilere bu noktada daha fazla sorumluluk düşeceğini düşünüyorum. Dijital dönüşüm ile birlikte yeni riskler yeni açıklar ortaya çıkacaktır, burada iç denetçiler her zaman bir adım önde olması gerekir diye düşünüyorum. Eskiden iç denetçi tipi biraz daha farklıydı, muhasebe bilmeyen yani sadece stok kontrolü yapan ya da yetkilendirme kontrollerini yapan iç denetçiler bile vardı. Artık önümüzdeki dönemlerde dijital dönüşüm ile birlikte daha farklı olacak diye düşünüyorum. Nasıl farklı olacak? Zaten muhasebe bilmesi kesinlikle gerekecek bunun üzerine iç denetçiler multidisipliner bir karaktere sahip olması gerecek. Mesela hem IT'den anlayan hem muhasebeden anlayan hem kontrolleri yapabilen yani hem işin teorik hem pratik yönüne hakim iç denetçilere gerek olacağına düşünüyorum."*

Katılımcılara göre dijital dönüşüm süreciyle birlikte üçlü savunma hattının üçlü hat modeli olarak revize edilmesiyle iç denetim faaliyetinin öneminin daha da artığı vurgulanmıştır.

Yedinci soru olarak katılımcılara "Kurumlar dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde nasıl değişiklikler yapmalıdır? Bu noktada iç denetimin rolü nedir?" sorusu yöneltilmiştir. Katılımcıların bu soruya verdikleri cevaplar aşağıdaki gibidir:

K1- *"Dijital dönüşümü bir takım teknolojik yeniliklerin alınması veya bunlara adaptasyon süreci olarak ele almak dar bir çerçeve çizmek anlamına gelmektedir. Dijital dönüşüm merkezine teknolojiyi alan yeniden bir yapılanma sürecini de beraberinde*

getirmektedir. Dolayısıyla kurum yapısının değişimi, kurumunun insan kaynağının geliştirilmesi ve/veya değişimi, kurum kültüründe birtakım değişiklikler bu dönüşümün bir parçasıdır. Diğer taraftan dijitalleşme ile özellikle hammaddenin kontrolü, fiyat kontrolleri, iş görenlerin ve nakit hareketlerinin kontrolü gibi iç kontrol sisteminin sorumluluğundaki gibi birtakım kontroller yazılım sistemlerine aktarılmaktadır. Bu kontroller sistemler tarafından otomatik olarak yapılmakta ve raporlanmaktadır. Bu nedenle iç kontrol sistemleri yeni yapıya uyumlandırılmalı, doğru bir şekilde yapılandırılmalı ve uygulanmalıdır. Bu süreçte iç denetim tarafından verilecek danışmanlık faaliyeti oldukça önemlidir.

Dijital dönüşüm ile daha önce manuel, fiziki belgelere dayalı olarak yapılan denetim yazılım sistemleri tarafından otomatik olarak yapılır hale gelmektedir. Bu nedenle kurumun kullandığı sistemin doğruluğunun denetimi önem kazanmaktadır. İç denetimce kullanılacak sistemlere yönelik denetim yapılmalıdır. Bu veri güvenilirliği açısından oldukça önemlidir."

K2- *" İç kontrol sisteminin risk ortamı ve kontrol faaliyetleri bileşenlerinin dijital riskleri kapsaması konusunda revize edilmesi gerekir. İç denetim iç kontrol sisteminin beş bileşeninden izleme faaliyetinin yerine getirilmesini sağlayan bir mekanizma olarak iç kontrol sisteminin eksikliklerini tespit ederek giderilmesini sağlamada özellikle güvence rolü ile katkı sağlayabilir. Risklerin belirlenmesi ve belirlenen bu risklere ilişkin oluşturulacak kontrol faaliyetlerinin belirlenmesinde ise danışmanlık verebilir."*

K4- *"Olaylar gerçekleştikten sonra değil de olayların gerçekleşmeden önce önlem alınması ve mevcut trendler takip edilerek/ pazar dinamikleri takip edilerek sürekli bir uyum içinde kalmak yeni dünya ile. İç kontrol belki bu anlamda değişebilir. Ya da entegre sistemler kullanılabilir, örneğin ERP kullanımı ön plana çıkıyor ya da ERP kullanmayı bilen kişilerin işe alınması. Bu noktada iç denetimde paralel olarak yetkinliklerini biraz daha bilgi sistemleri yetkinliği kazandıracak şekilde kendisine, bilgi sistemleri denetimi yapabilecek şekilde evrilebilir. Yine klasik geleneksel yöntemlerdense artık biraz daha ERP denetleyebilecek ileri düzeyde danışmanlık yapabilecek, süreçlerin birbiri arasındaki koordinasyon yönetebilecek demeyeyim ama o konular üzerinde danışmanlık yapabilecek bir rolü olmalıdır diye düşünüyorum."*

K5- *"Dijitalleşme bir strateji ile başlamalıdır. Risk yönetimi çerçevesinde kurumsal yönetim ilkelerine uygun olarak gerekli kontrol noktalarının oluşturulması sağlanmalıdır. İç denetim stratejik rol üstlenmelidir. Danışmanlık rolünü ön plana çıkarması uygun olacaktır."*

K6- *"Sistemde bir değişiklik yapmaya gerek yok. Dijital dönüşümden kaynaklı riskleri raporlayacak bir birim vardır, olması gerekir. Çünkü o hizmet birimleri faaliyet raporu ile ilgili şeyler yayınlıyorlar. Ama burada iç kontrol sisteminde değişikliğe gerek yok dememin sebebi zaten iç denetimin bu stratejiyi geliştirmekle birlikte zaten sağlıyor olmasıdır. İç kontrol sistemi içinde de risk yönetimi diye unsur var, yapılsa daha iyi olabilir, daha yaklaşımın iyi olmasını sağlayabilir. Bu noktada üst yönetimin bu konuyu sahiplenmesi bunu farkında olması önemlidir. Bizler çok güzel risk analizleri yapıyoruz ama üst yöneticiler faydalanmak istemezse; tamam siz neyi denetlemek istiyorsanız onu denetleyin de diyebilir ya da şu konuları da denetleyin de diyebilir. Ama böyle bir konuyu farkında olursa, kuruma değer katacağını farkında olursa daha etkili olur. Şu an tüm kamu için esas sorun iç kontrol sisteminin tam olarak ne olduğunu kavramamasıdır. Genellikle bütçenin hazırlanmasında strateji geliştirme başkanlığının bir fonksiyonu gibi görülmektedir. Görev tanımları ve süreçler çıkarılıyor ama bu kadar yani. Bu noktada istediğiniz kadar doküman yapın eğer istenmiyorsa bir anlam ifade etmiyor. Ama bu husus iş süreçlerine giydirilirse özellikle hizmetler dijitale döndükçe iç kontroldeki yaklaşımı içine koyabiliyoruz, yani dosyada kalmıyor. Böylece tamamen süreçlerin içerisinde değerlendirebiliyoruz. Örneğin işten ayrılan biri sisteme giriyor mu diye kontrolü yapılıyor. Böylece çok rahat bu analiz edilebiliyor. Dijitalleştikçe iç kontrol sisteminin bakış açısının kurumlarda artacağı yönünde olduğunu düşünüyorum. Kurumlarda iç kontrol sistemleri, risk yönetimi var fakat bu tanımlanmış değil/ihtiyaç halinde kullanılmaktadır. 5018 kamu iç kontrol kanunu bizi bu yönde zorluyor. Bu kanun riski yönetmek anlamında kullanılıyor. Kamunun özel sektörün uygulanmalarından faydalanması son zamanlarda söz konusudur. Bu noktada en önemlisi risk yönetimi, risk yönetiminde kurumlar bir şekil faydalanıyor. Günümüzde yaşanan değişim bizi de geliştiriyor."*

K8- *"Kurumdan kuruma değişir desem çok genel geçer bir cevap olur mu bilmiyorum ama, kurumların olgunluk seviyelerine bağlı aslında. Yani çok böyle evrimin başında olan bir şirket, yeni yazılım ne alabiliriz, kaynağımız nasıl büyütebiliriz diye*

bakarken; mevcut sistemini oturtmuş şirketler artık güvenlik, sızma testleri, iş sürekliliği testleri bunları yapmaya başlıyor. Kurumun büyüklüğü ve yeterliliğine göre diyebilirim.

İç denetimin danışmanlık şapkası açısından bakarsak sonuçta iç denetçinin belli bir profilinin ve öğrenme seviyesinin olmasını bekleriz. Örneğin şirkete yeni bir yazılım alınacaksa veya dijital dönüşüme geçiriyorsa alternatifleri neler olabilir, tedarikçileri kimler olabilir bunları yönetime sunabilir. Ya da halihazırda yeni bir sistem geçişi veya upgrade (üst modele geçmek) olduysa iç denetçi eğitimleri alıp bunu kuruma kendisi anlatabilir, eğitim vermek şeklinde de bir danışmanlık verebilir. Denetim kapsamında yeni sistemin denetlenmesi için üzerinden belli bir zaman geçmesi gerekir. Belli bir olayların olması ve içinden örneklem seçmek vs. daha sistem tasarım aşamasındayken aslında dizayn testleri yapabilir. Yani zorunlu alanlar şunlardır veya mükerrer girişe izin verenler bunlardır gibi. 3 ay olur 6 ay olur işlemler gerçekleştikçe içerisinden örneklem seçerek gerçekten operasyonel etkinliği var mı diye bakabilir. Yani danışmanlık şapkası altında eğitim vermek, literatürü araştırmak, kurumu yönlendirmek diyebilirim; denetim şapkası altında ise dizayn ve operasyonel işlerlik testi diyebilirim."

K11- *"Bir şirket iş süreçlerinde dijitalleşme adımları atmaya başladı ise ve bunu şirket kültürü haline getirdi ise doğal olarak iç kontrol yapısını da bu bakış açısı ile güncellemek zorundadır. Gerek çalışanların işlerini yaparken gerekse yöneticilerin hedeflerini ve iş akışlarını güncellerken bu yeniliklere sırtlarını çevirmeleri mümkün değildir. Rekabetin, yeni iş modellerinin fırsatlarının ve iş hedeflerinin karşılanmasındaki gücün azalmaması için bu iyileştirmelerin zamanında ve etkili bir şekilde işe yansıması gerekmektedir. Bu değişimin etkileri ya da risklerin varlığı, iç denetim sonuçlarında erken fark edilirse şirket kendi kararı ve yeteneği ile bu yenilikleri iş süreçlerine yansıtma şansını yakalayacaktır. Fakat, iç denetim ile fark edilebilecek bu tür dijital riskler yeterince iyi anlaşılamaz ise ya da iç denetim fonksiyonu bu konuları yakalayamaz ise, ciddi iş başarısızlıkları ya da daha ağır maliyetler ile yeniden dönüşüm, iyileştirme ya da dijital uyum süreçleri takip edilmek zorunda kalınacaktır. Elbette ki bu ikinci durum daha zorlu ve şirketler için daha sancılı geçecektir."*

K12- *"Öncelikle sürekli izleme yaklaşımlarının adapte edilmesi şart. Güvenlik açısından DLP, Firewall, SIEM gibi araçlar ile tüm şirket sistemleri anlık olarak izlenerek, anomaliler takip edilir. Bu diğer iş süreç fonksiyonları için de gerçekleşmeli. Performans, kritik alım/satım işlemleri, para havaleleri gibi risk barındıran işlemlerin*

yılda bir defa denetime tabi olması saçma bir durum. Dolayısıyla iç denetim fonksiyonlarının da teknoloji ile haşir neşir, GRC ve veri analitiği araçlarını kullanan yapılar hale gelmesi gerekiyor. Sistem veri tabanlarından doğrudan veri çekip analiz yapmayan hiçbir denetim biriminin modern iş süreçlerine katkı sağladığını iddia etmesi mümkün değil artık."

Katılımcılar dijitalleşmenin strateji ile başlaması gerektiği, iç kontrol sisteminin otomatikleşmesi ve yeni yapıya uyum sağlanması, insan kaynağının yetkinliği, iç kontrol sitemindeki değişimin kurumdan kuruma farklılaştığı konularını vurgulanmıştır.

Sekizinci soru olarak katılımcılara "Sizce dijital dönüşüm süreci ile birlikte iç denetçilerin taşıması gereken yeni özellikler nelerdir? Bu süreçte iç denetçilerin odak noktası ne olmalıdır?" sorusu yöneltilmiştir. Katılımcıların bu soruya verdikleri cevaplar aşağıdaki gibidir:

K1- *"Dijital dönüşüm, sürekli denetim yaklaşımının da gelişmesine neden olmuştur. Yaklaşık 30-35 yıllık bir geçmişi olan bu denetim yaklaşımı giderek daha fazla işletme tarafından uygulanmaya başlanmıştır. Dolayısıyla işletmelerin bu anlamda teknolojik alt yapılarını geliştirmeleri ve güçlendirmeleri, bununla birlikte iç denetçilerin bilgisayar tabanlı denetim yöntemlerini öğrenmeleri ve kendilerini bu alanda yetiştirmeleri yapılan denetimin kalite ve etkinliği artıracaktır."*

K2- *"Dijital dönüşüm ile birlikte yapılan iş tanımları da değişmektedir. Bu anlamda iç denetçilerden ve iç denetimden de beklentiler yaşanan dönüşüm ile birlikte yeniden şekillenmektedir. Günümüz iç denetçilerinin yaşanan dönüşümü kavrayabilecek ve proaktif bir şekilde olası gereksinimleri karşılayabilecek donanımda olması önemli bir husustur. Günümüz iç denetçileri teknolojik alanda yaşanan gelişmelerin yakından takip edilip söz konusu yeni teknolojilerin birer denetim aracı olarak kullanılmasını sağlamalı aynı zamanda yeni teknoloji kullanımının getireceği riskleri ise denetim alanı olarak ele almalıdır. Yeni teknolojilerin kullanımı ile tüm evrenin ve tam zamanlı güvence sağlanmasını mümkün kılan sürekli denetim, çevik denetim, denetim 4.0 gibi yeni denetim yaklaşımları iç denetçilerin odak noktası olmalıdır."*

K4- *"Bence bilgi sistemlerinin denetimini öğrenmek en azından temel kavramları öğrenmek çok önemli diye düşünüyorum. Dolayısıyla bilgi sistemleri bakış açısı elde etmek, süreç bilgisine daha derinden sahip olmak üst düzey bir süreç bilgisi değil de*

aslında sistem üzerinden yürüyen süreçlerin bilgisine sahip olmak, onların nasıl tespit edilebileceği konusunda bilgi sahibi olmak önemli diye düşünüyorum iç denetçilerin odak noktası bu yeni teknolojilere adaptasyonu olmalıdır. Kişinin hangi bölümden mezun olduğu mühim değil, programın nasıl yazıldığı değil o konuyu nasıl denetleyebileceğini bilmesi önemlidir. Dolayısıyla kullanılan tekniklerin farklı olması sebebiyle mühendislik kökenli birinin veya İİBF kökenli birinin katabileceği değerlerde farklıdır. Bu noktada denetçi cross functional (çapraz fonksiyonel) bir yeteneğe sahip olmalıdır."

K5- *"İç denetçilerin finansal okur yazarlıklarının yanında dijital okur yazarlıklarının olması için gerekli altyapının hızla oluşturulması önemlidir. Aksi takdirde itibar kaybına neden olabilir. Denetleyeceği iş süreçlerini bilmeyen denetçinin konular hakkında çözüm önermesi, tavsiyeler geliştirmesi ve katma değerli iş üretmesi beklenemez."*

K6- *"Bu kuruma ilk geldiğimde nasıl iç denetçilere ihtiyacımız olduğu konusunu ele aldım. Kurumum açısından baktığımda öncelikle vergi konusunda yetkinliğe sahip kişilerin alınması ikincisi de BT denetimini yapabilecek denetçilerin alınması yönünde üst yönetici ile fikirlerimi paylaştım. Şu an da CISA sertifikalı denetçi kamu kurumlarında olmadığı için alamıyoruz. CISA sertifikasına sahip olanlarda kendi kurumlarında çalışıyor. Biz bu eksiği gidermek adına hedefler koyduk kendimize. Kurumumuzda kamu iç denetim sertifikası alan bir elektronik mühendisi vardı, onun alımını gerçekleştirdik. Eğitimimizde birinci önceliğimiz bilgi güvenliği, BT denetimi bu tür denetimlere yöneliktir. Hatta bende bu kuruma atanmadan birkaç ay önce bu eğitimi aldım. Bu konunun önemli olacağını öngörerek kendi tercihim sonucu eğitim aldım. Bu yetkinliğe sahip denetçileri almanın yanında var olan denetçilerin yatkın olanları bu eğitimlere yönlendiriyoruz. Bu konu ben ve diğer arkadaşlar ile birlikte sürekli eğitim almak istiyoruz. Çünkü bu işin gözetimi yapmak için bu kavramlara hâkim olmamız lazım. Mühendislerin analitik yönde beceriye sahip olmalarına dayanarak sadece teknik denetim yaptırmıyoruz. Bu kişilere toplantı, müzakere ve iletişim gibi eğitimleri vermeye çalışıyoruz. Zaten seçerken sadece teknik konularda becerisi değil, iletişimin nasıl olması gerektiğine de dikkat edilmektedir. Burada sadece teknik zekanın yanında sosyal zekanın da güçlü olması gerekmektedir. İlk kez denetime başlayan arkadaşlara bir toplantı nasıl yönetilir, kişilerden bilginin nasıl alınması gerektiği, bilgi alma kısmında, karşındaki kişiyi nasıl rahat hissettirmen gerektiği, krize neden olmaması üzerine, raporlama,*

rapordaki üslup konusunda eğitimler veriyoruz. Dolayısıyla hem BT anlamında hem de denetim bakış açısına sahip olmaları önemli. Buradaki ekibimizde mühendis kökenli ve idari/gelir uzmanlığı kökenli iki arkadaşımız var. Gelir uzmanı arkadaşımızın bu konuya yatkınlığı var, çeşitli eğitimler almış. Her ikisinden de çok iyi verim alıyoruz. Hatta biz ekip kurarken teknik ve denetim yönünü karıştırarak kuruyoruz. Ne kadar çeşitli olursa o kadar iyidir."

K6- *"Siber güvenlik, veri analizi bu anlamda önemli. Algoritma ve veri kodlama yavaş yavaş iç denetçilerin de yapabileceği şeyler olmak durumunda. Örneğin bir kod yazması veya SQR gibi kod yazmak vb. Şöyle diyebilirim veri toplamak ve verileri analiz etmek ve aynı zamanda bu verilerin güvenliğini sağlayabilecek yetkinliklerin olması gerekiyor aslında. Bizler business process (iş süreçlerini) bilmesek aslında mali işlemleri veya bir finans sürecini tanımlayamıyorsak kod bilmeniz ya da algoritma bilmeniz ya da bu yetkinlikleri taşımanız tek başına yetmez. Aslında geleneksel yöntemleri bilip üzerine teknoloji tarafındaki eklemeleri yapmanız gerekir. Özellikle üniversiteler ile toplantılara katıldığımızda gelen sorulardan biri şu oluyor: özellikle mühendislik tarafından mı mezun olmamız gerekiyor. Hayır aslında böyle bir şey yok, finans grubundan insanlarında bu alanda kendisini geliştirmesi gerekiyor."*

K9- *"İç denetçiler daha multidisipliner bir karaktere sahip olmaları gerekir. Hem muhasebeye hem BT'ye hakim olması gerekir. Aynı zamanda çeşitli yazılımlara hakim, bunları kullanabilen bunlarla ilgili süreçleri yönetebilen denetçilere ihtiyaç olacak. Yine bence kurumsal firmalar sertifikalı iç denetçilerle çalışmayı tercih ediyorlar, bu durumun daha da artacağını düşünüyorum. Dijital dönüşüm ile birlikte bu teknoloji, IT ile ilgili sertifikalara sahip olmaları istenebilir denetçilerden. Muhasebe, iç denetim, iç kontrol birbirinden bağımsız şeyler. Her zaman şunu savunurum hiçbir zaman bir denetçi muhasebe bilmeden iyi bir denetçi olamaz. Muhasebeciden bir adım önde olmazsam ben onu denetleyemem. Dolayısıyla kendi düşüncem mühendisler denetçi olarak istihdam edilebiliyor fakat mühendis muhasebe, denetim dersleri almıyorlar. Ancak kendileri seçmeli ders alabiliyor. Bir kısmı yüksek lisans eğitim alıyor fakat maliye, işletme iktisat gibi bölümlerin dört yıl aldığı eğitim ile aynı olmayacağını düşünüyorum. Bence maliye, iktisat, işletme vs. bu alanlardaki arkadaşlara kendilerini daha geliştirmeleri, uygulama kısmına hakim olmaları, yabancı kaynakları tarayarak yurtdışında bunlar nasıl yapılıyor, uluslararası bağlamda nasıl yürütülüyor, IT yönünden geliştirilmesi daha iyi sonuçlar*

verecektir. Bu alanlardaki kişiler kendilerini yetiştirirlerse mühendislik alanındaki arkadaşlardan daha başarılı olacaklarını düşünüyorum. Mühendislik alanındaki arkadaşların analitik yönleri güçlü olması sebebiyle avantajlı olabiliyor ama muhasebe, denetim bunlar okyanus aslında. Bunları öğrenmek yıllar alıyor bunun için sadece analitik yönden güçlü olarak bunu başarmak zor aslında."

K10- *"En başta iletişim konusunu çözmelidir. Bunun altında da alışkanlıklar yatıyor. Yani iş yapış modelleri var, denetçiler belli bir yaş konumunda ve Z kuşağında şu an denetçi yok, onun için onlar buna alışkın değiller. Onlara bu donanımı yani bu alışkanlığı kazandırmamız lazım. Alışkanlık kazanılacak ki dönüşüm yaşanacak. BT'ye , internete, uzaktan denetime çok yabancı, iletişim kuramayan bir iç denetçi ise bu çağa ayak uydurması zor olacaktır. Çünkü iletişim çok önemli. Dolayısıyla bu nokta iletişim becerisinin sağlanması gerekir. Bir BT uzmanı gibi olmasa da BT'ye hakim olması gerekir. Bir veri çekmek nedir, istatistik yöntemler nelerdir. Big data dediğimizde ne anlıyoruz. Evren dediğimiz zaman ne anlıyoruz. Oradan nasıl örneklem alabilirim, nasıl bu dataları aktarabilirim, başka bir dile aktarabilirim. KIDDER adı altında COVID döneminde insanları motive etmek adına ders verdik. Bu katılımı sağlayanlara sertifika verdik ve bu sertifikaları tek tek yazmak zor olduğundan yazılım hazırladık. Bunlar ortaya bir ihtiyaç çıkıyor, o şekilde gelişiyor. Ama kişinin içinde bu yoksa yani doküman isteyen denetçilerde var. Bu durum sekteye uğratıyor süreci. Bu noktada yapacak bir şey var mı, çok da bir şey yok. Çünkü o alışkanlık, donanımı var, yetkin insanlar ama bu çağa ayak uyduramıyorlar. Belli bir süre böyle devam edecek bu geçiş döneminde. Kalkıp da herkesten bir an da bilgisayar kullanmasını, alışkın olmasını bekleyemeyiz. İlla Check list (kontrol listesi) yapmak istiyorlar çünkü normaldir öyle alışılmış. Burada bir oryantasyon dönemi lazım. Olabildiğince denetçiyi uyum sağlaması için oryantasyon yapılmalıdır. Onun dışında denetçinin bunu kendi de hissetmesi gerekecektir. Süreçlerin hepsinde şu yatıyor, ben kurum için ne yaparım diye düşünmesi lazım. Düşünüyorsa eğer bir yol buluyor. Modern dünya da o teknolojiyi kullanmayı bilmesi lazım. Örneğin; youtube çok kolay şekilde bilgiye ulaşılıp, öğrenilebilir. Artık her şey BT'e dayalı olduğu için ben bunları bilmiyorum yapamam diyemezsiniz. Denetimin bir felsefesi vardır. Ben mühendislerin denetçi olmasına karşı değilim, gerekte olduğunu düşünüyorum. Bazı yerlerde teknik mühendiste vardır. Denetim elemanı diye bir sınıf var orada yetişmek için bir usta-çırak ilişkisi gerekmektedir.*"

K13- " *İç denetçi aslında süreçlerle alakalı manuel dünyada neler yapabileceğini tahayyül edebiliyordu. Dijital dönüşüm ile birlikte yeni düzene entegrasyonun sağlanıp sağlanmadığı iç denetçi tarafından bakılmalıdır. Dijital ortamda nasıl hileler yapılabileceğine odaklanması lazım. Çünkü şimdiye kadar ki dünyasında hep manuel hileler yapılabilir, neler değiştirilebilir, neler aşılabilir konusuna odaklanıyordu. İç kontrol sistemlerinin doğru işleyip işlemediğini değerlendirmek sorumlu iç denetimin görevi, bu dijital ortama uyum sağlayacak kontrol noktaları yaratmaktır*."

Dokuzuncu soru olarak katılımcılara "Denetçinin sürecin doğru yönetilmesi adına hangi eğitimleri/sertifikaları alması gerekir? Bu dönüşüm çağının gerektirdiği yetkinlikte iç denetçilerin yetiştirilmesi adına neler yapılmalıdır?" sorusu yöneltilmiştir. Katılımcıların bu soruya verdikleri cevaplar aşağıdaki gibidir:

K1- *"Denetçinin yetkinliğinin artırılması için;*

- *Bilişim teknolojileri*
- *Bilgisayar tabanlı denetim yöntemleri*
- *Bilgi teknolojileri Genel ve Uygulama Kontrolleri eğitimleri verilmeli ve*
- *Denetimlerde çok daha fazla veri ile çalışılması gerekeceğinden verinin sınıflandırılması, analizi, değerlendirmesi gibi beceriler kazandırılmalıdır."*

Sertifikalar;

- *"Certified Information Systems Auditor (CISA) Sertifikası*
- *Information Technology Infrastructure Library (ITIL) Sertifikası"*

K2- *"Uluslararası İç Denetçiler Enstitüsü (IIA) tarafından verilen CIA ve CRMA, ISACA tarafından verilen CISA ve CGEIT gibi sertifikaların iç denetçi yetkinliğinin değerlendirilmesinde önemli olduğunu düşünüyorum. Ayrıca iç denetçilerin, denetim faaliyetini etkin, etkili ve verimli bir şekilde kıt kaynakların en iyi kullanabilmelerine olanak sağlayacak yeni teknolojilerin kullanımı konusunda da eğitimler alması önemli bir husustur. Söz konusu eğitimin ise sürekliliği ise esas olmalıdır."*

K3- *"İlk olarak mesleğin temel sertifikası olan CIA bütün iç denetçilerde olmalıdır. Bunun yanında işletmelerde yer alan mevcut ve riskleri tanımlamak ve bu risklere göre denetim faaliyetlerini gerçekleştirmek ve alınacak önlemleri tespit etmek için CRMA,*

güçlü bir muhasebe, finans, hukuk gibi konularda uzmanlaşmayı sağlayabilmek için SMMM sertifikalarına sahip olmaları önerilmektedir. İç denetçilerin yetiştirilmesi, sürekli gelişen ve değişen dünyada gerçekleştirilen faaliyetlerin daha etkin ve verimli olabilmesi adına eğitim ve gelişim faaliyetlerine ağırlık verilmelidir."

K6- *"Eğitimlerin alınması yönünden çalışmalar yapıyoruz. Uluslararası sertifikaların alınması yönünde de destekliyoruz. İç denetçiler gelişime açık. CISA ve kurum içinde eğitimler önemli. Eskiden eğitimler daha çok yapılıyordu. Hatta buna bir örnek bakanlıkta BT konusunda 13 saatlik bir eğitim verildi. Kendi çabalarımızla eğitimler almaya çalışıyoruz. Hizmet içi eğitimler düzenliyoruz. Bu eğitimde teknik konuda bilgili arkadaşlardan yararlanıyoruz. Her faaliyet için denetçi kendini hazırlaması lazım, araştırma yapması gerekir. Biz denetimimizin yüzde 40'ini ön hazırlığa harcıyoruz. Bundan dolayı iç denetçiler kendilerini sürekli geliştirmelidirler."*

K7- *"Ekiplerimden yola çıkarak söyleyeyim. CIA sertifikası zaten bizim için "must" olan sertifikalardan bir tanesi. Eğer teknolojik riskini yöneteceksek eğer TSE hep risk tabanlı. Ama veri analizi gibi çalışmalara gireceksek eğer burada spesifik bir sertifikasyon ile alakalı bir arayışımız yok ama bu bizim için bir artı olabilir. SQR tabanlı bir kod yazabilsin veri analizi yaparken herhangi bir veri analizi tool'u kullanabilsin. "Must" olarak düşündüğümde CIA; yine CISA öncelikli olmasa da "must"lardan bir tanesi. Yavaş yavaş kendi ekiplerimize robotik process automation (RPA) veri analizi çerçevesinde sertifikasyonları aldırıyoruz ama bu böyle "nice to have" gibi yani olursa daha iyi olur. Süreçlerimizi otomatize de ederken kullanabiliriz diye söyleyebilirim. Ekibimin hepsinde yok bu son saydığım sertifikalar. Ama bu sertifikaları almaları için destekliyoruz ekibimizi.*

Eğitim kurumları gelecek adına sahada işleri yürütecek şekilde süreçler tasarlanması lazım. Yani öğrenciler finans, satın alma, mali işler, üretim, bazı business(iş) operasyonlar için kulak dolgunluğu olarak ilerliyor olabilir ama özellikle iç denetim faaliyetleri için özellikle o süreçlerde ne gibi riskli alanlar olabilir, bunlarda ne gibi şeylerle karşılaşılıyordur. Buna ilişkin örneklerin gerçekten hayata ilişkin suistimal vb. konuların yaşanılan vakalar üzerinden gitmeleri fikir açığı olacaktır ve kendilerini geliştireceklerdir."

K12- *"ISACA tarafından sunulan CISA, CRISC, CDPSE, CET gibi sertifikasyonlar teknoloji alanındaki gerekliliklerin karşılanması açısından iç denetçiler açısından önemli. Yine IIA tarafından sunulan CIA içeriğini de çok beğeniyorum."*

Katılımcıların sekizinci ve dokuzuncu sorulara verdiği cevaplar incelendiğinde iç denetçilerin hem bilgi teknolojisi hem de denetim konusunda çapraz fonksiyona sahip olmaları gerektiği, denetim ekipleri kurulurken hem teknik hem de denetim bakış açısına sahip ekip kurulmasının yararlı olduğu vurgulanmaktadır. Ayrıca katılımcıların bir kısmının denetçinin mühendislik ve İİBF mezunu olmasının öneminin olmadığı diğerlerinin ise İİBF mezunlarının BT yönünden kendilerini geliştirmelerinin dijital dönüşüm çağında denetim mesleği için daha uygun olacağı yönünde düşünce hakimdir. Katılımcıların dijital dönüşüm çağında riskleri yönetmek adına özellikle IIA sertifikasyonu olan CIA ve ISACA'nın sertifikasyonu olan CISA sertifikalarını ön plana çıkardıklarını görülmektedir. Bunun yanında dönüşüm çağına ayak uydurulması adına eğitimde müfredat değişikliği veya güncellenmesine, gerçek hayattan vakaların incelenmesine vurgu yapılmıştır.

Onuncu soru olarak katılımcılara "Dijital dönüşüm ile birlikte gelen riskler karşısında iç denetim faaliyeti yürütülürken başlıca hangi düzenlemeler/kılavuzlar kullanılmalıdır? Bu kılavuzların içeriğini nasıl değerlendirirsiniz?" sorusu yöneltilmiştir. Katılımcıların bu soruya verdikleri cevaplar aşağıdaki gibidir:

K1- *"Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin Ekim 2021 yılında yayımladığı Bilgi ve İletişim Güvenliği Denetim Rehberi kullanılabilir. Rehber denetimlerin yapılabilmesi için yeterli içeriğe sahiptir.*"

K2-*" Kamu kurumları için Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından Bilgi ve İletişim Güvenliği Denetim Rehberi 2021 yılında yayınlanmıştır. Bu rehber birçok standardı gözeterek hazırlandığı için kamu iç denetçileri ve ayrıca kritik altyapı niteliğinde hizmet veren işletmeler için önemli ve kapsamlı referans kaynaklarının başında gelmektedir. Ayrıca COBIT, ISO 27000, NIST gibi bilgi ve iletişim güvenliği ile ilgili uluslararası standartlar ve çerçeveler de kullanılabilir.*"

K4- *"Aslında TİDE, IIA, ISACA gibi kurumların kılavuzları takip edilebilir. COSO Framework iç kontrol ve risk yönetiminde kullandığımız bir framework. ISO 31001 kurumsal risk yönetimi ile alakalı yararlandığımız bir standart. Böyle uluslararası*

standartların takip edilmesi, güncellemeleri takip edilmesi, içselleştirilmesinde yarar vardır."

K7- *"Aslında burada uluslararası standartların belli çerçeveleri zaten var. IIA, ISACA belli standartları var. Bilgi güvenliği açısından uluslararası bakıldığında ISO'nun standart ve çerçevelerde var. Dolayısıyla bu çerçevelerin takip edilmesi önemli ve bu çerçeveler devamlı olarak güncelleniyor ve güncel risklere ilişkin bilgiler de yükleniyor. Dolayısıyla bir risk kontrol matrisi oluyor. Bu her daim, her yapılan çalışmada her engagement'da (sözleşmede) güncellemeler devam ediyor. Bunlar önemli. Özellikle IIA'nin çıkardığı birçok standart ve çerçeve var. ISACA'nın var. Bunları takip ediyoruz."*

K9- *"IIA'ın mesleki uygulama çerçevesi baz alınabilir, zaten her zaman yenileniyor ve güncelleme sonucu da dijital dönüşüm dahil oluyor."*

K10- *"ISO 19001 kılavuzu var. DDO'nın yayınlamış olduğu rehberler var. İDKK'nın hazırlamış olduğu BT rehberimiz var. IIA'in bazı rehberleri vardı. Bunlar baz alınarak yürütülmesi lazım. Bu rehberlerinde birbiriyle çelişmemesi lazım. Çelişkilerin çözülmesi gerekir. Hangi eğitim hangi denetimi karşılar bunu biraz daha bariz hale getirilmesi gerekir. Bu noktada insan kaynağı ile ilgili bir kılavuz hazırlanabilir. DDO'un kılavuzu kapsamlı, her şeye değinmiş. Ama o rehberde birinci olarak iç denetçi kaynağı bunu yapabilir mi, ikincisi diğer mevzuatlarla bağlantısı. DDO'un kılavuzu çok değerli. Kurumlar henüz bu rehberi uygulayacak noktada değiller. Kurumların daha geliştirmesi gereken alanlar var. İç denetçilerin geliştirmesi gereken alanlar var, zihniyet değiştirilmeli. Kamu kurumlarındaki denetçiler verinin anlamlandırılması ve raporlanması konusunda kendilerini geliştirmelidirler."*

K11- *"Öncelikle hızlı değişen ve gelişen dijital süreçlere uyum sağlayabilen organizasyonların ya da kurumların takibi ve onların (sertifika, düzenleme, çerçeve, vb,) yaklaşımlarının benimsenmesi daha faydalı olacaktır. 6-7 yıldır güncellenmemiş bir çerçeve (framework) ya da 5-6 yıldır değişmemiş bir sertifika içeriği artık pek fazla bir katkı sağlamaz. Kendi doğrularına saplanmış organizasyonlar ya da katı kalıplara sahip dışa kapalı, yeniliklere direnen şirketlerin iç birimleri hep ayak bağı olacaktır. Yeni teknolojinin getirdiği hibrit iş modelleri, yeni iş anlayışları, yeni teknolojiler ve bunların insanlar, şirketler, çalışanlar, müşteriler, vb, üzerinde yarattığı beklentilerin*

karşılanması için "güncel ve geçerli" içeriklere ulaşmalıyız. Bu içerikler tek bir merkezde ya da tek bir kılavuzda karşılanamamaktadır maalesef. O yüzden, bir şirketin ya da bir iç denetim ekibinin, kendi iş modeline ve yeni yaklaşımlara göre farklı çerçeve ve düzenlemelere bakması, en doğru iş modelini oluşturmak için bir bakış açısı geliştirmesi gerekmektedir. Bu alanda, güncellenmiş ISO standartları bir çerçeve sunabildiği gibi ISACA gibi süreçlerini sürekli güncelleyen ve global olarak etkili olan organizasyonların içerikleri destekleyici olacaktır. Bu alanda en büyük risklerden biri de tepeden inme ve "ben yaptım, oldu" yaklaşımı ile ortaya çıkan düzenlemelerin/rehberlerin etkisi olabilir. İçerikleri güçlü ve etkili olsa bile uygulama aşamasında sahibi olmayan, ticari ya da sektör olarak desteği bulunmayan ve güncelleme konusunda tereddütleri olan düzenlemeler olumlu etkilerinin yanında yeni riskler ve uyumsuzluklar oluşturacaktır.

Yeni düzenleme ve kılavuzların ortak noktasının gelişmeye ve katkıya açık, güncel teknoloji, iş modelleri ve başka yapılar ile uyumlu olabilme şansını da beraberinde getirmesi olacaktır. Böylece denetçiler ya da şirketlerin iç denetim birimleri kendileri için en uygun modellemeyi, içeriği ya da süreç yönetimini yine kendileri belirleyebilecektir."

K12- *"COBIT çok önemli bir çerçeve. Ancak konu edinilen teknolojiye yönelik çerçevelerin araştırılması ve incelenmesi gerekiyor. ISACA, NIST, CSA gibi organizasyonların yeni teknolojilere ilişkin güzel içerikleri var. İç denetçiler bu kaynaklardan yararlanabilir."*

On birinci soru olarak katılımcılara "Türkiye'de dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeleri nasıl değerlendirirsiniz?" sorusu yöneltilmiştir. Katılımcıların bu soruya verdikleri cevaplar aşağıdaki gibidir:

K1- *"Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin Ekim 2021 yılında yayında yayımladığı Bilgi ve İletişim Güvenliği Denetim Rehberi bu doğrultuda atılmış önemli bir adımdır."*

K3- *"Belli başlı kurumlar haricinde maalesef Türkiye'de bu konulara ağırlık veren fazla kurum olduğunu düşünmüyorum."*

K4- *"Özellikle kamu olarak baktığımızda öncülere göre teknolojik dönüşüm anlamında biraz daha geriden geliyoruz. Farklı gündemleri tartışıyoruz. Örneğin Biz hala otomasyonu tartışıyoruz. Bizim peerlarımız (öncülerimiz) daha farklı konulara*

geçmiş oluyorlar. İnovatif bir kurum kültürü oluşturmak ise bizim ana hedefimiz biz hala otomasyon kısmındayız diyebilirim. Bazı Cumhurbaşkanlığı tarafından yayınlanan kılavuzlar var. Bilgi ve iletişim rehberi gibi. Türkiye'deki rehberler, uluslararası iyi uygulamaların çevirisi olabiliyor. Yine bu noktada uluslararası kaynakların takip edilmesinin önemli olduğunu düşünüyorum."

K6- *"Önceden farkındalık vardı ama düzenleme yoktu. Tüm kamuyu ilgilendiren böyle bir düzenleme olması (DDO'un sunduğu rehber) çok güzel oldu. Kurumları bilgi güvenliği sertifikaları almaya zorluyorlar. Cumhurbaşkanlığı DDO'nun rehberi tüm kamu kurumları zorunda bıraktığı için çok önemli oldu. Yine 5018 sayılı kanun iç kontrol sistemine atıf yapması sebebiyle önemlidir."*

K7- *"Açıkçası ben çoğu ülkeye göre bu anlamda ileride olduğumuzu düşünüyorum. Keza Cumhurbaşkanlığı DDO tarafından yapılan rehberler, düzenlemeler, sertifikasyonlar hayatımıza girdi ve bizde bu anlamda sertifikalarımızı alıyoruz. Geçtiğimiz 6 aylık bir süreçten bahsediyorum. Bu çerçeveler bizim için önemli ve kritik. Türkiye'ye özgü TSE tarafından çıkarılan sertifikasyonlar veya TSE tarafından çıkarılan ISO 27001 benzeri uyarlamalar için akredite kuruluşların düzenlemesi aslında önemli adımlar. Ben açıkçası Türkiye'yi birçok organizasyon açısında ve birçok ülkeye göre ilerde ve düzenlemeleri takip eden bir ülke olarak değerlendiriyor ve gözlemliyorum."*

K9- *" Aslında dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeleri yayınlayan çeşitli kuruluşlar var. Mesela Big Four zaman zaman yayınlıyor. Mesleki dernekler var. Hatta TUSİAD filan da yapabiliyor. Cumhurbaşkanlığı DDO var. O yüzden düzenlemeler yapılmıyor değil ama tabii bizim almamız gereken önemli yol olduğunu düşünüyorum. Gelişmeler olumlu aslında ama hala eksik çok."*

K10-*" DDO'un rehberi dokümantasyon olarak yeterli, bizde IDKK olarak BT rehberini hazırlarken Big Four'dan destek alarak hazırlamıştık. Kamuda Dokümantasyon olarak bir sorun yok sorun uygulamada, hayata geçirmede ve farkındalık oluşturma aşamasındadır. İnsanların bunları içselleştirmesi lazım. Bence düzenlemelerde sorun yok, düzenlemeler yeterlidir. Birbirileri arasındaki çelişkiler törpülenebilirse bence çok yeterli. Hatta belki dünyadaki birçok düzenlemeden iyidir. Bizim denetim rehberi, DDO rehberi, performans rehberi çok iyi. Özel sektörden iyidir kamunun dokümantasyonu. Rehberler yeterli, asıl önemli olan bu sürece insanları adapte*

edebilmektir. Birkaç denetim yapılsa aslında alışırlar. İç denetçi de denetim nosyonu vardır, ama geliştirmesi gereken yerler var."

K12- *"Türkiye teknolojiyi kullanma konusunda hevesli, ancak kısıtlı imkanlara sahip genç bir nüfusa sahibiz. Bu da dijital dönüşüm ve bu alana ilişkin kaynak konusunda bizi dezavantajlı hale getiriyor. Güçlü ve yaratıcı teknoloji firmalarımız var, ve bu çok gurur verici. Kamu tarafında teknoloji değişimi yakalayan bir mevzuat düzenleme değişimi imkanı olduğunu söyleyemem. Sonuçta bu düzenlemeleri yapacak olan insanlar."*

K13-*"Türkiye bu konulara çok hızlı adapte olan bir ülke ve bir yayın veya uygulama çıkıyor hızlıca aksiyon alıyor. Dolayısıyla ben bu konuda iyi gittiğimizi düşünüyorum."*

Katılımcılar onuncu ve on birinci sorularda başlıca IIA, TİDE, COBIT, DDO, ISO ve ISACA tarafından yayımlanan çerçeve ve rehberlerin takip edilmesi gerektiğine vurgu yapmışlardır. Ayrıca Türkiye'de belli kurumların bu alanda rehber, yönetmelik vb. düzenlemeler sunduğunu fakat bu düzenlemelere uyumda temel sorunun yeterli yetkinliğe sahip iç denetçinin var olmadığı vurgulanmaktadır. Diğer taraftan Türkiye'nin yasal düzenlemelere uyum konusunda hızlı şekilde harekete geçtiği belirtilmiştir.

3.9.2.Delphi II. turu

Delphi II. tur anketinde yer alan ifadeler Delphi I. tur aşamasında katılımcılarla yapılan yarı yapılandırılmış görüşme sonucu elde edilmiştir. Delphi I. turu on üç katılımcı ile gerçekleştirilirken Delphi II. turuna on bir katılımcı dönüt sağlamıştır. Birinci turda yer alan K7 ve K8 katılımcıları dönüt sağlamamıştır.

Delphi II. tur sonucu elde edilen bulgular aşağıda tablolar şeklinde sunulmuştur. Delphi tekniğinin asıl amacı uzman kişilerin ankette yer alan ifadeler üzerinde görüş birliğine ulaşmalarıdır.

"Soru 2- Dördüncü Sanayi Devrimi, Dördüncü Sanayi Devrimi teknolojileri, dijital dönüşüm, sizde ne çağrıştırıyor? Dijital dönüşümün kurumunuza yansımaları nelerdir?" sorusunda katılımcılardan alınan görüşler doğrultusunda anket formunda altı tane ifade elde edilmiştir. Katılımcılardan anket ifadelerine ilişkin geri bildirimleri sonucu "Dijital Dönüşüm-Endüstri 4.0" kategorisine yönelik Delphi II. tur anketine ilişkin bulgular

(ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar Tablo 3.3'te sunulmuştur.

Tablo 3. 3. *Dijital dönüşüm ve Endüstri 4.0 kategorisi Delphi II. tur bulguları*

Dijital Dönüşüm-Endüstri 4.0	Ortalama	Standart Sapma	Ortanca	ÇAF	Frekans (Yüzde)			Görüş Birliği
					1	2	3	
1. Endüstri 4.0; dijitalleşme, akıllı ev aletleri, denetimin dijitalleşmesi, robotların artık kullanılmaya başlanması, RPA teknolojileri, mükerrer işlemlerin azalması, insana duyulan ihtiyacın azalması şeklinde tanımlanabilir.	1,18	0,60	1	0	10 (90,9)	0 (0)	1 (9,1)	Var
2. Dördüncü sanayi devrimi birçok alanda dijitalleşmeyi ve dijital dönüşümü merkez alan yeni bir yapılanmadır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
3. Dijital dönüşüm, dördüncü sanayi devrimi teknolojilerinin üretim ve hizmet alanlarında kullanma sürecidir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
4. Dijital dönüşüm kurumların iş yapış şekillerinden, çözüm üretme stratejilerine kadar kurumları etkileyen önemli bir konudur.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
5. Dijital dönüşüm kurumların stratejik planlarından başlayıp tüm iş süreçlerini ele alınması gereken önemli bir konudur.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
6. İç denetim, iç kontrol süreçlerinin gerçek zamanlı izlenebilmesi dijital dönüşümün, dördüncü sanayi devriminin bir yansımasıdır.	1,27	0,65	1	0	9 (81,8)	1 (9,1)	1 (9,1)	Var

Tablo 3.3'te görüldüğü üzere ifadelerin ortalama değerleri 1 – 1,27; standart sapma değerleri 0 – 0,65; 1 frekans değerleri 9 (81,8) - 11(100), 2 frekans değeri 0 (0) - 1 (9,1), 3 frekans değerleri 0 (0) – 1 (9,1) arasında değiştiğine, ortanca değerlerinin 1'e ; çeyrekler arası farkın 0'a eşit olduğuna ulaşılmıştır.

Çalışmanın bulgularına göre "Dijital Dönüşüm-Endüstri 4.0" kategorisindeki tüm ifadeler konusunda katılımcıların görüş birliğine ulaştığı görülmektedir. "1.Endüstri 4.0; dijitalleşme, akıllı ev aletleri, denetimin dijitalleşmesi, robotların artık kullanılmaya

başlanması, RPA teknolojileri, mükerrer işlemlerin azalması, insana duyulan ihtiyacın azalması şeklinde tanımlanabilir.", "2.Dördüncü sanayi devrimi birçok alanda dijitalleşmeyi ve dijital dönüşümü merkez alan yeni bir yapılanmadır.", "3.Dijital dönüşüm, dördüncü sanayi devrimi teknolojilerinin üretim ve hizmet alanlarında kullanma sürecidir.", "4.Dijital dönüşüm kurumların iş yapış şekillerinden, çözüm üretme stratejilerine kadar kurumları etkileyen önemli bir konudur.", "5.Dijital dönüşüm kurumların stratejik planlarından başlayıp tüm iş süreçlerini ele alınması gereken önemli bir konudur.", "6.İç denetim, iç kontrol süreçlerinin gerçek zamanlı izlenebilmesi dijital dönüşümün, dördüncü sanayi devriminin bir yansımasıdır." ifadeleri üzerinde katılımcılar görüş birliği sağlamıştır.

"Soru 3- Kurumlar göz önüne alındığında yaşanan dijital dönüşümün getireceği başlıca riskler olarak neleri görüyorsunuz?" sorusundan katılımcılardan elde edilen görüşler doğrultusunda "Dijital Dönüşümden Kaynaklı Riskler" kategorisinde sekiz ifade oluşturulmuştur. Katılımcılardan gelen verilerin analizi sonucunda elde edilen "Dijital Dönüşümden Kaynaklı Riskler" kategorisine yönelik Delphi II. tur anketine ilişkin bulgular (ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar Tablo 3. 4'te sunulmuştur.

Tablo 3. 4. *Dijital dönüşümden kaynaklı riskler kategorisi Delphi II. tur bulguları*

Dijital Dönüşümden Kaynaklı Riskler	Ortalama	Standart Sapma	Ortanca	ÇAF	Frekans (Yüzde)			Görüş Birliği
					1	2	3	
1. Dijital dönüşüme uyum sağlama, kurumların değişim kültürüne sahip olmaması, geç kalınması veya yavaş ilerlemek riskler arasındadır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
2. Dijital dönüşüme kısa sürede uyum sağlama ihtiyacının doğurabileceği yanlış kararlar ve bunlardan kaynaklı katlanılan yüksek maliyetler önemli risklerden biridir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var

Tablo 3. 4.(Devamı) *Dijital dönüşümden kaynaklı riskler kategorisi Delphi II. tur bulgular*

3. Kurumun dijital dönüşüm süreci için yeterli düzeyde araştırma-geliştirme ve testlerin yapılmamasından kaynaklı kayıplar (zaman, iş gücü, bütçe, karlılık vb.) önemli risklerden biridir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
4. Dijital dönüşüm ile birlikte yaşanacak en önemli riskler kişisel verilerin korunması, bilgi güvenliği ve siber güvenlik riskleridir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
5. Dijital dönüşüm sürecine entegre olamayan veya kendini yenileyemeyen kişiler ve toplumlar için bazı iş kollarının yok olması ve işsizlik önemli bir sorundur.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
6. Dijital dönüşümden kaynaklı en büyük risk veri kapsamında olup sadece veri kaybı olarak değil verinin bütüncül ve anlamlı şekilde tutulamaması da büyük bir risktir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
7. Kurumların dijital dönüşüm sürecinde değişime direnç göstermesi ve yetkin iş gücüne/dijital iş gücüne sahip olmaması başlıca sıkıntılar/riskler arasındadır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
8. Kurumlar tarafından kullanılan otomatik sistemlerin en büyük riskleri algoritmanın doğru çalışıp çalışmadığı, algoritmanın kurumun istediği sonucu verip vermediği ve algoritmayı yetkisiz değiştirecek üçüncü bir kişinin var olup olmadığıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var

Tablo 3.4 incelendiğinde ortalama değerleri 1; standart sapma değerleri 0; ortanca değerleri 1; çeyrekler arası fark 0; 1 frekans değerleri 11(100), 2 frekans değeri 0 (0), 3 frekans değerleri 0 (0) olduğuna ulaşılmıştır.

Görüş birliği kıstaslarına göre "Dijital Dönüşümden Kaynaklı Riskler" kategorisinde yer alan sekiz ifadeye yönelik katılımcıların görüş birliği sağladığına ulaşılmıştır. "1.Dijital dönüşüme uyum sağlama, kurumların değişim kültürüne sahip olmaması, geç kalınması veya yavaş ilerlemek riskler arasındadır.", "2.Dijital dönüşüme kısa sürede uyum sağlama ihtiyacının doğurabileceği yanlış kararlar ve bunlardan

kaynaklı katlanılan yüksek maliyetler önemli risklerden biridir.", "3.Kurumun dijital dönüşüm süreci için yeterli düzeyde araştırma-geliştirme ve testlerin yapılmamasından kaynaklı kayıplar (zaman, iş gücü, bütçe, karlılık vb.) önemli risklerden biridir.", "4.Dijital dönüşüm ile birlikte yaşanacak en önemli riskler kişisel verilerin korunması, bilgi güvenliği ve siber güvenlik riskleridir.", "5.Dijital dönüşüm sürecine entegre olamayan veya kendini yenileyemeyen kişiler ve toplumlar için bazı iş kollarının yok olması ve işsizlik önemli bir sorundur.", "6.Dijital dönüşümden kaynaklı en büyük risk veri kapsamında olup sadece veri kaybı olarak değil verinin bütüncül ve anlamlı şekilde tutulamaması da büyük bir risktir.", "7.Kurumların dijital dönüşüm sürecinde değişime direnç göstermesi ve yetkin iş gücüne/dijital iş gücüne sahip olmaması başlıca sıkıntılar/riskler arasındadır.", "8.Kurumlar tarafından kullanılan otomatik sistemlerin en büyük riskleri algoritmanın doğru çalışıp çalışmadığı, algoritmanın kurumun istediği sonucu verip vermediği ve algoritmayı yetkisiz değiştirecek üçüncü bir kişinin var olup olmadığıdır." ifadeleri üzerinde görüş birliği sağlanmıştır.

"Soru 4- Dijital dönüşüm ile beraber karşılaşılan riskler karşısında iç denetim fonksiyonunun rolü nedir?" ve Soru 5- Dijital dönüşüm çerçevesinde iç denetimin güvence sağlama ve danışmanlık rolünü nasıl değerlendirirsiniz?" görüşme sorularına ilişkin katılımcıların verdiği cevaplar doğrultusunda "İç Denetimin Rolü" kategorisi altında 10 ifade oluşturulmuştur. Katılımcılardan gelen verilerin analizi sonucunda elde edilen "İç Denetimin Rolü" kategorisine yönelik Delphi II. tur anketine ilişkin bulgular (ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar Tablo 3.5'te sunulmuştur.

Tablo 3. 5. *İç denetimin rolü kategorisi Delphi II. tur bulguları*

İç Denetimin Rolü	Ortalama	Standart Sapma	Ortanca	ÇAF	Frekans (Yüzde)			Görüş Birliği
					1	2	3	
1. Dijital dönüşümden kaynaklı risklerin tanımlanması ve farkındalık oluşturulması aşamasında iç denetim danışmanlık rolü ile katkı sağlayacaktır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var

Tablo 3. 5.(Devamı) *İç denetimin rolü kategorisi Delphi II. tur bulguları*

2. Dijital dönüşüm çerçevesinde iç denetimin temel faaliyeti olan güvence ve danışmanlık görevi daha önemli bir seviyeye gelecektir.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
3. Dijital dönüşüm sürecinde iç denetim fonksiyonu ilk etapta danışmanlık rolü ile kurumlara katkı sağlayacaktır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
4. Dijital dönüşüm çerçevesinde iç denetimin mutlak güvence sağlayamama konusu devam etmekle birlikte giderek artabilir. Diğer taraftan dijital dönüşüm ile birlikte danışmanlık rolü daha kritik hale gelecektir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
5. İç denetim fonksiyonu dijital dönüşümden kaynaklı riskler karşısında bilgi teknolojileri denetimine ağırlık vermelidir.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
6. İç denetim fonksiyonu kurumun insan kaynağının dijital dönüşüm için yeterliliğini araştırmalıdır, ekip kurma aşamasında yer almalıdır.	1,36	0,67	1	1	8 (72,7)	2 (18,2)	1 (9,1)	Yok
7. İç denetim fonksiyonu dijital dönüşümün getirdiği teknolojiler, bu teknolojilere uyum sağlanması, gerektiğinde yeniden yapılanma ihtiyacı, buna ilişkin planlama vb. konularda çalışmalar yürütmek ve gerekli bilgilendirmeleri yapmalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
8. İç denetçiler dijital dönüşüm sürecine yönelik danışmanlık hizmeti aşamasında kurumlara özgü planlar oluşturmalıdırlar.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
9. Yeni teknolojilerin riskleri, yasa ya da standart anlamındaki uyum süreçlerinin etkisi, yeni nesil ürün ve sistemlerin kullanımı gibi alanlarda iç denetim süreçlerinin yeniden yapılanması gereklidir.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
10. Kurumların dijital dönüşüm sürecinde iç denetim, danışmanlık rolü çerçevesinde entegre sistemlerin kurulumu, bu sistemlerden alınacak verilerin izlenmesi ve bu sistemlerin güvenliği rolünü üstlenmektedir.	1,18	0,40	1	0	9 (81,8)	2 (18,2)	0 (0)	Var

Tablo 3.5'te görüldüğü üzere ifadelerin ortalama değerleri 1 - 1,36; standart sapma değerleri 0 - 0,67; çeyrekler arası fark 0 - 1; 1 frekans değerleri 8 (72,2) - 11(100), 2 frekans değeri 0 (0) - 2 (18,2), 3 frekans değerleri 0 (0) - 1 (9,1) arasında değiştiğine, ortanca değerlerinin 1'e eşit olduğuna ulaşılmıştır.

Çalışmanın bulgularına göre "İç Denetimin Rolü" kategorisine ilişkin katılımcıların verdikleri yanıtlar doğrultusunda " 6.İç denetim fonksiyonu kurumun insan kaynağının dijital dönüşüm için yeterliliğini araştırmalıdır, ekip kurma aşamasında yer almalıdır.", ifadesinde katılımcılar görüş birliği sağlanamamışken, "1.Dijital dönüşümden kaynaklı risklerin tanımlanması ve farkındalık oluşturulması aşamasında iç denetim danışmanlık rolü ile katkı sağlayacaktır.", "2.Dijital dönüşüm çerçevesinde iç denetimin temel faaliyeti olan güvence ve danışmanlık görevi daha önemli bir seviyeye gelecektir.", "3.Dijital dönüşüm sürecinde iç denetim fonksiyonu ilk etapta danışmanlık rolü ile kurumlara katkı sağlayacaktır.", "4. Dijital dönüşüm çerçevesinde iç denetimin mutlak güvence sağlayamama konusu devam etmekle birlikte giderek artabilir. Diğer taraftan dijital dönüşüm ile birlikte danışmanlık rolü daha kritik hale gelecektir.", "5.İç denetim fonksiyonu dijital dönüşümden kaynaklı riskler karşısında bilgi teknolojileri denetimine ağırlık vermelidir.", "7. İç denetim fonksiyonu dijital dönüşümün getirdiği teknolojiler, bu teknolojilere uyum sağlanması, gerektiğinde yeniden yapılanma ihtiyacı, buna ilişkin planlama vb. konularda çalışmalar yürütmek ve gerekli bilgilendirmeleri yapmalıdır.", "8.İç denetçiler dijital dönüşüm sürecine yönelik danışmanlık hizmeti aşamasında kurumlara özgü planlar oluşturmalıdırlar.", "9.Yeni teknolojilerin riskleri, yasa ya da standart anlamındaki uyum süreçlerinin etkisi, yeni nesil ürün ve sistemlerin kullanımı gibi alanlarda iç denetim süreçlerinin yeniden yapılanması gereklidir.", "10.Kurumların dijital dönüşüm sürecinde iç denetim, danışmanlık rolü çerçevesinde entegre sistemlerin kurulumu, bu sistemlerden alınacak verilerin izlenmesi ve bu sistemlerin güvenliği rolünü üstlenmektedir." ifadeleri üzerinde katılımcılar uzlaşma sağlamıştır.

Soru 6- Üçlü hat modelinin, üçüncü hat rolünde yer alan iç denetimi dijital riskler çerçevesinde nasıl değerlendirirsiniz? sorusu kapsamında katılımcılardan elde edilen görüşler doğrultusunda "Üçlü Hat Modeli" kategorisinde yedi ifade oluşturulmuştur. Katılımcılardan gelen verilerin analizi sonucunda elde edilen "Üçlü Hat Modeli" kategorisine yönelik Delphi II. tur anketine ilişkin bulgular (ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar Tablo 3.6'da sunulmuştur.

Tablo 3. 6. *Üçlü hat modeli kategorisi Delphi II. tur bulguları*

Üçlü Hat Modeli	Ortalama	Standart Sapma	Ortanca	ÇAF	Frekans (Yüzde)			Görüş Birliği
					1	2	3	
1. İç denetim, dijital dönüşüm sürecinin yönetişim, risk yönetimi ve iç kontrol sisteminde yaratacağı değişime ilişkin tavsiyelerde bulunmak, bu konularda kuruma ve yönetime danışmanlık yapmak ve destek sunmak gibi önemli rollere sahiptir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
2. İç denetim yeni sistemin yeterliği ve etkililiğinin değerlendirmesi kapsamında role sahiptir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
3. Üçlü hat modelinde iç denetimin önemi daha ön plana çıkarmakla birlikte dijitalleşmeden kaynaklı riskler karşısında iç denetim faaliyetini daha da gerekli kılmaktadır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
4. İç denetim artık riskleri daha proaktif yönettiği bir döneme giriyor.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
5. Dijital dönüşüm sürecinde iç denetimin geride kalması katma değeri azaltmaktadır.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
6. Dijitalleşme öncesi ile kıyaslandığında dijital dönüşüm sürecindeki risklerin değerlendirilme aşamasında üçüncü hat rolünde iç denetimin sorumluluklarında bir değişim yoktur.	1,54	0,52	2	1	5 (45,5)	6 (54,5)	0 (0)	Yok
7. Dijital dönüşüm süreciyle iç denetim fonksiyonu GRC (Governance, Risk, Compliance -Yönetişim, Risk, Uyum), veri analitiği kullanan yapılar haline gelmelidir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var

Tablo 3.6'dan da görüldüğü üzere ifadelerin ortalama değerleri 1 - 1,54; standart sapma değerleri 0 - 0,52; ortanca değerleri 1-2; çeyrekler arası fark 0 - 1; 1 frekans

değerleri 5 (45,5) - 11(100), 2 frekans değeri 0 (0) - 2 (54,5), 3 frekans değerleri 0 (0) - 0 (0) arasında değiştiğine ulaşılmıştır.

Çalışmada belirlenen görüş birliği ölçütlerine göre "Üçlü Hat Modeli" kategorisine yönelik ikinci turda üçlü hat modelinin dijital riskler çerçevesinde değerlendirilmesine yönelik "6.Dijitalleşme öncesi ile kıyaslandığında dijital dönüşüm sürecindeki risklerin değerlendirilme aşamasında üçüncü hat rolünde iç denetimin sorumluluklarında bir değişim yoktur." ifadesinde görüş birliği sağlanamazken, "1.İç denetim, dijital dönüşüm sürecinin yönetişim, risk yönetimi ve iç kontrol sisteminde yaratacağı değişime ilişkin tavsiyelerde bulunmak, bu konularda kuruma ve yönetime danışmanlık yapmak ve destek sunmak gibi önemli rollere sahiptir.", "2.İç denetim yeni sistemin yeterliği ve etkililiğinin değerlendirmesi kapsamında role sahiptir.", "3.Üçlü hat modelinde iç denetimin önemi daha ön plana çıkarmakla birlikte dijitalleşmeden kaynaklı riskler karşısında iç denetim faaliyetini daha da gerekli kılmaktadır.", "4.İç denetim artık riskleri daha proaktif yönettiği bir döneme giriyor.", "5.Dijital dönüşüm sürecinde iç denetimin geride kalması katma değeri azaltmaktadır.", "7.Dijital dönüşüm süreciyle iç denetim fonksiyonu GRC (Governance, Risk, Compliance -Yönetişim, Risk, Uyum), veri analitiği kullanan yapılar haline gelmelidir." ifadelerinde ise görüş birliği sağlanmıştır. Dolayısıyla "Üçlü Hat Modeli" kategorisine yönelik ikinci turda yedi maddenin birinde görüş birliği sağlanamamışken, altısında ise görüş birliği sağlanmıştır.

"Soru 7- Kurumları dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde nasıl değişiklikler yapmalıdır? Bu noktada iç denetimin rolü nedir?" sorusuna katılımcıların verdiği cevaplar doğrultusunda "İç Kontrol Sistemi" kategorisi oluşturulmuştur. "İç Kontrol Sistemi" kategorisine yönelik on beş ifade yer almakta olup ikinci turda oluşturulan ifadeler ve bu ifadelere ilişkin bulgular (ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar Tablo 3.7'de sunulmuştur.

Tablo 3. 7. *İç kontrol sistemi kategorisi Delphi II. tur bulguları*

İç Kontrol Sistemi	Ortalama	Standart Sapma	Ortanca	ÇAF	Frekans (Yüzde)			Görüş Birliği
					1	2	3	
1. Dijitalleşme kurumlarda bir strateji ile başlamalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
2. Kurumlardaki dijital dönüşüm sonucu iç kontrol sistemin sorumluluğundaki birtakım kontroller yazılım sistemine aktarılır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
3. Dijitalleşme sonucu denetimlerin otomatik şekilde yapılmasından kaynaklı iç denetimin otomatikleşen sistemlere yönelik denetimi önem kazanmaktadır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
4. İç kontrol sisteminin risk ortamı ve kontrol faaliyetleri bileşenlerinin dijital riskleri kapsaması konusunda revize edilmesi gerekir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
5. İç kontrol sisteminin beşinci bileşeni olarak izleme çerçevesinde iç denetim iç kontrol sisteminin dijital dönüşümden kaynaklı riskler karşısında etkinliğini değerlendirme aşamasında güvence rolü ile katkı sağlamaktadır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
6. Dijital dönüşüm ile birlikte kurumların bilgi teknolojileri departmanının risk ve açıklarının kontrolü için bağımsız kuruluşlarca düzenli olarak testleri yapılmalıdır.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
7. Dijital dönüşüm çağında iç kontrol sistemi olaylar gerçekleşmeden önce önlem almalı ve mevcut trendler ile sürekli bir uyum içinde kalmalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
8. Dijital dönüşüm ile entegre sistemler (Enterprise Resource Planning (ERP)-Kurumsal Kaynak Planlaması gibi) kullanılabilir.	1,18	0,60	1	0	10 (90,9)	0 (0)	1 (9,1)	Var

Tablo 3. 7.(Devamı) *İç kontrol sistemi kategorisi Delphi II. tur bulguları*

9. Dijital dönüşümden kaynaklı riskler karşında risk yönetimi çerçevesinde kurumsal yönetim ilkelerine uygun olarak gerekli kontrol noktalarının oluşturulması sağlanmalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
10. Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde değişim karşısında iç denetim stratejik rol üstlenmeli ve danışmanlık rolünü ön plana çıkarmalıdır.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
11. Dijitalleşme kurumlarda iç kontrol sisteminin bakış açısını artıracaktır.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
12. Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sistemindeki değişiklikler kurumun olgunluk seviyesine bağlıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
13. Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde kurumlar değişiklik yapmaya karar verdi ise yazılım alınacaksa alternatiflerin araştırılması, sisteme geçiş sürecinde eğitimlerin verilmesi konularında iç denetim danışmanlık rolünü üstlenebilir.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
14. Kurumlar dijitalleşme için adım atmış ve kurum kültürü oluşturmuş ise iç kontrol yapılarını da bu çerçevede güncellemek zorundadır.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
15. İç kontrol sistemlerine sürekli izleme yaklaşımları adapte edilmelidir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var

Tablo 3.7'den görüldüğü üzere ifadelerin ortalama değerleri 1 - 1,18; standart sapma değerleri 0 - 0,60; 1 frekans değerleri 10 (90,9) - 11(100), 2 frekans değeri 0 (0) - 1 (9,1), 3 frekans değerleri 0 (0) - 1 (9,1) arasında değişirken, ortanca değerleri 1'e; çeyrekler arası fark 0'a eşittir.

Çalışmada belirlenen görüş birliği ölçütlerine göre "İç Kontrol Sistemi" kategorisine yönelik ikinci turda "1.Dijitalleşme kurumlarda bir strateji ile başlamalıdır.", "2.Kurumlardaki dijital dönüşüm sonucu iç kontrol sistemin sorumluluğundaki birtakım

kontroller yazılım sistemine aktarılır.", "3.Dijitalleşme sonucu denetimlerin otomatik şekilde yapılmasından kaynaklı iç denetimin otomatikleşen sistemlere yönelik denetimi önem kazanmaktadır.", "4.İç kontrol sisteminin risk ortamı ve kontrol faaliyetleri bileşenlerinin dijital riskleri kapsaması konusunda revize edilmesi gerekir.", "5.İç kontrol sisteminin beşinci bileşeni olarak izleme çerçevesinde iç denetim iç kontrol sisteminin dijital dönüşümden kaynaklı riskler karşısında etkinliğini değerlendirme aşamasında güvence rolü ile katkı sağlamaktadır.", "6.Dijital dönüşüm ile birlikte kurumların bilgi teknolojileri departmanının risk ve açıklarının kontrolü için bağımsız kuruluşlarca düzenli olarak testleri yapılmalıdır.", "7.Dijital dönüşüm çağında iç kontrol sistemi olaylar gerçekleşmeden önce önlem almalı ve mevcut trendler ile sürekli bir uyum içinde kalmalıdır.", "8.Dijital dönüşüm ile entegre sistemler (Enterprise Resource Planning (ERP)-Kurumsal Kaynak Planlaması gibi) kullanılabilir.", "9.Dijital dönüşümden kaynaklı riskler karşında risk yönetimi çerçevesinde kurumsal yönetim ilkelerine uygun olarak gerekli kontrol noktalarının oluşturulması sağlanmalıdır.", "10.Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde değişim karşısında iç denetim stratejik rol üstlenmeli ve danışmanlık rolünü ön plana çıkarmalıdır.", "11.Dijitalleşme kurumlarda iç kontrol sisteminin bakış açısını artıracaktır.", "12.Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sistemindeki değişiklikler kurumun olgunluk seviyesine bağlıdır.", "13.Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde kurumlar değişiklik yapmaya karar verdi ise yazılım alınacaksa alternatiflerin araştırılması, sisteme geçiş sürecinde eğitimlerin verilmesi konularında iç denetim danışmanlık rolünü üstlenebilir.", "14.Kurumlar dijitalleşme için adım atmış ve kurum kültürü oluşturmuş ise iç kontrol yapılarını da bu çerçevede güncellemek zorundadır.", "15. İç kontrol sistemlerine sürekli izleme yaklaşımları adapte edilmelidir." ifadelerinin tamamında görüş birliği sağlanmıştır.

"Soru 8- Sizce dijital dönüşüm süreci ile birlikte iç denetçilerin taşıması gereken yeni özellikler nelerdir? Bu süreçte iç denetçilerin odak noktası ne olmalıdır?" ve "Soru 9-Denetçinin sürecin doğru yönetilmesi adına hangi eğitimleri/sertifikaları alması gerekir? Bu dönüşüm çağının gerektirdiği yetkinlikte iç denetçilerin yetiştirilmesi adına neler yapılmalıdır?" sorularına katılımcıların verdiği cevaplar doğrultusunda "İç Denetçi" kategorisi oluşturulmuştur. "İç Denetçi" kategorisine yönelik on iki ifade yer almakta

olup ikinci turda oluşturulan ifadeler ve bu ifadelere ilişkin bulgular (ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar Tablo 3.8'de sunulmuştur.

Tablo 3. 8. *İç denetçi kategorisi Delphi II. tur bulguları*

İç Denetçi	Ortalama	Standart Sapma	Ortanca	ÇAF	Frekans (Yüzde)			Görüş Birliği
					1	2	3	
1. İç denetçilerin bilgisayar tabanlı denetim yöntemlerini öğrenmeleri ve kendilerini bu alanda yetiştirmeleri yapılan denetimin kalite ve etkinliğini artıracaktır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
2. İç denetçi iletişim becerisine sahip olmalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
3. Denetçinin dijital dönüşüm sürecini ve riskleri doğru yönetmek adına CIA, CISA, ITIL, CGEIT, CRMA, PMP(Proje Yönetim Sertifikası) sertifikalarının biri ya da birkaçına sahip olmalıdır.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
4. İç denetçiler teknolojik alanda yaşanan gelişmeleri yakından takip etmeli ve söz konusu yeni teknolojilerin birer denetim aracı olarak kullanılmasını sağlamalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
5. İç denetçiler yeni teknoloji kullanımının getireceği riskleri denetim alanı olarak ele almalıdır.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
6. Sürekli denetim, çevik denetim, denetim 4.0 gibi yeni denetim yaklaşımları iç denetçilerin odak noktası olmalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
7. İç denetçilerin bilgi teknolojileri ve buna bağlı riskler konusunda farkındalıklarını arttırmaları gerekmektedir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
8. İç denetçilerin finansal okur yazarlıklarının yanında dijital okur yazarlık yeteneğine sahip olmalı ve gerekli altyapı hızla oluşturulmalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var

Tablo 3. 8.(Devamı) *İç denetçi kategorisi Delphi II. tur bulguları*

9. İç denetçiler kurumsal iletişim, kurumsal risk yönetimi, bilgi teknolojileri denetimi, siber güvenlik, uzaktan denetim teknikleri, veri analizi ve modelleme teknikleri, iş zekası programlama vb. genel eğitimler almalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
10. İç denetçiler dijital çağ ile birlikte multidisipliner (hem bilgi teknolojisi hem denetim, muhasebe) özelliklerine sahip olmalıdırlar.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
11. Dijital dönüşüm sürecinde iç denetim faaliyeti yürütülürken farklı yetkinlikte kişilerin bir arada birleşip denetim yapması gerekmektedir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
12. Kamu kurumundaki iç denetçiler dijital dönüşüm çerçevesinde kurumlarına danışmanlık hizmeti verecek seviye de değildir.	1,54	0,82	1	1	7 (63,6)	2 (18,2)	2 (18,2)	Yok

Tablo 3.8'den de görüldüğü üzere ifadelerin ortalama değerleri 1 - 1,54; standart sapma değerleri 0 - 0,82; çeyrekler arası fark 0 - 1; 1 frekans değerleri 7 (63,6) - 11(100), 2 frekans değeri 0 (0) - 2 (18,2), 3 frekans değerleri 0 (0) - 2 (18,2) arasında değişirken, ortanca değerlerin 1'e eşit olduğuna ulaşılmıştır.

Çalışmada belirlenen görüş birliği ölçütlerine göre "İç Denetçi" kategorisine yönelik ikinci turda "12.Kamu kurumundaki iç denetçiler dijital dönüşüm çerçevesinde kurumlarına danışmanlık hizmeti verecek seviye de değildir." ifadesinde katılımcılar görüş birliği sağlanamamışken, "1.İç denetçilerin bilgisayar tabanlı denetim yöntemlerini öğrenmeleri ve kendilerini bu alanda yetiştirmeleri yapılan denetimin kalite ve etkinliğini artıracaktır.", "2.İç denetçi iletişim becerisine sahip olmalıdır.", "3.Denetçinin dijital dönüşüm sürecini ve riskleri doğru yönetmek adına CIA, CISA, ITIL, CGEIT, CRMA, PMP(Proje Yönetim Sertifikası) sertifikalarının biri ya da birkaçına sahip olmalıdır.", "4.İç denetçiler teknolojik alanda yaşanan gelişmeleri yakından takip etmeli ve söz konusu yeni teknolojilerin birer denetim aracı olarak kullanılmasını sağlamalıdır.", "5.İç denetçiler yeni teknoloji kullanımının getireceği riskleri denetim alanı olarak ele almalıdır.", "6.Sürekli denetim, çevik denetim, denetim 4.0 gibi yeni denetim yaklaşımları iç denetçilerin odak noktası olmalıdır.", "7.İç denetçilerin bilgi teknolojileri

ve buna bağlı riskler konusunda farkındalıklarını arttırmaları gerekmektedir.", "8.İç denetçilerin finansal okur yazarlıklarının yanında dijital okur yazarlık yeteneğine sahip olmalı ve gerekli altyapı hızla oluşturulmalıdır.", "9.İç denetçiler kurumsal iletişim, kurumsal risk yönetimi, bilgi teknolojileri denetimi, siber güvenlik, uzaktan denetim teknikleri, veri analizi ve modelleme teknikleri, iş zekası programlama vb. genel eğitimler almalıdır.", "10.İç denetçiler dijital çağ ile birlikte multidisipliner (hem bilgi teknolojisi hem denetim, muhasebe) özelliklerine sahip olmalıdırlar.", "11.Dijital dönüşüm sürecinde iç denetim faaliyeti yürütülürken farklı yetkinlikte kişilerin bir arada birleşip denetim yapması gerekmektedir." ifadelerinde görüş birliği sağlanmıştır.

Son olarak "Soru 10- Dijital dönüşüm ile birlikte gelen riskler karşısında iç denetim faaliyeti yürütülürken başlıca hangi düzenlemeler/kılavuzlar kullanılmalıdır? Bu kılavuzların içeriğini nasıl değerlendirirsiniz? ve Soru 11-Türkiye'de dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeleri nasıl değerlendirirsiniz?" sorularına katılımcıların verdiği cevaplar doğrultusunda "Yasal Düzenlemeler" kategorisi oluşturulmuştur. "Yasal Düzenlemeler" kategorisine yönelik yedi ifade yer almakta olup ikinci turda oluşturulan ifadeler ve bu ifadelere ilişkin bulgular (ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar Tablo 3.9'da sunulmuştur.

Tablo 3. 9.*Yasal düzenlemeler kategorisi Delphi II. tur bulguları*

Yasal Düzenlemeler	**Ortalama**	**Standart Sapma**	**Ortanca**	**ÇAF**	**Frekans (Yüzde)**			**Görüş Birliği**
					1	**2**	**3**	
1. Dijital dönüşüm ile birlikte gelen riskler karşısında iç denetim faaliyeti yürütülürken başlıca takip edilmesi gereken düzenlemeler/kılavuzlar: • Cumhurbaşkanlığı DDO (Dijital Dönüşüm Ofisi) Bilgi ve İletişim Güvenliği Denetim Rehberi • COBIT, • ISO 27000, • NIST • IIA	1	0	1	0	11 (100)	0 (0)	0 (0)	Var

Tablo 3.9.(Devamı) *Yasal düzenlemeler kategorisi Delphi II. tur bulguları*

2. Cumhurbaşkanlığı DDO yayımladığı Bilgi ve İletişim Güvenliği Denetim Rehberi dijital riskleri yönetmek adına yeterli bir rehberdir.	1,36	0,67	1	1	8 (72,2)	2 (18,7)	1 (9,1)	Yok
3. Türkiye'de dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeler yeterli değildir, gelişmesi gereken alanlar vardır.	1,18	0,40	1	0	9 (81,8)	2 (18,2)	0 (0)	Var
4. Dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeler, Türkiye'de belli başlı kurumlar tarafından yapılmaktadır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
5. Kamu kurumları, Cumhurbaşkanlığı DDO yayımladığı Bilgi ve İletişim Güvenliği Denetim Rehberi'ni uygulayabilecek noktada değildir.	1,64	0,81	1	1	6 (54,5)	3 (27,3)	2 (18,2)	Yok
6. Kamu kurumları özel kurumlardan özellikle risk yönetimi uygulanmalarından son zamanlarda faydalanmaktadır.	1,27	0,65	1	0	9 (81,8)	1 (9,1)	1 (9,1)	Var
7. Türkiye'de dijital risklerin yönetimi adına özel sektör bilinci daha yüksek ve daha erken çalışmalar başlamıştır.	1,27	0,65	1	0	9 (81,8)	1 (9,1)	1 (9,1)	Var

Tablo 3.9'dan görüldüğü üzere ifadelerin ortalama değerleri 1 - 1,64; standart sapma değerleri 0 - 0,81; çeyrekler arası fark 0 - 1; 1 frekans değerleri 6 (54,5) - 11(100), 2 frekans değeri 0 (0) - 3 (27,3), 3 frekans değerleri 0 (0) - 2 (18,2) arasında değişirken, ortanca değerlerin 1'e eşit olduğuna ulaşılmıştır.

Çalışmada belirlenen görüş birliği ölçütlerine göre "Yasal Düzenlemeler" kategorisine yönelik ikinci turda, "2.Cumhurbaşkanlığı DDO yayımladığı Bilgi ve İletişim Güvenliği Denetim Rehberi dijital riskleri yönetmek adına yeterli bir rehberdir.", "5.Kamu kurumları, Cumhurbaşkanlığı DDO yayımladığı Bilgi ve İletişim Güvenliği Denetim Rehberi'ni uygulayabilecek noktada değildir." ifadelerinde görüş birliği sağlanamamışken, "1.Dijital dönüşüm ile birlikte gelen riskler karşısında iç denetim faaliyeti yürütülürken başlıca takip edilmesi gereken düzenlemeler/kılavuzlar (Cumhurbaşkanlığı DDO (Dijital Dönüşüm Ofisi) Bilgi ve İletişim Güvenliği Denetim Rehberi, COBIT,ISO 27000, NIST, IIA)'dir", "3.Türkiye'de dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeler yeterli değildir, gelişmesi

gereken alanlar vardır.", "4.Dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeler, Türkiye'de belli başlı kurumlar tarafından yapılmaktadır.", "6.Kamu kurumları özel kurumlardan özellikle risk yönetimi uygulanmalarından son zamanlarda faydalanmaktadır.", "7.Türkiye'de dijital risklerin yönetimi adına özel sektör bilinci daha yüksek ve daha erken çalışmalar başlamıştır." ifadelerinde görüş birliği sağlanmıştır. Dolayısıyla "Yasal Düzenlemeler" kategorisine yönelik ikinci turda yedi maddenin ikisinde görüş birliği sağlamamışken, beşinde ise görüş birliği sağlanmıştır.

3.9.3. Delphi III. turu

Delphi III. tur anketinde katılımcılardan gelen yanıtlar sonucu yapılan analizden elde edilen her bir kategoriye ilişkin bulgular (ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar tablolar şeklinde sırasıyla sunulmuştur. Delphi III. tur anketine toplamda on bir katılımcı dönüt sağlamıştır.

Katılımcılardan anket ifadelerine ilişkin geri bildirimler sonucu "Dijital Dönüşüm-Endüstri 4.0" kategorisine yönelik Delphi III. tur anketine ilişkin bulgular (ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar Tablo 3.10'da sunulmuştur.

Tablo 3.10. *Dijital dönüşüm- Endüstri 4.0 kategorisi Delphi III. tur bulguları*

Dijital Dönüşüm-Endüstri 4.0	**Ortalama**	**Standart Sapma**	**Ortanca**	**ÇAF**	**Frekans (Yüzde)**			**Görüş Birliği**
					1	**2**	**3**	
1. Endüstri 4.0; dijitalleşme, akıllı ev aletleri, denetimin dijitalleşmesi, robotların artık kullanılmaya başlanması, RPA teknolojileri, mükerrer işlemlerin azalması, insana duyulan ihtiyacın azalması şeklinde tanımlanabilir.	1,18	0,40	1	0	9 (81,8)	2 (18,2)	0 (0)	Var
2. Dördüncü sanayi devrimi birçok alanda dijitalleşmeyi ve dijital dönüşümü merkez alan yeni bir yapılanmadır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
3. Dijital dönüşüm, dördüncü sanayi devrimi teknolojilerinin üretim ve hizmet alanlarında kullanma sürecidir.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var

Tablo 3. 10. (Devamı) *Dijital dönüşüm- Endüstri 4.0 kategorisi Delphi III. tur bulguları*

4. Dijital dönüşüm kurumların iş yapış şekillerinden, çözüm üretme stratejilerine kadar kurumları etkileyen önemli bir konudur.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
5. Dijital dönüşüm kurumların stratejik planlarından başlayıp tüm iş süreçlerini ele alınması gereken önemli bir konudur.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
6. İç denetim, iç kontrol süreçlerinin gerçek zamanlı izlenebilmesi dijital dönüşümün, dördüncü sanayi devriminin bir yansımasıdır.	1,18	0,40	1	0	9 (81,8)	2 (18,2)	0 (0)	Var

Tablo 3.10'da görüldüğü üzere ifadelerin ortalama değerleri 1 – 1,18; standart sapma değerleri 0 – 0,40; 1 frekans değerleri 9 (81,2) - 11(100), 2 frekans değeri 0 (0) - 2 (18,2), 3 frekans değerleri 0 (0) – 0 (0); çeyrekler arası farkın 0'a, ortanca değerlerinin 1'e eşit olduğuna ulaşılmıştır.

Çalışmanın Delphi III. tur bulgularına göre "Dijital Dönüşüm-Endüstri 4.0" kategorisindeki tüm ifadeler konusunda katılımcıların görüş birliğine ulaştığı görülmektedir. "1.Endüstri 4.0; dijitalleşme, akıllı ev aletleri, denetimin dijitalleşmesi, robotların artık kullanılmaya başlanması, RPA teknolojileri, mükerrer işlemlerin azalması, insana duyulan ihtiyacın azalması şeklinde tanımlanabilir.", "2.Dördüncü sanayi devrimi birçok alanda dijitalleşmeyi ve dijital dönüşümü merkez alan yeni bir yapılanmadır.", "3.Dijital dönüşüm, dördüncü sanayi devrimi teknolojilerinin üretim ve hizmet alanlarında kullanma sürecidir.", "4.Dijital dönüşüm kurumların iş yapış şekillerinden, çözüm üretme stratejilerine kadar kurumları etkileyen önemli bir konudur.", "5.Dijital dönüşüm kurumların stratejik planlarından başlayıp tüm iş süreçlerini ele alınması gereken önemli bir konudur.", "6.İç denetim, iç kontrol süreçlerinin gerçek zamanlı izlenebilmesi dijital dönüşümün, dördüncü sanayi devriminin bir yansımasıdır." ifadeleri üzerinde katılımcılar uzlaşma sağlamıştır.

Katılımcılardan anket ifadelerine ilişkin geri bildirimler sonucunda elde edilen "Dijital Dönüşümden Kaynaklı Riskler" kategorisine yönelik Delphi III. tur anketine ilişkin bulgular (ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar Tablo 3. 11'de sunulmuştur.

Tablo 3. 11.*Dijital Dönüşümden kaynaklı Riskler kategorisi Delphi III. tur bulguları*

Dijital Dönüşümden Kaynaklı Riskler	Ortalama	Standart Sapma	Ortanca	ÇAF	Frekans (Yüzde)			Görüş Birliği
					1	2	3	
1. Dijital dönüşüme uyum sağlama, kurumların değişim kültürüne sahip olmaması, geç kalınması veya yavaş ilerlemek riskler arasındadır.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
2. Dijital dönüşüme kısa sürede uyum sağlama ihtiyacının doğurabileceği yanlış kararlar ve bunlardan kaynaklı katlanılan yüksek maliyetler önemli risklerden biridir.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
3. Kurumun dijital dönüşüm süreci için yeterli düzeyde araştırma-geliştirme ve testlerin yapılmamasından kaynaklı kayıplar (zaman, iş gücü, bütçe, karlılık vb.) önemli risklerden biridir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
4. Dijital dönüşüm ile birlikte yaşanacak en önemli riskler kişisel verilerin korunması, bilgi güvenliği ve siber güvenlik riskleridir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
5. Dijital dönüşüm sürecine entegre olamayan veya kendini yenileyemeyen kişiler ve toplumlar için bazı iş kollarının yok olması ve işsizlik önemli bir sorundur.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
6. Dijital dönüşümden kaynaklı en büyük risk veri kapsamında olup sadece veri kaybı olarak değil verinin bütüncül ve anlamlı şekilde tutulamaması da büyük bir risktir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
7. Kurumların dijital dönüşüm sürecinde değişime direnç göstermesi ve yetkin iş gücüne/dijital iş gücüne sahip olmaması başlıca sıkıntılar/riskler arasındadır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var

Tablo 3. 11. (Devamı) *Dijital Dönüşümden kaynaklı Riskler kategorisi Delphi III. tur bulguları*

8. Kurumlar tarafından kullanılan otomatik sistemlerin en büyük riskleri algoritmanın doğru çalışıp çalışmadığı, algoritmanın kurumun istediği sonucu verip vermediği ve algoritmayı yetkisiz değiştirecek üçüncü bir kişinin var olup olmadığıdır.	1,18	0,60	1	0	10 (90,9)	1 (9,1)	0 (0)	Var

Tablo 3.11'de görüldüğü üzere ifadelerin ortalama değerleri 1 – 1,18; standart sapma değerleri 0 – 0,60; 1 frekans değerleri 10 (90,9) - 11(100), 2 frekans değeri 0 (0) - 1 (9,1), 3 frekans değerleri 0 (0) – 0 (0) arasında değiştiğine, çeyrekler arası farkın 0'a ortanca değerlerinin 1'e eşit olduğuna ulaşılmıştır.

Çalışmanın Delphi III. tur bulgularına göre "Dijital Dönüşümden Kaynaklı Riskler" kategorisindeki tüm ifadelere ilişkin katılımcıların görüş birliği sağladığına ulaşılmıştır. "1.Dijital dönüşüme uyum sağlama, kurumların değişim kültürüne sahip olmaması, geç kalınması veya yavaş ilerlemek riskler arasındadır.", "2.Dijital dönüşüme kısa sürede uyum sağlama ihtiyacının doğurabileceği yanlış kararlar ve bunlardan kaynaklı katlanılan yüksek maliyetler önemli risklerden biridir.", "3.Kurumun dijital dönüşüm süreci için yeterli düzeyde araştırma-geliştirme ve testlerin yapılmamasından kaynaklı kayıplar (zaman, iş gücü, bütçe, karlılık vb.) önemli risklerden biridir.", "4.Dijital dönüşüm ile birlikte yaşanacak en önemli riskler kişisel verilerin korunması, bilgi güvenliği ve siber güvenlik riskleridir.", "5.Dijital dönüşüm sürecine entegre olamayan veya kendini yenileyemeyen kişiler ve toplumlar için bazı iş kollarının yok olması ve işsizlik önemli bir sorundur.", "6.Dijital dönüşümden kaynaklı en büyük risk veri kapsamında olup sadece veri kaybı olarak değil verinin bütüncül ve anlamlı şekilde tutulamaması da büyük bir risktir.", "7.Kurumların dijital dönüşüm sürecinde değişime direnç göstermesi ve yetkin iş gücüne/dijital iş gücüne sahip olmaması başlıca sıkıntılar/riskler arasındadır.", "8.Kurumlar tarafından kullanılan otomatik sistemlerin en büyük riskleri algoritmanın doğru çalışıp çalışmadığı, algoritmanın kurumun istediği sonucu verip vermediği ve algoritmayı yetkisiz değiştirecek üçüncü bir kişinin var olup olmadığıdır." ifadeleri üzerinde görüş birliği sağlanmıştır.

Katılımcılardan anket ifadelerine ilişkin geri bildirimler sonucunda elde edilen "İç Denetimin Rolü" kategorisine yönelik Delphi III. tur anketine ilişkin bulgular (ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar Tablo 3.12'de sunulmuştur.

Tablo 3. 12. *İç denetimin rolü kategorisi Delphi III. tur bulguları*

İç Denetimin Rolü	Ortalama	Standart Sapma	Ortanca	ÇAF	Frekans (Yüzde)			Görüş Birliği
					1	2	3	
1. Dijital dönüşümden kaynaklı risklerin tanımlanması ve farkındalık oluşturulması aşamasında iç denetim danışmanlık rolü ile katkı sağlayacaktır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
2. Dijital dönüşüm çerçevesinde iç denetimin temel faaliyeti olan güvence ve danışmanlık görevi daha önemli bir seviyeye gelecektir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
3. Dijital dönüşüm sürecinde iç denetim fonksiyonu ilk etapta danışmanlık rolü ile kurumlara katkı sağlayacaktır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
4. Dijital dönüşüm çerçevesinde iç denetimin mutlak güvence sağlayamama konusu devam etmekle birlikte giderek artabilir. Diğer taraftan dijital dönüşüm ile birlikte danışmanlık rolü daha kritik hale gelecektir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
5. İç denetim fonksiyonu dijital dönüşümden kaynaklı riskler karşısında bilgi teknolojileri denetimine ağırlık vermelidir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
6. İç denetim fonksiyonu dijital dönüşümün getirdiği teknolojiler, bu teknolojilere uyum sağlanması, gerektiğinde yeniden yapılanma ihtiyacı, buna ilişkin planlama vb. konularda çalışmalar yürütmek ve gerekli bilgilendirmeleri yapmalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
7. İç denetçiler dijital dönüşüm sürecine yönelik danışmanlık hizmeti aşamasında kurumlara özgü planlar oluşturmalıdırlar.	1	0	1	0	10 (100)	0 (0)	0 (0)	Var

Tablo 3.12. (Devamı) *İç denetimin rolü kategorisi Delphi III. tur bulguları*

8. Yeni teknolojilerin riskleri, yasa ya da standart anlamındaki uyum süreçlerinin etkisi, yeni nesil ürün ve sistemlerin kullanımı gibi alanlarda iç denetim süreçlerinin yeniden yapılanması gereklidir.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
9. Kurumların dijital dönüşüm sürecinde iç denetim, danışmanlık rolü çerçevesinde entegre sistemlerin kurulumu, bu sistemlerden alınacak verilerin izlenmesi ve bu sistemlerin güvenliği rolünü üstlenmektedir.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var

Tablo 3.12'de görüldüğü üzere ifadelerin ortalama değerleri 1 – 1,09; standart sapma değerleri 0 – 0,30; 1 frekans değerleri 10 (90,9) - 11(100), 2 frekans değeri 0 (0) - 1 (9,1), 3 frekans değerleri 0 (0) – 0 (0) arasında değiştiğine, çeyrekler arası farkın 0'a ortanca değerlerinin 1'e eşit olduğuna ulaşılmıştır.

Çalışmanın Delphi III. tur bulgularına göre "İç Denetimin Rolü" kategorisindeki tüm ifadelere ilişkin katılımcıların görüş birliği sağladığına ulaşılmıştır. "1.Dijital dönüşümden kaynaklı risklerin tanımlanması ve farkındalık oluşturulması aşamasında iç denetim danışmanlık rolü ile katkı sağlayacaktır.", "2.Dijital dönüşüm çerçevesinde iç denetimin temel faaliyeti olan güvence ve danışmanlık görevi daha önemli bir seviyeye gelecektir.", "3.Dijital dönüşüm sürecinde iç denetim fonksiyonu ilk etapta danışmanlık rolü ile kurumlara katkı sağlayacaktır.", 4.Dijital dönüşüm çerçevesinde iç denetimin mutlak güvence sağlayamama konusu devam etmekle birlikte giderek artabilir. Diğer taraftan dijital dönüşüm ile birlikte danışmanlık rolü daha kritik hale gelecektir.", "5.İç denetim fonksiyonu dijital dönüşümden kaynaklı riskler karşısında bilgi teknolojileri denetimine ağırlık vermelidir.", "6.İç denetim fonksiyonu dijital dönüşümün getirdiği teknolojiler, bu teknolojilere uyum sağlanması, gerektiğinde yeniden yapılanma ihtiyacı, buna ilişkin planlama vb. konularda çalışmalar yürütmek ve gerekli bilgilendirmeleri yapmalıdır.", "7.İç denetçiler dijital dönüşüm sürecine yönelik danışmanlık hizmeti aşamasında kurumlara özgü planlar oluşturmalıdırlar.", 8. Yeni teknolojilerin riskleri, yasa ya da standart anlamındaki uyum süreçlerinin etkisi, yeni nesil ürün ve sistemlerin kullanımı gibi alanlarda iç denetim süreçlerinin yeniden yapılanması gereklidir.",

“9.Kurumların dijital dönüşüm sürecinde iç denetim, danışmanlık rolü çerçevesinde entegre sistemlerin kurulumu, bu sistemlerden alınacak verilerin izlenmesi ve bu sistemlerin güvenliği rolünü üstlenmektedir.” ifadeleri üzerinde görüş birliği sağlanmıştır.

Katılımcılardan anket ifadelerine ilişkin geri bildirimler sonucunda elde edilen “Üçlü Hat Modeli” kategorisine yönelik Delphi III. tur anketine ilişkin bulgular (ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar Tablo 3.13’te sunulmuştur.

Tablo 3. 13. *Üçlü hat modeli kategorisi Delphi III. tur bulguları*

Üçlü Hat Modeli	Ortalama	Standart Sapma	Ortanca	ÇAF	Frekans (Yüzde)			Görüş Birliği
					1	2	3	
1. İç denetim, dijital dönüşüm sürecinin yönetişim, risk yönetimi ve iç kontrol sisteminde yaratacağı değişime ilişkin tavsiyelerde bulunmak, bu konularda kuruma ve yönetime danışmanlık yapmak ve destek sunmak gibi önemli rollere sahiptir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
2. İç denetim yeni sistemin yeterliği ve etkililiğinin değerlendirmesi kapsamında role sahiptir.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
3. Üçlü hat modelinde iç denetimin önemi daha ön plana çıkarmakla birlikte dijitalleşmeden kaynaklı riskler karşısında iç denetim faaliyetini daha da gerekli kılmaktadır.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
4. İç denetim artık riskleri daha proaktif yönettiği bir döneme giriyor.	1,27	0,65	1	0	9 (81,8)	1 (9,1)	1 (9,1)	Var
5. Dijital dönüşüm sürecinde iç denetimin geride kalması katma değeri azaltmaktadır.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var

Tablo 3. 13. (Devamı) *Üçlü hat modeli kategorisi Delphi III. tur bulguları*

6. Dijital dönüşüm süreciyle iç denetim fonksiyonu GRC (Governance, Risk, Compliance -Yönetişim, Risk, Uyum), veri analitiği kullanan yapılar haline gelmelidir.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var

Tablo 3.13'te görüldüğü üzere ifadelerin ortalama değerleri 1 – 1,27; standart sapma değerleri 0 – 0,65; 1 frekans değerleri 9 (81,8) - 11(100), 2 frekans değeri 0 (0) - 1 (9,1), 3 frekans değerleri 0 (0) - 1 (9,1) arasında değiştiğine, çeyrekler arası farkın 0'a ortanca değerlerinin 1'e eşit olduğuna ulaşılmıştır.

Çalışmanın Delphi III. tur bulgularına göre " Üçlü Hat Modeli" kategorisindeki tüm ifadelere ilişkin katılımcıların görüş birliği sağladığına ulaşılmıştır. "1.İç denetim, dijital dönüşüm sürecinin yönetişim, risk yönetimi ve iç kontrol sisteminde yaratacağı değişime ilişkin tavsiyelerde bulunmak, bu konularda kuruma ve yönetime danışmanlık yapmak ve destek sunmak gibi önemli rollere sahiptir.", "2.İç denetim yeni sistemin yeterliği ve etkililiğinin değerlendirmesi kapsamında role sahiptir.", "3.Üçlü hat modelinde iç denetimin önemi daha ön plana çıkarmakla birlikte dijitalleşmeden kaynaklı riskler karşısında iç denetim faaliyetini daha da gerekli kılmaktadır.", "4.İç denetim artık riskleri daha proaktif yönettiği bir döneme giriyor.", "5.Dijital dönüşüm sürecinde iç denetimin geride kalması katma değeri azaltmaktadır.", "6. Dijital dönüşüm süreciyle iç denetim fonksiyonu GRC (Governance, Risk, Compliance -Yönetişim, Risk, Uyum), veri analitiği kullanan yapılar haline gelmelidir." ifadeleri üzerinde görüş birliği sağlanmıştır.

Katılımcılardan anket ifadelerine ilişkin geri bildirimler sonucunda elde edilen "İç Kontrol Sistemi" kategorisine yönelik Delphi III. tur anketine ilişkin bulgular (ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar Tablo 3.14'te sunulmuştur.

Tablo 3. 14. *İç kontrol sistemi kategorisi Delphi III. tur bulguları*

İç Kontrol Sistemi	Ortalama	Standart Sapma	Ortanca	ÇAF	Frekans (Yüzde)			Görüş Birliği
					1	2	3	
1. Dijitalleşme kurumlarda bir strateji ile başlamalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
2. Kurumlardaki dijital dönüşüm sonucu iç kontrol sistemin sorumluluğundaki birtakım kontroller yazılım sistemine aktarılır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
3. Dijitalleşme sonucu denetimlerin otomatik şekilde yapılmasından kaynaklı iç denetimin otomatikleşen sistemlere yönelik denetimi önem kazanmaktadır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
4. İç kontrol sisteminin risk ortamı ve kontrol faaliyetleri bileşenlerinin dijital riskleri kapsaması konusunda revize edilmesi gerekir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
5. İç kontrol sisteminin beşinci bileşeni olarak izleme çerçevesinde iç denetim iç kontrol sisteminin dijital dönüşümden kaynaklı riskler karşısında etkinliğini değerlendirme aşamasında güvence rolü ile katkı sağlamaktadır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
6. Dijital dönüşüm ile birlikte kurumların bilgi teknolojileri departmanının risk ve açıklarının kontrolü için bağımsız kuruluşlarca düzenli olarak testleri yapılmalıdır.	1,18	0,40	1	0	9 (81,8)	2 (18,2)	0 (0)	Var
7. Dijital dönüşüm çağında iç kontrol sistemi olaylar gerçekleşmeden önce önlem almalı ve mevcut trendler ile sürekli bir uyum içinde kalmalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
8. Dijital dönüşüm ile entegre sistemler (Enterprise Resource Planning (ERP)-Kurumsal Kaynak Planlaması gibi) kullanılabilir.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var

Tablo 3.14. (Devamı) *İç kontrol sistemi kategorisi Delphi III. tur bulguları*

9. Dijital dönüşümden kaynaklı riskler karşında risk yönetimi çerçevesinde kurumsal yönetim ilkelerine uygun olarak gerekli kontrol noktalarının oluşturulması sağlanmalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
10. Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde değişim karşısında iç denetim stratejik rol üstlenmeli ve danışmanlık rolünü ön plana çıkarmalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
11. Dijitalleşme kurumlarda iç kontrol sisteminin bakış açısını artıracaktır.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
12. Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sistemindeki değişiklikler kurumun olgunluk seviyesine bağlıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
13. Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde kurumlar değişiklik yapmaya karar verdi ise yazılım alınacaksa alternatiflerin araştırılması, sisteme geçiş sürecinde eğitimlerin verilmesi konularında iç denetim danışmanlık rolünü üstlenebilir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
14. Kurumlar dijitalleşme için adım atmış ve kurum kültürü oluşturmuş ise iç kontrol yapılarını da bu çerçevede güncellemek zorundadır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
15. İç kontrol sistemlerine sürekli izleme yaklaşımları adapte edilmelidir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var

Tablo 3.14'te görüldüğü üzere ifadelerin ortalama değerleri 1 – 1,18; standart sapma değerleri 0 – 0,40; 1 frekans değerleri 9 (81,8) - 11(100), 2 frekans değeri 0 (0) - 2 (18,2), 3 frekans değerleri 0 (0) – 0 (0); çeyrekler arası farkın 0'a, ortanca değerlerinin 1'e eşit olduğuna ulaşılmıştır.

Çalışmanın Delphi III. tur bulgularına göre "İç Kontrol Sistemi" kategorindeki tüm ifadelere ilişkin katılımcıların görüş birliği sağladığına ulaşılmıştır. "1.Dijitalleşme kurumlarda bir strateji ile başlamalıdır.", "2.Kurumlardaki dijital dönüşüm sonucu iç kontrol sistemin sorumluluğundaki birtakım kontroller yazılım sistemine aktarılır.",

“3.Dijitalleşme sonucu denetimlerin otomatik şekilde yapılmasından kaynaklı iç denetimin otomatikleşen sistemlere yönelik denetimi önem kazanmaktadır.”, “4.İç kontrol sisteminin risk ortamı ve kontrol faaliyetleri bileşenlerinin dijital riskleri kapsaması konusunda revize edilmesi gerekir.”, “5.İç kontrol sisteminin beşinci bileşeni olarak izleme çerçevesinde iç denetim iç kontrol sisteminin dijital dönüşümden kaynaklı riskler karşısında etkinliğini değerlendirme aşamasında güvence rolü ile katkı sağlamaktadır.”, “6.Dijital dönüşüm ile birlikte kurumların bilgi teknolojileri departmanının risk ve açıklarının kontrolü için bağımsız kuruluşlarca düzenli olarak testleri yapılmalıdır.”, “7.Dijital dönüşüm çağında iç kontrol sistemi olaylar gerçekleşmeden önce önlem almalı ve mevcut trendler ile sürekli bir uyum içinde kalmalıdır.”, “8.Dijital dönüşüm ile entegre sistemler (Enterprise Resource Planning (ERP)-Kurumsal Kaynak Planlaması gibi) kullanılabilir.”, “9.Dijital dönüşümden kaynaklı riskler karşında risk yönetimi çerçevesinde kurumsal yönetim ilkelerine uygun olarak gerekli kontrol noktalarının oluşturulması sağlanmalıdır.”, “10.Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde değişim karşısında iç denetim stratejik rol üstlenmeli ve danışmanlık rolünü ön plana çıkarmalıdır.”, “11.Dijitalleşme kurumlarda iç kontrol sisteminin bakış açısını artıracaktır.”, “12.Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sistemindeki değişiklikler kurumun olgunluk seviyesine bağlıdır.”, “13.Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde kurumlar değişiklik yapmaya karar verdi ise yazılım alınacaksa alternatiflerin araştırılması, sisteme geçiş sürecinde eğitimlerin verilmesi konularında iç denetim danışmanlık rolünü üstlenebilir.”, “14.Kurumlar dijitalleşme için adım atmış ve kurum kültürü oluşturmuş ise iç kontrol yapılarını da bu çerçevede güncellemek zorundadır.”, “15. İç kontrol sistemlerine sürekli izleme yaklaşımları adapte edilmelidir.” ifadeleri üzerinde görüş birliği sağlanmıştır.

Katılımcılardan anket ifadelerine ilişkin geri bildirimler sonucunda elde edilen “İç Denetçi” kategorisine yönelik Delphi III. tur anketine ilişkin bulgular (ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar Tablo 3.15’te sunulmuştur.

Tablo 3. 15. *İç denetçi kategorisi Delphi III. tur bulguları*

İç Denetçi	Ortalama	Standart Sapma	Ortanca	ÇAF	Frekans (Yüzde)			Görüş Birliği
					1	2	3	
1. İç denetçilerin bilgisayar tabanlı denetim yöntemlerini öğrenmeleri ve kendilerini bu alanda yetiştirmeleri yapılan denetimin kalite ve etkinliğini artıracaktır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
2. İç denetçi iletişim becerisine sahip olmalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
3. Denetçinin dijital dönüşüm sürecini ve riskleri doğru yönetmek adına CIA, CISA, ITIL, CGEIT, CRMA, PMP(Proje Yönetim Sertifikası) sertifikalarının biri ya da birkaçına sahip olmalıdır.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
4. İç denetçiler teknolojik alanda yaşanan gelişmeleri yakından takip etmeli ve söz konusu yeni teknolojilerin birer denetim aracı olarak kullanılmasını sağlamalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
5. İç denetçiler yeni teknoloji kullanımının getireceği riskleri denetim alanı olarak ele almalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
6. Sürekli denetim, çevik denetim, denetim 4.0 gibi yeni denetim yaklaşımları iç denetçilerin odak noktası olmalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
7. İç denetçilerin bilgi teknolojileri ve buna bağlı riskler konusunda farkındalıklarını arttırmaları gerekmektedir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
8. İç denetçilerin finansal okur yazarlıklarının yanında dijital okur yazarlık yeteneğine sahip olmalı ve gerekli altyapı hızla oluşturulmalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
9. İç denetçiler kurumsal iletişim, kurumsal risk yönetimi, bilgi teknolojileri denetimi, siber güvenlik, uzaktan denetim teknikleri, veri analizi ve modelleme teknikleri, iş zekası programlama vb. genel eğitimler almalıdır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var

Tablo 3. 15. (Devamı) *İç denetçi kategorisi Delphi III. tur bulguları*

10. İç denetçiler dijital çağ ile birlikte multidisipliner (hem bilgi teknolojisi hem denetim, muhasebe) özelliklerine sahip olmalıdırlar.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
11. Dijital dönüşüm sürecinde iç denetim faaliyeti yürütülürken farklı yetkinlikte kişilerin bir arada birleşip denetim yapması gerekmektedir.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var

Tablo 3.15'te görüldüğü üzere ifadelerin ortalama değerleri 1 – 09; standart sapma değerleri 0 – 0,30; 1 frekans değerleri 10 (90,9) - 11(100), 2 frekans değeri 0 (0) - 1 (9,1), 3 frekans değerleri 0 (0) – 0 (0); çeyrekler arası farkın 0'a, ortanca değerlerinin 1'e eşit olduğuna ulaşılmıştır.

Çalışmanın Delphi III. tur bulgularına göre "İç Denetçi" kategorisindeki tüm ifadelere ilişkin katılımcıların görüş birliği sağladığına ulaşılmıştır. "1.İç denetçilerin bilgisayar tabanlı denetim yöntemlerini öğrenmeleri ve kendilerini bu alanda yetiştirmeleri yapılan denetimin kalite ve etkinliğini artıracaktır.", "2.İç denetçi iletişim becerisine sahip olmalıdır.", "3.Denetçinin dijital dönüşüm sürecini ve riskleri doğru yönetmek adına CIA, CISA, ITIL, CGEIT, CRMA, PMP(Proje Yönetim Sertifikası) sertifikalarının biri ya da birkaçına sahip olmalıdır.", "4.İç denetçiler teknolojik alanda yaşanan gelişmeleri yakından takip etmeli ve söz konusu yeni teknolojilerin birer denetim aracı olarak kullanılmasını sağlamalıdır.", "5.İç denetçiler yeni teknoloji kullanımının getireceği riskleri denetim alanı olarak ele almalıdır.", "6.Sürekli denetim, çevik denetim, denetim 4.0 gibi yeni denetim yaklaşımları iç denetçilerin odak noktası olmalıdır.", "7.İç denetçilerin bilgi teknolojileri ve buna bağlı riskler konusunda farkındalıklarını arttırmaları gerekmektedir.", "8. İç denetçilerin finansal okur yazarlıklarının yanında dijital okur yazarlık yeteneğine sahip olmalı ve gerekli altyapı hızla oluşturulmalıdır.", "9.İç denetçiler kurumsal iletişim, kurumsal risk yönetimi, bilgi teknolojileri denetimi, siber güvenlik, uzaktan denetim teknikleri, veri analizi ve modelleme teknikleri, iş zekası programlama vb. genel eğitimler almalıdır.", 10.İç denetçiler dijital çağ ile birlikte multidisipliner (hem bilgi teknolojisi hem denetim, muhasebe) özelliklerine sahip olmalıdırlar.", "11.Dijital dönüşüm sürecinde iç denetim faaliyeti yürütülürken farklı yetkinlikte kişilerin bir arada birleşip denetim yapması gerekmektedir." ifadeleri üzerinde görüş birliği sağlanmıştır.

Katılımcılardan anket ifadelerine ilişkin geri bildirimler sonucunda elde edilen "Yasal Düzenlemeler" kategorisine yönelik Delphi III. tur anketine ilişkin bulgular (ortalama, standart sapma, ortanca, ÇAF ve frekanslar) ve yorumlar Tablo 3.16'da sunulmuştur.

Tablo 3. 16. *Yasal düzenlemeler kategorisi Delphi III. tur bulguları*

Yasal Düzenlemeler	Ortalama	Standart Sapma	Ortanca	ÇAF	Frekans (Yüzde)			Görüş Birliği
					1	2	3	
1. Dijital dönüşüm ile birlikte gelen riskler karşısında iç denetim faaliyeti yürütülürken başlıca takip edilmesi gereken düzenlemeler/kılavuzlar: • Cumhurbaşkanlığı DDO (Dijital Dönüşüm Ofisi) Bilgi ve İletişim Güvenliği Denetim Rehberi • COBIT, • ISO 27000, • NIST • IIA	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
2. Türkiye'de dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeler yeterli değildir, gelişmesi gereken alanlar vardır.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var
3. Dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeler, Türkiye'de belli başlı kurumlar tarafından yapılmaktadır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
4. Kamu kurumları özel kurumlardan özellikle risk yönetimi uygulanmalarından son zamanlarda faydalanmaktadır.	1	0	1	0	11 (100)	0 (0)	0 (0)	Var
5. Türkiye'de dijital risklerin yönetimi adına özel sektör bilinci daha yüksek ve daha erken çalışmalar başlamıştır.	1,09	0,30	1	0	10 (90,9)	1 (9,1)	0 (0)	Var

Tablo 3.16'da görüldüğü üzere ifadelerin ortalama değerleri 1 – 1,09; standart sapma değerleri 0 – 0,30; 1 frekans değerleri 10 (90,9) - 11(100), 2 frekans değeri 0 (0) -

1 (9,1), 3 frekans değerleri 0 (0) – 0 arasında değiştiğine, çeyrekler arası farkın 0'a, ortanca değerlerinin 1'e eşit olduğuna ulaşılmıştır.

Çalışmanın Delphi III. tur bulgularına göre "Yasal düzenlemeler" kategorisindeki tüm ifadelere ilişkin katılımcıların görüş birliği sağladığına ulaşılmıştır. "1.Dijital dönüşüm ile birlikte gelen riskler karşısında iç denetim faaliyeti yürütülürken başlıca takip edilmesi gereken düzenlemeler/kılavuzlar (Cumhurbaşkanlığı DDO (Dijital Dönüşüm Ofisi) Bilgi ve İletişim Güvenliği Denetim Rehberi, COBIT,ISO 27000, NIST,IIA)'dir", "2.Türkiye'de dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeler yeterli değildir, gelişmesi gereken alanlar vardır.", "3.Dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeler, Türkiye'de belli başlı kurumlar tarafından yapılmaktadır.", "4.Kamu kurumları özel kurumlardan özellikle risk yönetimi uygulanmalarından son zamanlarda faydalanmaktadır.", "5.Türkiye'de dijital risklerin yönetimi adına özel sektör bilinci daha yüksek ve daha erken çalışmalar başlamıştır." ifadeleri üzerinde görüş birliği sağlanmıştır.

SONUÇ ve ÖNERİLER

Endüstri 4.0 teknolojileri ile kurumlar, tüketiciler, tedarikçiler gibi birçok paydaşın birbirine entegre şekilde çalışma ortamının yaratılması dijital dönüşüm olarak ifade edilen sürecin bir sonucudur. Yaşanan dijital dönüşüm üretim sektörü başta olmak üzere eğitimden sağlığa kadar birçok sektörde gelişimi ve imkanı berberinde getirmektedir. Olumlu gelişmelerin yanında literatürde yapılan araştırmalar sonucunda başta kurum yöneticileri ve iç denetçiler olmak üzere birçok birey tarafından etkisinin büyüklüğü değişmekle birlikte çeşitli riskler sayılmaktadır. Bunların başında siber güvenlik riski yer almaktadır. Bu çalışmada özel ve kamu kurumu ayrımı yapılmaksızın iş yapış şekillerinde değişikliğin yaşandığı bu süreçte iç denetim faaliyetleri ve iç denetçi yetkinliği değişiminin kaçınılmaz olduğu yapılan teorik açıklamalarla ortaya konulmuştur. Ayrıca sürecin doğru yönetilmesi adına iç denetime düşen rol açıklanmaya çalışılmıştır. Akabinde çalışmada dijital dönüşüm sürecinde akademisyenler, kamu kurumu, bağımsız denetim kurumu ve mesleki kuruluşlarda çalışan iç denetçiler tarafından başlıca görülen riskler, iç denetim fonksiyonunun bu süreci doğru yönetmek adına hangi rolü ile ön plana çıktığı, iç denetçinin yetkinliği ve yasal düzenlemeler çerçevesinde araştırma yapılmıştır.

Araştırmada Delphi tekniği kullanmıştır. Bu çerçevede üç aşamadan oluşan süreç izlenmiştir. İlk olarak katılımcılar ile toplamda on bir sorudan oluşan yarı yapılandırılmış görüşme gerçekleştirilmiştir. İkinci aşamada görüşmelerin çözümlenmesi sonucunda altmış beş ifadeden oluşan bir anket formu oluşturulmuş ve katılımcılardan görüşleri alınmıştır. İkinci aşamada katılımcılardan sağlanan geri bildirimler sonucu yapılan analizden elde edilen sonuçlara göre görüş birliği sağlanmayan beş ifade çıkarılmış ve altmış ifadeden oluşan yeni anket formu hazırlanmıştır. Üçüncü aşamada son anket formundaki ifadeler için katılımcılardan görüşleri alınmıştır. Katılımcılardan sağlanan geri bildirimlerin analizi sonucunda araştırma sonunda altmış ifade üzerinde görüş birliği sağlandığına ulaşılmıştır. Görüş birliği sağlanan ve görüş birliği sağlanamayan ifadeler aşağıda kategoriler baz alınarak açıklanmıştır.

Çalışma sonucunda dijital dönüşüm ve Endüstri 4.0 kategorisine yönelik katılımcıların verdiği yanıtlara göre "1.Endüstri 4.0; dijitalleşme, akıllı ev aletleri, denetimin dijitalleşmesi, robotların artık kullanılmaya başlanması, RPA teknolojileri, mükerrer işlemlerin azalması, insana duyulan ihtiyacın azalması şeklinde tanımlanabilir.", "2.Dördüncü sanayi devrimi birçok alanda dijitalleşmeyi ve dijital

dönüşümü merkez alan yeni bir yapılanmadır.", "3.Dijital dönüşüm, dördüncü sanayi devrimi teknolojilerinin üretim ve hizmet alanlarında kullanma sürecidir.", "4.Dijital dönüşüm kurumların iş yapış şekillerinden, çözüm üretme stratejilerine kadar kurumları etkileyen önemli bir konudur.", "5.Dijital dönüşüm kurumların stratejik planlarından başlayıp tüm iş süreçlerini ele alınması gereken önemli bir konudur.", "6.İç denetim, iç kontrol süreçlerinin gerçek zamanlı izlenebilmesi dijital dönüşümün, dördüncü sanayi devriminin bir yansımasıdır." ifadeleri üzerinde görüş birliği sağlanmıştır.

Çalışma sonucunda dijital dönüşümden kaynaklı riskler kategorisine yönelik katılımcıların verdiği yanıtlara göre "1.Dijital dönüşüme uyum sağlama, kurumların değişim kültürüne sahip olmaması, geç kalınması veya yavaş ilerlemek riskler arasındadır.", "2.Dijital dönüşüme kısa sürede uyum sağlama ihtiyacının doğurabileceği yanlış kararlar ve bunlardan kaynaklı katlanılan yüksek maliyetler önemli risklerden biridir.", "3.Kurumun dijital dönüşüm süreci için yeterli düzeyde araştırma-geliştirme ve testlerin yapılmamasından kaynaklı kayıplar (zaman, iş gücü, bütçe, karlılık vb.) önemli risklerden biridir.", "4.Dijital dönüşüm ile birlikte yaşanacak en önemli riskler kişisel verilerin korunması, bilgi güvenliği ve siber güvenlik riskleridir.", "5.Dijital dönüşüm sürecine entegre olamayan veya kendini yenileyemeyen kişiler ve toplumlar için bazı iş kollarının yok olması ve işsizlik önemli bir sorundur.", "6.Dijital dönüşümden kaynaklı en büyük risk veri kapsamında olup sadece veri kaybı olarak değil verinin bütüncül ve anlamlı şekilde tutulamaması da büyük bir risktir.", "7.Kurumların dijital dönüşüm sürecinde değişime direnç göstermesi ve yetkin iş gücüne/dijital iş gücüne sahip olmaması başlıca sıkıntılar/riskler arasındadır.", "8.Kurumlar tarafından kullanılan otomatik sistemlerin en büyük riskleri algoritmanın doğru çalışıp çalışmadığı, algoritmanın kurumun istediği sonucu verip vermediği ve algoritmayı yetkisiz değiştirecek üçüncü bir kişinin var olup olmadığıdır." ifadeleri üzerinde görüş birliği sağlanmıştır.

Çalışma sonucunda iç denetimin rolü kategorisine ilişkin katılımcıların verdikleri yanıtlara göre "1.Dijital dönüşümden kaynaklı risklerin tanımlanması ve farkındalık oluşturulması aşamasında iç denetim danışmanlık rolü ile katkı sağlayacaktır.", "2.Dijital dönüşüm çerçevesinde iç denetimin temel faaliyeti olan güvence ve danışmanlık görevi daha önemli bir seviyeye gelecektir.", "3.Dijital dönüşüm sürecinde iç denetim fonksiyonu ilk etapta danışmanlık rolü ile kurumlara katkı sağlayacaktır.", "4. Dijital

dönüşüm çerçevesinde iç denetimin mutlak güvence sağlayamama konusu devam etmekle birlikte giderek artabilir. Diğer taraftan dijital dönüşüm ile birlikte danışmanlık rolü daha kritik hale gelecektir.", "5.İç denetim fonksiyonu dijital dönüşümden kaynaklı riskler karşısında bilgi teknolojileri denetimine ağırlık vermelidir.", "7. İç denetim fonksiyonu dijital dönüşümün getirdiği teknolojiler, bu teknolojilere uyum sağlanması, gerektiğinde yeniden yapılanma ihtiyacı, buna ilişkin planlama vb. konularda çalışmalar yürütmek ve gerekli bilgilendirmeleri yapmalıdır.", "8.İç denetçiler dijital dönüşüm sürecine yönelik danışmanlık hizmeti aşamasında kurumlara özgü planlar oluşturmalıdırlar.", "9.Yeni teknolojilerin riskleri, yasa ya da standart anlamındaki uyum süreçlerinin etkisi, yeni nesil ürün ve sistemlerin kullanımı gibi alanlarda iç denetim süreçlerinin yeniden yapılanması gereklidir.", "10.Kurumların dijital dönüşüm sürecinde iç denetim, danışmanlık rolü çerçevesinde entegre sistemlerin kurulumu, bu sistemlerden alınacak verilerin izlenmesi ve bu sistemlerin güvenliği rolünü üstlenmektedir." ifadeleri üzerinde katılımcılar görüş birliği sağlarken; " 6.İç denetim fonksiyonu kurumun insan kaynağının dijital dönüşüm için yeterliliğini araştırmalıdır, ekip kurma aşamasında yer almalıdır.", ifadesi üzerinde görüş birliği sağlamamıştır.

Çalışma sonucunda üçlü hat modeli kategorisine ilişkin katılımcıların verdikleri yanıtlara göre, "1.İç denetim, dijital dönüşüm sürecinin yönetişim, risk yönetimi ve iç kontrol sisteminde yaratacağı değişime ilişkin tavsiyelerde bulunmak, bu konularda kuruma ve yönetime danışmanlık yapmak ve destek sunmak gibi önemli rollere sahiptir.", "2.İç denetim yeni sistemin yeterliği ve etkililiğinin değerlendirmesi kapsamında role sahiptir.", "3.Üçlü hat modelinde iç denetimin önemi daha ön plana çıkarmakla birlikte dijitalleşmeden kaynaklı riskler karşısında iç denetim faaliyetini daha da gerekli kılmaktadır.", "4. İç denetim artık riskleri daha proaktif yönettiği bir döneme giriyor.", "5.Dijital dönüşüm sürecinde iç denetimin geride kalması katma değeri azaltmaktadır.", "7.Dijital dönüşüm süreciyle iç denetim fonksiyonu GRC (Governance, Risk, Compliance -Yönetişim, Risk, Uyum), veri analitiği kullanan yapılar haline gelmelidir." ifadelerinde görüş birliği sağlanırken; "6.Dijitalleşme öncesi ile kıyaslandığında dijital dönüşüm sürecindeki risklerin değerlendirilme aşamasında üçüncü hat rolünde iç denetimin sorumluluklarında bir değişim yoktur." ifadesinde görüş birliği sağlanamamıştır.

Çalışma sonucunda iç kontrol sistemi kategorisine ilişkin katılımcıların verdikleri yanıtlara göre "1.Dijitalleşme kurumlarda bir strateji ile başlamalıdır.", "2.Kurumlardaki dijital dönüşüm sonucu iç kontrol sistemin sorumluluğundaki birtakım kontroller yazılım sistemine aktarılır.", "3. Dijitalleşme sonucu denetimlerin otomatik şekilde yapılmasından kaynaklı iç denetimin otomatikleşen sistemlere yönelik denetimi önem kazanmaktadır.", "4.İç kontrol sisteminin risk ortamı ve kontrol faaliyetleri bileşenlerinin dijital riskleri kapsaması konusunda revize edilmesi gerekir.", "5.İç kontrol sisteminin beşinci bileşeni olarak izleme çerçevesinde iç denetim iç kontrol sisteminin dijital dönüşümden kaynaklı riskler karşısında etkinliğini değerlendirme aşamasında güvence rolü ile katkı sağlamaktadır.", "6.Dijital dönüşüm ile birlikte kurumların bilgi teknolojileri departmanının risk ve açıklarının kontrolü için bağımsız kuruluşlarca düzenli olarak testleri yapılmalıdır.", "7.Dijital dönüşüm çağında iç kontrol sistemi olaylar gerçekleşmeden önce önlem almalı ve mevcut trendler ile sürekli bir uyum içinde kalmalıdır.", "8.Dijital dönüşüm ile entegre sistemler (Enterprise Resource Planning (ERP)-Kurumsal Kaynak Planlaması gibi) kullanılabilir.", "9.Dijital dönüşümden kaynaklı riskler karşında risk yönetimi çerçevesinde kurumsal yönetim ilkelerine uygun olarak gerekli kontrol noktalarının oluşturulması sağlanmalıdır.", "10.Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde değişim karşısında iç denetim stratejik rol üstlenmeli ve danışmanlık rolünü ön plana çıkarmalıdır.", "11.Dijitalleşme kurumlarda iç kontrol sisteminin bakış açısını artıracaktır.", "12.Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sistemindeki değişiklikler kurumun olgunluk seviyesine bağlıdır.", "13.Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde kurumlar değişiklik yapmaya karar verdi ise yazılım alınacaksa alternatiflerin araştırılması, sisteme geçiş sürecinde eğitimlerin verilmesi konularında iç denetim danışmanlık rolünü üstlenebilir.", "14.Kurumlar dijitalleşme için adım atmış ve kurum kültürü oluşturmuş ise iç kontrol yapılarını da bu çerçevede güncellemek zorundadır.", "15. İç kontrol sistemlerine sürekli izleme yaklaşımları adapte edilmelidir." ifadelerinin tamamında görüş birliği sağlanmıştır.

Çalışma sonucunda iç denetçi kategorisine ilişkin katılımcıların verdikleri yanıtlara göre "1.İç denetçilerin bilgisayar tabanlı denetim yöntemlerini öğrenmeleri ve kendilerini bu alanda yetiştirmeleri yapılan denetimin kalite ve etkinliğini artıracaktır.", "2.İç denetçi iletişim becerisine sahip olmalıdır.", "3.Denetçinin dijital dönüşüm sürecini

ve riskleri doğru yönetmek adına CIA, CISA, ITIL, CGEIT, CRMA, PMP(Proje Yönetim Sertifikası) sertifikalarının biri ya da birkaçına sahip olmalıdır.", "4.İç denetçiler teknolojik alanda yaşanan gelişmeleri yakından takip etmeli ve söz konusu yeni teknolojilerin birer denetim aracı olarak kullanılmasını sağlamalıdır.", "5.İç denetçiler yeni teknoloji kullanımının getireceği riskleri denetim alanı olarak ele almalıdır.", "6.Sürekli denetim, çevik denetim, denetim 4.0 gibi yeni denetim yaklaşımları iç denetçilerin odak noktası olmalıdır.", "7.İç denetçilerin bilgi teknolojileri ve buna bağlı riskler konusunda farkındalıklarını arttırmaları gerekmektedir.", "8.İç denetçilerin finansal okur yazarlıklarının yanında dijital okur yazarlık yeteneğine sahip olmalı ve gerekli altyapı hızla oluşturulmalıdır.", "9.İç denetçiler kurumsal iletişim, kurumsal risk yönetimi, bilgi teknolojileri denetimi, siber güvenlik, uzaktan denetim teknikleri, veri analizi ve modelleme teknikleri, iş zekası programlama vb. genel eğitimler almalıdır.", "10.İç denetçiler dijital çağ ile birlikte multidisipliner (hem Bilgi Teknolojileri hem denetim, muhasebe) özelliklerine sahip olmalıdırlar.", "11.Dijital dönüşüm sürecinde iç denetim faaliyeti yürütülürken farklı yetkinlikte kişilerin bir arada birleşip denetim yapılması gerekmektedir." ifadelerinde görüş birliği sağlanırken; "12.Kamu kurumundaki iç denetçiler dijital dönüşüm çerçevesinde kurumlarına danışmanlık hizmeti verecek seviye de değildir." ifadesinde görüş birliği sağlanamamıştır.

Çalışma sonucunda yasal düzenlemeler kategorisine ilişkin katılımcıların verdikleri yanıtlara göre "1.Dijital dönüşüm ile birlikte gelen riskler karşısında iç denetim faaliyeti yürütülürken başlıca takip edilmesi gereken düzenlemeler/kılavuzlar (Cumhurbaşkanlığı DDO (Dijital Dönüşüm Ofisi) Bilgi ve İletişim Güvenliği Denetim Rehberi, COBIT,ISO 27000, NIST,IIA)'dir", "3.Türkiye'de dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeler yeterli değildir, gelişmesi gereken alanlar vardır.", "4.Dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeler, Türkiye'de belli başlı kurumlar tarafından yapılmaktadır.", "6.Kamu kurumları özel kurumlardan özellikle risk yönetimi uygulanmalarından son zamanlarda faydalanmaktadır.", "7.Türkiye'de dijital risklerin yönetimi adına özel sektör bilinci daha yüksek ve daha erken çalışmalar başlamıştır." ifadelerinde görüş birliği sağlanırken; "2.Cumhurbaşkanlığı DDO yayımladığı Bilgi ve İletişim Güvenliği Denetim Rehberi dijital riskleri yönetmek adına yeterli bir rehberdir.", "5.Kamu kurumları, Cumhurbaşkanlığı DDO yayımladığı Bilgi ve

İletişim Güvenliği Denetim Rehberi'ni uygulayabilecek noktada değildir." ifadelerinde görüş birliği sağlanamamıştır.

Çalışma kapsamında hem yapılan görüşmeler hem de anketten elde edilen bulgular sonucunda aşağıdakilere ulaşılmıştır:

- Türkiye'de Endüstri 4.0, dijital dönüşümün iç denetim fonksiyonu üzerinde etkisi konusunda farkındalığının olduğu söylenebilir. Fakat kamu ve özel kurum karşılaştırması yapıldığında kurumlarda yararlanılan Endüstri 4.0 teknolojilerinin özel kurumlarda daha fazla yoğunlaştığı görülmektedir.
- Dijital dönüşümün iç denetime yansıması gerçek zamanlı izleme imkanı sunmasıyla ön plana çıkmaktadır.
- Dijitalleşmenin kurumların yeni riskler ile karşılaşmasına ve riskin boyutunun değişmesine sebebiyet verdiğine ulaşılmıştır. Başlıca veri bütünlüğünün sağlanması, kişisel verilerin korunması, bilgi güvenliği, siber güvenlik riskinin ön plan çıktığına ulaşılmıştır. Yaşanan teknolojik gelişmelerin insan gücüne olan ihtiyacın azalmasından kaynaklı bazı iş kollarının yok olma tehlikesi yaşadığı veya mevcut yetkinliğin beklentiyi karşılayamaması diğer önemli riskler arasında görülmektedir.
- Pandeminin bir yansıması olan uzaktan çalışma sürecinin siber güvenlik riskinin ön plana çıkmasında etkili olduğu görülmektedir.
- Kamu ve özel kurumlarda yeni teknolojilere ilişkin müşteri işletmenin (bağımsız denetim kurumları yönünden) ya da kurum yöneticisinin yeni teknoloji kullanımına direnç göstererek alışkanlıklarından vazgeçmemesi iç denetçilerin karşılaştıkları kısıtlamalardan biri olarak görülmektedir.
- Dijital dönüşüm çerçevesinde iç denetim fonksiyonunun öncelikle danışmanlık rolünün ön plana çıktığına ve danışmanlık rolüne ihtiyacın arttığına ulaşılmıştır.
- Danışmanlık rolü çerçevesindeki beklentinin artışında diğer bir etken ise COVID-19 pandemisidir.
- Dijital dönüşüm ile birlikte danışmanlık rolüne ilişkin ihtiyacın artışının iç denetçilerin bağımsızlığını ve tarafsızlığını olumsuz yönde etkilemediğine ulaşılmıştır. Ayrıca kurumlar tarafından üçlü hat modeline uyum

sağlanması halinde iç denetçilerin bağımsızlığının ve tarafsızlığının olumsuz yönde etkilenmeyeceği diğer önemli sonuçlardan biridir.

- Dijital dönüşüm süreci stratejik hedefler arasında yer alması gerektiği ve kurum yapısından insan kaynağına kadar tüm kurum kültürünü kapsayacak şekilde ilerlemesi önemlidir. Kurumlarda dijital dönüşümün bir teknolojinin alınıp kuruma adaptasyonundan öte bir süreç olduğunu göz önünde bulundurarak tüm kurumu kapsayacak yönde strateji belirlenmesi gerekmektedir. Ayrıca iç denetim fonksiyonu, bu süreçte danışmanlık rolü ile yer almalıdır.
- Dijital dönüşüm sürecinde iç denetçilerin kendilerini geliştirmeleri gerektiği, iç denetim mesleğini etkin şekilde icra etmek adına mühendislik ya da iktisadi ve idari bilimler fakültesi kökenli olmalarının bir öneminin olmadığı, kişilerin çapraz fonksiyonlara sahip olması önem arz etmektedir. Diğer önemli konu ise Z kuşağının teknolojiye karşı bakış açısından yararlanarak denetim mesleğine ilişkin ilgilerini çekmenin mesleğin gelişimi açısında önemli nokta olarak görülmektedir.
- Kamu kurumlarında bilgi güvenliğine yönelik iç denetim zorunlu hale gelmiştir ve denetim rehberi şartlarından biri CISA sertifikalı iç denetçi zorunluluğudur. Fakat kamu kurumlarının bu şartı sağlayacak yetkinlikte personele sahip olma konusunda yolun başında oldukları görülmektedir.
- Yasal düzenlemeler çerçevesinde BDDK ve SPK kurumlarının bilgi güvenliğine ilişkin düzenleme ve uygulamalarıyla diğer kamu kurumlarındaki uygulamalara nazaran daha önde olduğu görülmektedir. Esasında kamu kurumlarında bilgi ve iletişim güvenliği denetimi yapılma zorunluluğu gelmeden 2019 yılında bilgi ve iletişim güvenliği rehberinin yayımlanması ile sürece yönelik denetim anlamında gelişmelerin olabileceği yönünde bir işaret olarak nitelendirilebilir. Fakat kurumların şu an denetimi yapacak ve denetim rehberinin şartlarından olan CISA sertifikalı iç denetçilerin olmadığı kamu kurumlarında bilgi ve iletişim güvenliği denetimi kapsamında yolun başında oldukları söylenebilir.

Çalışmanın sonuçlarına göre dijital dönüşümden kaynaklı riskleri etkin yönetmek adına kurumlara, eğitim kurumlarına, iç denetçilere, dijital alanda yetkin çalışanlara ve yöneticilere birtakım görevler düşmektedir. Bunları aşağıdaki şekilde sıralayabiliriz:

- İç denetçiler kurumlarda yeni teknolojinin kuruma kazandıracağı değere yönelik, öncelikle kurum yöneticilerine yönelik farkındalık çalışmaları yaparak teknoloji kullanımına ilişkin direncin ortadan kaldırılmasında ve bir kurum kültürü haline getirilmesinde çalışmalar yürütmelidir. Diğer taraftan bu teknolojinin faydasının yanında getireceği riskleri proaktif yönetmeye yönelik kurumun iç kontrol isteminin etkinliğini değerlendirmek, kurum yöneticilerine süreci etkin yönetmek adına ihtiyaç duyulan iş gücü profili ve ilgili teknolojilere yönelik danışmanlık vermelidir.
- Kurumlar açısından değerlendirme yapılırken iç denetim fonksiyonuna dijitalleşme ile birlikte daha çok ihtiyacın artığı göz önünde bulundurularak, kurum yapısının bu yönde şekillenmesinde adımlar atılmalıdır.
- Kamu kurumlarında ihtiyaç duyulan CISA sertifikasına sahip iç denetçiler, öncelikle diğer kamu kurumlarından veya dışardan sağlanma yolu seçilmesine rağmen kurum kültürüne hakim personel yetkiliğinin kamu kurumları tarafından en kısa sürede sağlanması sürecin etkin yönetilmesi adına yararlı olacaktır.
- Kurum yöneticilerinin gelişen teknolojiye yönelik bakış açılarını geliştirerek kurumun iş yapış şekillerine entegre etmeleri ve bireysel adaptasyonlarını sağlamaları süreçlerin etkin yönetimine yönelik fayda sağlayacaktır.
- Dijital alanda yetkin çalışanlar iç denetim ekiplerinde yer almaları, dijital dönüşümden kaynaklı riskler konusunda danışmanlık ve güvence hizmetlerinin daha etkin yürütülmesi adına yararlı olacak ve ekibi güçlendirecektir.
- Eğitim kurumları gelecek kuşağın dikkatini denetim mesleğine çekmenin yanında dijital dönüşüm karşısında yetkinliğini geliştirecek şekilde çalışmalar yapmalıdır. Bu süreç kurumların karşılaşacağı yetenek yönetim riskinin yönetilmesi açısından da yararlı olacaktır.

Çalışmanın sonuçlarına göre gelecekte yapılabilecek çalışmalar için öneriler aşağıda sıralanmıştır:

- Çalışmada Delphi tekniği kullanılmış olup yapılan bu çalışma farklı veri toplama araçları veya analizleri kullanılarak desenlenebilir.
- Çalışmanın örneklemi özel sektör ağırlıklı olup örneklemin homojen hale getirilmesi ile kamu ve özel sektör karşılaştırması şeklinde yürütülebilir.
- Çalışma özel sektör kapsamında farklı iki sektör seçilerek sektörler arasında farklılıklar ortaya konulabilir.
- Çalışma Türkiye'deki katılımcılar için tasarlanmıştır. Dijital dönüşümden kaynaklı riskler karşısında iç denetim fonksiyonuna önemini ortaya koymak adına akademisyenler, kamu iç denetçileri, bağımsız denetim kurumlarında çalışan iç denetçiler ve mesleki kuruluşlar ile görüşme yapılmıştır. Yurtdışından katılımcıların yer aldığı karşılaştırmalı analiz yapılabilir.
- Araştırma evreninde uluslararası kuruluşların Türkiye temsilciliğinden olan Türkiye İç Denetçiler Enstitüsü, İç Kontrol Enstitüsü ve diğer önemli ulusal kuruluş olan İç Denetim Koordinasyon Kurulu dahil edilmiş olmasına rağmen görüşmeler gerçekleştirilememiştir. Türkiye'de iç denetim adına önemli olan bu kuruluşların gelecek çalışmalarda örnekleme dahil edilmesi ile daha yol gösterici noktalar açığa çıkarılabilir.
- Araştırma hem kamu hem özel kurumları kapsayacak şekilde tasarlanmıştır. Kamu kurumu özelinde dijital dönüşümün süreci ve iç denetimin fonksiyonunun sorumluluğu kapsamında çalışma yapılabilir.
- Kamu ve özel kurumlar kapsamında Endüstri 4.0 teknolojilerinin iç denetim uygulamalarına yansımaları karşılaştırılabilir.

KAYNAKÇA

Ağdeniz, Ş. (2020). İç Denetçiler Neden Makine Öğrenmesi Kullanmak Zorunda? H. Kıral (Editör), *İç Denetim Kuruma Değer Katmak* içinde (s. 15-38). Ankara: Seçkin Yayıncılık.

Ağdeniz, Ş. (2021). Bilgi ve İletişim Güvenliği Denetiminde Kamu İç Denetçilerinin Rolü ve Yetkinliklerine İlişkin Bir Araştırma. *Alanya Akademik Bakış, 5*(2), 525-545.

Ağdeniz, Ş. ve Çetin, C. (2021). Uzaktan İç Denetim ve Uzaktan İç Denetim Sınırlılıkları. *Muhasebe Bilim Dünyası Dergisi*(23(Özel Sayı)), 58-80.

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. *2017 IEEE Technology & Engineering Management Conference (TEMSCON)*, Santa Clara, CA, USA, 8-10 June 2017, pp. 137-141.

Ak, H. (2020). ITIL Nedir ?.https://halisak.medium.com/itil-nedi%CC%87r-e9ec3de68187.(Erişim tarihi:15.11.2021).

Akbaş, A. ve Çarıkçı, O. (2022). Endüstri 4.0'ın Bağımsız Denetçilere Ve Denetim Uygulamalarına Etkisi. *Muhasebe ve Finansman Dergisi*(94), 53-72.

Akçakanat, Ö., Özdemir, O. ve Mazak, M. (2021). İşletmelerde Siber Güvenlik Riskleri ve Bilgi Teknolojileri Denetimi: Bankaların Siber Güvenlik Uygulamalarının İncelenmesi. *Mehmet Akif Ersoy Üniversitesi Uygulamalı Bilimler Dergisi, 5*(2), 246-270.

Akmeşe, S. (2020). Kamuda Dijital Dönüşümün Siber Güvenlik ve Dijital Güvence Boyutları ve İç Denetimin Rolü. *Denetişim Dergisi*(20), 108-119.

Albukhitan, S. (2020). Developing Digital Transformation Strategy for Manufacturing. *Procedia Computer Science (170)*, 664-671.

Aldawood, H. and Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. *In 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, Wollongong, NSW, Australia, 4-7 December 2018, pp. 62-68.

Alina, C. M., Cerasela, S. E. and Gabriela, G. (2018). Internal Audit Role in Artificial Intelligence. *"Ovidius" University Annals, Economic Sciences Series, 18*(1), 441-444.

Allegrini, M. and D'Onza, G. (2003). Internal Auditing and RiskAssessment in Large ItalianCompanies: an Empirical Survey. *International Journal of Auditing, 7*, 1191-208.

Altunışık, R. (2015). Büyük Veri: Fırsatlar Kaynağı Mı Yoksa Yeni Sorunlar Yumağı Mı? *Yıldız Social Science Review, 1*(1), 45-76.

Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain Technology Applications in Health Care. *Circulation: Cardiovascular Quality and Outcomes*,10(9), 1-3.

ASTM. (2010). Standard Terminology for Additive Manufacturing Technologies. https://web.mit.edu/2.810/www/files/readings/AdditiveManufacturingTerminology.pdf. (Erişim tarihi: 17.11.2020).

Atzori, L., Iera, A. and Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*, 2787-2805.

Aydın, A. H. ve Durgun, S. (2017). Yeni Bir Yönetim Anlayışı Olarak Yönetişimin Gelişmesinde Bilgi Edinme Hakkının Önemi. *Eurasian Conference on Language and Social Sciences*, Antalya, Türkiye, (s. 25-37).

Aytekin, A., Erdoğan, Y. ve Kavalcı, K. (2016). Yeni Bir İş Modeli: Muhasebe Alanında Bulut Bilişim. *Uluslararası Yönetim İktisat ve İşletme Dergisi, Özel Sayı*, 46-62.

Babaoğlan, İ. (2019). İşletmeler İçin Dİjital Dönüşüm Yol Haritası. https://www.linkedin.com/pulse/i%C5%9Fletmeler-i%C3%A7in-dijital-d%C3%B6n%C3%BC%C5%9F%C3%BCm-yol-haritasi-irfan-babaoglan/?originalSubdomain=tr. (Erişim tarihi: 9.2.2021).

Bagheri, B., Yang, S., Kao, H.-A. and Lee, J. (2015). Cyber-physical Systems Architecture for Self-Aware Machines in Industry 4.0 Environment. *IFAC PapersOnLine, 48*(3), 1622-1627.

Bahar, M. ve Demir, N. S. (2021). Delphi Tekniği Uygulama Sürecine Yönelik Örnek Bir Çalışma: Çok Fonksiyonlu Tarım Okuryazarlığı. *Bolu Abant İzzet Baysal Üniversitesi Eğitim Fakültesi Dergisi, 21*(1), 35-53.

Bahrin, M. A., Othman, M. F., Azli, N. H. and Talib, M. F. (2016). Industry 4.0: A Revıew On Industrıal Automatıon And Robotıc. *Jurnal Teknologi (Sciences & Engineering), 78*(6-13), 137-143.

Bandyopadhyay, K., Mykytyn, P. P. and Mykytyn, K. (1999). A framework for integrated risk management in information technology. *Management Decision, 37*(5), 437-444.

Banger, G. (2018). *Endüstri 4.0 ve Akıllı İşletme* (2. Baskı). Eskişehir: Dorlion Yayınları.

Bartevyan, L. (2015). *Industry 4.0 – Summary report.* DLG. org. https://www.pac.gr/bcm/uploads/industry-4-0-summary-report.pdf. (Erişim tarihi: 17.10. 2020)

Bayuk, M. N. ve Demir, B. N. (2019). Endüstri 4.0 Kapsaminda Yapay Zekâ ve Pazarlamanin Geleceği. *Journal Of Social, Humanities and Administrative Sciences, 5*(19), s. 781-799.

BDDK. (2021). Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Hakkında Yönetmelik. Bankacılık Düzenleme ve Denetleme Kurumu.(Erişim tarihi: 8.3.2022).

Beck, R. (2018). Beyond Bitcoin: The Rise of Blockchain World. *Computer Publıshed By The IEEE Computer Socıety*, s. 54-58.

Berryman, D. R. (2012). Augmented Reality: A Review. *Medical Reference Services Quarterly, 31*(2), 212-218.

Betti, N. and Sarens, G. (2021). Understanding the internal audit function in a digitalised business environment. *Journal of Accounting & Organizational Change, 17*(2), 197-216.

Betti, N., Sarens, G. and Poncin, I. (2021). Effects of digitalisation of organisations on internal audit activities and practices. *Managerial Auditing Journal, 36*(6), 872-888.

Bilgin, B. Ö. (2016). *Bilgi Teknolojilerinin Denetimi ve Bir Uygulama.* İstanbul: Marmara Üniversitesi, Sosyal Bilimler Enstitüsü.

Bircan, N. G. (2020). İç Denetimde Yapısal Değişim ve Dönüşüm: İç Denetçilerin Farkındalığı ve Beklentileri Üzerine Bir Araştırma. *Muhasebe Enstitüsü Dergisi, 63*, 67-83.

Bolat, S. (2019). *Dördüncü Sanayi Devriminin Lojistik Sektörüne Etkileri: Antalya Bölgesinde Lojistik Faaliyette Bulunan İşletmelerde Bir Araştırma, Yüksek Lisans Tezi.* Antalya: Akdeniz Üniversitesi, Sosyal Bilimler Enstitüsü.

Braudel, F. (1991). *Maddi Medeniyet ve Kapitalizm.* (Çev: M. Özel). İstanbul: Ağaç Yayıncılık.

Brennan, B., Flynn, M. and Baccala, M. (2017). Artificial Intelligence Comes to Financial Statement Audits. https://www.cfo.com/accounting-tax/2017/02/artificial-intelligence-audits/. (Erişim tarihi: 15.4.2021).

Brettel, M., Friederichsen, N., Keller, M. and Rosenberg, M. (2014). How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective. *International Scholarly and Scientific Research & Innovation, 8*(1), 37-44.

Burca, N. (2020). Üçlü Savunma Hattı Modelinde Yapılan Değişiklikler. https://nazifburca.com/2020/08/08/uclu-savunma-hatti-modelinde-yapilan-degisiklikler/ (Erişim tarihi: 6.11. 2021).

Büyükkalaycı, G. ve Karaca, H. M. (2019). Pazarlama 4.0: Nesnelerin Interneti. *Üçüncü Sektör Sosyal Ekonomi Dergisi, 54*(1), 463-477.

Can, E. N. ve Çetin, C. (2019). COSO ERM 2017 Çerçevesinde Kurumsal Risk Yönetiminde İç Denetimin Rolü . *Akademik Sosyal Araştırmalar Dergisi, 6*(41), 153-166.

Cardoso, J., Voigt, K. and Winkler, M. (2008). Service Engineering for the Internet of Services . J. Filipe, & J. Cordeiro (Eds.), *Enterprise Information System* (pp. 15-27). Barcelona: Springer.

Cartlidge, A., Rudd, C., Smith, M., Wigzel, P., Rance, S., Shaw, S. and Wright, T. (2012). *An Introductory Overview of ITIL 2011.* London: itSMF US.

Chambers, R. (2020). *New IIA Three Lines Model Offers Timely Evolution of a Trusted Tool.* Internal Auditor: https://iaonline.theiia.org/blogs/chambers/Pages/New-IIA-Three-Lines-Model-Offers-Timely-Evolution-of-a-Trusted-Tool.aspx. (Erişim tarihi: 15.11.2021).

Chang, S. E. and Lin, C.-S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data, 107*(3), 438-458.

COSO. (2017). *Enterprise Risk Management Integrating with Strategy and Performance Executive Summary.* COSO. https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf. (Erişim tarihi: 21.5.2021).

COSO. (2019). *Mananaging Cyber Risk in Digital Age.* COSO. https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf. (Erişim tarihi: 21.5.2021).

Creswell, J. W. (1999). Mixed-Method Research: Introduction and Application. *Academic Press,* 455-472.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S. and Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. *Applied Inovation Review, 2,* 6-19.

Cyganek, B., Graña, M., Krawczyk, B., Kasprzak, A., Porwik, P., Walkowia, K. and Woźniak, M. (2016). A Survey of Big Data Issues in Electronic Health Record Analysis. *Applıed Artıfıcıal Intellıgence, 30*(6), 497-520.

Çetinkaya, G. (2020). *Dördüncü Sanayi Devriminin Kamu Harcamaları Üzerine Etkisi.* İstanbul: T.C. İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü.

Çolak, F. (2020). NIST Cyber Security Framework Nedir?. https://www.fatihcolak.com.tr/nist-cyber-security-framework-nedir.html. (Erişim tarihi: 15.12.2021).

Dai, J. (2017). Three Essays On Audıt Technology: Audıt 4.0, Blockchaın, And Audıt App. New Jersey: The State University of New Jersey. https://rucore.libraries.rutgers.edu/rutgers-lib/55154/PDF/1/play/ (Erişim tarihi: 9.9.2020).

Dai, J., & Vasarhelyi, M. A. (2016). Imagineering Audit 4.0. *Journal Of Emerging Technologies In Accounting, 13*(1), 1-15.

Dalenogare, L. S., Benitez, G. B. and Ayala, N. F. (2018). The expected contribution of Industry 4.0 technologies for industrial performance. *International Journal of Production Economics, 204*, 383-394.

DDO. (2021). *Bilgi ve İletişim Güvenliği Denetim Rehberi.* Anakara: T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi.

DeHaes, S., Grembergen, W. V. and Debreceny, R. S. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *Journal of Information Systems, 2*(1), 307-324.

Deloitte. (2017a). *Auditing the risks of disruptive technologies Keep the tempo.* Deloitte. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-risk-digitization-banking.pdf. (Erişim tarihi: 12.1.2021).

Deloitte. (2017b). *Cybersecurity and the role of internal audit An urgent call to action.* Deloitte. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-cyber-ia-urgent-call-to-action.pdf. (Erişim tarihi: 20.5.2021).

Deloitte. (2018a). *Auditing the risks of disruptive technologies Internal Audit in the age of digitalization.*https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-rfa-auditing-the-risks-of-disruptive-technologies.pdf. (Erişim tarihi: 8.3.2021)

Deloitte. (2018b). *Internal Audit 3.0 The future of Internal Audit is now.* Deloitte. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Audit/gx-internal-audit-3.0-the-future-of-internal-audit-is-now.pdf. (Erişim tarihi 8.3.2021)

Deloitte. (2018d). *SPK'dan yeni Bilgi Sistemleri düzenlemeleri.* The Deloitte Times. https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/the-deloitte-times/haziran-2018-SPKdan-yeni-bilgi-sistemleri-d%C3%BCzenlemeleri.pdf. (Erişim tarihi: 21.6.2021).

Deloitte. (2018c). *16 Artificial Intelligence projects from Deloitte Practical cases of applied AI.* Deloitte. https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/innovatie/deloitte-nl-innovatie-artificial-intelligence-16-practical-cases.pdf. (Erişim tarihi: 8.5.2021).

Deloitte. (2021). *The social enterprise in a world disrupted Leading the shift from survive to thrive 2021 Deloıtte Global Human Capıtal Trends.* Deloitte.

Demirezen, B. (2019). Artırılmış Gerçeklik Ve Sanal Gerçeklik Teknolojisinin Turizm Sektöründe Kullanılabilirliği Üzerine Bir Literatür Taraması. *Uluslararası Glabal Turizm Araştırmaları Dergisi, 3*(1), 1-26.

Demirkol, Ö. F. ve İkvan, A. (2020). Denetimin Geleceği: Endüstri 4.0'ın Etkisinde Denetimin Yeniden Dizaynı. *Muhasebe ve Finans Araştırmaları Dergis, 2*(1), 55-72.

DEWAN P.N. CHOPRA & CO. (2020). Internal Audıt Update Future Of Internal Audıt. https://www.dpncindia.com/blog/wp-content/uploads/2020/11/Future-of-Internal-Audit-1.pdf. (Erişim tarihi:8.4.2021).

Dilberoglu, U. M., Gharehpapagh, B., Yaman, U. and Dolen, M. (2017). The role of additive manufacturing in the era of Industry 4.0. *Procedia Manufacturing, 11*, 545-554.

Drath, R. and Horch, A. (2014). Industrie 4.0: Hit or Hype? *IEEE Industrial Electronics Magazine, 8*(2), 56-58.

Earley, C. E. (2015). Data analytics in auditing: Opportunities and challenges. *Business Horizon, 58*(5), 493-500.

EBSO. (2015). *Sanayi 4.0 Uyum Sağlamayan Kaybedecek.* İzmir: Ege Bölgesi Sanayi Odası.

Eğilmez, M. (2019). *Tarihsel Süreç İçinde Dünya Ekonomisi* (6. Baskı). İstanbul: Remzi Kitabevi.

Erdoğan, M. (2019). Denetim 4.0 ve Ötesi. *Muhasebe ve Vergi Uygulamaları Dergisi, 12*(3), 809-834.

Ertel, W. (2017). *Introduction to Artificial Intelligence.* Germany: Springer International Publishing.

Erturan, İ. E. ve Ergin, E. (2017). Muhasebe Denetiminde Nesnelerin İnterneti: Stok Döngüsü. *Muhasebe ve Finansman Dergisi*(75), 13-30.

Erturan, İ. ve Ergin, E. (2018). Dijital Denetim ve Dİjital İkiz Yönetimi. *Muhasebe Bilim Dünyası Dergisi, 20*(4), 810-830.

Etikan, l. and Abubakar, S. (2017). Sampling and Sampling Methods. *Biometrics & Biostatistics International Journal, 5*(6), 1-3.

EY. (2020). *EY Türkiye Üçüncü Taraf Kaynaklı Teknoloji ve Siber Risk Yönetimi Değerlendirme Raporu.* Ernst & Young Global Limited. https://assets.ey.com/content/dam/ey-sites/ey-com/tr_tr/pdf/2020/11/ucuncu-taraf-kaynakli-teknoloji-ve-siber-risklerinizi-nasil-yonetiyorsunuz. (Erişim tarihi: 12.1.2021).

Feiner, S. K. (2002). Augmented Reality: A New Way of Seeing. *JSTOR, 286*(4), 48-55.

Ferhat, S. (2016). Dijital Dünyanın Gerçekliği, Gerçek Dünyanın Sanallığı Bir Dijital Medya Ürünü Olarak Sanal Gerçeklik. *TRT Akademi, 2*(1), 724-746.

Firican, G. (2017). The 10 Vs of Big Data. https://tdwi.org/articles/2017/02/08/10-vs-of-big-data.aspx. (Erişim tarihi: 10.11.2020)

Freina, L. and Ott, M. (2015). A Literature Review on Immersive Virtual Reality in Education: State Of The Art and Perspectives. *The international scientific conference elearning and software for education, 1*(133), 100-1007.

Frenehard, T. (2020). GRC Tuesdays: Internal Audit 4.0. https://blogs.sap.com/2020/08/18/grc-tuesdays-internal-audit-4.0/(Erişim tarihi: 8.3.2021)

Furtuna, C. and Cıucıoı, A. (2019). Internal Audit in the Era of Continuous Transformation. Survey of Internal Auditors in Romania. *Audit Financiar, 3*(155), 452-472.

Fülberth, G. (2011). *Kapitalizmin Kısa Tarihi.* (Çev: S. Usta) İstanbul: e-Kitap, Yordam Kitap. http://eds.a.ebscohost.com/eds/ebookviewer/ebook?sid=517e15fa-86e3-

4ff9-968e-c433b9561f40%40sdc-v-sessmgr01&vid=0&format=EB (Erişim Tarihi: 19.10.2021

Galloway, R. (1999). *Desıred Characterıstıcs Of Park And Recreatıon Executıve Board Members: A Delphı Study.* Texas A&M University.

Gartner. (2013). Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three "V"s. https://blogs.gartner.com/svetlana-sicular/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/. (Erişim tarihi: 5.11.2020)

Gerhardt, B., Griffin, K. and Klemann, R. (2012). *Unlocking Value in the Fragmented World of Big Data Analytics.* Cisco Internet Business Solutions Group.

Ghanoum, S., & Alaba, F. M. (2020). *Integration of Artificial Intelligence in Auditing: The Effect on Auditing Process.* Kristianstad, Kristianstad University, Faculty of Business.

Ghobakhloo, M. (2020). Industry 4.0, digitization, and opportunities for sustainability. *Journal of Cleaner Production, 252*, 1-21.

Gracht, H. A. and Darkow, I.-L. (2010). Scenarios for the logistics services industry: A Delphi-based analysis for 2025. *Internationa Journal of Production Economics, 127*, 46-59.

Green, B., Jones, M., Hughes, D. and Williams, A. (1999). Applying the Delphi technique in a study of GPs' information requirements. *Health & social care in the community*, *7*(3), 198-205.

Grisham, T. (2009). The Delphi technique: a method for testing complex and multifaceted topics. *International Journal of Managing Projects in Business, 2*(1), 112-130.

GTAI. (2014). *Industries 4.0-Smart Manufacturing for the Future.* Berlin: GTAI (Germany Trade & Invest).

Güler, A., & Arkın, A. K. (2019). Siber Hijyenin Sağlanmasında İç Denetimin Rolü. *Denetişim Dergisi, 9*(19), 17-40.

Güler, E. (2018). Endüstri 4.0'ın Muhasebe ve Denetim Mesleğine Etkileri. *Akademik Sosyal Araştırmalar Dergisi, 6*(78), 522-531.

Güngör, N. (2021). *İç Denetimde Bilgi Teknolojileri Ve Siber Güvenlik: Borsa İstanbul Şirketlerinde Bir İnceleme.* İstanbul: İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü.

Gür, N., Ünay, S. ve Dilek, Ş. (2017). *Sanayiyi Yeniden Düşünmek Küresel Teknolojik Dönüşümün Dünya ve Türkiye Ekonomisine Yansımaları.* İstanbul: Turkuvaz Haberleşme ve Yayıncılık.

Gürbüz, S. ve Şahin, F. (2018). *Sosyal Bilimlerde Araştırma Yöntemleri Felsefe-Yöntem-Analiz.* Ankara: Seçkin Yayıncılık.

Gürel, U. (2020). Bilgi Sistemleri Güvenliği ve Etik Konular. N. Sağlam, & Ö. Oktal (Editörler), *İşletme Bilgi Sistemleri* içinde (s. 215-226). Eskişehir: Anadolu Üniversitesi.

Hadı, H. J., Shnaın, A. H., Hadıshaheed, S. and Ahmad, A. H. (2015). Big Data and Five V's Characteristics. *International Journal of Advances in Electronics and Computer Science, 2*(1), 16-23.

Haes, S. D., Grembergen, W. V., Joshi, A. and Huygh, T. (2020). *Enterprise Governance of Information Technology Achieving Alignment and Value in Digital Organizations* (Third Edition). Switzerland: Springer.

Haller, S., Karnouskos, S. and Schroth, C. (2008). The Internet of Things in an Enterprise Context. J. Domingue, D. Fensel, & P. Traverso (Eds.), *First Future Internet Symposium* (pp. 14-28). Berlin: Springer.

Hasson, F., Keeney, S. and McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing, 32*(4), 1008-1015.

HBR. (2020). *The Necessity of Cyber Risk Quantification.* PWC. https://hbr.org/resources/pdfs/comm/pwc/TheNecessityofCyberRiskQuantification.pdf. (Erişim tarihi: 22.10.2021).

Heinonen, S., Karjalainen, J. and Ruotsalainen, J. (2015). *Towards The Thırd Industrıal Revolutıon Neo-Carbon Energy Futures Clinique.* Filandiya: Finland Futures Research Centre, e-Kitap.

Hermann, M., Pentek, T. and Otto, B. (2016). Design Principles for Industrie 4.0 Scenarios: A Literature Review. *49th Hawaii International Conference on System Sciences* Koloa, HI, USA, 2016, pp. 3928-3937.

Hu, L., Ngoc-TuNguyen, WenjinTao, C.Leu, M., FrankLiu, X., RakibShahriar, M. and Nahian Al Sunny, S. M. N.A (2018). Modeling of Cloud-Based Digital Twins for Smart Manufacturing with MTConnect. *Procedia Manufacturing, 26*, 1193-1203.

Huang, S. H., Liu, P., Mokasdar, A. and Hou, L. (2013). Additive manufacturing and its societal impact: a literature review. *The International Journal of Advanced Manufacturing Technology*, *67*(5), 1191-1203.

IIA. (2016a). *Assessing Cybersecurity Risk Roles of the Three Lines of Defense.* IIA-Global Technologies Audit Guide (GTAG).

IIA. (2016b). *Güvenilir Bir Siber Danışman Olarak İç Denetim.* IIA.

IIA. (2017a). *Mesleki Uygulama Çerçevesi Kapsamında Uluslararası İç Denetim Standartları (Standartlar).* The Institute Of Internal Auditors. https://www.theiia.org/globalassets/documents/standards/standards-2017/ippf-standards-2017-turkish.pdf. (Erişim tarihi: 15.2.2021).

IIA. (2017b). *Artificial Intelligence: The Future for Internal Auditing.* IIA. https://global.theiia.org/knowledge/Public%20Documents/Tone-at-the-Top-December-2017.pdf. (Erişim tarihi: 15.2.2021).

IIA. (2018a). *2018 Global Risk Raporu İç Denetim Yöneticilerinin Karşılaştıkları En Büyük Riskler.* The Institute of Internal Auditors.

IIA. (2018b). *Yıkıcı Dönüşüm Çağında İç Denetim.* IIA.

IIA. (2019). *Sürekli Değişen Denetim Evreninde Yetenek Yönetiminin İyileştirilmesi.* Florida-ABD: IIA.

IIA. (2020a). *Üçlü Hat Modeli – Her Kurumun Başarısı için Önemli Bir Araç.* IIA. https://na.theiia.org/translations/PublicDocuments/GPI-Three-Lines-Model-Turkish.pdf. (Erişim tarihi: 22.10.2021).

IIA. (2020b). *IIA'nın Üçlü Hat Modeli-Üçlü Savunma Hattı ile ilgili güncelleme.* Florida-USA: IIA.

IIA. (2020c). *OnRisk 2021: A Guide to Understanding, Aligning and Optimizing Risk.* The Institute of Internal Auditors.

IIA. (2021). *OnRisk 2022: A Guide to Understanding, Aligning and Optimizing Risk 2022.* The Institute of Internal Auditors.

International Organization for Standardization. (2012). ISO/IEC 27032:2012 Information technology -Security techniques -Guidelines for cybersecurity. https://www.iso.org/standard/44375.html (Erişim tarihi: 10.10.2022).

International Organization for Standardization. (2017). SO/IEC 27003:2017 Information technology- Security techniques - Information security management systems - Guidance. https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-2:v1:en (Erişim tarihi: 10.10.2022).

International Organization for Standardization. (2020). ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection-Guidelines for information security management systems auditing. https://www.iso.org/standard/77802. (Erişim tarihi: 10.10.2022).

International Organization for Standardization. (2022a). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/82875.(Erişim tarihi: 10.11.2022).

International Organization for Standardization. (2022b). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. https://www.iso.org/standard/75652.(Erişim tarihi: 10.11.2022).

International Organization for Standardization. (2022c). ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks. https://www.iso.org/standard/80585. (Erişim tarihi: 10.11.2022).

ISACA. (2019). *COBIT 2019 Çerçevesi: Giriş ve Metodoloji.* Ankara: ISACA. https://isaca-ankara.org/wp-content/uploads/2019/12/COBIT-2019-Cercevesi-Giris-ve-Metodoloji-ISACA-Ankara-Chapter.pdf. (Erişim adresi: 20.5.2021).

Islam, M. S., Farah, N. and Stafford, T. F. (2018). Factors associated with security/ cybersecurity audit by internal audit function An international study. *Managerial Auditing Journal, 33*(4), 377-409.

Ismail, M. H., Khater, M., & Zaki, M. (2017). Digital Business Transformation and Strategy: What Do We Know So Far?, University of Cambridge, Cambridge Service Alliance, https://cambridgeservicealliance.eng.cam.ac.uk/system/files/documents/2017NovPaper_Mariam.pdf. (Erişim tarihi: 9.2.2021).

İşgüden, B. (2012). *Bilgi Teknolojilerinin İç Denetimde Yarattığı Değişimler ve İç Denetim Birimlerinin Değişimleri Değerlendirmesine Yönelik İMKB–100 İşletmelerinde Bir Uygulama.* Eskişehir: Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü.

Ivanov, S. H. (2017). Robonomics - Principles, Benefits, Challenges, Solutions. *Yearbook of Varna University of Management, 10,* 283-293.

Jazdi, N. (2014). Cyber Physical Systems in the Context of Industry 4.0. *IEEE International Conference on Automation, Quality and Testing, Robotics(AQTR),* Cluj-Napoca, Romania, 22-24 May 2014, pp. 1-4.

Jia, X., Feng, Q., Fan, T. and Lei, Q. (2012). RFID Technology and Its Applications in Internet of Things (IOT). *2nd International Conference on Consumer Electronics, Communications and Networks (CECNet),* Yichang, China, 21-23 April 2012, pp. 1282-1285.

Kabaklarlı, E. (2016). *Endüstri 4.0 ve Paylaşım Ekonomisi -Dünya ve Türkiye Ekonomisi İçin Fırsatlar, Etkiler ve Tehditler.* İstanbul: Nobel Bilimsel Eserler.

Kablan, A. (2018). Endüstri 4.0, "Nesnelerin İnterneti" - Akıllı İşletmeler ve Muhasebe Denetimi. *Süleyman Demirel Üniversitesi, 23*, 1561-1579.

Kagermann, H., Walhster, W. and Helbig, J. (2013). *Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0.* Forschungsunion.

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

Kahyaoğlu, S. B., & Aksoy, T. (2021). Artificial Intelligence in Internal Audit and Risk Assessment. Ü. Hacıoğlu, & T. Aksoy (Eds.), *Financial Ecosystem and Strategy in the Digital Era Global Approaches and New Opportunities* (s. 179-192). Cham, Switzerland: Springer.

Kalbandi, I. and Anuradha, J. (2015). A Brief Introduction on Big Data 5Vs Characteristics and Hadoop Technology. *Procedia Computer Science, 48*, 319-324.

Karacaoğlu, Ö. C. (2009). İhtiyaç analizi ve delphi tekniği; öğretmenlerin eğitim ihtiyacını belirleme örneği. *I. Uluslararası Eğitim Araştırmaları Konferansı*, (s. 1-20). Çanakkale. http://www.eab.org.tr/eab/2009/cd.php. (Erişim tarihi: 2.2.2022).

Karahan, Ç. ve Tüfekçi, A. (2019). Blokzincir Teknolojisinin İç Denetim Faaliyetlerine Etkileri: Fırsatlar Ve Tehditler. *Denetişim Dergisi, 9*(19), 55-72.

Karakaya, E. ve Karakaya, G. (2017). Developing a Risk Management Framework and Risk Assessment for Non-profit Organizations: A Case Study. *In Risk Management, Strategic Thinking and Leadership in the Financial Services Industry*, 297-308.

Karakaya, G. (2018). COSO Kurumsal Risk Yönetimi - Riskin Strateji Ve Performansla Uyumlaştırılmasına İlişkin Düzenleme Çerçevesinde Getirilen Güncellemeler. *Denetişim, 8*(18), 15-22.

Kavzaoğlu, T. ve Şahin, E. K. (2012). Bulut Bilişim Teknolojisi ve Bulut CBS Uygulaması. *IV. Uzaktan Algılama ve Coğrafi Bilgi Sistemleri Sempozyumu*, Zonguldak, (s. 1-9).

Kaya, B. (2018). Dijital Dönüşümde İç Denetçilerin Rol ve Sorumlulukları: https://bertankaya.net/2018/06/dijital-donusumde-ic-denetcilerin-rol-ve-sorumluluklari/ (Erişim tarihi: 9.2.2021).

Kesbiç, Ö. Ö. (2020). *Üretimde Dijital Dönüşüm Ve Etkileri: Türkiye Ekonomisi Açısından Bir Analiz*, Yüksek Lisans Tezi. Manisa: Manisa Celal Bayar Üniversitesi, Sosyal Bilimler Üniversitesi.

Keser, A. D. (2018). *An Investıgatıon On The Exıt Crıterıa Of Englısh Language Preparatory Programs Of Turkısh Unıversıtıes: A Delphı Method Analysıs.* Eskişehir: Anadolu University, Graduate School of Educational Sciences.

Khan, M. A.-u.-d., Uddin, M. F. and Gupta, N. (2014). Seven V's of Big Data Understanding Big Data to extract Value. *Proceedings of 2014 Zone 1 Conference of the American Society for Engineering Education,* Bridgeport, CT, USA, 2014, pp. 1-5.

Khan, R., Khan, S. U., Zaheer, R. and Khan, S. (2012). Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. *10th International Conference on Frontiers of Information Technology*, Islamabad, Pakistan, 17-19 December 2012, (pp. 257-260).

Khayun, V., Ractham, P. and Firpo, D. (2012). Assessing E-Excise Sucess with Delone and McLean's Model. *Journal of Computer Information Systems, 52*(3), 31-40.

Klein, M. (2020). İşletmelerin Dijital Dönüşüm Senoryaları-Kavramsal Bir Model Önerisi. *Elektronik Sosyal Bilimler Dergisi, 19*(74), 997-1019.

Kounavis, C. D., Kasimati, A. E. and Zamani, E. D. (2012). Enhancing the Tourism Experience through Mobile Augmented Reality: Challenges and Prospects. *International Journal of Engineering Business Management, 4*, 1-6.

Köse, H. Ö. ve Polat, N. (2021). Dijital Dönüşümün Denetimin Geleceğine Etkisi. *Sayıştay Dergisi, 32*(123), 9-41.

KPMG. (2013). *Bilgi Teknolojileri Yönetişimi İçin Yeni Bir Adım: COBIT 5.* KPMG. https://assets.kpmg/content/dam/kpmg/pdf/2016/06/tr-kpmg-gundem-13-cobit-5.pdf. (Erişim tarihi:12.3.2021)

KPMG. (2017). *IT Internal Audit: Multiplying risks amid scarce resources.* Switzerland: KPMG.https://assets.kpmg/content/dam/kpmg/ch/pdf/it-internal-audit-en.pdf. (Erişim tarihi: 15.4.2021)

KPMG. (2018). *SPK Bilgi Sistemleri Mevzuatı.* https://assets.kpmg.com/content/dam/kpmg/tr/pdf/2018/03/spk-bilgi-sistemleri-mevzuati.pdf. (Erişim tarihi: 21.6.2021).

KPMG. (2020). *Üçüncü Taraf Risk Yönetimi'ne Bakış 2020.* Türkiye: KPMG. https://assets.kpmg/content/dam/kpmg/tr/pdf/2020/12/ucuncu-taraf-risk-yonetimine-bakis-2020.pdf. (Erişim tarihi: 12.1.2021).

KPMG. (2022). *Third-Party Risk Management Outlook 2022*. KPMG International Cooperative. https://assets.kpmg/content/dam/kpmg/xx/pdf/2022/01/third-party-risk-management-outlook-2022.pdf. (Erişim tarihi: 12.12.2022).

KUKA. (2017). *Sensitive robotics_LBR iiwa.* https://www.kuka.com/-/media/kuka-downloads/imported/9cb8e311bfd744b4b0eab25ca883f6d3/kuka_lbr_iiwa_ja.pdf?rev=fd7ba98b190141a48a0ba25788f0ada3. (Erişim tarihi: 12.11.2020)

Kupec, V. (2017). Digital Possibilities of Internal Audit. *Acta VSFS, 11*(1), 28-44.

Kurt, G., ve Uysal, T. U. (2015). Siber Riskler ve COSO İç Kontrol Bütünleşik Çerçevesi. *Muhasebe ve Denetime Bakış, 15*(46), 1-10.

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

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M. and Hohler, B. (2013). Employees' Information Security Awareness and Behavior: A Literature Review. *46th Hawaii International Conference on System Sciences*, Wailea, HI, USA, 7-10 January 2013, pp. 2978-2987.

Lee, B., Michaloski, J., Proctor, F., Venkatesh, S., & Bengtsson, N. (2010). MT Connect-Based Kaizen For Machıne Tool Processes. *Proceedings of ASME 2010 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference*, Montreal, Quebec, Canada, 15-18 August 2010, (pp. 1183-1190).

Lee, C. K., Zhang, S. Z. and Ng, K. K. (2017). Development of an Industrial Internet of Things Suite For Smart Factory Towards Re-industrialization. *Advances in Manufacturing, 5*, 335-343.

Lee, G. M. and Crespi, N. (2010). Shaping Future Service Environments with the Cloud and Internet of Things: Networking Challenges and Service Evolution. T. Margaria, & B. Steffen (Eds.), *Leveraging Applications of Formal Methods, Verification, and Validation* (pp. 399-410). Berlin: Springer.

Lee, G. M., Crespi, N., Choi, J. K. and Boussard, M. (2013). Internet of Things. E. Bertin, N. Crespi, & T. Magedanz (Eds.), *Evolution of Telecommunication Services* (pp. 257-282). Berlin: Springer.

Lee, G.-Y., Kim, M., Quan, Y.-J., Kim, M.-S., Kim, T. J., Yoon, H.-S., Min, S., Kim, D. H., Mun, J. W., Oh, J. W., Choi, n G., Kim, C. S., Chu, W. S., Yang, J., Bhandari, B.,; Lee, C. M., Ihn, J.-B. and Ahn, S.-H. (2018). Machine health management in smart factory: A review. *Journal of Mechanical Science and Technology, 32*(3), 987-1009.

Lee, I. and Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*, 431-440.

Lee, J., Bagheri, B. and Kao, H.-A. (2015). A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters, 3*, 18-23.

Lois, P., Drogalas, G., Karagiorgos, A. and Tsikalakis, K. (2020). Internal audits in the digital era: opportunities risks and challenges. *EuroMed Journal of Business, 15*(2), 205-217.

Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A. and Vrontis, D. (2021). Internal auditing and cyber security: audit role and procedural contribution. *Int. J. Managerial and Financial Accounting, 13*(1), 25-46.

Loughlin K.and Moore L. (1979) Using Delphi to achieve congruent objectives and activities in a pediatrics department. *Journal of Medical Education* 54(2), 101-106.

Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration, 6*, 1-10.

Macmillan, T. T. (1971). The Delphi Technique. *Paper presented at the annual meeting of the California Junior Colleges Associations Committee on Research and Development*, 1-24.

Matt, C., Hess, T., & Benlian, A. (2015). Digital Transformation Strategies. *Business & Information Systems Engineering, 57*(5), 339-343.

Mell, P. and Grance, T. (2011). *The NIST Definition of Cloud Computing.* Gaithersburg: NIST.

Mervelito, M. A., Lintang, B. A. and Adri, A. (2021). Internal Auditing Paradigm Shift: From Traditional Audits to Audits in the 4.0 Industry Era. *International Journal of Innovative Science and Research Technology, 6*(3), 56-63.

Meva, D. (2018). Issues and Challenges with Blockchain: A Survey. *International Journal of Computer Sciences and Engineering, 6*(12), 488-491.

Mohajan, H. (2020). The Second Industrial Revolution has Brought Modern Social and Economic Developments. *Journal of Social Sciences and Humanities, 6*(1), 1-14.

Mokyr, J. and Strotz, R. H. (1998). The Second Industrial Revolution, 1870-1914. https://faculty.wcas.northwestern.edu/jmokyr/castronovo.pdf. (Erişim tarihi: 19.10.2020)

Mollaoğulları, B. F. ve Özdoğan, B. (2018). İletişim Teknolojilerindeki Gelişmeler, Riskler ve İç Denetimin Rolü. *Yönetim ve Ekonomi Dergisi, 25*(3), 625-639.

Monostori, L., Kadar, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Shin W. and Ueda, K. (2016). Cyber-physical systems in manufacturing. *CIRP Annals - Manufacturing Technology, 63*, 621-641.

Morgan, J. (2016). The One Thing AI And Automation Cannot Take Away From Us: https://medium.com/jacob-morgan/the-one-thing-ai-and-automation-cannot-take-away-from-us-a76519f17829. (Erişim tarihi: 8.4.2021)

Mrugalska, B. and Wyrwicka, M. K. (2017). Towards Lean Production in Industry 4.0. *7th International Conference on Engineering, Project, and Production Management, 182*, 466-473.

MÜSİAD. (2017). *Endüstri 4.0 ve Geleceğin Lojistik.* İstanbul: Müstakil Sanayıcı Ve İşadamları Derneği.

Nair, B. (2022). The Evolution of Internal Audit in a Digital-First Environment. https://www.isaca.org/resources/news-and-trends/industry-news/2022/the-evolution-of-internal-audit-in-a-digital-first-environment. (Erişim tarihi: 25.10.2022).

NIST. (2013). *Foundations for Innovation in Cyber-Physical Systems Workshop Report.* Columbia: National Institute of Standards and Technology.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.(Erişim tarihi: 21.5.2021).

Nworie, J. (2011). Using the Delphi Technique in EducationalTechnology Research. *TechTrends, 55*(5), 24-30.

Ocak, H. S. (2021). *İç Denetimin Gelişen ve Değişen Dünyasında: Siber Güvenlik ve Denetimi.* İstanbul: Marmara Üniversitesi, Sosyal Bilimler Enstitüsü.

Okoli, C. and Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & Managemen, 42*, 15-29.

O'Leary, D. E. (2013). Bıg Data','Internet Of Thıngs'and'Internet Of Sıgns. *Intellıgent Systems In Accountıng, Fınance And Management, 20*(1), 53-65.

Opoku, A. and Ahmed, V. (2013). Understanding Sustainability: A View from Intra-organizational Leadership within UK Construction Organizations. *International Journal of Architecture Engineering and Construction, 2*(2), 133-143.

Osborne, J., Collins, S., Ratcliffe, M., Millar, R. and Duschl, R. (2003). What ''Ideas-about-Science'' Should Be Taught in School Science? A Delphi Study of the Expert Community. *Journal Of Research In Scıence Teachıng, 40*(7), 692-720.

Oussous, A., Benjelloun, F.-Z., Lahcen, A. A. and Belfkih, S. (2018). Big Data technologies: A survey. *Journal of King Saud University – Computer and Information Sciences, 30*, 431-448.

Özbilger, H. İ. (2021). İç Denetime Yeni Bir Bakış: Üçlü Hat Modelinin Değerlendirilmesi. *Denetişim Degisi, 11*(21), 40-54.

Özsoy, K. ve Duman, B. (2017). Eklemeli İmalat (3 Boyutlu Baskı) Teknolojilerinin Eğitimde Kullanılabilirliği. *Internatıonal Journal Of 3d Prıntıng Technologıes And Dıgıtal Industry, 1*(1), 36-48.

Öztürk, M. S. (2018). Siber Saldırılar, Siber Güvenlik Denetimleri Ve Bütüncül Bir Denetim Modeli Önerisi. *Muhasebe ve Vergi Uygulamaları Dergisi*(10. Yıl Özel Sayı), 208-232.

Pereira, A. C. and Romero, F. (2017). A review of the meanings and the implications of the Industry 4.0 concept. *Procedia Manufacturing, 13,* 1206-1214.

Philbeck, T. and Davis, N. (2018). The fourth industrial revolution: Shaping A New Age. *Journal of International Affairs, 72*(1), 17-22.

Pop, A. M. (2020). New perspectives on the priorities and challenges of the internal audit function. *Studia UBB Negotia, 65*(1), 47-68.

PWC. (2015). *Dijitalleşen İç Denetim.* https://www.pwc.com.tr/tr/risk-surec-teknoloji-hizmetleri/assets/ic-denetim-ve-kontrol-hizmetleri/dijitallesen-ic-denetim.pdf. (Erişim tarihi: 20.5.2021).

PWC. (2018a). *SPK Bilgi Sistemleri Tebliğleri.* https://www.pwc.com.tr/tr/Hizmetlerimiz/denetim/bilgi-teknolojileri-risk-hizmetleri/spknin-bilgi-sistemleri-tebligleri-yururluge-girdi/spk-bilgi-sistemleri-tebligleri-2018.(Erişim tarihi: 21.6.2021).

PWC. (2018b). *GL.ai PwC's anomaly detection for the general ledger.* https://www.pwc.com/m1/en/events/socpa-2020/documents/gl-ai-brochure.pdf. (Erişim tarihi: 15.4.2021).

Qina, J., Liua, Y. and Grosvenor, R. (2016). A Categorical Framework of Manufacturing for Industry 4.0 and Beyond. *Changeable, Agile, Reconfigurable & Virtual Production, 52,* 173-178.

Rad, C.-R., Hancu, O., Takacs, I.-A. and Olteanu, G. (2015). Smart Monitoring of Potato Crop: A Cyber-Physical System Architecture Model in the Field of Precision Agriculture. *Agriculture and Agricultural Science Procedia, 6,* 73-79.

Rakipi, R., Santis, F. D. and D'Onza, G. (2021). Correlates of the internal audit function's use of data analytics in the big data era: Global evidence. *Journal of International Accounting, Auditing and Taxation, 42,* 1-12.

Rasgen, M. ve Gönen, S. (2019). Endüstri 4.0 ve Muhasebenin Dijital Dönüşümü. *Manas Sosyal Araştırmalar Dergisi, 8*(3), 2898-2917.

Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M. (2018). On blockchain and its integration with IoT.Challenges and opportunities. *Future Generation Computer Systems, 88,* 173-190.

Rosa, R., Rahayu, S., Yudi Y. and Gowon, M. (2021). Internal Auditor Transformation Strategy in the Industrial Revolution 4.0 Era: Literature Review. *LePALISSHE*. Malang, Indonesia.

Rowe, G. and Wright, G. (2001). Expert Opinions in Forecasting: The Role of the Delphi Technique. J. S. Armstrong (Ed.), *Principles Of Forecasting: A Handbook for Researchers and Practitioners* (s. 125-144). USA: Kluwer Academic Publishers.

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P. and Harnisch, M. (2015). Industry 4.0: The future of productivity and growth in manufacturing industries. *Boston Consulting Group, 9*(1), 54-89.

Sabuncu, B. (2018). İç Denetim Anlayışındaki Değişiklikler ve Gelişmeler. *Muhasebe Bilim Dünyası*(20 (Özel Sayı)), 779-789.

Sağlam, N., & Orhan, A. (2020). Sistem Geliştirme. N. Sağlam, & Ö. Oktal (Editörler), *İşletme Bilgi SİstemleriI* içinde (s. 191-206). Eskişehir: Anadolu Üniversitesi.

Sahibudin, S., Sharifi, M. and Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. *2008 Second Asia International Conference on Modelling & Simulation (AMS),* Kuala Lumpur, Malaysia, 13-15 May 2008, (pp. 749-753).

Saldı, M. H. (2022). *The Cyber Securıty Governance By Internal Audıt In The Turkısh Bankıng Sector.* Eskişehir: Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü.

Salkin, C., Oner, M., Ustundag, A., & Cevikcan, E. (2018). A Conceptual Framework for Industry 4.0. E. Cevikcan & Alp Ustundag (Eds.), *Industry 4.0: Managing The Digital Transformation* (pp. 3-24). Switzerland: Springer International Publishing.

Schoemaker, P. J., Heaton, S. and Teece, D. (2018). Innovation, Dynamic Capabilities, and Leadership. *California Management Review, 61*(1), 15-42.

Schuh, G., Potente, T., Wesch-Potente, C., Weber, A. R. and Prote, J.-P. (2014). Collaboration Mechanisms to increase Productivity in the Context of Industrie 4.0. *Procedia CIRP, 19,* 51-56.

Schwab, K. (2016). *Dördüncü Sanayi Devrimi.* (Çev:Z. Dicleli). İstanbul:Optimist Yayın.

Schwab, K., & Davıs, N. (2019). *Dördüncü Sanayi Devriminin Şekillendirilmesi.* (Çev: N. Özata). İstanbul: Optimistik Yayıncılık.

Selimoğlu, S. K. ve Saldı, H. M. (2022). Türk Bankacılık Sektöründe İç Denetim Yoluyla Siber Güvenlik Yönetişimi. *İşletme Akademisi Dergisi, 3*(2), 161-187.

Selimoğlu, S. K. ve Saldı, M. H. (2019). İşletmelerde Siber Risklerin Analizinde, Haritalanmasında Ve Değerlendirilmesinde İç Denetimin Rolü. *Muhasebe ve Denetime Bakış, 57*, 1-18.

Selimoğlu, S. ve Altunel, M. (2019). Siber Güvenlik Risklerinden Korunmada Köprü ve Katalizör Olarak İç Denetim. *Denetişim Dergisi*(19), 5-16.

Seyrek, İ. H. (2011). Bulut Bilişim: İşletmeler için Fırsatlar ve Zorluklar. *Gaziantep Üniversitesi Sosyal Bilimler Dergisi, 10*(2), 701-713.

Shrouf, F., Ordieres, J. and Miragliotta, G. (2014). Smart Factories in Industry 4.0: A Review of the Concept and of Energy Management Approached in Production Based on the Internet of Things Paradigm. *IEEE International Conference on Industrial Engineering and Engineering Management*, 697-701.

Simons, S., Abe, P. and Neser, S. (2017). Learning in the AutFab – the fully automated Industrie 4.0 learning factory of the University of Applied Sciences Darmstadt. *Procedia Manufacturing, 9*, 81-88.

Smart, J., Cascio, J., & Paffendorf, J., Bridges, C., Hummel, J., Hursthouse, J. and Moss, R. (2007). A Cross-Industry Public Foresight Project. *Metaverse Roadmap Pathways to the 3D Web*., 1-28

Soğuksu, Z. Y. (2020). Muhasebe Denetiminde Dijital Dönüşüm: Denetim Yazılımları. *Muhasebe ve Vergi Uygulamaları Dergisi, 13*(2), 281-308.

SPK. (2018). Bilgi Sistemleri Bağımsız Denetim Tebliği. Sermaya Piyasası Kurulu. https://www.resmigazete.gov.tr/eskiler/2018/01/20180105-8. (Erişim tarihi: 21.6.2021).

SPK. (2018). Bilgi Sistemleri Yönetimi Tebliği. Sermaya Piyasası Kurulu. https://www.resmigazete.gov.tr/eskiler/2018/01/20180105-9. (Erişim tarihi: 21.6.2021).

Stancioiu, A. (2017). The Fourth Industrial Revolution 'Industry 4.0'. *Fiabilitate si Durabilitate , 1*(19), 74-78.

Şahin, A. (2017). *Akıllı üretim çağı: Endüstri 4.0.* Fortune: http://www.fortuneturkey.com/akilli-uretim-cagi-endustri-40-42841. (Erişim tarihi: 11.11.2020)

Şahin, A. E. (2001). Egitim Araştırmalarında Delphi Tekniği ve Kullanımı. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi, 20*, 215-220.

Şentürk, Ö. (2021). Türkiye'de İç Denetim Faaliyetlerinde Dijital Dönüşüm ve Dijital Dönüşümün Önemi. *TİDE Academia Research, 3*(2), 157-186.

Tang, F., Norman, C. S. and Vendrzyk, V. P. (2017). Exploring perceptions of data analytics in the internal audit function. *Behaviour & Information Technology, 36*(11), 1125-1136.

Taş, H. Y. (2018). Dördüncü Sanayi Devrimi'nin (Endüstri 4.0) Çalışma Hayatına ve İstihdama Muhtemel Etkileri. *luslararası Toplum Araştırmaları Dergisi, 9*(16), 1818-1836.

Tiberius, V. and Hirth, S. (2019). Impacts of digitization on auditing: A Delphi study for Germany. *Journal of International Accounting, Auditing and Taxation, 37*, 1-14.

Tok, O. (2019). *Muhasebe Denetiminde Bilgi Teknolojilerinin Kullanımı Üzerine Bir Araştırma.* Kayseri: Erciyes Üniversitesi, Sosyal Bilimler Enstitüsü.

Turan, Y. (2020). *Dijital dönüşümün bankacılık sektörü iç denetim süreç mekanizmaları üzerindeki etkisi ve vaka analizi.* İstanbul: Bahçeşehir Üniversitesi, Sosyal Bilimler Enstitüsü.

Türnüklü, A. (2000). Eğitimbilim Araştırmalarında Etkin Olarak Kullanılabilecek Nitel BirAraştırma Tekniği: Görüşme. *Kuram ve Uygulamada Eğitim Yönetimi, 24*, 543-559.

Ucoglu, S. (2020). Current Machıne Learnıng Applıcatıons In Accountıng And Audıtıng. *Istanbul Finance Congress, Istanbul, Turkey, 5-6 November 2020,* (pp. 1-7). Press Academia Procedia.

Uzun, A. K. (2018). İç Denetim 3.0 ve Kontrol Okuryazarlığı. *The Deloitte Times*, 68-71.

Vaidya, S., Ambad, P. and Bhosle, S. (2018). Industry 4.0 – A Glimpse. *Procedia Manufacturing, 20*, 233-238.

Verhoefa, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research, 122*, 889-901.

Wohlgenannt, I., Simons, A. and Stieglitz, S. (2020). Virtual Reality. *Business & Information Systems Engineering, 62*(5), 455-461.

Xie, X. (2020). Internal Audit Strategies for Dealing With Digital Risk in the Digital Economy. *2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020)*, 184-187.

Xu, L. D., He, W. and Li, S. (2014). Internet of Things in Industries: A Survey. *IEEE Transactions On Industrial Informatics, 10*(4), 2233-2243.

Xu, L. D., Xu, E. L. and Li, L. (2018). Industry 4.0: state of the art and future trends. *International Journal of Production Research, 56*(8), 2941-2962.

Yalçın, S. (2020). İç Denetimin Gelecekteki Rolü: İç Denetçilerin Sahip Olması Gereken Yetkinlikler. H. Kıral (Editör), *İç Denetim Kuruma Değer Katmak* içinde (s. 65-79). Ankara: Seçkin Yayıncılık.

Yang, K. and Jia, X. (2012). Data storage auditing service in cloud computing: challenges, methods and opportunities. *World Wide Web, 15*, 409-428.

Yeşilçelebi, G. (2019). *Entegre Raporlarda Bütünleşik Güvence Oluşturulması: Türkiye'deki Farkındalığın Delphi Tekniği ile Araştırılması.* Eskişehir: Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü.

Yıldız, B. ve Ağdeniz, Ş. (2019). Denetim 4.0'ın Teknolojik Altyapısı. *Muhasebe ve Denetime Bakış, 19*(58), 83-102.

Yıldız, M. ve Yıldırım, B. F. (2018). Yapay Zekâ ve Robotik Sistemlerin Kütüphanecilik Mesleğine Olan Etkileri. *Türk Kütüphaneciliği, 32*(1), 26-32.

Yıldız, Ö. R. (2011). Bilişim Dünyasının Yeni Modeli: Bulut Bilişim ve Denetim. *Sayıştay Dergisi*(74-75), 5-23.

Yürekli, E., Gönen, S. ve Şahiner, A. (2016). E-fatura Uygulamasına İlişkin Bir Değerlendirme. *Akademik Sosyal Araştırmalar Dergisi, 4*(35), 290-302.

Zaralı, M. (2022). *Dijital Dönüşüm Çağında Siber Güvenlik ve Mahremiyet.* İstanbul: Bahçeşehir Üniversitesi, Sosyal Bilimler Enstitüsü.

Zheng, J. M., Chan, K. W. and Gibson, I. (1998). Virtual reality. *IEEE Potentials, 17*(2), 20-23.

Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE 6th International Congress on Big Data*, Honolulu, HI, USA, 25-30 June 2017, (pp. 557-564).

Zhou, K., Liu, T. and Zhou, L. (2015). Industry 4.0: Towards Future Industrial Opportunities and Challenges. *12th International Conference on Fuzzy Systems and Knowledge Discovery*, 2147-2152.

EKLER

EK- 1. Araştırmaya Katılım Çağrısı / Davet e-postası

Sayın Katılımcı (Soyadı),

Anadolu Üniversitesi Muhasebe Bilim Dalı doktora öğrencisiyim ve Prof. Dr. Seval Kardeş Selimoğlu danışmanlığında tezimi yürütmekteyim. Tez konum dijital dönüşümün yarattığı riskler ve bu risklerin yönetiminde iç denetim fonksiyonu kapsamındadır.

Tez çalışmamda Delphi tekniği kullanmakta olup, konumla ilgili alanında uzman kişilerle görüşme yapmam gerekmektedir. Bu anlamda tezime katkı sağlamayı kabul etmeniz önemli olup memnuniyetimi en içten samimiyetimle belirtmek ister ve teşekkür ederim.

Katılım sağlamaya yönelik olumlu veya olumsuz kararınızı tarafıma iletmenizi rica ederim. Eğer cevabınız olumlu ise arzunuza göre yüz yüze, video konferans uygulaması, e-mail veya telefon ile size uygun bir günde görüşmeyi gerçekleştirmek isterim.

Saygılarımı sunarım,

Mehtap Altunel

EK- 2. Araştırmada Kullanılan Delphi I. Tur Görüşme Formu

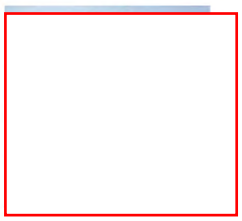
Dijital dönüşümün yarattığı riskler karşısında iç denetim fonksiyonuna ilişkin bir araştırma,

Sayın Katılımcı (Soyadı),

Dijital dönüşümün yarattığı riskler karşısında iç denetim fonksiyonunun rolü amacıyla yapılan bu çalışmaya katılımcı olmayı kabul ettiğiniz için çok teşekkür ederiz. Çalışma sırasında ve sonrasında isminiz ve verdiğiniz yanıtlar kesinlikle gizli tutulacaktır. Ayrıca görüşme esnasında, ses kaydı alınacaktır.

Araştırmayla ilgili herhangi bir konuda iletişim kurmak isterseniz, bize e-posta ve/veya telefon ile istediğiniz zaman ulaşabilirsiniz. Değerli vaktinizi ayırdığınız için çok teşekkür ederiz.

Saygılarımızla,



Doktora Öğrencisi

Mehtap ALTUNEL

Anadolu Üni. SBE İşletme/Muhasebe

Danışman

Prof. Dr. Seval SELİMOĞLU

Anadolu Üni. İİBF İşletme/Muhasebe

GÖRÜŞME SORULARI

1- Kurumdaki göreviniz nedir ve bu görevinizde ne zamandan beri çalışıyorsunuz?
2- Dördüncü Sanayi Devrimi, Dördüncü Sanayi Devrimi teknolojileri, dijital dönüşüm, sizde ne çağrıştırıyor? Dijital dönüşümün kurumunuza yansımaları nelerdir?
3- Kurumlar göz önüne alındığında yaşanan dijital dönüşümün getireceği başlıca riskler olarak neleri görüyorsunuz?
4- Dijital dönüşüm ile beraber karşılaşılan riskler karşısında iç denetim fonksiyonunun rolü nedir?
5- Dijital dönüşüm çerçevesinde iç denetimin güvence sağlama ve danışmanlık rolünü nasıl değerlendirirsiniz?
6- Üçlü hat modelinin, üçüncü hat rolünde yer alan iç denetimi dijital riskler çerçevesinde nasıl değerlendirirsiniz?
7- Kurumları dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde nasıl değişiklikler yapmalıdır? Bu noktada iç denetimin rolü nedir?
8- Sizce dijital dönüşüm süreci ile birlikte iç denetçilerin taşıması gereken yeni özellikler nelerdir? Bu süreçte iç denetçilerin odak noktası ne olmalıdır?
9- Denetçinin sürecin doğru yönetilmesi adına hangi eğitimleri/sertifikaları alması gerekir? Bu dönüşüm çağının gerektirdiği yetkinlikte iç denetçilerin yetiştirilmesi adına neler yapılmalıdır?
10- Dijital dönüşüm ile birlikte gelen riskler karşısında iç denetim faaliyeti yürütülürken başlıca hangi düzenlemeler/kılavuzlar kullanılmalıdır? Bu kılavuzların içeriğini nasıl değerlendirirsiniz?
11- Türkiye'de dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeleri nasıl değerlendirirsiniz?

EK- 3. Araştırmada Kullanılan Delphi II. Tur Anket Formu

ANKET FORMU

Sayın Katılımcı (Soyadı),

Bu anket formu "Dijital Dönüşümün İç Kontrol Sisteminde Yarattığı Riskler ve Bu Risklerin Yönetiminde İç Denetim Fonksiyonunun: Türkiye'deki Farkındalığın Araştırılması" konusunda Anadolu Üniversitesi Sosyal Bilimler Enstitüsü'nde yürütmekte olduğumuz doktora tezi kapsamındaki araştırma amacıyla hazırlanmıştır. Delphi yönteminin üçüncü turu için hazırlanan ankette yer alan sorular tamamen ilgili akademik çalışma için kullanılacak olup, vereceğiniz cevaplar kesinlikle gizli tutulacaktır. Yanıtlarınızı 10.10.2022 tarihine kadar göndermenizi rica ederiz.

Katılımınızdan dolayı şimdiden teşekkür ederiz.

Saygılarımla,

Doktora Öğrencisi

Mehtap ALTUNEL

Anadolu Üni. SBE İşletme/Muhasebe

Danışman

Prof. Dr. Seval SELİMOĞLU

Anadolu Üni. İİBF İşletme/Muhasebe

Aşağıdaki soruları "Katılıyorum, Katılmıyorum, Uygun Değil" seçeneklerine karşılık gelecek şekilde cevaplayınız.

I.Delphi Anketi		Lütfen size uygun olan seçeneği işaretleyiniz			Her bir ifadeye ilişkin, ayrıntılı görüşünüzü belirtebilirsiniz
Ana Kriterler	**İfadeler**	**Katılıyorum**	**Katılmıyorum**	**Uygun Değil**	
Dijital Dönüşüm-Endüstri 4.0	1. Endüstri 4.0; dijitalleşme, akıllı ev aletleri, denetimin dijitalleşmesi, robotların artık kullanılmaya başlanması, RPA teknolojileri, mükerrer işlemlerin azalması, insana duyulan ihtiyacın azalması şeklinde tanımlanabilir.	☐	☐	☐	
	2. Dördüncü sanayi devrimi birçok alanda dijitalleşmeyi ve dijital dönüşümü merkez alan yeni bir yapılanmadır.	☐	☐	☐	
	3. Dijital dönüşüm, dördüncü sanayi devrimi teknolojilerinin üretim ve hizmet alanlarında kullanma sürecidir.	☐	☐	☐	
	4. Dijital dönüşüm kurumların iş yapış şekillerinden, çözüm üretme stratejilerine kadar kurumları etkileyen önemli bir konudur.	☐	☐	☐	
	5. Dijital dönüşüm kurumların stratejik planlarından başlayıp tüm iş süreçlerini ele alınması gereken önemli bir konudur.	☐	☐	☐	
	6. İç denetim, iç kontrol süreçlerinin gerçek zamanlı izlenebilmesi dijital dönüşümün, dördüncü sanayi devriminin bir yansımasıdır.	☐	☐	☐	
Dijital Dönüşümden Kaynaklı Riskler	1. Dijital dönüşüme uyum sağlama, kurumların değişim kültürüne sahip olmaması, geç kalınması veya yavaş ilerlemek riskler arasındadır.	☐	☐	☐	
	2. Dijital dönüşüme kısa sürede uyum sağlama ihtiyacının doğurabileceği yanlış kararlar ve bunlardan kaynaklı katlanılan yüksek maliyetler önemli risklerden biridir.	☐	☐	☐	
	3. Kurumun dijital dönüşüm süreci için yeterli düzeyde araştırma-geliştirme ve testlerin yapılmamasından kaynaklı kayıplar (zaman, iş gücü, bütçe, karlılık vb.) önemli risklerden biridir.	☐	☐	☐	
	4. Dijital dönüşüm ile birlikte yaşanacak en önemli riskler kişisel verilerin korunması, bilgi güvenliği ve siber güvenlik riskleridir.	☐	☐	☐	
	5. Dijital dönüşüm sürecine entegre olamayan veya kendini yenileyemeyen kişiler ve toplumlar için bazı iş kollarının yok olması ve işsizlik önemli bir sorundur.	☐	☐	☐	
	6. Dijital dönüşümden kaynaklı en büyük risk veri kapsamında olup sadece veri kaybı olarak değil verinin bütüncül ve anlamlı şekilde tutulamaması da büyük bir risktir.	☐	☐	☐	

	7. Kurumların dijital dönüşüm sürecinde değişime direnç göstermesi ve yetkin iş gücüne/dijital iş gücüne sahip olmaması başlıca sıkıntılar/riskler arasındadır.	☐	☐	☐	
	8. Kurumlar tarafından kullanılan otomatik sistemlerin en büyük riskleri algoritmanın doğru çalışıp çalışmadığı, algoritmanın kurumun istediği sonucu verip vermediği ve algoritmayı yetkisiz değiştirecek üçüncü bir kişinin var olup olmadığıdır.	☐	☐	☐	
İç Denetim Rolü	1. Dijital dönüşümden kaynaklı risklerin tanımlanması ve farkındalık oluşturulması aşamasında iç denetim danışmanlık rolü ile katkı sağlayacaktır.	☐	☐	☐	
	2. Dijital dönüşüm çerçevesinde iç denetimin temel faaliyeti olan güvence ve danışmanlık görevi daha önemli bir seviyeye gelecektir.	☐	☐	☐	
	3. Dijital dönüşüm sürecinde iç denetim fonksiyonu ilk etapta danışmanlık rolü ile kurumlara katkı sağlayacaktır.	☐	☐	☐	
	4. Dijital dönüşüm çerçevesinde iç denetimin mutlak güvence sağlayamama konusu devam etmekle birlikte giderek artabilir. Diğer taraftan dijital dönüşüm ile birlikte danışmanlık rolü daha kritik hale gelecektir.	☐	☐	☐	
	5. İç denetim fonksiyonu dijital dönüşümden kaynaklı riskler karşısında bilgi teknolojileri denetimine ağırlık vermelidir.	☐	☐	☐	
	6. İç denetim fonksiyonu kurumun insan kaynağının dijital dönüşüm için yeterliliğini araştırmalıdır, ekip kurma aşamasında yer almalıdır.	☐	☐	☐	
	7. İç denetim fonksiyonu dijital dönüşümün getirdiği teknolojiler, bu teknolojilere uyum sağlanması, gerektiğinde yeniden yapılanma ihtiyacı, buna ilişkin planlama vb. konularda çalışmalar yürütmek ve gerekli bilgilendirmeleri yapmalıdır.	☐	☐	☐	
	8. İç denetçiler dijital dönüşüm sürecine yönelik danışmanlık hizmeti aşamasında kurumlara özgü planlar oluşturmalıdırlar.	☐	☐	☐	
	9. Yeni teknolojilerin riskleri, yasa ya da standart anlamındaki uyum süreçlerinin etkisi, yeni nesil ürün ve sistemlerin kullanımı gibi alanlarda iç denetim süreçlerinin yeniden yapılanması gereklidir.	☐	☐	☐	

	10. Kurumların dijital dönüşüm sürecinde iç denetim, danışmanlık rolü çerçevesinde entegre sistemlerin kurulumu, bu sistemlerden alınacak verilerin izlenmesi ve bu sistemlerin güvenliği rolünü üstlenmektedir.	☐	☐	☐	
Üçlü Hat Modeli	1. İç denetim, dijital dönüşüm sürecinin yönetişim, risk yönetimi ve iç kontrol sisteminde yaratacağı değişime ilişkin tavsiyelerde bulunmak, bu konularda kuruma ve yönetime danışmanlık yapmak ve destek sunmak gibi önemli rollere sahiptir.	☐	☐	☐	
	2. İç denetim yeni sistemin yeterliği ve etkililiğinin değerlendirmesi kapsamında role sahiptir.	☐	☐	☐	
	3. Üçlü hat modelinde iç denetimin önemi daha ön plana çıkarmakla birlikte dijitalleşmeden kaynaklı riskler karşısında iç denetim faaliyetini daha da gerekli kılmaktadır.	☐	☐	☐	
	4. İç denetim artık riskleri daha proaktif yönettiği bir döneme giriyor.	☐	☐	☐	
	5. Dijital dönüşüm sürecinde iç denetimin geride kalması katma değeri azaltmaktadır.	☐	☐	☐	
	6. Dijitalleşme öncesi ile kıyaslandığında dijital dönüşüm sürecindeki risklerin değerlendirilme aşamasında üçüncü hat rolünde iç denetimin sorumluluklarında bir değişim yoktur.	☐	☐	☐	
	7. Dijital dönüşüm süreciyle iç denetim fonksiyonu GRC (Governance, Risk, Compliance -Yönetişim, Risk, Uyum), veri analitiği kullanan yapılar haline gelmelidir.	☐	☐	☐	
İç Kontrol Sistemi	1. Dijitalleşme kurumlarda bir strateji ile başlamalıdır.	☐	☐	☐	
	2. Kurumlardaki dijital dönüşüm sonucu iç kontrol sistemin sorumluluğundaki birtakım kontroller yazılım sistemine aktarılır.	☐	☐	☐	
	3. Dijitalleşme sonucu denetimlerin otomatik şekilde yapılmasından kaynaklı iç denetimin otomatikleşen sistemlere yönelik denetimi önem kazanmaktadır.	☐	☐	☐	
	4. İç kontrol sisteminin risk ortamı ve kontrol faaliyetleri bileşenlerinin dijital riskleri kapsaması konusunda revize edilmesi gerekir.	☐	☐	☐	

	5. İç kontrol sisteminin beşinci bileşeni olarak izleme çerçevesinde iç denetim iç kontrol sisteminin dijital dönüşümden kaynaklı riskler karşısında etkinliğini değerlendirme aşamasında güvence rolü ile katkı sağlamaktadır.	☐	☐	☐	
	6. Dijital dönüşüm ile birlikte kurumların bilgi teknolojileri departmanının risk ve açıklarının kontrolü için bağımsız kuruluşlarca düzenli olarak testleri yapılmalıdır.	☐	☐	☐	
	7. Dijital dönüşüm çağında iç kontrol sistemi olaylar gerçekleşmeden önce önlem almalı ve mevcut trendler ile sürekli bir uyum içinde kalmalıdır.	☐	☐	☐	
	8. Dijital dönüşüm ile entegre sistemler (Enterprise Resource Planning (ERP)-Kurumsal Kaynak Planlaması gibi) kullanılabilir.	☐	☐	☐	
	9. Dijital dönüşümden kaynaklı riskler karşında risk yönetimi çerçevesinde kurumsal yönetim ilkelerine uygun olarak gerekli kontrol noktalarının oluşturulması sağlanmalıdır.	☐	☐	☐	
	10. Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde değişim karşısında iç denetim stratejik rol üstlenmeli ve danışmanlık rolünü ön plana çıkarmalıdır.	☐	☐	☐	
	11. Dijitalleşme kurumlarda iç kontrol sisteminin bakış açısını artıracaktır.	☐	☐	☐	
	12. Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sistemindeki değişiklikler kurumun olgunluk seviyesine bağlıdır.	☐	☐	☐	
	13. Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde kurumlar değişiklik yapmaya karar verdiyse yazılım alınacaksa alternatiflerin araştırılması, sisteme geçiş sürecinde eğitimlerin verilmesi konularında iç denetim danışmanlık rolünü üstlenebilir.	☐	☐	☐	
	14. Kurumlar dijitalleşme için adım atmış ve kurum kültürü oluşturmuş ise iç kontrol yapılarını da bu çerçevede güncellemek zorundadır.	☐	☐	☐	
	15. İç kontrol sistemlerine sürekli izleme yaklaşımları adapte edilmelidir.	☐	☐	☐	

Yasal Düzenleme	1. Dijital dönüşüm ile birlikte gelen riskler karşısında iç denetim faaliyeti yürütülürken başlıca takip edilmesi gereken düzenlemeler/kılavuzlar: • Cumhurbaşkanlığı DDO (Dijital Dönüşüm Ofisi) Bilgi ve İletişim Güvenliği Denetim Rehberi • COBIT, • ISO 27000, • NIST • IIA	☐	☐	☐	
	2. Cumhurbaşkanlığı DDO yayımladığı Bilgi ve İletişim Güvenliği Denetim Rehberi dijital riskleri yönetmek adına yeterli bir rehberdir.	☐	☐	☐	
	3. Türkiye'de dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeler yeterli değildir, gelişmesi gereken alanlar vardır.	☐	☐	☐	
	4. Dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeler, Türkiye'de belli başlı kurumlar tarafından yapılmaktadır.	☐	☐	☐	
	5. Kamu kurumları, Cumhurbaşkanlığı DDO yayımladığı Bilgi ve İletişim Güvenliği Denetim Rehberi'ni uygulayabilecek noktada değildir.	☐	☐	☐	
	6. Kamu kurumları özel kurumlardan özellikle risk yönetimi uygulanmalarından son zamanlarda faydalanmaktadır.	☐	☐	☐	
	7. Türkiye'de dijital risklerin yönetimi adına özel sektör bilinci daha yüksek ve daha erken çalışmalar başlamıştır.	☐	☐	☐	
İç Denetçi	1. İç denetçilerin bilgisayar tabanlı denetim yöntemlerini öğrenmeleri ve kendilerini bu alanda yetiştirmeleri yapılan denetimin kalite ve etkinliğini artıracaktır.	☐	☐	☐	
	2. İç denetçi iletişim becerisine sahip olmalıdır.	☐	☐	☐	
	3. Denetçinin dijital dönüşüm sürecini ve riskleri doğru yönetmek adına CIA, CISA, ITIL, CGEIT, CRMA, PMP(Proje Yönetim Sertifikası) sertifikalarının biri ya da birkaçına sahip olmalıdır.	☐	☐	☐	

	4. İç denetçiler teknolojik alanda yaşanan gelişmeleri yakından takip etmeli ve söz konusu yeni teknolojilerin birer denetim aracı olarak kullanılmasını sağlamalıdır.	☐	☐	☐	
	5. İç denetçiler yeni teknoloji kullanımının getireceği riskleri denetim alanı olarak ele almalıdır.	☐	☐	☐	
	6. Sürekli denetim, çevik denetim, denetim 4.0 gibi yeni denetim yaklaşımları iç denetçilerin odak noktası olmalıdır.	☐	☐	☐	
	7. İç denetçilerin bilgi teknolojileri ve buna bağlı riskler konusunda farkındalıklarını arttırmaları gerekmektedir.	☐	☐	☐	
	8. İç denetçilerin finansal okur yazarlıklarının yanında dijital okur yazarlık yeteneğine sahip olmalı ve gerekli altyapı hızla oluşturulmalıdır.	☐	☐	☐	
	9. İç denetçiler kurumsal iletişim, kurumsal risk yönetimi, bilgi teknolojileri denetimi, siber güvenlik, uzaktan denetim teknikleri, veri analizi ve modelleme teknikleri, iş zekası programlama vb. genel eğitimler almalıdır.	☐	☐	☐	
	10. İç denetçiler dijital çağ ile birlikte multidisipliner (hem Bilgi Teknolojileri hem denetim, muhasebe) özelliklerine sahip olmalıdırlar.	☐	☐	☐	
	11. Dijital dönüşüm sürecinde iç denetim faaliyeti yürütülürken farklı yetkinlikte kişilerin bir arada birleşip denetim yapması gerekmektedir.	☐	☐	☐	
	12. Kamu kurumundaki iç denetçiler dijital dönüşüm çerçevesinde kurumlarına danışmanlık hizmeti verecek seviye de değildir.	☐	☐	☐	

II-Demografik Özellikler

Yaş (☐)20-24 (☐) 25-29 (☐) 30-34 (☐) 35-39 (☐) 40-44 (☐) 45-49 (☐) 50-ve üstü

Cinsiyet (☐) Kadın (☐) Erkek (☐) Diğer (☐) Belirtmek istemiyorum

Öğrenim (☐) Lisans (☐) Yüksek Lisans (☐) Doktora

Çalışma Süresi (yıl) (☐) 0-4 (☐) 5-9 (☐) 10-14 (☐) 15-19 (☐) 20-ve üstü

Uzmanlık (☐) Akademisyen (☐) İç Denetçi (Kamu Sektörü)

(☐) İç Denetçi (Özel Sektör) (☐)Mesleki Kuruluş- Sorumlu Kişiler (TİDE, ISACA, KIDDER vb.)

III-Eklemek İstediklerinız

(Bize söylemek istediğiniz başka noktalar varsa duymak isteriz.)

EK- 4. Araştırmada Kullanılan Delphi III. Tur Anket Formu

ANKET FORMU

Sayın Katılımcı (Soyadı),

Bu anket formu "Dijital Dönüşümün İç Kontrol Sisteminde Yarattığı Riskler ve Bu Risklerin Yönetiminde İç Denetim Fonksiyonunun: Türkiye'deki Farkındalığın Araştırılması" konusunda Anadolu Üniversitesi Sosyal Bilimler Enstitüsü'nde yürütmekte olduğumuz doktora tezi kapsamındaki araştırma amacıyla hazırlanmıştır. Delphi yönteminin üçüncü turu için hazırlanan ankette yer alan sorular tamamen ilgili akademik çalışma için kullanılacak olup, vereceğiniz cevaplar kesinlikle gizli tutulacaktır. Yanıtlarınızı 11.11.2022 tarihine kadar göndermenizi rica ederiz.

Katılımınızdan dolayı şimdiden teşekkür ederiz.

Saygılarımla,

Doktora Öğrencisi

Mehtap ALTUNEL

Anadolu Üni. SBE İşletme/Muhasebe

Danışman

Prof. Dr. Seval SELİMOĞLU

Anadolu Üni. İİBF İşletme/Muhasebe

Aşağıdaki soruları "Katılıyorum, Katılmıyorum, Uygun Değil" seçeneklerine karşılık gelecek şekilde cevaplayınız.

II.Delphi Anketi		Lütfen size uygun olan seçeneği işaretleyiniz			Her bir ifadeye ilişkin, ayrıntılı görüşünüzü belirtebilirsiniz.
Ana Kriterler	**İfadeler**	**Katılıyorum**	**Katılmıyorum**	**Uygun Değil**	
Dijital Dönüşüm-Endüstri 4.0	1. Endüstri 4.0; dijitalleşme, akıllı ev aletleri, denetimin dijitalleşmesi, robotların artık kullanılmaya başlanması, RPA teknolojileri, mükerrer işlemlerin azalması, insana duyulan ihtiyacın azalması şeklinde tanımlanabilir.	☐	☐	☐	
	2. Dördüncü sanayi devrimi birçok alanda dijitalleşmeyi ve dijital dönüşümü merkez alan yeni bir yapılanmadır.	☐	☐	☐	
	3. Dijital dönüşüm, dördüncü sanayi devrimi teknolojilerinin üretim ve hizmet alanlarında kullanma sürecidir.	☐	☐	☐	
	4. Dijital dönüşüm kurumların iş yapış şekillerinden, çözüm üretme stratejilerine kadar kurumları etkileyen önemli bir konudur.	☐	☐	☐	
	5. Dijital dönüşüm kurumların stratejik planlarından başlayıp tüm iş süreçlerini ele alınması gereken önemli bir konudur.	☐	☐	☐	
	6. Iç denetim, iç kontrol süreçlerinin gerçek zamanlı izlenebilmesi dijital dönüşümün, dördüncü sanayi devriminin bir yansımasıdır.	☐	☐	☐	
Dijital Dönüşümden Kaynaklı Riskler	1. Dijital dönüşüme uyum sağlama, kurumların değişim kültürüne sahip olmaması, geç kalınması veya yavaş ilerlemek riskler arasındadır.	☐	☐	☐	
	2. Dijital dönüşüme kısa sürede uyum sağlama ihtiyacının doğurabileceği yanlış kararlar ve bunlardan kaynaklı katlanılan yüksek maliyetler önemli risklerden biridir.	☐	☐	☐	
	3. Kurumun dijital dönüşüm süreci için yeterli düzeyde araştırma-geliştirme ve testlerin yapılmamasından kaynaklı kayıplar (zaman, iş gücü, bütçe, karlılık vb.) önemli risklerden biridir.	☐	☐	☐	
	4. Dijital dönüşüm ile birlikte yaşanacak en önemli riskler kişisel verilerin korunması, bilgi güvenliği ve siber güvenlik riskleridir.	☐	☐	☐	
	5. Dijital dönüşüm sürecine entegre olamayan veya kendini yenileyemeyen kişiler ve toplumlar için bazı iş kollarının yok olması ve işsizlik önemli bir sorundur.	☐	☐	☐	

	6. Dijital dönüşümden kaynaklı en büyük risk veri kapsamında olup sadece veri kaybı olarak değil verinin bütüncül ve anlamlı şekilde tutulamaması da büyük bir risktir.	☐	☐	☐	
	7. Kurumların dijital dönüşüm sürecinde değişime direnç göstermesi ve yetkin iş gücüne/dijital iş gücüne sahip olmaması başlıca sıkıntılar/riskler arasındadır.	☐	☐	☐	
	8. Kurumlar tarafından kullanılan otomatik sistemlerin en büyük riskleri algoritmanın doğru çalışıp çalışmadığı, algoritmanın kurumun istediği sonucu verip vermediği ve algoritmayı yetkisiz değiştirecek üçüncü bir kişinin var olup olmadığıdır.	☐	☐	☐	
İç Denetim Rolü	1. Dijital dönüşümden kaynaklı risklerin tanımlanması ve farkındalık oluşturulması aşamasında iç denetim danışmanlık rolü ile katkı sağlayacaktır.	☐	☐	☐	
	2. Dijital dönüşüm çerçevesinde iç denetimin temel faaliyeti olan güvence ve danışmanlık görevi daha önemli bir seviyeye gelecektir.	☐	☐	☐	
	3. Dijital dönüşüm sürecinde iç denetim fonksiyonu ilk etapta danışmanlık rolü ile kurumlara katkı sağlayacaktır.	☐	☐	☐	
	4. Dijital dönüşüm çerçevesinde iç denetimin mutlak güvence sağlayamama konusu devam etmekle birlikte giderek artabilir. Diğer taraftan dijital dönüşüm ile birlikte danışmanlık rolü daha kritik hale gelecektir.	☐	☐	☐	
	5. İç denetim fonksiyonu dijital dönüşümden kaynaklı riskler karşısında bilgi teknolojileri denetimine ağırlık vermelidir.	☐	☐	☐	
	6. İç denetim fonksiyonu dijital dönüşümün getirdiği teknolojiler, bu teknolojilere uyum sağlanması, gerektiğinde yeniden yapılanma ihtiyacı, buna ilişkin planlama vb. konularda çalışmalar yürütmek ve gerekli bilgilendirmeleri yapmalıdır.	☐	☐	☐	
	7. İç denetçiler dijital dönüşüm sürecine yönelik danışmanlık hizmeti aşamasında kurumlara özgü planlar oluşturmalıdır.	☐	☐	☐	

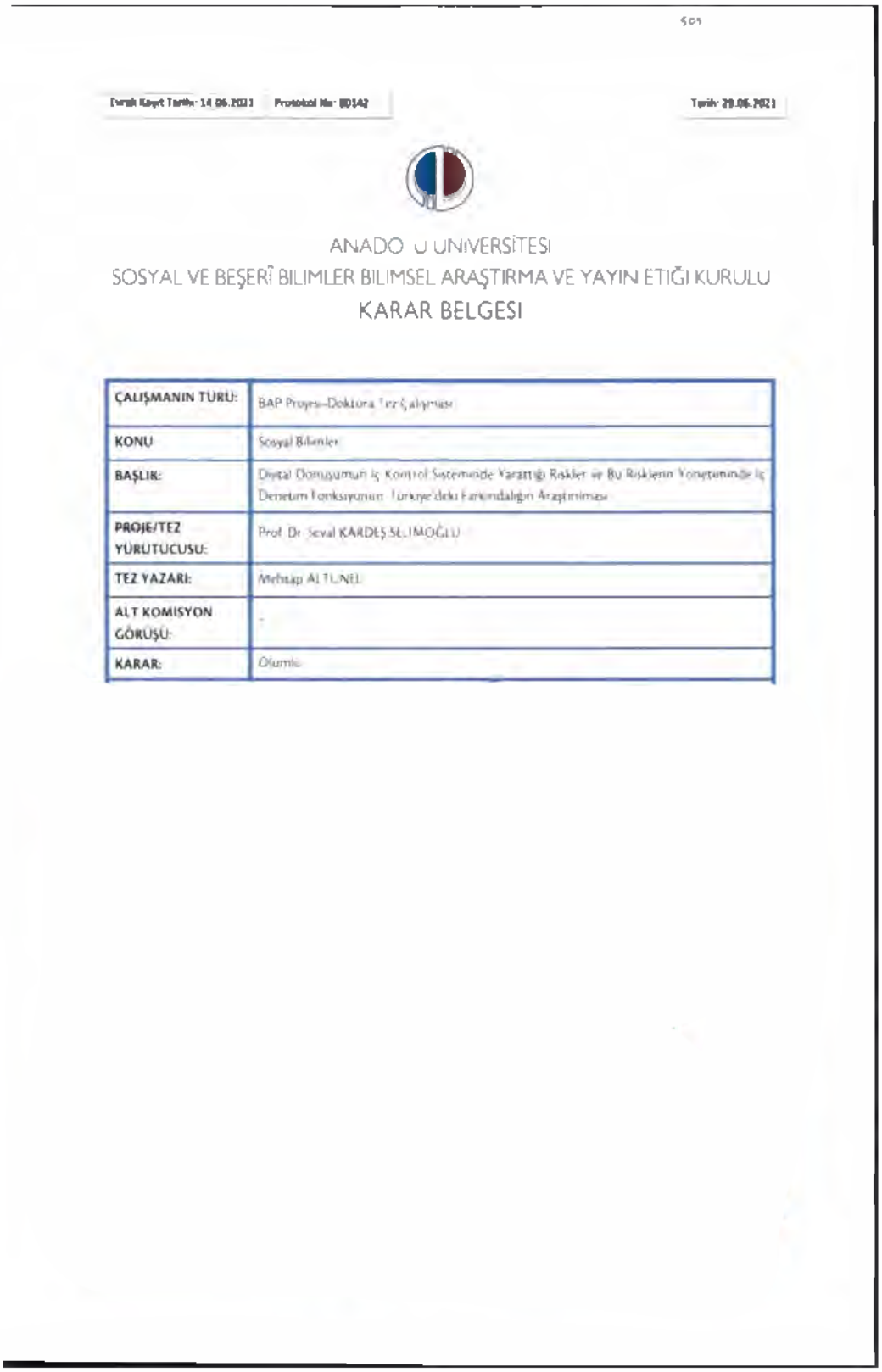
	8. Yeni teknolojilerin riskleri, yasa ya da standart anlamındaki uyum süreçlerinin etkisi, yeni nesil ürün ve sistemlerin kullanımı gibi alanlarda iç denetim süreçlerinin yeniden yapılanması gereklidir.	☐	☐	☐	
	9. Kurumların dijital dönüşüm sürecinde iç denetim, danışmanlık rolü çerçevesinde entegre sistemlerin kurulumu, bu sistemlerden alınacak verilerin izlenmesi ve bu sistemlerin güvenliği rolünü üstlenmektedir.	☐	☐	☐	
Üçlü Hat Modeli	1. İç denetim, dijital dönüşüm sürecinin yönetişim, risk yönetimi ve iç kontrol sisteminde yaratacağı değişime ilişkin tavsiyelerde bulunmak, bu konularda kuruma ve yönetime danışmanlık yapmak ve destek sunmak gibi önemli rollere sahiptir.	☐	☐	☐	
	2. İç denetim yeni sistemin yeterliği ve etkililiğinin değerlendirmesi kapsamında role sahiptir.	☐	☐	☐	
	3. Üçlü hat modelinde iç denetimin önemi daha ön plana çıkarmakla birlikte dijitalleşmeden kaynaklı riskler karşısında iç denetim faaliyetini daha da gerekli kılmaktadır.	☐	☐	☐	
	4. İç denetim artık riskleri daha proaktif yönettiği bir döneme giriyor.	☐	☐	☐	
	5. Dijital dönüşüm sürecinde iç denetimin geride kalması katma değeri azaltmaktadır.	☐	☐	☐	
	6. Dijital dönüşüm süreciyle iç denetim fonksiyonu GRC (Governance, Risk, Compliance -Yönetişim, Risk, Uyum), veri analitiği kullanan yapılar haline gelmelidir.	☐	☐	☐	
İç Kontrol Sistemi	1. Dijitalleşme kurumlarda bir strateji ile başlamalıdır.	☐	☐	☐	
	2. Kurumlardaki dijital dönüşüm sonucu iç kontrol sisteminin sorumluluğundaki birtakım kontroller yazılım sistemine aktarılır.	☐	☐	☐	
	3. Dijitalleşme sonucu denetimlerin otomatik şekilde yapılmasından kaynaklı iç denetimin otomatikleşen sistemlere yönelik denetimi önem kazanmaktadır.	☐	☐	☐	

	4. Iç kontrol sisteminin risk ortamı ve kontrol faaliyetleri bileşenlerinin dijital riskleri kapsaması konusunda revize edilmesi gerekir.	☐	☐	☐	
	5. Iç kontrol sisteminin beşinci bileşeni olarak izleme çerçevesinde iç denetim iç kontrol sisteminin dijital dönüşümden kaynaklı riskler karşısında etkinliğini değerlendirme aşamasında güvence rolü ile katkı sağlamaktadır.	☐	☐	☐	
	6. Dijital dönüşüm ile birlikte kurumların bilgi teknolojileri departmanının risk ve açıklarının kontrolü için bağımsız kuruluşlarca düzenli olarak testleri yapılmalıdır.	☐	☐	☐	
	7. Dijital dönüşüm çağında iç kontrol sistemi olaylar gerçekleşmeden önce önlem almalı ve mevcut trendler ile sürekli bir uyum içinde kalmalıdır.	☐	☐	☐	
	8. Dijital dönüşüm ile entegre sistemler (Enterprise Resource Planning (ERP)-Kurumsal Kaynak Planlaması gibi) kullanılabilir.	☐	☐	☐	
	9. Dijital dönüşümden kaynaklı riskler karşısında risk yönetimi çerçevesinde kurumsal yönetim ilkelerine uygun olarak gerekli kontrol noktalarının oluşturulması sağlanmalıdır.	☐	☐	☐	
	10. Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde değişim karşısında iç denetim stratejik rol üstlenmeli ve danışmanlık rolünü ön plana çıkarmalıdır.	☐	☐	☐	
	11. Dijitalleşme kurumlarda iç kontrol sisteminin bakış açısını artıracaktır.	☐	☐	☐	
	12. Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sistemindeki değişiklikler kurumun olgunluk seviyesine bağlıdır.	☐	☐	☐	
	13. Dijital dönüşümden kaynaklı riskler karşısında mevcut iç kontrol sisteminde kurumlar değişiklik yapmaya karar verdi ise yazılım alınacaksa alternatiflerin araştırılması, sisteme geçiş sürecinde eğitimlerin verilmesi konularında iç denetim danışmanlık rolünü üstlenebilir.	☐	☐	☐	

	14. Kurumlar dijitalleşme için adım atmış ve kurum kültürü oluşturmuş ise iç kontrol yapılarını da bu çerçevede güncellemek zorundadır.	☐	☐	☐	
	15. İç kontrol sistemlerine sürekli izleme yaklaşımları adapte edilmelidir.	☐	☐	☐	
Yasal Düzenleme	1. Dijital dönüşüm ile birlikte gelen riskler karşısında iç denetim faaliyeti yürütülürken başlıca takip edilmesi gereken düzenlemeler/kılavuzlar: • Cumhurbaşkanlığı DDO (Dijital Dönüşüm Ofisi) Bilgi ve İletişim Güvenliği Denetim Rehberi • COBIT, • ISO 27000, • NIST • IIA	☐	☐	☐	
	2. Türkiye'de dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeler yeterli değildir, gelişmesi gereken alanlar vardır.	☐	☐	☐	
	3. Dijital dönüşümden kaynaklı risklerin yönetilmesi adına yapılan düzenlemeler, Türkiye'de belli başlı kurumlar tarafından yapılmaktadır.	☐	☐	☐	
	4. Kamu kurumları özel kurumlardan özellikle risk yönetimi uygulanmalarından son zamanlarda faydalanmaktadır.	☐	☐	☐	
	5. Türkiye'de dijital risklerin yönetimi adına özel sektör bilinci daha yüksek ve daha erken çalışmalar başlamıştır.	☐	☐	☐	
İç Denetçi	1. İç denetçilerin bilgisayar tabanlı denetim yöntemlerini öğrenmeleri ve kendilerini bu alanda yetiştirmeleri yapılan denetimin kalite ve etkinliğini artıracaktır.	☐	☐	☐	
	2. İç denetçi iletişim becerisine sahip olmalıdır.	☐	☐	☐	
	3. Denetçinin dijital dönüşüm sürecini ve riskleri doğru yönetmek adına CIA, CISA, ITIL, CGEIT, CRMA, PMP(Proje Yönetim Sertifikası) sertifikalarının biri ya da birkaçına sahip olmalıdır.	☐	☐	☐	

	4. İç denetçiler teknolojik alanda yaşanan gelişmeleri yakından takip etmeli ve söz konusu yeni teknolojilerin birer denetim aracı olarak kullanılmasını sağlamalıdır.	☐	☐	☐	
	5. İç denetçiler yeni teknoloji kullanımının getireceği riskleri denetim alanı olarak ele almalıdır.	☐	☐	☐	
	6. Sürekli denetim, çevik denetim, denetim 4.0 gibi yeni denetim yaklaşımları iç denetçilerin odak noktası olmalıdır.	☐	☐	☐	
	7. İç denetçilerin bilgi teknolojileri ve buna bağlı riskler konusunda farkındalıklarını arttırmaları gerekmektedir.	☐	☐	☐	
	8. İç denetçiler finansal okur yazarlıklarının yanında dijital okur yazarlık yeteneğine sahip olmalı ve gerekli altyapı hızla oluşturulmalıdır.	☐	☐	☐	
	9. İç denetçiler kurumsal iletişim, kurumsal risk yönetimi, bilgi teknolojileri denetimi, siber güvenlik, uzaktan denetim teknikleri, veri analizi ve modelleme teknikleri, iş zekası programlama vb. genel eğitimler almalıdır.	☐	☐	☐	
	10. İç denetçiler dijital çağ ile birlikte multidisipliner (hem Bilgi Teknolojileri hem denetim, muhasebe) özelliklere sahip olmalıdır.	☐	☐	☐	
	11. Dijital dönüşüm sürecinde iç denetim faaliyeti yürütülürken farklı yetkinlikte kişiler bir arada birleşip denetim yapması gerekmektedir.	☐	☐	☐	

EK- 5. Etik Kurul İzni



ANADOLU ÜNİVERSİTESİ
SOSYAL VE BEŞERÎ BİLİMLER BİLİMSEL ARAŞTIRMA VE YAYIN ETİĞİ KURULU
KARAR BELGESİ

ÇALIŞMANIN TÜRÜ:	BAP Projesi-Doktora Tez Çalışması
KONU	Sosyal Bilimler
BAŞLIK:	Dijital Dönüşümün İç Kontrol Sisteminde Yarattığı Riskler ve Bu Risklerin Yönetiminde İç Denetim Fonksiyonunun Türkiye'deki Farkındalığın Araştırılması
PROJE/TEZ YÜRÜTÜCÜSÜ:	Prof. Dr. Seval KARDEŞ SELİMOĞLU
TEZ YAZARI:	Mehtap ALTUNEL
ALT KOMİSYON GÖRÜŞÜ:	-
KARAR:	Olumlu