Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

İşletme Anabilim Dalı

İÇ DENETİMİN BİLGİ GÜVENLİĞİNE KATKISI: BİR ALAN ARAŞTIRMASI

Borga KÜÇÜKKAYALAR

Doktora Tezi

Ankara, 2024

İÇ DENETİMİN BİLGİ GÜVENLİĞİNE KATKISI: BİR ALAN ARAŞTIRMASI

Borga KÜÇÜKKAYALAR

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

İşletme Anabilim Dalı

Doktora Tezi

Ankara, 2024

KABUL VE ONAY

Borga KÜÇÜKKAYALAR tarafından hazırlanan “İç Denetimin Bilgi Güvenliğine Katkısı: Bir Alan Araştırması” başlıklı bu çalışma, 12.06.2024 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Doktora Tezi olarak kabul edilmiştir.

Prof.Dr. Özlem ATAY (Başkan)

Prof.Dr. Mustafa KILIÇ (Danışman)

Prof.Dr. Semra KARACAER (Üye)

Prof.Dr. M. Devrim AYDIN (Üye)

Doç.Dr. Çağlar DOĞRU (Üye)

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Prof.Dr. Uğur ÖMÜRGÖNÜLŞEN

Enstitü Müdürü

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin tamamını veya herhangi bir kısmını, basılı (kağıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinleri yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan ***"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"*** kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / H.Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- Enstitü / Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir. (1)
- Enstitü / Fakülte yönetim kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren ….. ay ertelenmiştir. (2)
- Tezimle ilgili gizlilik kararı verilmiştir. (3)

07.08.2024

Borga KÜÇÜKKAYALAR

1"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"

*(1) Madde 6. 1. Lisansüstü tezle ilgili patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda, tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu** iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.*

*(2) Madde 6. 2. Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkanı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulunun** gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.*

*(3) Madde 7. 1. Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, **tezin yapıldığı kurum** tarafından verilir *. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, **ilgili kurum ve kuruluşun önerisi** ile **enstitü** veya **fakültenin** uygun görüşü üzerine **üniversite yönetim kurulu** tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.*
Madde 7.2. Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

****** Tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu tarafından karar verilir.***

ETİK BEYAN

Bu çalışmadaki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi, görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, yararlandığım kaynaklara bilimsel normlara uygun olarak atıfta bulunduğumu, tezimin kaynak gösterilen durumlar dışında özgün olduğunu, **Prof. Dr., Mustafa KILIÇ** danışmanlığında tarafımdan üretildiğini ve Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesine göre yazıldığını beyan ederim.

Borga KÜÇÜKKAYALAR

TEŞEKKÜR

Doktora süreci boyunca, çalışmanın her aşamasında bana yol gösteren, anlayış ve sabır ile desteğini esirgemeyen tez danışmanım Prof. Dr. Mustafa KILIÇ'a en içten teşekkürlerimi sunarım.

Yorum ve önerileriyle araştırmama yaptıkları katkılardan dolayı tez izleme komite üyeleri ve doktora tez savunma jüri üyeleri değerli hocalarım Prof. Dr. Özlem ATAY, Prof. Dr. M. Devrim AYDIN, Prof. Dr. Semra KARACAER ve Doç. Dr. Çağlar DOĞRU'ya teşekkür ederim.

Her zaman varlığını ve sevgisini arkamda hissettiğim sevgili eşim Ferhan KÜÇÜKKAYALAR'a sonsuz teşekkür ederim. Doktora süreci başladığından beri desteğini esirgemeyen kıymetli anneme teşekkürlerimi sunarım. Tez çalışması sürecinin yoğun dönemlerinde, onlarla oynayamadığım her bir oyun için beni çoktan affeden canım kızım Beril'e ve canım oğlum Bartu'ya teşekkürlerin en büyüğünü borç bilirim.

Anketimizi cevaplayarak tez çalışmasına çok değerli katkılar veren denetim alanında çalışmakta olan tüm meslektaşlarıma ve üstadlarıma teşekkür ederim.

ÖZET

Küçükkayalar, Borga. *İç Denetimin Bilgi Güvenliğine Katkısı: Bir Alan Araştırması*, Doktora Tezi, Ankara, 2024.

Bu tez çalışmasında öncelikle organizasyonlardaki bilgi güvenliği ve iç denetim fonksiyonları arasındaki ilişkinin niteliği ve anılan ilişkinin niteliğini etkileyen faktörler incelenmiştir. Ardından söz konusu ilişkinin potansiyel faydaları, iç denetimin bilgi güvenliği denetimleri neticesinde ortaya çıkan katma değeri ve organizasyonun bilgi güvenliği faaliyetlerinin genel etkinliği hakkındaki algıyı nasıl etkilediği değerlendirilmiştir. Bu bağlamda organizasyona değer katma temelinde ortak amaçlara yönelmiş iki ayrı organizasyonel fonksiyon olan iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin niteliğine yönelik iç denetçilerin algıları araştırılmıştır. Bu maksatla 272 iç denetim personelinden toplanan veriler ile değişkenler arasındaki ilişkiler model yardımıyla incelenmiştir. Çalışmada 2 araştırma sorusu kapsamında beş hipotez test edilmiştir. Hipotezleri test etme aşamasında mevcut model için değişken çiftleri arasındaki direkt ve indirekt etkilere ait yol katsayıları, güven aralıkları, t-istatistikleri ve p-değeri analizleri yapılmıştır. Çalışma sonucunda iç denetçilerin; iç denetim fonksiyonunu, mevzuatın uygulayıcısı rolünden ziyade danışmanlık rolü olarak değerlendirmeleri durumunda, iç denetim ve bilgi güvenliği arasındaki ilişkiye dair algılarının daha olumlu olduğu görülmüştür. Ardından iç denetçilerin; iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin niteliğine dair algılarının, iç denetimin gerçekleştirdiği bilgi güvenliği denetimlerinin sıklığıyla ve iç denetçilerin bilgi güvenliği hakkındaki yetkinliğine dair algılarıyla pozitif yönde ilişkili olduğu sonucu elde edilmiştir. Buna müteakip iç denetim ve bilgi güvenliği arasındaki ilişkinin niteliğinin, iç denetçilerin içinde bulundukları iç denetim fonksiyonunun, organizasyona sağladığı katma değere dair algılarıyla pozitif yönde ilişkili olduğu ve son olarak iç denetim ve bilgi sistemleri fonksiyonları arasındaki ilişkinin algılanan niteliğinin; iç denetçilerin, bilgi güvenliği etkinliğine olan algılarıyla pozitif yönde ilişkili olduğu görülmüştür.

Anahtar Sözcükler

İç denetim, bilgi güvenliği, iç denetçi, bilgi, denetim, katma değer.

ABSTRACT

KÜÇÜKKAYALAR, Borga. *The Contribution of Internal Auditing to Information Security: A Field Study,* Doctoral Thesis, Ankara, 2024.

In this thesis study, firstly, the nature of the relationship between information security and internal audit functions in organizations, and the factors affecting the nature of the mentioned relationship, were examined. Then, the potential benefits of this relationship, the added value resulting from internal audit's information security audits, and how it affects the perception of the overall effectiveness of the organization's information security activities were evaluated. In this context, the perceptions of internal auditors regarding the nature of the relationship between internal audit and information security functions, which are two separate organizational functions aimed at adding value to the organization based on common goals, were investigated. For this purpose, the data collected from 272 internal audit personnel were analysed using modelling to examine the relationships between variables. In the study, five hypotheses were tested within the scope of two research questions. During the hypothesis testing stage, path coefficients, confidence intervals, t-statistics, and p-values analyses for direct and indirect effects between variable pairs in the current model were conducted. As a result of the study, it was observed that when internal auditors evaluate the internal audit function as a consultancy role rather than a regulator role, their perceptions of the relationship between internal audit and information security are more positive. Then, it was observed that internal auditors' perceptions of the nature of the relationship between internal audit and information security functions are positively associated with the frequency of information security audits conducted by internal audit and their perceptions of competence in information security. Following this, it was found that the nature of the relationship between internal audit and information security is positively associated with internal auditors' perceptions of the added value provided by the internal audit function to the organization, and finally, the perceived nature of the relationship between internal audit and information systems functions is positively associated with internal auditors' perceptions of information security effectiveness.

Keywords

Internal audit, information security, internal auditor, information, audit, value-added.

İÇİNDEKİLER

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

KISALTMALAR DİZİNİ

AICPA	:	Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü (American Institute of Certified Public Accountants)
AVE	:	Ortalama Açıklanan Varyans (Average Variance Extracted)
BGYS	:	Bilgi Güvenliği Yönetim Sistemleri
BT/IT	:	Bilgi Teknolojileri (Information Technologies)
CBDDO	:	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
CGEIT	:	Sertifikalı Kurumsal BT Yönetişim Uzmanı (Certified in the Governance of Enterprise IT)
CIA	:	Sertifikalı İç Denetçi (Certified Internal Auditor)
CISA	:	Sertifikalı Bilgi Sistemleri Denetçisi (Certified Information Systems Auditor)
CISM	:	Sertifikalı Bilgi Güvenliği Yöneticisi (Certified Information Security Manager)
COBIT	:	Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri (Control Objectives for Information and related Technology)
COSO	:	Sponsor Olan Kurumlar Birliği (Committee of Sponsoring Organizations)
CRISC	:	Sertifikalı Risk ve Bilgi Sistemleri Kontrol Uzmanı (Certified in Risk and Information Systems Control)
ECIIA	:	Avrupa İç Denetim Enstitüleri Konfederasyonu (European Confederation of Institutes of Internal Auditing)
GAGAS	:	Amerikan Genel Kabul Görmüş Devlet Denetim Standartları (Generally Accepted Government Auditing Standards)
GAO	:	Amerika Birleşik Devletleri Genel Muhasebe Ofisi (Government Accounting Office)
IFAC	:	Uluslararası Muhasebeciler Federasyonu (International Federation of Accountants)
IIA	:	İç Denetçiler Enstitüsü (The Institute of Internal Auditors)

INTOSAI	:	Uluslararası Sayıştaylar Birliği (International Organization of Supreme Audit Institutions)
ISACA	:	Bilgi Sistemleri Denetimi ve Kontrolü Derneği (Information Systems Audit and Control Association)
ISO/IEC	:	Uluslararası Standardizasyon Teşkilatı/ Uluslararası Elektroteknik Komisyonu (The International Organization for Standardization/ the International Electrotechnical Commission)
ISSAI	:	Uluslararası Yüksek Denetim Kurumları Standartları (International Standards of Supreme Audit Institutions)
ITGI	:	Bilgi Teknolojileri Yönetişim Enstitüsü (Information Technology Governance Institute)
JTC	:	Müşterek Teknik Komite (Joint Tecnical Committee)
KEKK/PLSR	:	Kısmi En Küçük Kareler (Partial Least Square Regression)
KİDDER	:	Kamu İç Denetçileri Derneği
PCAOB	:	ABD Kamu Gözetimi ve Muhasebe Standartları Kurulu (Public Company Accounting Oversight Board)
RMSE	:	Ortalama Hata Kareleri Toplamı Kökü (Root Mean Square Error)
SAS	:	Denetim Standartları (Statements on Auditing Standards)
SEC	:	ABD Sermaye Piyasası Kurulu (U.S. Securities and Exchange Commission)
TİDE	:	Türkiye iç Denetim Enstitüsü
TSE	:	Türk Standartları Enstitüsü
UMUÇ/IIPF	:	Uluslararası Mesleki Uygulama Çerçevesi (International Professional Practices Framework)
YEM/SEM	:	Yapısal Eşitlik Modeli (Structural Equation Modelling)

GİRİŞ

Organizasyonlarda tüm süreçler ve iş akışı olabilecek en doğru şekilde oluşturulmuş olsa da iç paydaşlar eğer süreçlerdeki faaliyetleri amaçlandığı şekilde yürütmek istemezlerse hedeflenen çıktıların elde edilmesi her zaman mümkün olmamaktadır. Bu durum paydaşların süreçlere ilişkin olumsuz yaklaşımı, kurum içi ve bölümler arası uyumsuzluk, farklı kişisel gündemler, üst yönetimin yetersiz desteği gibi nedenlerden kaynaklanabilir. Çalışma kapsamında ele alınacak olan iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişki kuruluşun bilgi varlıklarını korumak temelinde bir ortak amaç olarak ortaya çıkmaktadır. Ortak amaç bir başka deyişle iki fonksiyon arasındaki iş birliğinden doğması beklenen olası karşılıklı faydalar şeklinde belirtilebilir. Varlıkların korunması için gerek iç denetim gerekse bilgi güvenliği alanlarında detaylı standartlar ve çerçeve dokümanları söz konusudur. İç denetim ve bilgi güvenliği arasındaki ilişkiyi, bu ilişkiyi etkileyen faktörleri ve ortaya çıkabilecek olası faydaları ve değerleri ele alabilmek için öncellikle iç denetim ve bilgi güvenliği alanlarının incelenmesi gereklidir. İç denetim noktasında klasik teftiş anlayışından başlayarak iç denetime uzanan kavramsal değişim incelenmiştir. Bilgi güvenliği açısından da bilgi kavramı ve bilginin güvenliğini sağlama süreci ele alınacak ve tüm bu kavramlarla ilişkili kurum ve kuruluşlar ile standart ve çerçeveler incelenecektir.

Denetim fonksiyonu, günümüz denetim yaklaşımları çerçevesinde ele alındığında, organizasyonların hedeflerine ulaşmalarında önemli bir noktada değerlendirilebilmektedir. Başarılı ve güvenilir denetim fonksiyonu aynı zamanda başarılı ve güvenilir bir organizasyon anlamına da gelebilir. Denetim fonksiyonunun etkin ve etkili işleyişi neticesinde bir kurum ya da organizasyonun iş ve işlemlerindeki hesap verilebilirliği güçlenmektedir. Hesap verilebilirliğin artması, organizasyonun tüm paydaşlarının güvenini kazanmakla beraber organizasyona da değer katar. Geçmişten günümüzde iç denetim faaliyetleri güvence verme

süreçlerinin yanı sıra daha ziyade danışma hizmetleri ve denetim alanının daha da derinleşmesiyle organizasyona daha fazla değer katan bir anlayışa doğru evrilmiştir (Kotb ve ark., 2020, s. 3). Bununla beraber 2000'li yılların başlarında uluslararası alanda meydana gelen Enron, Arthur Andersen vb. denetim skandalları, denetim uygulamalarının güvenilirliğini tartışma konusu yapmıştır (S. Y. Kara, Ayşe N., 2012, s. 66). Global anlamda kalitesi ve başarısı ölçülebilir bir denetim uygulaması, kurumların amaçlarına ulaşmasını olumsuz yönde etkileme riski içeren belki de pek çok problemin önlenmesine yardımcı olabilecektir. Bu bağlamda "Uluslararası İç Denetim Standartları" ve COSO İç Kontrol Modeli gibi uluslararası alanda genel kabul görmüş yaklaşımların, organizasyonların ilgili denetim birimleri tarafından daha dikkatli bir şekilde ele alınır hale gelmesi kaçınılmaz olmuştur.

Söz konusu denetim standartları ve modellerin organizasyonlara uyarlanması elbette çok önemlidir ancak şu unutulmamalıdır ki, anılan adaptasyonun ne kadar etkili olduğu da ayrı bir değerlendirme konusu olmalıdır. Bir standart ya da modeli organizasyonda, amaçlanan doğrultuda kabul görüp görmediği ya da organizasyonun kaynakları doğru bir şekilde kullanılmakta olup olmadığı anlamında incelemek de önem arz etmektedir. İşte tüm bu etkenlik ve etkililik değerlendirmesinde denetçi gerek organizasyonun iç çevresinde gerek ise de dış çevresinden bilgi elde etmek durumundadır. İç denetim ve bilgi edinimi ilişkisi işte bu suretle başlamaktadır. Denetleyen taraf belirli bir sonuca ya da kanaate varabilmek için denetlenen taraftan denetim konusu kapsamında çeşitli düzeyde bilgi talep eder. Elde ettiği bilgileri değerlendirir, belirlenen standartlarla, mevzuatla ya da diğer önceden belirlenmiş olan plan ve prosedürler çerçevesinde değerlendirerek görevini tamamlama aşamasında gelir ve denetim raporunu ortaya koyar. Söz konusu denetim faaliyeti neticesinde örneğin organizasyonda dolaşımda olan finansal bilginin güvenilirliğinin artması, finansal raporlarda yer alan bilgilerin doğruluğunun artması gibi sonuçlar söz konusu olmaktadır (Kotb ve ark., 2020, s. 3). Dolayısıyla "bilgi" denetim faaliyetinin en kilit noktada yer alan unsurlarından birisidir. İşte bu noktada bilginin sağlıklı olup olmadığı, doğruları yansıtıp yansıtmadığı ya da dışsal faktörlerden etkilenerek kirlenip kirlenmediği gibi açılardan belirli bir güvenirlik seviyesinde olması gerekmektedir. Bilgi güvenliği tam

da bu süreçte ele alınmalıdır. Bilgi güvenliği standartlarına ve prosedürlerine tam uyumlu bir organizasyonun üreteceği veri sağlıklı bir denetimin yolunu açar ve buna bağlı olarak ortaya çıkarılacak bulguların ve gerekli düzeltmelerin tam da problemlerin çözümüne odaklı olabilmesini sağlar. Güvenli bir ortamdan elde edilmeyen bilginin gerek değerlendirme gerek ise de nihai bir kanaate varma anlamında organizasyonun amaçlarına yönelik olumlu sonuçlar doğurması beklenemez.

Bu çalışma kapsamında öncelikle Yönetim ve Organizasyon kavramları ele alınmıştır. Ardından bir yönetim fonksiyonu olarak Kontrol ve İç Kontrol kavramları incelenmiştir. İzleyen kısımlarda Denetim kavramı üzerinde durulmuştur. Klasik teftiş anlayışından risk odaklı modern denetim uygulamalarına kadar ki süreçte ortaya atılan ve tartışılan temel unsurlar incelenecektir. Bununla beraber denetim geçmişten bugüne farklı şekillerde uygulanabilmektedir. Denetim, amaçlarına ve yapılarına göre sınıflandırılabilir. Amaçlarına göre denetime finansal tablolar denetimi, uygunluk denetimi ve faaliyet denetimi, yapılarına göre denetime ise kamu denetimi, iç denetim ve bağımsız denetim (dış denetim) örnek verilebilir.

Genel olarak denetim kavramı ele alındıktan sonra iç denetimin incelenmesine başlanmaktadır. İç denetim güvence ve danışmanlık yoluyla olarak faaliyetleri geliştirmek ve organizasyona değer katmak amacını güder (Al-Taee ve Flayyih, 2023, s. 96). İç denetim, kurumun risk yönetimi, kontrol ve yönetişim süreçlerinin etkililiğini geliştirmek sistematik bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur (Kincaid ve Sampias, 2005, s. 14). Tanımdan da anlaşıldığı gibi iç denetim risk yönetimi, kontrol ve yönetişim süreçlerinin etkililiği gibi üç ana kavram üzerine oturmuştur. Bu üç kavram üzerinde yapılacak çalışmaların ise sistemli ve disiplinli bir şekilde gerçekleştirileceğine vurgu yapılmıştır.

İç denetiminin işleyişini ve unsurlarını inceleme aşamasında iç denetim fonksiyonunun sınırlarını ve içeriğini belirleyen uluslararası standartlar, ulusal mevzuat ve iç kontrol modeli incelenmektedir. Uluslararası standartlar arasında; Avrupa Birliği İç Denetim Standartları, ECIIA Avrupa İç Denetim Enstitüleri Konfederasyonu, A.B.D. Sertifikalı Kamu Muhasebecileri Enstitüsü Standartları

(AICPA), Amerikan Genel Kabul Görmüş Devlet Denetim Standartları (GAGAS), Uluslararası Muhasebeciler Federasyonu (IFAC) İlkeleri, Uluslararası Sayıştaylar Birliği (INTOSAI) - Kamu Kesimi İç Kontrol Standartları Rehberi ve son olarak da İç Denetçiler Enstitüsü (IIA) - Uluslararası Mesleki Uygulama Çerçevesi - Uluslararası İç Denetim Mesleki Uygulama Standartları (Standartlar) sayılabilir. Bu standartlarından uluslararası alanda en çok kabul gören ve yaygın kullanım alanına sahip olanlarından birisi olan İç Denetçiler Enstitüsü Uluslararası Mesleki Uygulama Çerçevesi önemli bir konumdadır. Çerçeve; iç denetimin tanımı, etik kuralları, standartlar, uygulama önerileri ile gelişme ve uygulama yardımları olmak üzere beş bölümden oluşmaktadır (Kincaid ve Sampias, 2005, s. 11).

Standartların ardından incelenecek olan Ulusal Mevzuat da standartlar gibi iç denetimin sınırlarını ve doğasını şekillendirir. İç denetim fonksiyonunu ilgilendiren temel mevzuat; 2006 yılı 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu, 6102 Sayılı Türk Ticaret Kanunu ve 6335 Sayılı Türk Ticaret Kanunu ile Türk Ticaret Kanununun Yürürlüğü ve Uygulama Şekli Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun, Sayıştay Kanunu, 22147 Sayılı Hazine Müsteşarlığı İle Dış Ticaret Müsteşarlığı Teşkilat ve Görevleri Hakkında Kanun, 5684 Sayılı Sigortacılık Kanunu, KHK/660 Karar Sayılı Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumunun Teşkilat ve Görevleri Hakkında Kanun Hakkında Kararname şeklinde belirtilebilir. Standartlar ve mevzuatın ardından iç denetim fonksiyonunun doğasını belirleyen temel etkenlerden biri de COSO iç kontrol modelidir. İç kontrol; kurumun yönetim kurulu, diğer yönetim birimleri ve tüm çalışanları ile etkileşim içinde bulunan ve operasyonel, raporlama ve uygunluk hedeflerine ulaşmada makul düzeyde teminat sağlamak için tasarlanan bir süreç olmakla beraber kontrol çevresi, risk değerleme, kontrol aktiviteleri, bilgi ve iletişim aktiviteleri ve izleme aktiviteleri olmak üzere beş farklı bileşeni içermektedir (Lupu, 2013, s. 7). COSO iç kontrol modeli, modelin gelişimi, özel sektör-kamu sektörü uygulanabilirlik durumu gibi çeşitli açılardan da incelenecektir.

İzleyen bölümde ise denetim uygulama süreci incelenecektir. Her süreç gibi denetim sürecinin yönetimi de sürecin başarısı açısından büyük önem arz etmektedir. Bu

bağlamda denetim sürecinin resmi bir belge ile garanti altına alınması ve sınırlarının belirlenmesi, konu ile ilgili politika ve prosedürlerin oluşturulması, planlama ve denetim için gerekli personelin belirlenip atanması gerekmektedir. Uygulama sürecinde belirlenmesi gereken bir başka konu da hangi tür denetimin uygulanacağıdır. Bu noktada iç denetçi uygunluk denetimi, performans/operasyonel denetim, bilgi teknolojileri denetimi, danışmanlık hizmetleri ve soruşturma hizmetleri gibi seçenekler arasından duruma uygun olan türü seçecektir. Uygun denetim türü veya türlerinin seçimini takiben iç denetçi denetim boyunca çeşitli yöntemlerden yararlanabilir. İç denetçinin yaralanabileceği yöntemler arasında, performans değerleme, program değerleme, niceliksel ve niteliksel yöntemler, usulsüzlükleri tanımlama ve soruşturma teknikleri, araştırma ve veri toplama teknikleri sayılabilir.

Çalışmanın üçüncü bölümünde Bilgi Güvenliği Yönetim Sistemleri (BGYS) ve İç Denetim ilişkisi çeşitli yönlerden incelenmiştir. Bu bölümde öncelikle, bilgi güvenliğine ilişkin temel kavramlar tanımlanacak ve bölümün izleyen bölümlerinde incelenecek olan konulara giriş niteliğinde bilgi verilmektedir. Ardından bilgi güvenliği yönetim sisteminin ana unsurları olan ISO/IEAC komitesi, Türk Standartları Enstitüsü ve ISO/IEC 27001 standardı detaylı bir şekilde incelenecektir. İzleyen kısımda BGYS iç tetkik faaliyetine ilişkin genel kavramlar ve konuyla ilişkili roller incelenecektir. Kavramlar ve kişilerin ele alınmasının ardından ise iç tetkik faaliyetinin aşamaları değerlendirilecektir. Bölümün son kısmında bilgi güvenliği ve iç denetim ilişkisi kurum içeriği, üst yönetim, planlama, destek, operasyon ve performans değerleme başlıkları altında incelenmiştir. Bölümün son kısmında ise Cumhurbaşkanlığı Dijital Dönüşüm Ofisince hazırlanan Bilgi ve İletişim Güvenliği Rehberi ve Bilgi ve İletişim Denetim rehberlerine değinilmiştir.

Çalışmanın uygulama aşamasında Bilgi Güvenliği Yönetim Sistemleri ve İç Denetimin fonksiyonu arasındaki ilişki çeşitli açılardan incelenecektir. Uygulama aşamasında amaçlanan konulardan biri, yapılacak alan çalışması ile iç denetim süreci ve sürecin çıktıları bağlamında iç denetim fonksiyonunda görevli iç denetçilerin bilgi güvenliği farkındalığının incelenmesidir. Amaçlanan bir diğer konu da elde edilen sonuçların değerlendirilerek iç denetim faaliyetlerinde bilgi güvenliği

standart, politika ve prosedürlerini kapsayan bir iç denetim faaliyetinin gerçekleştirilmesine yönelik olarak mesleki öneriler sunmaktır.

1 BÖLÜM
ORGANİZASYON VE İÇ DENETİM ÇERÇEVESİNDE TEMEL KAVRAMLAR

Bu bölümde çalışmada yer alacak kavramlar açıklanmaya çalışılacak ve bu çerçevede genelden özele gidilerek öncelikle Yönetim ve Organizasyon kavramları incelenecektir. Ardından belirtilen yaklaşım çerçevesinde, kontrol ve iç kontrol kavramları üzerinde durulmuştur. İzleyen kısımda iç denetim kavramından önceki son açıklanacak kısım olan denetim kavramı incelenmiştir. Son olarak İç Denetim kavramı incelenecek ve bu bağlamda ele alınan tüm kavramlar birbirleri ile olan ilişkileri, benzerlikleri ve farklılıkları açısından net bir şekilde ortaya konulmaya çalışılacaktır.

1.1 YÖNETİM VE ORGANİZASYON

Kurum ve organizasyonlar insanlar tarafından kurulur. Bu çerçevede genel tabloya bakıldığında insanlar tarafından kurulan, işletilen, faaliyetlerini devam ettiren organizasyonların; iş ve işlemleri, organizasyon yapıları, hukuki durumları ve benzeri özellikleri incelemeye konu olmaktadır. İşin özünde birey ve organizasyon vardır. Bireyler organizasyon içince karar verici ve faaliyetlerinden sorumlu organ olarak yönetimi oluştururlar. Organizasyon ve bu organizasyona yön veren yönetim birbirini bütünleyen iki kavramdır. Organizasyon bir anatomi, yönetim ise fizyoloji olarak düşünülebilir (Can, 1999, s. 21).

1.1.1 Yönetim Fonksiyonu

Denetim fonksiyonunu tanımlamak için öncelikle yönetim kavramının doğuşu ve gelişiminin kısaca değerlendirilmesi gerekmektedir. Yönetim kavramı insanlık tarihi ile benzer şekilde evrilmiştir. İlkel çağlarda insanlar avcı ve toplayıcı olarak yaşarlarken, küçük çaplı aile birliklerini yönetme ve onların ihtiyaçlarını karşılamaya yönelik kararlar verebilmekteydi. Aile bireyleri acıktığında, av ile sorumlu kişi bu

görevini yerine getirmek üzere ava çıkıyor ve ele geçirdiği avlar ile topluluğun yemek ihtiyacını karşılıyordu. İnsanlar bu dönemde göçebe ve tüketici konumda idi. Tarımı öğrenmeleri ve yerleşik hayata geçmeleri ile artık üretici konumunu da geçmişlerdi ve üretim kendisiyle içkin olarak teknik ve sosyal gelişimi de getirmekteydi (Ergeneli, 2006, s. 23).

1970'li yıllardan itibaren öne çıkmaya başlayan ve günümüzde en çok ele alınan konulardan biri olan küreselleşme dünyayı çeşitli boyutlardan etkilemektedir (Basku, 2009, s. 8). Benzer şekilde insanlığın tarihine bakıldığından yerleşik hayata geçiş de insanlığın gelişimini çeşitli yönlerden etkilemiştir. Bir yerde yerleşik olarak yaşamaya başlayan insan, yaşadığı yerdeki tüm çevresi ile etkileşim haline oluyordu ve bu etkileşim onu kendisi ve beraber yaşadıkları insanlar adına karar verme durumuna itiyordu. Gerçekten de tarihi sürece bakıldığında örneğin en eski uygarlıklardan biri olan Mısır uygarlığında insanlar belirli bir idari düzen oluşturmuş ve özellikle Nil nehrinde yer yer meydana gelen taşmalar ile savaşmak için sulama tesisi oluşturulması gerekmiş ve bunu yapabilecek bir memur sınıfı ortaya çıkmıştır (Ergeneli, 2006, s. 51).

Yönetim kavramı ele alınırken, şu unutulmamalıdır ki yukarıda da belirtildiği gibi fizyoloji, anatomiden ayrı düşünülemez. Dolayısıyla yönetim kavramı incelenirken organizasyon kavramı da ele alınmalıdır. Denetim sürecinde denetlenen kurum ya da organizasyon, yani denetim sürecinin nesnesi olarak organizasyon kavramı nasıl tanımlanmaktadır. Organizasyonun literatürde pek çok tanımı olmakla beraber birkaç temel özellik yardımı ile organizasyon açıklanabilir. Öncelikle organizasyon; bizim inceleyeceğimiz anlamı ile belirli amaçlar doğrultusunda, bireylerin gayretlerini birleştirdikleri, yapılandırılmış bir süreç, iş bölümü ve koordinasyon sistemi olarak tanımlanabilir (Koçel, 2001, s. 128).

Organizasyonun tanımı, tanımında yer alan ifadeler ve tespitler tek tek değerlendirilmeli ve denetlenen kurumu ele alırken tüm bu sosyal ve teknik gelişmeler dikkate alınmalıdır. Yukarıdaki tanımlar çerçevesinde organizasyon kavramı ele alındığında, öncellikle görülmektedir ki organizasyon bir yönetim

fonksiyonudur. Henri Fayol 1916 tarihli Genel ve Endüstriyel Yönetim adlı kitabında organizasyonların yönetim süreçlerini evrensel ve değişmez olduğunu belirtmiştir (Arslan, 2013, s. 1). Fayol yukarıda anılan ve bir maden işletmesinde edindiği deneyimler neticesinde ortaya çıkardığı eserinde tüm sınai işlerin bazı işlemleri gerektirdiğini ve bu işlemlerin sırasıyla; teknik işler, ticari işler, mali işler, güvenlik işleri, muhasebe işleri ve yönetim işleri olduğunu belirtmiştir (Memiş, 2006, s. 11). Fayol'a göre yönetim süreci beş fonksiyondan oluşmaktadır, bunlar öngörme ve planlama, örgütleme (organizasyon), yönlendirme, koordine etme ve kontroldür (Alp, 2012, s. 11). Bu tanım organizasyonun bir insanlardan oluşan bir bütün olarak değerlendiren anlamda değil; organizasyonu, yönetimin bir fonksiyonu olarak elen alan bir açıklamadır. Yukarıdaki bir diğer tanımda organizasyonun insan, iş ve teknoloji faktörlerini birleştiren bir sistem olduğu bahsedilmiştir. Gerçekten de organizasyonu sadece insan, sadece iş ya da teknoloji olarak anlamlandırmak bütünü görme açısından çok da yararlı olmamaktadır. Bu unsurların birbiri ile ilişkilendirilmesi gereklidir. Başka bir ifade ile organizasyon; iş ile iş, iş ile insan ve insan ile insan arasında oluşan ilişkilerdeki düzen ve düzenlemelerdir (Koçel, 2001, s. 124). İzleyen tanımda organizasyonun teknik ve sosyal faktörlerle ilgili bir düzenleme olduğu belirtilmiştir ki, bu tanım bir önceki cümlede açıklanan organizasyon içi ilişkilerin bir başka tarifi olarak düşünülebilir. Bir sonraki tanım çalışanlar, işler ve mevkilerin arasındaki otorite ve haberleşmeye dikkat çekmektedir. Bu kapsamda personel hareketleri, organizasyon içi tasarım ve işleyiş açılarından bir tanım yapılmıştır.

Yukarıda da görüldüğü üzere organizasyona ilişkin pek çok tanım vardır. Bunlardan bir başkası da organizasyonun deneyime olan yaklaşımına göre sınıflandırma yapan, bilen-anlayan-düşünen-öğrenen örgüt karşılaştırmasıdır. Organizasyonlar bu karşılaştırmalı yaklaşımda aslında bir anlamda hızla değişen dünyaya ve giderek çeşitlenen ve karmaşıklaşan bilgi akışına nasıl tepki verebilecekleri yönünden ayrıştırılmaktadır. Söz konusu karşılaştırma Tablo-1 yardımı ile ele alınmaktadır.

Tablo 1: Deneyim Sürecine Organizasyonel Yaklaşımlar Karşılaştırması

	Bilen Örgütler	**Anlayan Örgütler**	**Düşünen Örgüt**	**Öğrenen Örgüt**
Felsefe	Tek bir doğruya odaklanma	Strateji ve eylemlere rehberlik edecek güçlü kültürel değerler. "Yöneten efsane" ye inanmak.	İşletme faaliyetlerinin bir problemler silsilesi olarak görülmesi. Eğer bozulduysa tamir et.	Kendimizin nasıl deneyim yaşadığı da dahil olmak üzere, iş deneyimlerini irdelemek, geliştirmek ve değerini artırmak.
Yönetim Uygulamaları	Kontrollerin kurallar ve düzenlemeler ile sağlanması, kitabına uygunluk.	İşletme kültürünü netleştir, ilet ve pekiştir.	Problemleri belirle ve izole et, veri topla, çözümleri hayata geçir.	Cesaretlendirilmiş deneysel yaklaşım, kolaylaştırılmış sorgulama, yapıcı görüş farklılıkları, örnekli öğrenme, başarısızlıklardan ders çıkar.
Çalışanlar	Kurallara uy, neden diye sorma.	Davranışlara rehber olarak ortak değerleri kullan.	Programlı çözümleri istekli şekilde sahiplen ve yürürlüğe koy.	Bilgiyi topla ve kullan, yapıcı olacak şekilde tartış.

Müşteriler	İşletmenin en iyiyi bildiğine inanmalıdır.	İşletme değerlerine inan olumlu deneyimi güvence altına al.	Çözülmesi gereken birer problem olarak değerlendirilirler.	Açık ve süregiden bir diyaloğa sahip öğretme/öğrenme ilişkisinin bir parçasıdır.
Değişim	Artan şekilde, hali hazırdaki "en iyi yola "uygun olmalıdır.	Sadece "yöneten efsane" bünyesinde bir değişim olmalıdır.	Her derde deva olarak görülen problem-çözme programları ile hayata geçirilir.	Süregelen deneyim-değerlendirme-hipotez oluşturma-deney-deneyim sürecinin bir parçasıdır.

Kaynak: (McGill, 1993, pp. 67-79)

Tablo 1'de görüldüğü gibi organizasyonların değişime karşı verdikleri tepkiler farklılık göstermektedir. Bu gruplandırmada organizasyonlar, işletme felsefesi, yönetim uygulamaları, çalışanlar, müşteriler ve değişime karşı verilen tepkiler bağlamında incelenmişler ve bu tepkiler sonucunda bilen, anlayan, düşünen ve öğrenen organizasyonlar olarak sınıflandırılmışlardır. Bilen organizasyonların temel felsefesi işletme için en iyi tek bir yol olduğu ve bunun da düzenlemeler ile net bir şekilde belirlenerek, bu yolun izlenmesi her adımın kuralına uygun şekilde atılmasıdır. Çalışanlar işlemlerini gerçekleştirirken yaptıkları işleri sorgulamalı, bir diğer deyişle kuralda öngörülen şekilde gerçekleştirmelidir. Müşteriler de işletmenin en doğrusunu bileceğine inanmalıdır. Bu tür organizasyonda değişime yönelik geliştirmeler yapılsa da söz konusu geliştirmeler önceden belirlenen kurallar çerçevesinde gerçekleştirildiğinden, değişim taleplerine karşı yeterli esnekliği sağlamakta zorlanılabilir. Anlayan organizasyonlarda ise bilen organizasyondan farklı olarak işletmenin strateji ve eylemlerine rehberlik edecek güçlü kültürel

değerler ön plandadır. Yönetim çalışanlarına bu değerleri açıkça belirler ve iletir. Çalışanlardan da bu değerlere uygun hareket etmeleri beklenir. Değişim karşısında da işletme kendi temel değerleri çerçevesinde bir değişime olanak sağlamaktadır. Düşünen organizasyonlar ise tabloda da görülebileceği üzere problem odaklı bir işletme felsefesine sahiptir. İşletme faaliyetleri bir problem zinciri olup, bu zincirdeki herhangi bir problem var ise bunu düzeltmek esas amaçtır. Yönetim bir problem ile karşılaşıldığında onun ile ilgili veri toplar, problem üzerinde değerlendirmeler yapar ve problemi tamamen gidermeye çalışır. Problemin nedenine inilmekten ziyade problemin başarılı bir şekilde ortadan kaldırılması ön planda görülmektedir. Çalışanların da işletmenin bu problem çözüm odaklı felsefesini benimsemesi ve bu süreçte aktif görev alması beklenir. Müşteriler işletme faaliyetlerinin içinde yer alan problemlerden biridir. Müşterinin nasıl tatmin edileceği ya da neden işletmeyi tercih etmiyor oldukları da çözülmesi gereken problemlerdendir. Belirtilenlerden de anlaşılabileceği gibi işletme için değişime yönelik adımlar da yine her derde deva olarak gördükleri problem çözme felsefesi kapsamında atılmaktadır.

Öğrenen organizasyonlar ise diğerlerinden farklı olarak deneyime, deneyim sonra öğrenilen derslere odaklanmaktadır (McGill, 1993, s. 76). İşletmenin değişime karşı tepkilerini kuralına uygun olarak yapmak gerek işletme değerleri çerçevesinde gerçekleştirmek ya da her bir değişim gereğini nedenini incelemeden bir problem olarak görmek işletmenin zorlu ve değişen çevreye ilişkin alacağı konumu zorlaştırır. Oysa öğrenen organizasyonların temel felsefesi iş deneyimlerini derinlemesine incelemek, iyileştirmek ve geliştirmektedir. İşletmedeki kurallar ve değerler değişmez değildir. Yönetim, çalışanların deneyimler edinmesini, iş sürecinde sorgulayıcı davranmalarını, görüş farklılıklarından yapıcı sonuçlar doğmasını desteklemektedir. Böylece çalışan yanlış yapmaktan korkmadan hareket eder ve yaşadığı bu deneyimlerden veri elde eder. Elde edilen veriler de sonraki işlemleri için kendini geliştirebilmesini sağlar. Müşteriler ile açık ve süregiden bir diyalog vardır. Müşteri bir problem olarak görülmemekte olup müşterinin anlaşılabilmesi için açık diyalog yolları kullanılmaktadır. Değişime karşı işletmenin tepkisi deneyim sonu veri elde etmek, bu çerçevede bir hipotez oluşturmak ve deneyimlemek. Ardından değişime karşı gerekli adımı atmaktır. İşletme kendini sürekli geliştirmekte,

hatalarından ya da doğru adımlarından dersler çıkarmaktadır. Bununla beraber öğrenme kapasitesi olan organizasyonların Covid-19 salgını gibi radikal aksama durumlarında esnek kalmalarına yardımcı olduğu değerlendirilmiştir (Orth ve Schuldis, 2021, s. 518)

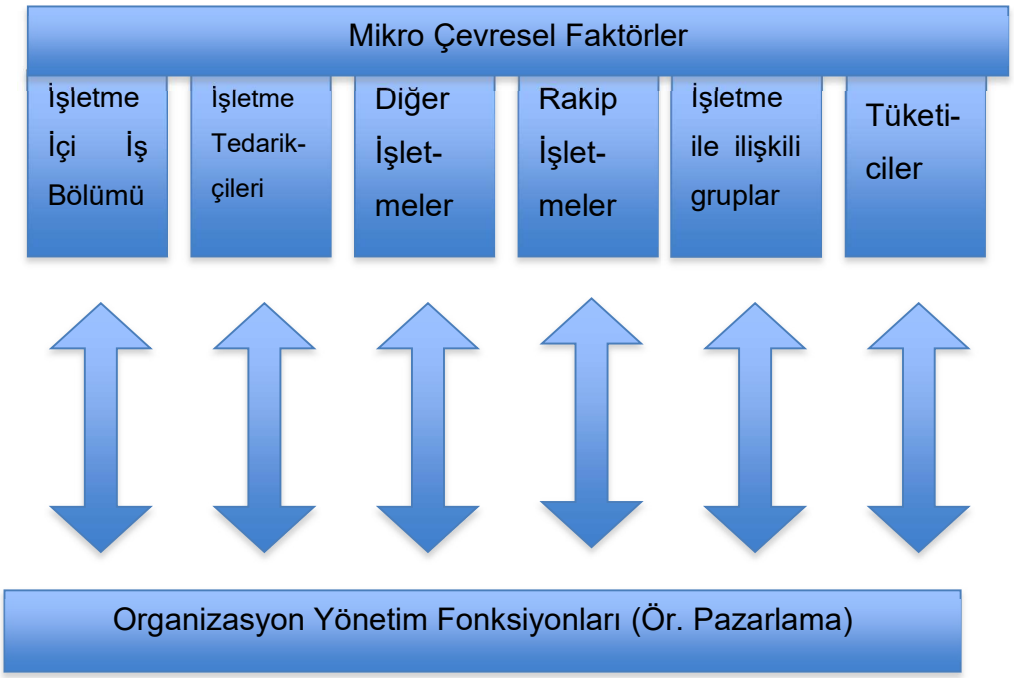
Çalışmanın ana konusu olan iç denetim ve bilgi güvenliği yönetimi çerçevesinde organizasyonların yenilikçi ve muhafazakâr olarak da sınıflandırılması faydalı olarak değerlendirilmektedir. Özellikle günümüzde hızla gelişen teknoloji, muhafazakâr organizasyonlar için bir meydan okuma ortaya çıkarmaktadır. Muhafazakâr organizasyonlar, mevcut ürün, hizmet, pazar ve dağıtım kanallarının, teknoloji ve süreçlerin devam edeceğini; yenilikçi organizasyon ise söz konusu iç ve dış çevrenin er ya da geç eskiyeceğini öngörür (Kılıç, 1989, s. 108). Örneğin bilginin dijitalleşmesi, bu çerçevede bilgi güvenliğine ilişkin yeni önlemlerin alınması gerekliliğini de beraberinde getirir. Kâğıt çıktı olarak çelik kasalarda korunan pek çok değerli evrak artık elektronik halde dijital güvenlik duvarlarının arkasında korunmaktadır. Teknolojideki bu tür gelişmeleri takip edebilmek, bu gelişmelere yönelik aksiyon alabilmek için yenilikçi organizasyon yapısında olmak ilgililere avantaj sağlayabilecektir. Yenilikçi organizasyon sadece bilgi güvenliği ve teknoloji ile ilgili alanlarda değil organizasyonun diğer unsurları çerçevesinde de bu yaklaşımı uygulayabilir. Örneğin yapılan bir araştırmada personel alımı sürecinde, adayın işletme ya da proje ekibinde yer alan diğer kişilerden çeşitli açılardan farklı olmasına önem veren organizasyonlarda diğer organizasyonlara göre piyasaya daha fazla sayıda yeni ürün sürüldüğü tespit edilmiştir (Kılıç ve Bariş, 2010, s. 238).

Günümüzde denetlenen organizasyonun yukarıdaki sınıflandırma içindeki yerini anlayabilmek, denetçinin, denetlenen organizasyonun yapısını ve yönetim felsefesi anlayabilmesi açısından da kolaylık sağlayabilir. Kurum ya da organizasyonu yukarıda belirtilen sınıflandırmalar çerçevesinde tanımak onun bilgiye verdiği değeri de belirlemek açısından faydalı olabilir.

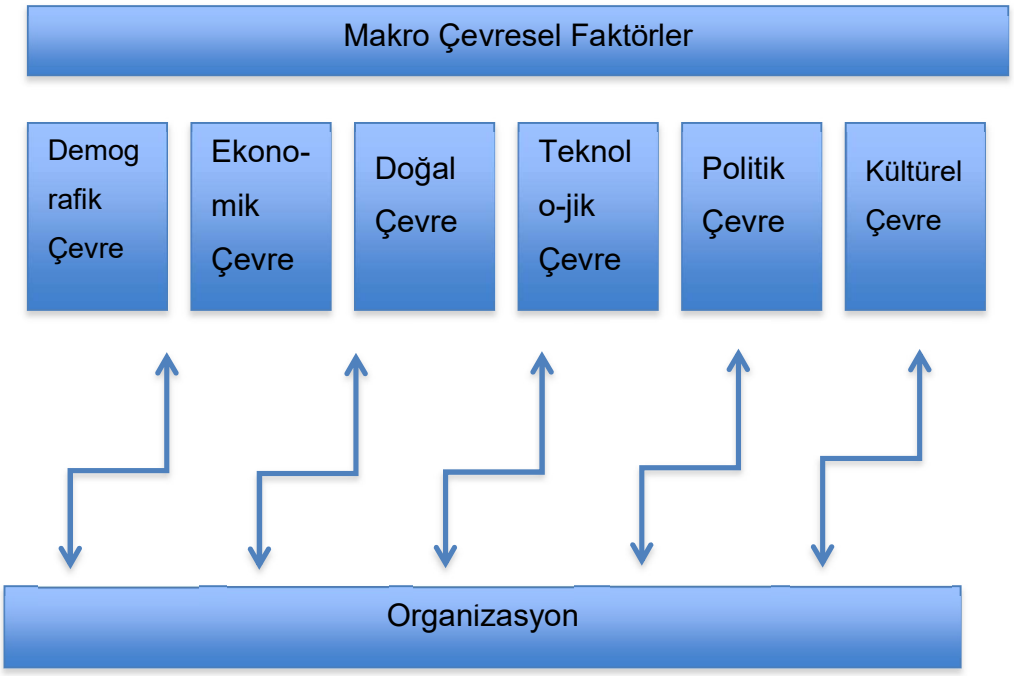
Organizasyonlar stratejik hedefleri doğrultusunda çeşitli kararlar alır ve bu kararları uygularlar. Söz konusu kararlar, personele ilişkin, bilgi güvenliğine ilişkin, iç düzene ilişkin ya da dış ilişkilere ilişkin olabilir. Tüm bu kararlar organizasyonun yetkili bir organı olan yönetim tarafından verilmektedir. Denetçi denetlediği organizasyonda

yönetimin rolünü ve sorumluluklarını kavrayabilmek için yönetim anlayışını, doğuşunu ve tarihsel gelişimini de kısaca değerlendirmelidir. Daha önce yönetim ve organizasyon ilişkisi incelenirken anatomi-fizyoloji örneği verilmişti. Bu bağlamda faaliyetine devam eden ve içinde yönetimi barındıran yapı organizasyondur ve yönetim bu yapı içindeki işlevdir (Koçel, 2001, s. 21). Bu işlev aslında organizasyonun karar verme yöntemlerine, faaliyetler arası eşgüdüm sağlama yollarına, çevreye uyum sağlayabilme esnekliğine, iletişim ağına ve amaçlarına ulaşmada elde edilenleri değerlendirecek araçlara gerek duyması, başka bir deyişle yönetime ihtiyaç duyması sonucu ortaya çıkan yönetim işlevidir (Koçel, 2001, s. 21). Bir örnek üzerinden yukarıdaki tanım incelenebilir. Örneğin yazılım sektöründe yer alan bir işletmenin yönetim ihtiyaçları nelerdir? İlk olarak işletmenin karar verme yöntemlerinin belirlenmesi gerekmektedir. Yönetim kurulu oluşturulabilir. Kurulun yetkileri, işletme sahibinin yetkileri arasındaki denge netleştirilebilir. Ardından faaliyetler arası eş güdüm sağmala amacıyla organizasyon içi iş bölümüne gidilebilir. Bölge ve il ofisleri oluşturulabilir. Bu birimlerden sorumlu yöneticiler ilgili görevlere atanabilir. Günümüzde belki de en önemli yönetim gereklerinden biri de çevreye uyum sağlama yeteneğinin geliştirilmesidir. Sosyal, kültürel, ekonomik ve teknolojik değişkenler organizasyon ile etkileşim halindedir. Yönetim tüm bu değişkenlerle olan etkileşimi yürütebilmelidir. Örnekteki işletme çerçevesinde düşünüldüğünde ürettiği yazılım çözümlerinin, global anlamda ortaya çıkan sistem virüsleri ya da zararlı yazılımlara karşı ne kadar güvenli olduğu, kullanıcıların bu tür siber saldırılara ilişkin bilinç düzeyi, yazılım güvenliği konusundaki son teknolojik gelişmeler ve bunun sonucunda rakip işletmelerde gözlemlenen ürün fiyatı değişimleri gibi faktörler çevresel değişkenlere örnek verilebilir.

Kaynakta, pazarlama fonksiyonu özelinde belirtilmiş olmakla beraber işletmenin geneline de uygulanabilecek olan bu çevresel faktörler işletmeye daha yakın olan ve işletmenin müşterilerine verdiği hizmeti etkileyen mikro çevresel faktörler ve bu mikro çevresel faktörleri etkileme gücüne sahip daha büyük çaplı faktörler olan makro çevresel faktörler olarak tanımlanmakta olup Şekil-1 ve Şekil-2'de belirtilmektedir (Kotler ve Armstrong, 2012, pp. 91-96).



Şekil 1: Mikro Çevresel Faktörler



Şekil 2: Makro Çevresel Faktörler

Şekil1 ve Şekil 2'de de görüldüğü gibi bir organizasyon yönetiminin kararları gerek mikro çevresel faktörlerin ve gerekse de makro çevresel faktörlerin etkisinde alınır. Söz konusu etki tüm çevre ile geçekleşen bilgi alışverişleri neticesinde söz konusu olmaktadır. İşletmeler çevreleri ile etkileşim halinde bulunan sistemler olarak düşünülebilir. Mikro çevresel faktörlerin etkisi çeşitli boyutlarda ele alınabilir. Örneğin bir işletme pazarlama fonksiyonu ile ilgili bir karar alma aşamasında, tedarik sağlayıcının hammaddenin kendisine ne zaman teslim edileceğini dolayısıyla kendisinin de ne zaman üretimi tamamlayabileceğini planlamalıdır. Ya da diğer işletmeler ile yapılan ortak girişimler işletmenin pazarlama fonksiyonunu etkiler. Bununla beraber rakip işletmede ortaya çıkan bir yenilik, yeni teknoloji, yeni pazarlama taktikleri, işletmenin de kendi pazarlama stratejisini gözden geçirmesini gerektirmektedir. Benzer şekilde işletmenin ilişkili olduğu kişi grupları da mikro çevresel faktörler kapsamındadır. Bu kişi gruplarına, finansal kişi grupları, medya kişi grupları, hükümet kişi grupları, sivil-hareket kişi grupları gibi işletmenin amaçlarına ulaşmasında etkisi olabilecek gruplar örnek verilebilir (Kotler ve Armstrong, 2012, s. 93). Şekil.2'de ise yönetimin etkileşim içinde makro çevresel faktörler belirtilmektedir. Yukarıda da belirtildiği gibi bu faktörler daha büyük çapta ve güçte etki unsurlarını kapsamaktadır. İşletme öncelikle satış yapmayı ya da hizmet sunmayı hedeflediği demografik çevreyi dikkate almalıdır. Örneğin bilgisayar okur yazarlığı olan bir kesime yönelik hizmet sunacak olan bir kurum ürün ve hizmetlerini bu doğrultuda oluşturmalıdır. Ya da benzer şekilde çocuklara yönelik sunulan bir hizmet ile yaşlılara sunulması hedeflenen hizmetlerin arasında farklar olması normal karşılanmaktadır. Ekonomik çevrede kaçınılmaz olarak organizasyon yönetiminin etkileşim içinde olduğu bir diğer makro çevresel faktördür. Ekonomik durgunluk ya da hızlı yükseliş dönemlerinde yıllık hedefler yeniden gözden geçirilerek güncellenir. Doğal çevre ise bugün özellikle gerek işletmelerin gerek tüketicilerin bilinç düzeylerinin artması ile önemli bir çevresel faktör haline gelmiştir. Bu bağlamda işletmeler çevreci üretim teknikleri ile fark yaratmayı amaçlamaktadırlar. Çevresel sürdürebilirlik, kendi enerjisini kendi üreten fabrikalar vb. kavramlar günümüzde önemli bir anlam kazanmaktadır. Bir diğer faktör olan teknolojik çevrede en hızlı değişim yaşanan faktörlerden biri olmaktadır. Özellikle

çevrim içi alışverişin geldiği nokta düşünüldüğünde işletmelerin bu faktörü dikkate almaları ve değişime hazırlıklı olmaları kaçınılmaz görünmektedir. Politik çevre ise adından da anlaşılabileceği gibi hükümetlerin belirli politikalarının işletme üzerindeki etkisini belirtir. Örneğin güneş enerjisi ve yeşil enerjiyi destekleme ve nükleer enerjiyi sonlandırma kararı alınan bir ülkede nükleer enerji temelli bir üretim organizasyonu oluşturmak mantıkla bağdaşmayabilmektedir. Makro çevresel faktörlerin sonuncusu ise kültürel çevredir. Burada toplumun temel kültürel değerleri ön plana çıkmaktadır. Çalışmanın önemi, evliliğin önemi, bireysel özgürlükler gibi kültürel değerler işletme ile tüketiciler arasındaki ilişkiyi şekillendirebilmektedir (Kotler ve Armstrong, 2012, s. 110).

Daha önce yönetimin, organizasyonun bazı ihtiyaçları karşılamak için gerek duyulan bir işlev olduğu ve bu gereklerin organizasyonun karar verme yöntemlerine, faaliyetler arası eşgüdüm sağlama yollarına, çevreye uyum sağlayabilme esnekliğine, iletişim ağına ve amaçlarına ulaşmada elde edilenleri değerlendirecek araçlara gerek duyması olduğu belirtilmişti. Çevreye uyum sağlama kavramı da yukarıdaki mikro ve makro çevresel faktörler bağlamında ele alınmıştır.

Bir diğer yönetim gereği de iletişim ağıdır. İletişim ağı işletmenin iç tasarımını oluşturan hiyerarşi, şube ağı, pozisyon konumlandırmaları gibi, işletmenin çeşitli durumlara karşı vereceği tepkilerin hızını ve karmaşıklığını belirleyen düzenlemeler olarak açıklanabilir. İletişimin özellikle bilgi güvenliği kavramı ile yakından ilgisi bulunmaktadır. Organizasyon gerek iç gerek ise de dış çevresiyle iletişimi kapsamında sürekli bilgi alışverişi söz konusu olmaktadır. Bu çerçevede elde edilen ya da iletilen bilginin güvenli ve sağlıklı bir şekilde el değiştirmesi, organizasyonun bu bilgileri kullanarak alacağı kararların yerindeliğine doğrudan etki edebilecek durumdadır. İşte yönetim, tüm bu gereklerin karşılanmasında sorumluluk alacak işlevin kendisidir.

1.1.2 Yönetim Düşüncesinin Tarihsel Gelişimi

Organizasyon ve işletme fonksiyonu olarak yönetim kavramları kısaca ele alındıktan sonra şimdi de yönetim düşüncesinin kısaca tarihsel gelişim aşamaları incelenecektir.

Bugünün organizasyonlarının yönetsel yapılarını anlayabilmek için yönetim anlayışının tarihçesi önem kazanmaktadır. Bu bağlamda şu bir gerçektir tarihin belirli dönemlerinde yönetim ve organizasyonlar açısından önemli kilometre taşları ortaya çıkmıştır. Bunlardan belki en eskisi yukarıda da bahsedildiği gibi insansın avcı-toplayıcı yaşam tarzından tarım yaşamına geçiş dönemi olmuştur. Tarım işleme ile beraber yerleşik hayata geçen insan ilk topluluklarını oluşturmuş, ürettiği ürün ve topluluk ihtiyaçları arasında bir denge bulmaya çalışırken belki de ilk yönetim işlevini yerine getirmiştir. İzleyen çağlarda insanoğlu yönetsel çabalarda bulunmaya devam etmiştir. Gerçekten de eski dönemlere ait olan ve bugün hala bir operasyon başarısı olarak ayakta duran Mısır Piramitleri, Machu Pichu Kasabası gibi yapılar bize tüm bu karmaşık operasyonların başarılı bir şekilde yönetildiğine dair ipuçları vermektedir. O günün teknolojisi ve mühendisliğe ile bugün hala ayakta duran Mısır Piramitlerinin yapım aşamasında yönetsel başarının söz konusu olması işten bile değildir. Buna benzer pek çok yapı ya da günümüze uzanan eski yazıtlarda yönetim çabalarına dair çeşitli fikirler ileri sürülmüştür.

Yönetim açısından önemli bir adım 15.YY sonlarında İtalya'da bugün hala geçerliliğini koruyan çift taraflı kayıt sisteminin bulunması ve yine aynı dönemlerde Niccolo Machiavelli ortaya attığı liderlik ve yönetime dair fikirlerdir (Can, 1999, s. 31). Muhasebe alanında yapılan bu büyük buluş işletmelerin finansal durumlarını sağlıklı bir şekilde takip edebilmelerine ve doğal olarak da daha karlılık ve düşük maliyet gibi hedefler doğrultusunda daha etkin bir yönetim anlayışını geliştirmelerine yardımcı olmuştur. Ayrıca çift taraflı kayıt sisteminin bulunması, bilginin kayıt altına alınması, değerlendirilmesi ve saklanması anlamında da bir ilk olarak değerlendirilebilir.

Dünya tarihinde yönetsel gelişimi anlamada yardımcı olabilecek belki de en önemli kilometre taşlarından biri sanayi devrimidir. Çünkü sanayi devrimi ile toplumların organizasyonların yapısında köklü değişimler meydana gelmiştir. Sanayi devrimi ile kısaca;

- İnsan emeği ve becerisi makinalara dönüştürülmeye başladı,
- Başkalarının işinde çalışmaktan dolayı ücretli işçi sınıfı ortaya çıktı,

- Yeni düzende sermayedar girişimciler, iş, hammadde ve makinaları yönetmek, ortak bir amaç uğruna kişilerin çabalarını eşgüdümlemek görevini üstlendiler,
- Endüstriyel devrimin sonucu olarak işletme yönetim anlayışında sahiplik ve yöneticilik arasında bir fark görülmediğinden hemen olmasa da ilerleyen dönemlerde yönetsel devrim ortaya çıktı(Can, 1999, s. 31).

Söz konusu bu köklü gelişmeler sonrasında yönetsel alanda pek çok çalışma ve sınıflandırma yapıldı. İzleyen kısımda bu yönetim anlayışları kısaca ele alınmakta ve ardından dünyada ve Türkiye'de denetim kavramının tarihsel gelişimi üzerinde durulmaktadır. Tarihsel gelişim çerçevesinde ilk ele alınacak yönetim akımı Klasik akımdır. Klasikler yönetim alanındaki ilk sistematik bilgi kümesini oluşturan yazarlar olarak adlandırılabilir (Can, 1999, s. 32). Klasiklerden ilk alınacak anlayış Bilimsel Yönetim anlayışıdır. Taylor'un başını çektiği mühendislerden oluşan bu akımın temel özellikleri kısaca şu şekildedir:

- Yönetim uygulamasında bilimsel yöntemlerin kullanılması ve geliştirilmesi, o işler ilgili tasarlanan en iyi yolun izlenmesi,
- İşe en uygun kişinin işe alınması ve alım sürecinde bilimsel yaklaşımların kullanılması,
- İşçiye bilimleş bir eğitim, öğretim ve kendini geliştirme olanağı sunulması ve böylece içten bir iş birliği oluşturulması,
- Yönetim ve işçilerin görevlerini ayırmak (Can, 1999, s. 34).

Klasikler içindeki bir sonraki anlayış Genel Yönetim Anlayışıdır. Anlayışın öncülerinde olan Fayol'a göre yönetimin beş işlevi vardır. Bunlar planlama, örgütleme, kumanda etme, eşgüdüm sağlama ve kontrol etmedir. Görüldüğü gibi Genel Yönetim anlayışı, adından da anlaşıldığı gibi bir önceki anlayış olan Bilimsel yönetim anlayışına nazaran daha makro bir çerçevede işletmeyi ele almaktadır. Klasikler içinde bir diğer anlayış işe Bürokrasi Modelidir. Max Weber'in geliştirdiği modelde bürokratik örgütlerin, iş bölümü, merkezileşmiş otorite, rasyonel personel yönetimi, yazılı kayıt tutma ve arşivleme, açıkça belirlenmiş işletme politikası gibi keyfiliği önleyici ilkeler tanımlanmıştır.

Klasik akımı, onların bazı yönlerini eleştiren ve yeni fikirler ile ortaya çıkan Neo-Klasik Akım izlemektedir. Çok kısa bir şekilde açıklamak gerekirse Neo-Klasik akım daha ziyade klasik akımın insana yönelik eksik yönlerini tamamlama yoluna gitmişlerdir. İnsanın davranışlarının iş koşullarına ve güdülere göre değişebileceğini belirtmişlerdir. Neo-Klasikleri izleyen akım ise Modern Yönetim Kuramları olarak belirtilebilir. Modern yönetim kuramlarında öne çıkan ve bu çalışmada ele alınacak olan yaklaşım ise Sistem yaklaşımıdır. Sistem yaklaşımın temelinde sistem olarak ele alınan bütünün amacını gerçekleştirmesi vardır ve bu bakış açısında ağırlık o sistemin amaçları, sistemin içerdiği alt sistemler, alt sistemler arasındaki ilişkiler ile bunların bütüncül sisteme yaptığı katkı üzerine yönelmektedir (Koçel, 2001, s. 187). Son olarak bu üç temel akımın birbiri ile karşılaştırmaya yardımcı olacak kıyas tablosu aşağıda gösterilmektedir.

Tablo 2: Yönetsel Akımlar Karşılaştırmalı Tablo

Organizasyon Teorisi	Organizasyon Yapısı	Başlıca Süreçler	İlgili Değer Yargıları
Klasik	-Ayrıntılı Görev Tanımları -Departmanlaşma -Hiyerarşi	-Amaçlar -Planlama -Organizasyon -Emir Komuta -Karar verme	-Rasyonellik -Başarı Motifi -Çok çalışma -Tüketim değil tasarruf
Neo-Klasik	-Enformel Organizasyon -Enformel Küçük Gruplar	-Kararlara katılma	-Duygular -Anlama -Doğruluk
Sistem	-Bilgi işleyen bir birim olarak organizasyon -Açık Sistem -Bilgi Akışı	-Bilgi / Haber -Bilgi işleme -Karar verme -Kontrol	-Açıklık -Gestalt (Bütüncü-lük)

	-Alt sistemler arası ilişkiler		

Kaynak: (Koçel, 2001, s. 199).

Sistem yaklaşımının, organizasyon yapısı, başlıca faaliyetleri ve ilgili değer yargıları açısından klasik ve neo-klasik yaklaşımlar ile karşılaştırılmasını gösterir tablo yukarıda verilmektedir. Tablodan da görüldüğü gibi Klasik yaklaşımda organizasyon yapısının özellikleri arasında açık ve net görev tanımları, pozisyonların belirlenmesi, ast-üst ilişkilerinin belirlenmesi yer alırken neo-klasik yaklaşımda enformel organizasyon ve enformel küçük gruplar ele alınmıştır. Sistem yaklaşımında ise aynı başlık altında sistemi ele alan özellikler belirtilmiştir.

Tüm bu yaklaşımlarda belki de en büyük ortak nokta organizasyon yönetimlerinin tüm faaliyet dönemleri boyunca çeşitli kararlar alacak olmalarıdır. Bu kararlar işletmeyi amaçlarına, paydaşları da fayda maksimizasyonuna taşımayı hedeflemektedir. Söz konusu kararlar departman içi, departmanlar arası, organizasyonun bütününü kapsayan ya da sadece belirli çalışanları ilgilendiren kararlar olabilir. Görüldüğü üzere çeşitli karar türleri söz konusu olabilmektedir ancak buradaki tek ortak nokta bir kararın alınması için karar alıcının yeterli bilgi ile donatılmış olması gerektiğidir. Yöneticinin karar almada ihtiyacı olan bilgi iki türe ayrılabilir (Büyükmirza, 2008, s. 23):

- Yöneticide var olan bilgi; bu bilgi bir tür kişisel tecrübe ve eğitimin sonucu yöneticinin biriktirdiği toplam olarak değerlendirilebilir
- Çevreden sağlanan bilgi; yöneticinin kendisinde hali hazırda olmayan ve belirli olaylara ilişkin ihtiyaç duyduğu bilgi türüdür. Karlılığa ilişkin bir karar alınmasında yönetici finans departmanından bilgi talebinde bulunur ya da personel istihdamı konusunda insan kaynakları departmanı devreye girer.

Görüldüğü üzere yönetimin karar alma aşamasında en önemli girdilerden biri bilgidir. Bilgi kurumların gerek iç işleyişlerinde gerek ise de karşılaşılan sorunların çözülmesinde kolaylaştırıcı bir etken olabilmektedir (Ünlü ve Çakmak, 2023, s. 2). Genel anlamda bilginin organizasyon içinde güvenli şekilde tutulması ve yönetilmesi hem yönetim açısından hem de denetim açısından çok önemlidir. Yönetim

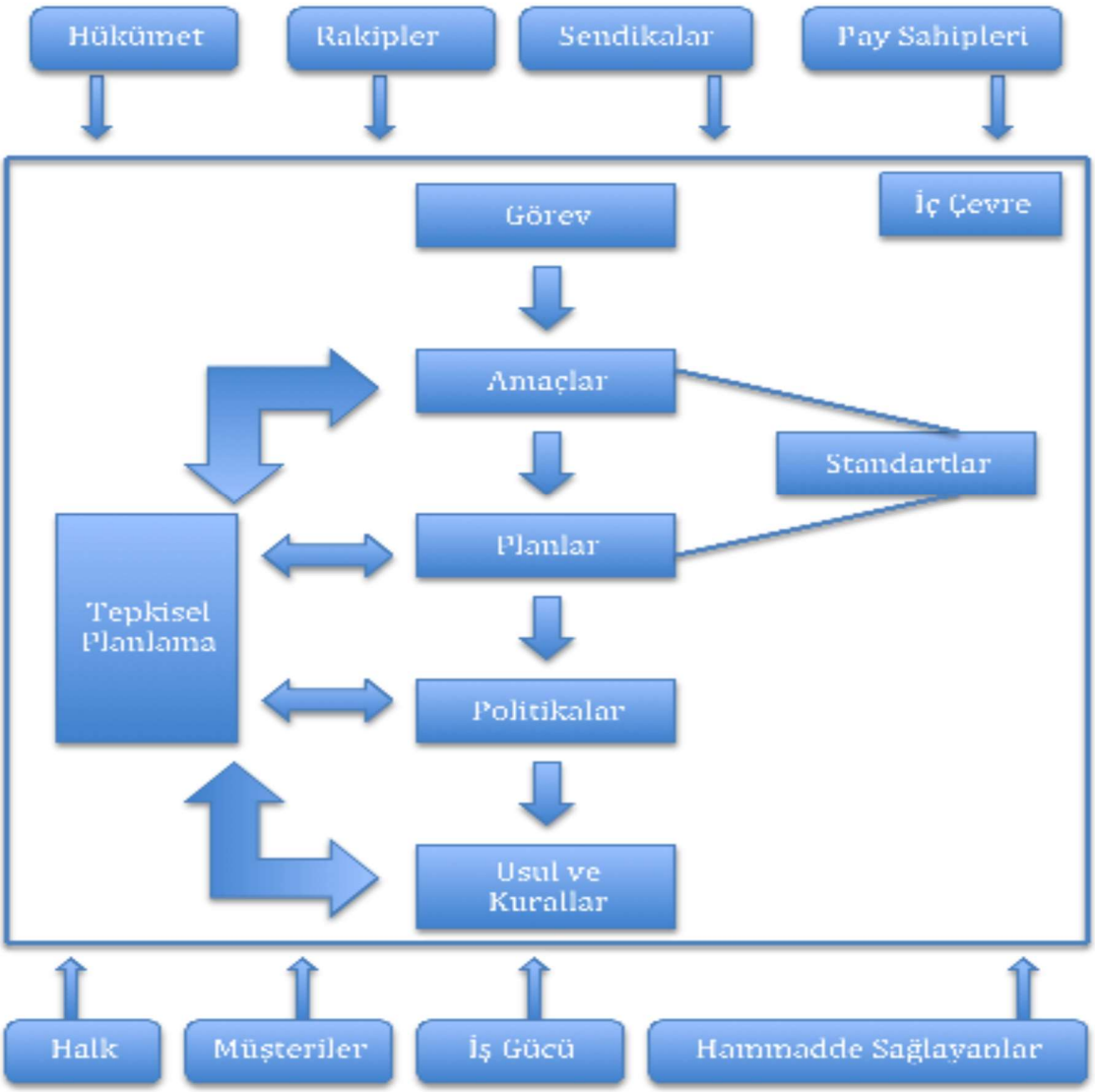
açısından önemlidir çünkü kararlarına esas teşkil eder. Denetim için önemlidir çünkü incelenecek, tespit edilecek ve rapor bağlanacak tüm bulgular, elde edilen bilgiler ışığında gelişmektedir. Bilgi; organizasyondaki diğer tüm varlıklar gibi, organizasyon için önemlidir ve korunması gerekmektedir (TSE, 2015a, s. 12). Söz konusu bilginin korunması konusu ise çalışmanın ilerleyen bölümlerinde bilgi güvenliği başlığı altında detaylı bir şekilde ele alınmaktadır.

1.2 KONTROL VE İÇ KONTROL

Denetim kavramı ele alınırken, onunla beraber birçok kavrama da atıflarda bulunulmaktadır. Bu çerçevede kontrol ve iç kontrol fonksiyonları da iç denetim kavramının açıklanmasında önem teşkil eden başlıklardandır. İşletme fonksiyonları esas itibariyle içinde bulundukları zamanın ve toplumların ekonomik, teknolojik ve kültürel değişimleri paralelinde değişebilmektedir. Daha açık bir ifadeyle önceki bölümlerde belirtilen işletmenin beş temel fonksiyonundan biri olan kontrol fonksiyonu, organizasyonların tarihsel gelişimine paralel olarak gelişmiş ve şekillenmiştir. Ancak burada dikkat edilmesi gereken husus kontrolün işletme bilimi açısından bir yönetim fonksiyonu olduğu ve yönetim fonksiyonu dışında başka kişi veya organizasyonlarca yapılan ve yönetim fonksiyonu olan kontrol ile benzer özellikler taşıyan faaliyetlerin denetim olarak adlandırılmasının kavram karmaşasının önüne geçmek açısından önem teşkil ediyor olmasıdır (Çatıkkaş, 2005, s. 4). Dolayısıyla genelden özele doğru bir yaklaşım çerçevesinde denetim kavramının ele alınmasından önce kontrol ve iç kontrol kavramları incelenecektir.

1.2.1 Kontrol

Çalışmanın önceki bölümlerinde Fayol'un yönetim süreci fonksiyonlarının öngörme ve planlama, örgütleme (organizasyon), yönlendirme, koordine etme ve kontrol olduğu belirtilmişti. İlk dört fonksiyon kısaca ele alınacak ve ardından kontrol fonksiyonun tanımı ve diğer fonksiyonlar içindeki konumu ve önemi değerlendirilecektir. Öngörme ve planlama süreci bir tablo ile özetlenecek olursa;



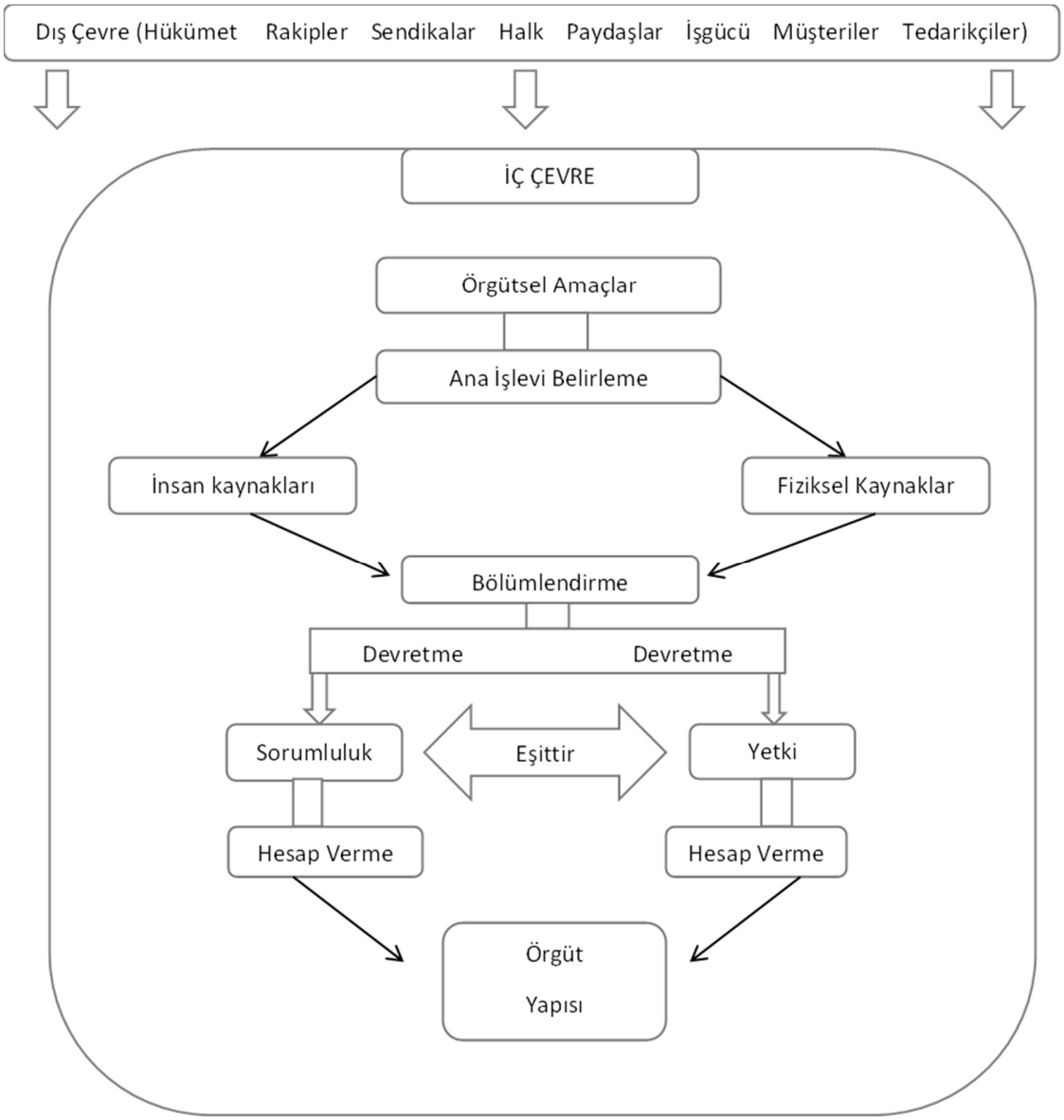
Kaynak : (Can, 1999, s. 61)

Şekil 3: Planlama Süreci

Planlamanın; özellikle denetçi bakış açısından ele alındığında, ilerideki bölümlerde açıklanacak olan kontrol çevresinin oluşmasındaki rolü düşünüldüğünde önemli bir noktada olduğu söylenebilir. Bununla beraber planlamanın iki temel ayağından biri geleceğe dönük olarak yapılması ve bir diğeri de organizasyonun risk ve amaçları

ile ilişkili olmasıdır (Koçel, 2001, s. 89). Denetimin en genel anlamı ile organizasyon iş ve işlemlerinin belirli mevzuat ve kurallara uygunluğunun değerlendirilmesi olduğu düşünüldüğünde, planlama fonksiyonu tam da organizasyonun iş ve işlemlerinin oluşturulması aşamasını işaret eder. Gerçekten de planlama aşaması organizasyonun tabiri caiz ise yol haritasının belirlendiği ve ileride denetime konu olacak iş ve işlemlerinin temellerinin atıldığı ilk ve belki de en önemli yönetim fonksiyonudur. Bu süreçte amaçlar ve söz konusu amaçlara ulaşılması için gerekli olan faaliyetler belirlenir (Can, 1999, s. 61). Yukarıda verilen tablo çerçevesinde bir kuruluşun planlama süreci örneği verilebilir. Kuruluşunun insanı yardım faaliyetleri alanında hizmet verdiğini düşünülsün. Bu çerçevede örneğimizde yer alan organizasyonun görevi yardım muhtaç kişilere yardım götürülmesini sağlamak denebilir. Amaçlar ise görevin saptanmasından sonra istenen sonuçların elde edilmesi saikiyle oluşturulur ve ardından bu amaçları başaracak yöntemler olan planlar geliştirilir (Can, 1999, s. 62). Tabloda amaçlar ve planlar arasında standartlar kısmı yer almaktadır. Standartlar özellikle bu çalışma için çok önemli bir noktadadır çünkü gerek Uluslararası İç Denetçiler Enstitüsü Standartları gerek ise ISO 27001: 2013 Bilgi Güvenliği Yönetim Sistemi standartları olsun incelenecek temel konular daima veri standartlar ile gerçekleşen uygulamalar arasındaki uyum çerçevesinde olacaktır. Tablodaki standartlar kavramı bir örnek ile şu şekilde ele alınabilir. Örneğin organizasyon geçen yıla göre yardım götürdüğü insan sayısını 1/3 oranında artırmayı hedefleyen bir plan oluşturmuştur. Bu hedeflenen 1/3'lük oran organizasyonun başarı oranı olarak değerlendirilebileceği ya da değerlendirilemeyeceği bir standart olmaktadır. Tablo üzerinden devam edilirse politikalar ile usul ve kurallar ve tüm bu sürecin aşamalı ile ilişkilendirilen tepkisel planlama kavramları ortaya çıkmaktadır. Organizasyon amaçlarının analizine dayanan ve planların başarılmasına yardımcı olan genel rehberlere politikalar denilirken, usuller ortaya konan adımları, kurallar ise eylemlerin sınırlarını çizen ayrıntılı belirlemeler olup tepkisel planlama ise bu dinamik süreç içinde ortaya çıkan değişikliklere gerekli uyumlaştırmaların yapılabilmesi anlamına gelmektedir.

Planlama fonksiyonu ve kontrol fonksiyonları arasında örgütleme, yönlendirme ve koordine etme fonksiyonları yer almaktadır. Örgütleme, yukarıda değerlendirilen planlama fonksiyonu çerçevesinde uygulanabilmesini sağlayacak koşulların oluşturulması olarak tanımlanabilir. Koşulların oluşturulmasından kasıt, organizasyon içi iş bölümünün gerçekleştirilmesi, çalışanlara kendi sorumluluklarının net bir şekilde açıklanması, uzmanlaşmanın teşvik edilmesi, ayrıca her bir işin iş akışının belirlenmesi ve bu çerçevede tüm fiziki şartların belirlenmesi ve uygulanması olarak belirtilebilir. Örgütleme süreci bir tablo yardımı ile aşağıdaki gibi gösterilebilir:



Kaynak :(Can, 1999, s. 102)

Şekil 4: Örgütleme Süreci

Tablodan da görüleceği üzere, örgütleme sürecinin dış çevre faktörleri arasında Hükümet, Rakipler, Sendikalar, Halk, Paydaşlar, İşgücü, Müşteriler ve Tedarikçiler (Ham madde sağlayanlar) olarak belirtilmiştir. Dış çevre faktörlerine örnek olarak Hükümetin Avrupa Birliği uyum çalışmaları kapsamında çıkardığı bir yeni bir iş kanunu ya da yurt dışı kaynaklı petrol ham maddesinin üretici ülkeler tarafından kısıtlanması sonucu oluşan petrol talep fazlası verilebilir. Dış çevreden sonra

örgütleme sürecinin iç çevresi ele alındığında, organizasyon faaliyet gösterdiği alandaki amaçlarını belirlemek ve bu amaçlara ulaşmadaki ana işlevlerini ortaya koymalıdır. Bir örnek üzerinden gidilecek web tasarım işletmesinin örgütsel amacı piyasadaki en güvenilir ve kullanıcı dostu arayüze sahip web siteleri tasarlaması ve hizmete sunması olacaktır. Bu amaç doğrultusunda dünyadaki en güvenilir bulut depolama sistemleri ile iş ortaklığı yapması, en başarılı kod yazıcı bilgisayar yazılımcılarını bünyesinde barındırması gerekecektir. Nihai olarak tüm bu gerekleri eşgüdümleyecek bir örgüt yapısı meydana getirilecektir.

Kontrol fonksiyonuna gelmeden bir önceki fonksiyon ise yukarıda yer alan örgütleme fonksiyonun ardından gelen yöneltmedir. Yöneltme yukarıda anlatılan organizasyon hedeflerine ulaşmada ortaya konan planlara uygun şekilde katılım sağlamaları amacıyla organizasyon çalışanlarını harekete geçirecek önlemlerin alınması olarak tanımlanabilir. Bu bölümde son olarak kontrol fonksiyonu incelenmektedir. Özellikle iç kontrol, denetim ve iç denetim kavramlarının ele alınacağı izleyen bölümler için kontrol fonksiyonu önemli bir konumdadır. Kontrol en geniş anlamıyla; bir kişinin, bir konu ya da bir organizasyonun üzerinde egemenlik kurmayı ve onu istenilen yöne yöneltmeyi sağlayan yöntem ve davranıştır. Fayol'un kontrol tanımının İngilizceye çevirileri arasında bazı farklılıklar olmakla beraber temel fark geniş ve dar kontrol tanımı olmasından kaynaklı olmakla beraber sırasıyla kontrol, bir işletmede işlerin programa, verilen talimatlara ve kabul edilen ilkelere göre yürüyüp yürümediğinin doğrulanması ve diğer tanım da kontrol, her şeyin yerine getirildiğinin tespiti olarak belirtilebilir (Kulak, 2009, s. 8). Kontrol kavramının literatürde karşılaşılan pek çok tanımı olmakla beraber özetle organizasyon bünyesinde yürütülen faaliyetlerin ve bu faaliyetler neticesinde ulaşılan sonuçların planlara uygunluğunun sağlanması olarak tanımlanabilir (Büyükmirza, 2008, s. 38). Kontrolun temel unsurları; konu, amaç ve amaca ulaşa gücü şeklinde sıralanabilir (Yılancı, 2015, s. 11). Yukarıda da değinildiği üzere kontrol temel olarak, daha önceden belirlenen ya da planlanan sonuçlara ulaşılmada uygulanan karar ve politikalar bütünüdür. Bu çerçevede kontrolün dört temel aşamasından söz edilebilir (Can, 1999, s. 227):

- *Amaç, Plan ve Politikaların Işığında Standartların Belirlenmesi;* ileride denetim ve iç denetim bölümlerinde daha detaylı değinilecek olan standartlar kavramı kontrol açısından da önemli bir noktadadır. Burada temel anlayış organizasyonun faaliyetlerinin sonuçlarının bir ölçüt ile karşılaştırılması gereğidir. Bu ölçütler standartlar olarak adlandırılır. Standartlar organizasyonun yönetimi tarafından belirlenebileceği gibi üst-organizasyonlar (birlikler-odalar vs), hükümetler, uluslararası organizasyonlar (Uluslararası İç Denetçiler Enstitüsü) ya da çok uluslu siyası yapılar (Avrupa Birliği) tarafından belirlenebilir. Standartlara en basit örnek üretim yapan bir organizasyonda planlanan üretim birimidir.
- *Yapılan Faaliyetlerin Ölçülmesi;* bu aşamada belirlenen standartlar ile karşılaştırma aşamasına hazırlık olması anlamında yapılan faaliyetlerin ölçülmesidir. Elde edilen sonuçlar bir sonraki aşamada belirlenen standartlar ile karşılaştırılır.
- *Mevcut Faaliyetlerin Sonuçlarının Önceden Belirlenen Standartlarla Karşılaştırılması;* ölçülen faaliyet sonuçları daha önceden belirlenen standartlar ile karşılaştırılır. Ortaya çıkan farka sapma adı verilmekle beraberi, belirlenen sınırlar altındaki sapmalar kabul edilebilir ancak belirlenen sınır üstündeki sapmalar için yönetici bir karar vermelidir,
- *Düzeltme Kararı Verme;* bu aşamada yönetici bir karar alma durumunda olabilir, söz konusu faaliyeti düzeltme kararı verir ya da ortaya çıkan sapmayı kabul edilebilir seviyede görerek herhangi bir düzeltmeye ihtiyaç olmadığına karar verir.

Denetim kavramı kapsamında kontrol ise denetim sürecinin başlangıç kısmı ya da organizasyonda denetimden önce hali hazırda gerçekleştirilmiş olan faaliyetlerdir (Kaval, 2008, s. 4). Fayol'a göre denetim ise organizasyon tüm iş ve işlemlerinin verilen emirlere, önceden belirlenmiş kurallara uygun yapılıp yapılmadığı olarak tanımlanabilir (TİDE, 2012a, s. 76). Yönetim bilimleri açısından denetim ise kısaca planlanan amaçlara ulaşılıp, ulaşılamadığının tespiti ve ulaşılamadı ise nedenleri ve yapılması gerekenler bütünü olarak değerlendirilebilir (Tok, 2010, s. 4). Her

organizasyonda hedeflere ulaşmada ortaya çıkacak risklere ya da bozulmalara karşı çeşitli önlemler alınmaktadır. Bu çerçevede örneğin finansal bir şirkette söz konusu kontroller bir kontrol listesi (checklist) yardımı ile yapılabilir. Riskler sadece kontrollerde meydana gelen bozulmalar olarak değerlendirilmemeli, risk kavramı daha genel bir çerçeve ile ele alınmalıdır (IIARF, 2016c, s. 80)

1.2.2 İç Kontrol

İç kontrol, organizasyona duyulan güvenin en temel sağlayıcılarından biri olarak düşünülebilir. Kısaca açıklamak gerekirse; iç kontrol organizasyon üst yönetimi, diğer yöneticileri ve çalışanlarının da içinde bulunduğu bir süreç olup, amacı işletme faaliyetlerinin etkililiği, verimliliği, ve mevzuata uygunluğu gibi amaçların gerçekleştirilmesinde yeterli güvence sağlamaktır (Kurnaz ve Çetinoğlu, 2010, s. 36). Kamu maliyesi anlamında ise kaynakların gereklere uygun şekilde, süreçleri yaratma ve uygulama konusundaki yönetimin sorumlulukları olarak anlaşılmaktadır (BÜMKO, 2016). İç kontroller kurumun tüm sistemlerini kapsar ve iç kontrollerin kalitesinde oluşabilecek bir bozulma dış denetim süreçlerinde aksamaya kadar varabilecek zincirleme problemlere neden olabilir (Ettredge ve ark., 2006, s. 20). Örneğin bir iç kontrol faaliyeti adımının atlanması ya da eksik yapılması kuruma gelen denetçinin söz konusu adımı tekrar gerçekleştirmesine, denetim sürecinin gereksiz olarak uzaması ve dolayısıyla kaynakların etkin olarak kullanılmaması durumuna yol açabilir. Yukarıda da belirtildiği üzere iç kontroller işletme faaliyetlerinde çeşitli amaçlar doğrultusunda gerçekleştirilir. Söz konusu amaçlar bilginin doğruluğu, kaynak sağlama, varlıkların korunması şeklinde sıralanabilir (Kapic, 2013, s. 63).

İç kontrol kurum kaynaklarının verimli olarak kullanılmasını sağlamayı hedeflerken, iç kontrol faaliyetlerinin verimliliğini sağlamak da ayrıca öne çıkan bir aşamadır. Kurumlar iç kontrol faaliyetlerini izleyerek bunların etkinliği konusunda çalışmalar yapmaktadırlar. Özellikler 2002 yılında Amerika'da çıkarılan "Sarbanes Oxley" kanunu, kurumların etkin iç kontrol izleme faaliyetlerine daha fazla kaynak ayırmalarına öncülük etmiştir (Masli ve ark., 2010, s. 1029). Ayrıca iç kontrol raporlaması da bir iç kontrol izleme fonksiyonu olarak özellikle ABD'de dikkat ile

incelenen bir konu olarak öne çıkmaktadır (Munsif ve ark., 2012, s. 203). İç kontrollerin izlenmesi ile ilişki olarak bir diğer uygulama da organizasyon ya da kurumun yönetim kurulunun iç denetim faaliyetinden, kurumun stratejik hedefleri doğrultusunda oluşturulmuş bulunan iç kontroller hakkında bir genel görüş talep etme durumudur (IIARF, 2016b, s. 271).

Yukarıda anılan amaçlar doğrultusunda iç kontrol sistemi, mali kontroller ve idari kontroller olarak sınıflandırılabilir (Kurnaz ve Çetinoğlu, 2010, s. 37):

- Muhasebe Kontrolleri; muhasebeye özgü olan işlemler (kayıt tutma, raporlama vs.), envanter işlemleri.
- İdari Kontroller; organizasyonun tüm idari faaliyetlerini kapsayan kontrollerdir. Bu tür kontrollere organizasyon faaliyetlerinin verimliliğini, finansal ve örgütsel başarısını gerektirecek kontroller, bir başka deyişle hareket ve zaman etütleri ile kalite güvence kontrolleri örnek verilebilir.

İç kontrol özellikle 90'lı yıllarda, henüz organizasyonda bütüncül olarak kabul görmüş bir uygulama değil iken sadece kurumun çeşitli alanları ile ilgili görülmekte idi. Bu alanlar özellikle finansal kontroller ve finansal raporlama alanları olarak öne çıkmaktaydı (Spira ve Page, 2003, s. 643). Ancak günümüzde iç kontrol faaliyetleri sadece finansal boyutta değil kurumsal anlamda da değerlendirmektedir.

İç kontrolün birbiriyle ilişkili beş unsuru söz konusu olup bunlar aşağıdaki gibi sıralanabilir (Kurnaz ve Çetinoğlu, 2010, s. 37) :

- Kontrol Ortamı
- Risk Değerlemesi
- Kontrol Faaliyetleri
- Bilgi ve İletişimler
- İzleme; iç kontrol sisteminin performans, kalite ve kontrolleri anlamında tasarım ve işleyişinin gözden geçirilerek, alınması gerekli görülen önlemlerin alınmasıdır (Pehlivanlı, 2014, s. 37).

Yukarıda belirtilen unsurlar çalışmanın ikinci bölümünde COSO İç Kontrol Modeli başlığı altında detaylı olarak ele alınmıştır.

1.3 DENETİM

Çalışmanın bu bölümünde denetim ve ilgili kavramları kısaca ele alınacak, klasik ve modern anlayışlar çerçevesinde kavramların gelişimi, karşılaşılan sorunlar ve bu sorunlara yönelik alınan tedbirlere değinilecektir. Bölümde, son olarak denetim türleri kısaca incelenecektir.

1.3.1 Tanım ve Temel Kavramlar

Günümüzde denetim uygulamalarında; kontrol, denetim, teftiş, soruşturma, inceleme gibi denetim ile ilişkili kavramların birbirileri ile sık sık karıştırıldığına rastlanılmaktadır (Akpınar, 2011, s. 287). Bu sebeple çalışmanın izleyen kısmında söz konusu kavramlar incelenecektir. Öncelikler teftiş kavramının İngilizce karşılığı olan “audit” kelimesi ele alınacaktır. “Audit” kelimesi latince duymak, işitmek anlamına gelen “auditus” kökeninden gelmektedir (Adiloğlu, 2011, s. 3). Dilimize bakıldığında ise teftiş kavramı Türk Dil Kurumu sözlüğünde “denetleme” olarak tanımlanmakla beraber, denetleme kavramı da yine aynı kaynakta teftiş, kontrol şeklinde tanımlanmıştır. Bu tanıma ek olarak müfettiş kavramı Türk Dil Kurumu sözlüğünde “denetmen” olarak tanımlanmakta, denetmen ise aynı kaynakta müfettiş anlamına gelmektedir. Organizasyon içinde denetim fonksiyonu teftiş veya denetim kurulları/birimleri tarafından gerçekleştirilmektedir. Verilen tanımlar çerçevesinde teftişin, en genel anlamı ile organizasyonun faaliyetlerin yolunda yürütülüp yürütülmediğinin araştırılması ve ilgili birimlere raporlanması demek olduğu söylenebilir.

Teftiş kurulu kavramı ise güncel Türkçe sözlükte denetleme kurulu olarak tanımlanmaktadır. Teftiş kurulları içinde bulundukları organizasyonların iş ve işlemlerini çeşitli açılardan denetimini gerçekleştirmekle sorumlu, içerisinde başkan ve başkan yardımcılarından oluşan bir yönetici yapısı bulunduran ve çeşitli kıdemlere sahip müfettişlerden oluşan denetim organları olarak tanımlanabilir.

Teftiş kurulu bünyesinde gerçekleştirilen faaliyetler ise teftiş, soruşturma ve inceleme faaliyetleri olarak sınıflandırılmakta olup; teftiş, daha ziyade periyodik aralıklar ile gerçekleştirilen, organizasyondaki eksikleri ortaya çıkarmayı hedefleyen denetim türü olarak değerlendirilir. Soruşturma yapılan denetimin neticesinde ilgililer hakkında suç teşkil edilecek sonuçlar elde edilmesi durumu söz konusu olduğunda teftiş süreci soruşturma adı altında tanımlanmakla beraber, belirli bir hedefe yönelik yapılan denetime ise inceleme denilmektedir (Yurtsever, 2009, s. 27). Söz konusu tanımlar farklı durumları açıklamakla beraber denetim türleri arasında her zaman katı bir ayrım olması gerekmemektedir. Örneğin her yıl gerçekleştirilen bir teftiş faaliyeti esnasında şüpheli bir durum görülmesi üzerine söz konusu teftiş faaliyeti bir soruşturmaya dönüştürülebilir. İnceleme ise daha ziyade belirli bir çerçeve içinde yapılan ve o konuya ilişkin özel ihtisasa sahip denetim elemanlarınca gerçekleştirilen denetim türü olarak açıklanabilir. Örneğin vergi incelemesi, ya da ilgili faydalanıcıların, kamu finansal desteğinden faydalanabilmek için gerekli olan şartların yerine getirilip getirilmediğinin incelenmesi belirtilebilir. Diğer yandan yapılan bir denetim misyonu neticesinde hukuki ya da idari bir işlem yapma gereği doğurabilecek bulgular elde edilmişse bu denetime soruşturma; eğer anılan türde bulgulara rastlanılmamış ise inceleme adı verildiği de denetim mesleki uygulamalarında görülmektedir.

Denetim faaliyetleri kapsamında diğer bir kavram da murakabe kavramıdır. Murakabe güncel Türkçe sözlükte denetleme olarak tanımlanmakla beraber günümüz denetim literatüründe çok sık rastlanmayan bir kavramdır.

Denetim faaliyetlerine ilişkin bazı önemli kavramlar aşağıda ele alınmaktadır (Kaval, 2008, s. 64):

Denetim süreci; gelen ihbardan ya da denetim planı çerçevesinde alınan denetim kararından, denetim raporunun ilgili birimlere sunulması aşamasında kadar söz konusu olan sürece denetim süreci denir.

Denetim sebebi; denetim sürecinin başlaması için ortada bir iddia, şikâyet ya da önceden planlanmış bir denetim programı olması beklenir. Söz konusu sebep sürecin başlaması için bir tetikleyici görevi üstlenir.

Denetim ölçütleri; yukarıdaki tanımda görüldüğü gibi işlerin yolunda gidip gitmediği denetimin temel konusudur. Denetim yolunda gidip gitmediği kararının temel kaynağı ise söz konusu yolu oluşturan standartların ya da mevzuatın kendisidir. Denetçi ilgili faaliyet ya da işlemin, uyulması gereken standartlar ya da mevzuat çerçevesinde gerçekleşip gerçekleşmediğini inceler. Özellikle iç denetim faaliyeti esnasında uygulanması beklenen Uluslararası İç Denetim Startları ya da bilgi güvenliği denetimi sürecinde uygulanması beklenen ISO 27001 BGYS standartları bu ölçütlere örnek verilebilir.

İlgililere bildirme; yapılan denetim sonucu hazırlanan raporun ve kanaatin doğrudan ve dolaylı ilgili kişilere sunulması aşamasıdır.

İlgililere bildirme başlığı çerçevesinde denetim sürecinin belki de en önemli noktalarından birisi üst yönetimin denetim kavramına yönelik yaklaşımıdır. Özellikle yapılan denetim sonucu ilgililere bildirilen rapordaki bulgularda yer alan eksikliklerin giderilmesine ilişkin üst yönetime önemli görevler düşmektedir. Üst yönetim denetim raporunda yer alan bulguları kurum içinde ilgili bölümler ile paylaşır. İlgili bölümler söz konusu bulgularda yer alan eksikliklerin giderilmesine yönelik adımlar atmak üzere kendilerine bir yol haritası belirler. Belirledikleri bu yol haritasını da üst yönetime sunarlar. Üst yönetim söz konusu sürecin her aşamasında gerekli özen ve dikkati göstererek, gerçekçi ve etkili bir eylem planı hazırlanmasında öncülük etmiş olmaktadır. Üst yönetimce benimsenmemiş bir denetim sürecinin etkililiğinden bahsetmek çok zor olabilir. Esas olarak şunu da belirtmek gerekir ki, kurumun ya da organizasyonun dış ya da iç denetim benimseme durumu, yapılacak olan dış ya da iç denetim başarısını etkileyen temel faktörlerdendir. Yukarıda belirtilmiş olan elde edilen denetim bulgularına ilişkin eylem planının hazırlanması aşaması yanında, denetim sürecinin diğer aşamalarında da aynı şekilde denetimin benimsenmesi önem arz etmektedir.

Denetimin benimsenmesi, denetim bilgisinin kuruma iletilmesinden, ileride bahsedilecek olan izleme sürecine kadar tüm aşamalarda kurumun ya da organizasyonun ilgili bölümlerinin denetim sürecine gerekli önemi vermesi ve söz konusu denetimin denetlenenin ileriye dönük hedeflerine ve güvenilirliğine sağlayacağı katkıyı tam ve doğru olarak anlaması olarak açıklanabilir. Özellikle geçmişte denetim, bir korkutma ya da cezalandırma yöntemi olarak kullanılmış ve bu şekilde oluşan algı neticesinde, denetimin iyileştirici yönünden çok cezalandırıcı yönü ön plana çıkmıştır. Buna benzer şekilde denetleyen ve denetlenen arasındaki ilişkilerin öneminin yanında, denetleyen taraf olan denetim heyeti ile denetimin üst yönetimi olarak da tabir edilebilecek olan denetim komitesi arasındaki ilişki de klasik anlayışta resmi bir şekilde devam ettirilirken, yapılan çalışmalarda denetim komitesinin denetim/iç denetim fonksiyonu ile olan ilişkisinde enformel yollar da izlemeye başladığı görülebilmektedir (Zaman ve Sarens, 2013, s. 512). Cezalandırıcı yönü ön planda olan denetim sürecinde denetlenen eksiklikleri ile yüzleşme ve onların iyileşmesi ya da giderilmesi için çaba harcamaktan çok, cezadan kaçınmak için söz konusu eksikleri gizleme yolunu seçebilmektedir. Gerçekten de özelikler geçmiş dönemlerde teftiş, ilgili müesseselere ani ziyaretler gerçekleştiren, aksaklıkları ortaya koyan ve görevini ihmal edenleri tespit eden bir memuriyet haline gelmiş idi (Erdem, 2009, s. 56). Denetimin etkililiği açısından bu durum hiçbir tarafa fayda sağlamamaktadır. Oysa iyileştirici yaklaşımın ön planda olduğu denetim anlayışında eksiklikler biz cezalandırma sebebi değil aksine iyileştirici bir sürecin başlamasına vesile olan kavramlar olarak değerlendirilir.
Günümüzde ise söz konusu klasik süreçlerin yanında denetçilerin kendi denetim raporları dahi inceleyerek iç kontrol süreci oluşturmalarını tavsiye etmektedir (Asare ve Wright, 2012, s. 171). Son dönemlerde denetim raporları birer inceleme konusu olmuş, hatta ABD'de denetim raporunu etkileyen faktörler incelenmiş özellikle "önyargılar" konusunda çalışmalar da gerçekleştirilmiştir (Palmer, 2008, s. 266).

Teftiş ve denetim kavramları aynı anlamları taşısalar da mesleki uygulama bazı durumlarda farklılıklar gözlenebilmektedir. Örneğin teftiş faaliyetinde insan unsuru ön plana çıkmakta, ilgili müfettişin teftişin gerçekleşeceği yere fiilen gitmesinin gerektiği düşünülmektedir oysa denetim kavramında insandan ziyade işin kendisi

ön plana çıkmaktadır. Gerçekten de yerinden denetim kavramı kulağa normal gelse de yerinden teftiş sözü pek uygun gelmemektedir. Görüldüğü üzere klasik teftiş kavramları günümüzde boyut değiştirmekte, denetçilerin kendi raporları dahi birer inceleme konusu olmakta ve bu raporları etkileyen çok farklı unsurlar ele alınmaya başlanmaktadır. Bu çerçevede geçmişten günümüze teftişin gelişimi ve konuya ilişkin değişen eğilimlerin incelenmesi faydalı görülmektedir.

1.3.2 Geçmişten Günümüze Denetim

Geleneksel teftiş anlayışından bahsederken verilebilecek en bilindik örnek ilköğretim müfettişleridir. İlkokul çağındaki pek çok öğrenci müfettiş kavramı ile daha okul sıralarında tanışmıştır. Özellikle Milli Eğitim ve Maliye müfettişliği meslekleri ülkemizde köklü bir geçmişe sahiptir. Bunun yanında diğer farklı alanlarda da teftiş örgütlenmeleri görülebilmektedir bu tür yapılara gerek Maliye Bakanlığının teftiş kurulu gerek ise de 19.yy. sonunda kurulan Teftiş-i Umumi-i Askeri Komisyonu örnek verilebilir (Ölmez, 2012, s. 117). Milli Eğitim Müfettişliğinin tarihsel gelişimine baktığımızda müfettiş kavramının ilk kez 1838 yılında Meclis-i Umur-ı Nafia'nın layihasıyla atanan "yardımcıların" mahalle mekteplerinde görevli öğretmenlerin mesleki yeterliliklerinin tespiti ile görevlendirilmeleri ile söz konusu olduğu ve bu yardımcıların bir anlamda müfettiş olarak görev yaptıkları belirtilebilir (Gençoğlu, 2012, s. 34). Bununla beraber bazı vakalarda gerek naipler ile müfettişler, gerek ise de kadılar ile müfettişler arasında yetki anlaşmazlıkları çıktığı da arşivlerden tespit edilmiştir (Günay, 2009, s. 35).

Osmanlı'da, özellikte tanzimat döneminde Anadolu ve Rumeli'ye müfettişler atandığı ve atanan bu müfettişlerin maliye, tarım, adalet gibi alanlarda milleti ve devleti kalkındırmak, tanzimat reformlarını hayata geçirmek gibi hedeflerle görevlendirildikleri bilinmektedir (Serbestoğlu, 2014, s. 118). Ayrıca 19. Yüzyılın sonlarında kurulan Umumi Müfettişlikler ise klasik teftiş anlayışından farklı olarak sadece idari ve askeri amaçlar ile değil onun yanında sosyal ve ekonomik nedenler ile de kurulmuşlardır (Bulut, 2015, s. 95). Umumi müfettişliklerin uygulanmaya başlama tarihi Sultan İkinci Abdülhamid devrinde başladığı bilinmekte olup, iyi derece de eğitim almış ve dönemin yenilikçi yapısına uygun devlet memurlarının, olağanüstü yetkiler ile donatılıp Anadolu ve Rumeli'de çeşitli idari görevlere

atandıkları görülmektedir (Alkan, 2015, s. 247). Söz konusu Umumi Müfettişliklerin isyancılara yönelik önleme çalışmaları dahi yaptıkları ve örneğin Rumeli Umumi Müfettişliğinin Manastır, Kosova ve Selanik vilayetlerinde Bulgar çetelerine karşı mücadele çalışmalarında bulunmaları söz konusu olmuştur (Alkan, 2015, s. 252). Ayrıca incelenen bazı arşiv belgelerinde 19.yy. sonunda idari düzende meydana gelen bazı bozulmaları ele almak ve iyileştirmeler sağlamak için dönemin Padişahı tarafından teftiş heyetlerinin turneye çıkartılarak çeşitli konularda denetim raporları hazırlamalarının istendiği görülmüştür (Oğuz, 2006, s. 78). Söz konusu teftiş çalışmaları gerek idari yapının incelenerek eksiklerinin ortaya çıkarılması şeklinde gerek ise de kamu kurumlarının hesaplarının ve harcamalarının incelenmesini kapsayabiliyordu. Son olarak bir diğer örnek de II. Abdülhamid döneminde Rumeli vilayetlerine gönderilen teftiş heyeti olarak verilebilir. Burada ilgili vilayetlerde Maarif müfettişleri sermaye eksikliğinin yol açtığı sorunlar, maarife ait gelir ve giderlerin kullanılma ve harcama şeklini inceleme ile görevlendirilmişlerdi (Nurdoğan, 2009, s. 200)

Dünyada denetim kavramına örnek gösterilebilecek ilk adımlar ise aşağıda verilmektedir (Duman, 2008, s. 10):

- 1845 yılında İngiltere'de çıkan demiryolu şirketlerinin bilanço denetimine ilişkin yasa,
- 1845 tarihli İngiliz şirketler kanununda yer alan tescil edilmek istenen şirkete denetçi tayinini zorunlu kılan maddeler,
- 1850'li yıllarda İskoçya'da modern muhasebe denetiminin yazılı hale getirilmesi,
- 1880'de Quebec'te ve 1886'da New York'ta Muhasebeci örgütlerinin kurulması,

Denetime ilişkin ilk adımların İngiltere'den başlaması, Sanayi devrimini ilk gerçekleştiren ülke olması ve buna bağlı olarak geniş çaplı işletmelerin ortaya çıkması ve yatırımcılarında bu şirketlere yatırım yapmak için gerekli güvenilir bilgiye ihtiyaç duymalarının bir sonucu olarak değerlendirilebilir. Görüldüğü üzere denetim ve bilgi kavramları birbirlerinin hem girdi hem de çıktıları olması anlamında devamlı olarak birlikte düşünülmesi gerekebilecek iki kavramdır.

Günümüzde ise artık küresel anlamda genel kabul görmüş enstitüler, ilkeler, kural ve uygulamalar söz konusudur. Bu çerçevede ülke sınırlarını aşan, üretim için girdilerini dünyanın çeşitli bölgelerinden tedarik eden, üretimini de aynı şekilde dünyanın farklı ülkelerinde gerçekleştiren ve pazarlayan şirketlere çok uluslu şirketler denilmektedir (Yalçıner, 2008, s. 297). Çok uluslu şirketlerin söz konusu olduğu bir dünyada ise küresel kabul görmüş denetim ilkelerinin varlığı kaçınılmaz bir sonuçtur. Görüldüğü üzere sanayinin gelişmesiyle beraber ihtiyaç duyulmaya başlanan denetim kavramı küreselleşen dünyayla beraber ortak bir değerler ve kurallar bütünü halini almıştır.

Denetimi daha iyi anlayabilmek için bazen farklı bir bakış açısından denetim kavramı ele alınabilir. Özellikle iç denetim fonksiyonu gibi sürekli organizasyon bünyesinde bulunan bir yapının, belki de her şeyden önce denetlemekte olduğunu organizasyonu en iyi şekilde tanıması gerekmektedir. Burada tanımak kavramıyla anlatılmak istenen, organizasyon içinde çalışanların şahsen tanınması değil, aksine organizasyonu kişilerden uzak bir şekilde içinde bulunduğu dış çevre, yönetim yapısı, organizasyona hâkim yönetim felsefesi, organizasyonun bilgi güvenliği farkındalığı gibi faktörler denetçinin denetleyeceği kurum hakkında daha doğru ve anlaşılır sonuçlar elde etmesine yardımcı olabilmektedir.

1.3.3 Denetim Türleri

Denetim çalışmaları, çeşitli açılardan kendi içinde farklılaşmıştır. Bu farklılaşma aşağıdaki boyutlar çerçevesinde değerlendirilebilir.

- Amaçlarına göre denetim;
    - Faaliyet Denetimi
    - Uygunluk Denetimi
    - Finansal tablolar denetimi
    - Vergi Denetimi
- Gerçekleşme zamanına göre denetim;
    - Yıl sonu denetimi
    - Ara dönem denetimi
    - Özel denetim

- Denetçinin statüsüne göre denetim;
  - Kamusal Denetim
  - Dış Denetim
  - İç Denetim

Söz konunu denetim biçimleri sırası ile aşağıda incelenmektedir.

1.3.3.1 Faaliyet Denetimi

Faaliyet denetimi organizasyon tüm faaliyetlerinin ya da önceden belirlenmiş veya seçilmiş bir faaliyetinin, organizasyonun hedeflerine göre denetlenmesidir. Denetimin içeriği ise mali kontroller, performans göstergeleri ve bilgi sistemlerinin incelenmesi olarak değerlendirilebilir. Faaliyet denetimi pek çok farklı isimle de anılmaktadır. Bunlardan bazıları, performans denetimi, iktisadilik denetimi, etkinlik denetimi, yönetim denetimi gibi denetim türleridir. Farklı isimlerde olsa da faaliyet denetimi genel kapsamda organizasyonun başarısı, yönetim politikaları, etkinliği etkileyen faktörler gibi çeşitli alanlarda gerçekleşen faaliyetleri inceler. Yukarıda tanımlandığı üzere faaliyet denetimi sadece muhasebe işlemleri ile ilişkili değildir. Bu durumda denetimi bir noktada diğer denetimlere kıyasla daha öznel bir konuma getirmektedir. Örneğin vergi denetiminde incelenen örneklem tamamen rakamsaldır ve bu çerçevede öznelliğe yer yoktur. Organizasyonun kar/zararı, içinde bulunduğu vergi dilimi, faaliyet tutarları hepsi rakamsal ve kesin tutarlar olduklarından bu tür denetimin nesnelliği ön plana çıkmaktadır. Faaliyet denetiminde ise öncelikle denetlenecek faaliyet veya faaliyetler belirlenir. Ardından söz konusu faaliyet ya da faaliyetlerine ilişkin bütçeleri ve faaliyet süreçleri belirlenir. İzleyen aşamada ise organizasyonun içinde yer aldığı sektörün ilgili faaliyet alanlarına ilişkin bütçeleri ve faaliyet süreçlerine ilişkin veriler elde edilir. Sektöre ilişkin veriler iler organizasyon verileri karşılaştırılır, aynı zamanda işletmenin faaliyet süreçlerindeki sapmaların nedenleri araştırılır. Elde edilen sonuçlar raporlanarak, tavsiyeleriyle birlikte üst yönetime sunulur. Ayrıca söz konusu denetim çerçevesinde kullanılan ölçütlerin genel olarak sübjektif olması nedeni ile faaliyet denetimi diğer denetim türlerine kıyasla daha zor olarak değerlendirilebilir (Akbulut, 2010, s. 7).

1.3.3.2 Uygunluk Denetimi

Çalışmanın daha önceki bölümlerinde ele alındığı üzere organizasyonun gerek iç çevresinde gerek de dış çevresinde uymak durumunda olduğu yazılı kaynaklar mevcuttur. Uygunluk denetimi kapsamında yazılı kaynaklar TBMM ve Bakanlar Kurulunca çıkarılan mevzuat yanında kalkınma planlarını, yıllık plan ve programları, yönergeler ve işlem prosedürlerini de kapsar (Gökalp, 2013, s. 12). İşte bu noktada uygunluk denetimi organizasyonun faaliyetlerinin gerek yönetim kademesinin belirlemiş olduğu gerek ise organizasyon dışında yasa yapıcılar tarafından belirlenmiş kurallara uygunluğunu denetler. Organizasyon içi kurallara örnek olarak Finans ve mali işler departmanının yönergeleri, organizasyon dışı kurallara da asgari ücret kuralları örnek verilebilir (Duman, 2008, s. 163). Bu tür denetiminde ortaya çıkan sonuçlar genelde kurumun iç kontrol faaliyetlerinin başarısını ortaya koyar. Zira organizasyonel çevrede belirlenen kurallara uyum iç kontrol faaliyetlerinin temel fonksiyonlarından biri olarak değerlendirilebilir. Uygunluk denetiminin bir başka tanımı ise kamu denetimleri çerçevesinde yapılabilir. Buna göre uygunluk denetimi, idarenin tüm harcama ve mali kararlarının ilgili tüm mevzuata olan uygunluğunun denetlemesi olarak tanımlanabilir (Akçay, 2012, s. 60)

1.3.3.3 Finansal Tablolar Denetimi

Finansal tablolar denetimi diğer bir adıyla muhasebe ya da bağımsız denetimi kavramını açıklamadan önce, ilk olarak finansal tabloların ne demek olduğu kısaca incelenmektedir. Finansal tablolar işletmenin faaliyetlerinin rakamsal boyuta konumlandırıldığı, adeta ilgili organizasyonun finansal kimliğidir. Bilanço, gelir tablosu, nakit akım tablosu ve öz kaynaklarda değişim tablosu finansal tablolara örnek verilebilir. Organizasyon dışı çevre, organizasyon hakkında finansal değerlendirmesini söz konusu finansal tablolar aracılığıyla yapar bu sebeple tabloların daha önceden belirlenmiş ve kabul edilmiş belirli ilke ve kurallara uygun olması gerekmektedir. Bu ilke ve kurallara uygun olduğu belirlenen organizasyonun finansal durumu artık diğer benzer durumdaki organizasyonların finansal durumları ile karşılaştırılabilir konuma gelmektedir. Bu açıklama ışığında finansal tablolar denetimi, organizasyonun mali tablolarının, genel kabul görmüş muhasebe

ilkelerine uygun olup olmadığının incelenmesi olarak tanımlanabilir (Dunn, 2010, s. 55). Muhasebe denetiminin organizasyona yararları aşağıdaki gibidir :

- Yanlışları ortaya çıkarma ve ortaya çıkan bulgular bağlamında bir öğrenme yöntemi olması,
- Yönetimde görev alanların kendini aklama konusunda güvenilir bir araç olması,
- Kurumsal yönetim anlayışının yerleşmesine yardımcı olmasıdır.

Bu tür denetim ilgi duyanların gereksinimlerini karşılamak üzere yapılan genel amaçlı bir çalışmadır (Dal ve Çalış, 2012, s. 91). Bilindiği üzere kurumsal yönetim, organizasyonun en yüksek performansını göstermesini, en karlı, en başarılı ve en rekabetçi olmasını hedefler ve söz konusu hedeflere ulaşmanın, müşterilerine, çalışanlarına, tedarikçilerine ve toplumdaki diğer paydaşlarına karşı sorumluluk bilinci ile hareket ederek mümkün olabileceğini belirtir (Sayılgan, 2011, s. 14). Bu çerçevede finansal tablolar denetimi kurumsal yönetim anlayışı kapsamında gerek yatırımcılara gerek ise diğer ilgili paydaşlara güvenilir bilgi ve kaynak sunulmasına yardımcı olur. Ayrıca organizasyon üst yönetiminin bu konuda kararlı olması ve üst yönetim arasındaki uyum da finansal raporlama sürecinin dolayısıyla finansal tabloların doğruluğunun sağlanmasında önemli faktörlerden biridir (Yılancı, 2015, s. 77).

1.3.3.4 Vergi Denetimi

Vergi denetimi özünde organizasyonun işlemleri çerçevesinde yükümlü olduğu vergilerin faaliyet göstermekte olduğu ülkenin ilgili vergi mevzuatına uygun olarak hesaplanıp hesaplanmadığının ortaya çıkarılması amacıyla, organizasyonun vergiye konu olan hesaplarının incelenmesidir. Vergi denetimin hukuksal boyutu Türk Vergi Mevzuatında geniş bir biçimde ele alınmış olup çalışmanın konusu itibarıyla daha fazla derinlemesine incelenmeyecektir. Ancak Vergi denetiminin mükellefleri yani kişileri ya da organizasyonları etkilemesi bakımında en çok karşılaşılan türü vergi incelemesidir. Denetim çerçevesinde vergi yükümlülerinin defter kayıtları incelenir ve bildirimlerindeki doğruluk derecesi değerlendirilir (Altuğ, 2000, s. 4) Bu çerçevede vergi denetiminin amaçları arasında, vergi kaçırılmasının

engellenmesi, bütçeye kaynak olarak düşünüldüğünde mali etkiler, gelir dağılımında adaletin sağlanmasının bir aracı olarak alının tedbirler sayılabilir. Vergi denetiminin kökenlerine bakıldığında ise, 1838 yılında Maliye Nezareti'nin kurulması ise başlandığı, vergi tahsilatlarında yaşanan sorunların giderilmesine yönelik olarak çeşitli komisyonlar kurulduğu görülmektedir (Tabakoğlu, 2015, s. 92).

1.3.3.5 Yıl Sonu Denetimi

Yıl sonu denetimi bir diğer adıyla sürekli denetim, temel mantığı itibarıyla ilgili organizasyonların yıl sonu mali tablolarının genel kabul görmüş muhasebe standartlarına uygun olup olmadığının denetlenmesidir. Bu tür denetime tabii olan şirketler arasında halka açık şirketler, Sermaye Piyasası Kurulu gözetimine tabi diğer şirketler, finans kurumları ve reasürans şirketleri sayılabilir.

1.3.3.6 Ara Dönem Denetimi

Ara dönem denetimi bir diğer isimle sınırlı denetim, yukarıda kısaca açıklanan yıl sonu denetiminden farklı olarak yıl sonu mali tablolarının değil ara mali tablolarının belirli periyodlarla denetlenmesidir. Bu tür denetime tabi şirketler arasında menkul, gayrimenkul yatırım ortaklıkları ve fonları, emeklilik yatırım fonları ve aracı kurumlar gösterilebilir. Ara dönem denetimleri bir anlamda genel denetimlerin sürelerinin kısalmasında yardımcı olabilecek, önleyici bir denetim türü olarak tanımlanabilir (Korkmaz, 2013, s. 16).

1.3.3.7 Özel Denetim

İlgili mevzuatta tanımlanmış şirketlerin, tasfiye, devir, birleşme ve bölünme gibi durumlarında ya da halka ilk kez açılacak şirketlerde, söz konusu şirketlerin mali tablolarının uygunluğunun denetlenmesi ve raporlanmasıdır.

1.3.3.8 Kamusal Denetim

Kamusal denetim kısaca kamu kurum ve kuruluşlarını ilgilendiren denetimler olarak tanımlanabilir. Denetim faaliyeti devletin çeşitli denetim birimleri eliyle yürütülür (Korkmaz, 2013, s. 17). Diğer bir deyişle kamusal denetim, ilgili ülke vatandaşlarının

haklarının korunması amacı ile ilgili bakanlık ya da kamu kurumlarının denetçileri tarafından gerçekleştirilen denetim türüdür.

1.3.3.9 Dış Denetim

Dış denetim adından da anlaşılabileceği üzere denetlenen organizasyondan bağımsız bir birim tarafından gerçekleştirilen denetimdir. Dış denetimde gerek kamu sektörü gerek de özel sektörde olsun ilgili organizasyonun ilgili mali tablolarının önceden belirlenmiş ve kabul görmüş ilkelere uygunluğu incelenir. Benzer şekilde söz konusu tabloların gerçeği yansıtıp yansıtmadığı da tespit edilir ve raporlanır (Duman, 2008, s. 164). Ülkemizde kamu bünyesinde yapılan dış denetim Sayıştay tarafından gerçekleştirilmektedir (TİDE, 2012a, s. 38). 5018 sayılı kanunda Sayıştay'ın genel uygunluk bildirimine kaynak olarak sayılan dokümanlardan biri de dış denetim raporlarıdır (BÜMKO, 2003, s. md. 43)

1.4 İÇ DENETİM

İç denetim önceki kısımlarda tanımlanan iç kontrol sistemi çerçevesinde, bu sistemde meydana gelen saplamaların ortaya çıkarılması konusunda ve söz konusu saplamaların organizasyon üst yönetimine raporlanması konusunda sorumlu olan fonksiyondur (Kaval, 2008, s. 136). Çalışmanın izleyen bölümünde iç denetime ilişkin temel kavramlar incelenmektedir.

1.4.1 İç Denetimin Özellikleri ve Temel Kavramlar

Bilindiği üzere gerek canlı organizmalar olsun gerek ise organizasyonlar olsun hepsinin yaşadıkları çevre ve zaman boyutları dahilinde çeşitli hedefleri bulunmaktadır. Canlı organizmaların hedefleri arasında en temel hayatta kalma güdüsü yer alırken organizasyonların ise stratejik, finansal, operasyonel ve uyumluluk alanlarında hedeflerine ulaşması olabilir. İç denetim fonksiyonu ve dolayısıyla iç denetçiler organizasyonun hedeflerine ulaşmasında bağımsız güvence ve danışma hizmeti temin ederler. İç denetim, bir denetim fonksiyonu olarak sistematik bir yaklaşımla kurumun amaçlarına ulaşmasına yardımcı olur (Kincaid ve Sampias, 2005, s. 39). İç denetçiler yukarıda bahsi geçen tanım kapsamında şu soruları yöneltirler (IIA, 2016b, s. 2):

- Organizasyonun başarmak istediği nedir? Hedefleri nelerdir?

- Organizasyonu hedeflerine ulaşmasından alıkoyan ne gibi durumlar söz konusu olabilir?
- Söz konuşu riskleri minimize edecek ne gibi kontrol süreçleri yürürlüğe konabilir?

Bu üç soru temelinde iç denetçiler organizasyonun risklerini belirlemeye ve onları değerlendirmeye çalışırlar. Olumsuz sonuç doğuracak gelişmelerin engellenmesi ve organizasyon lehine olacak gelişmelerin sağlanması amacı ile tüm paydaşlara yardımcı olmaya çalışırlar. Söz konusu paydaşlar arasında, yönetim kurulu, hissedarlar, kurum içi çalışanlar ve müşteriler sayılabilir. İç denetçiler görevlerinin gereklerini yerine getirirlerse, organizasyonun raporlama fonksiyonu güvenilir, iç kontrol süreçleri güçlü, etik konularında yeterli, riskleri azaltılmış, etkin bir gözetim sağlanmış ve yatırımcılar korunmuş olacaktır.

İç denetimin kapsamı, yukarıda verilen tanım çerçevesinde kurum ya da organizasyon bünyesinde yer alan risk yönetimi ve iç kontrol sistemlerinin etkinliği ve verimliliğinin incelenmesidir. Bu çerçevede finansal ve operasyonel veriler incelenir ve alınacak kararlara temel olması anlamında doğruluğu ve güvenilirliği ele alınır. İzleyen süreçte uyumluluk denetimi olarak da belirtilen, organizasyonun kullanmakta olduğu politika ve prosedürleri ile yasal mevzuat bağlamında, faaliyetlerinin ne kadarının bu mevzuata ve prosedürlere uygun olduğu değerlendirilir. Organizasyonun giderleri harcamaları ve varlıkları incelenerek, kurumsal hedefler doğrultusunda bu kalemlerin uygun bir şekilde kullanılıp kullanılmadığı incelenir. Ayrıca iç denetim faaliyeti, Covid-19 salgını süreci gibi olağan dışı durumlarda da koşulların yarattığı risklerin etkilerinin azaltılmasında rol oynamaktadır (Bajary ve ark., 2023, s. 5).

İç denetimin kapsamı belirtildikten sonra genel özellikleri de incelenmektedir. İç denetim fonksiyonun özellikleri aşağıdaki gibi sıralanabilir (Kurnaz ve Çetinoğlu, 2010, s. 35):

- Bireysel iş ve işlemlerden ziyade sisteme yönelik bir inceleme gerçekleştirir.
- Üst yönetime raporlama yapmakla beraber fonksiyonel bağımsızlığa sahip olduğundan kurum ya da organizasyonun hesap verilebilirliğini kolaylaştırır.

- İç denetim fonksiyonu iç kontrol sisteminin etkinliğini ele alır.
- Operasyonel ve mali verilerin güvenilir olup olmadığını inceler.
- Organizasyonun tüm yazılı politika ve prosedürlere uyumlu olup olmadığını inceler.

Bununla beraber, kurum içinde konumlandırılmış bir birim olarak iç denetim, sürekli bir denetim fonksiyonudur (Yılancı, 2015, s. 14).

İç denetim organizasyonun tüm iş ve işlemlerini denetlemek ile sorumlu olmakla beraber, beş ana başlı altında iç denetim türleri açıklanabilir.

Finansal Denetim, adından da anlaşılabileceği üzere organizasyonun ekonomik verilerinin, raporlarının, yıl sonu muhasebe tabloların ve bu çerçevede yer alan tüm verilerin incelenerek söz konusu verileri ya da tabloların doğruluğunu ve güvenilirliğini sağlamaya yöneliktir.

Performans Denetimi, kurum ya da organizasyonun stratejik hedeflerine ulaşma sürecinde yer alan faaliyetlerinde kullanılan gerek beşerî gerek mali tüm kaynaklarının verimlilik, etkinlik ve etkililik anlamında incelenmesidir.

Uygunluk Denetimi, kurumun tüm iş ve işlemlerinin önceden belirlenmiş olan standart, politika, prosedür ya da yasal mevzuat ile uyumlu olup olmadığının denetlenmesidir.

Sistem Denetimi, kurumun faaliyetlerinde ortaya çıkabilecek bazı eksikliklerin, gerektiğinde ve zamanında ortaya çıkarılarak giderilip giderilemediğinin ele alınmasıdır.

Bilgi Teknolojileri Denetimi, kurumun kullanmakta olduğu bilgi güvenliği yönetim sistemleri, bilgi güvenliği prosedürleri, ilgili yazılım ve donanımların incelenerek, kurumda dolaşan bilginin güvenilir ve yeterli olup olmadığının incelenmesidir. Bazı durumlarda bilgi teknolojileri denetimi gerçekleştirmek için ilgili kurumdaki iç denetçilerin tümünü bilgi teknolojileri eğitimi vermek ve denetim yapabilir hale getirmek yerine fayda-maliyet analizi çerçevesinde denetimi gerçekleştirme konusunda uzman desteği de talep edilebilir (IIA, 2016c, s. 71)

Son olarak belirtilmelidir ki diğer tüm denetim kavramları gibi iç denetimde zaman içinde gerek amaç gerek ise de kapsam anlamında değişmekte ve gelişmektedir. Söz konusu gelişim ve değişim 1950'li yıllardan günümüze doğru Tablo-3 yardımı ile incelenebilir (Yılancı, 2015, s. 20).

Tablo 3: İç Denetimde Amaç-Kapsam Değişimi

Dönemler	İç Denetim Amacı	İç Denetim Kapsamı
1950-1960	İşletmeye ait varlıkların korunması	Muhasebe kayıtlarının denetlenmesi
1960-1970	İşletmenin finansal verilerinin güvenirliğini sağlamak	Finansal ve uygunluk denetimlerinin yapılması
1970-1980	İşletmenin finansal ve finansal olmayan tüm verilerinin güvenirliğini sağlamak	Tüm faaliyetlerin finansal ve uygunluk denetimlerinin yapılması
1980-1990	İşletmenin finansal ve finansal olmayan tüm verilerinin güvenirliğini sağlamak	Tüm faaliyetlerin süreçlerin ve kontrollerin etkinliğinin denetlenmesi
1990-2000	İşletme amaçlarına ulaşmada yönetime yardımcı olmak	Tüm iç kontrol sisteminin ve risk yönetiminin denetlenmesi
2000-…	İşletme amaçlarına ulaşmada yönetime yardımcı olmak	Organizasyonel anlamda iç kontrol ve risk yönetimi ile ilgili tüm süreçlerin denetlenmesi ve işletmeye artı değer katma amacıyla danışma hizmeti.

İç denetimin unsurları, kurum faaliyetlerini geliştirmek ve değer katmak, bağımsızlık ve objektiflik, güvence ve danışmanlık, risk odaklılık, iç kontrol, standartlara uygunluk ile etik davranış ve meslek ahlak kurallarına uymak olarak belirtilebilir (Can, 2013, s. 10).

İç denetim fonksiyonuna, standartlarına ve uygulama süreçlerine ilişkin detaylı inceleme çalışmanın ikinci bölümünde incelenmektedir.

1.4.2 İç Kontrol ve İç Denetim İlişkisi

Özellikle profesyonel yaşamda iç kontrol ve iç denetim kavramlarının sık sık karıştırıldığı, hatta bazı durumlarda birbirlerinin yerine kullanıldığı gözlenebilmektedir. Çalışmanın bu bölümünde iç kontrol ve iç denetim kavramları arasındaki ilişki incelenmektedir. Önceki bölümlerde gerek iç kontrol gerek ise iç denetim kavramları incelenmiştir. Daha önce de açıklandığı üzere iç kontrol COSO'ya göre organizasyonun hedeflerine ulaşmasında yeterli güvence sağlayan bir süreç olarak tanımlanmaktadır. Buna göre iç kontrol (BÜMKO, 2015, s. 1):

- Organizasyonun işlemlerinin etkinliğini ve etkililiğini artırmalı,
- Finansal raporlama sisteminin genel kabul görmüş standartları çerçevesinde güvenilir olmasını sağlamalı,
- Mevzuat ve diğer ilgili düzenlemelere uygunluğu sağlamalıdır.

Bu bağlamda iç denetim, disiplini ve sistematik değerlendirme yöntemi ile bir kurumun önceden belirlenmiş hedeflerine ulaşmasında rol oynamaktadır.

Tüm bu tanımlar ve değerlendirmeler bir bütün olarak değerlendirildiğinde ortaya iç denetim ve iç kontrol ilişkisine dair temel noktalar ortaya çıkmaktadır. Buna göre ilk temel nokta iç denetimin, iç kontrol sisteminin bir parçası olan yönetimsel bir fonksiyon olmasıdır. Unutulmamalıdır ki iç kontrol bir sistemdir ve organizasyonun iş akışları içine yerleştirilmelidir. Örneğin önüne diğer bölümden bir evrak gelen çalışan, evrakı teslim alırken öncelikle organizasyonun prosedürlerinde açıkça belirtilmiş olan kontrol listesi kağıdına ilgili noktaları kapsayacak şekilde tik atarak evrakı teslim alır. Bu doğrultuda iş akışı arasında bir iç kontrol örneği gerçekleşmiş olur. İç denetim ise söz konusu kontrol listesinde yer alan başlıkların değerlendirilmesi, sürecin sağlıklı işleyip işlemediği gibi noktaları ele almaktadır. İç kontrol sistemi, organizasyonun işlemlerindeki dikkate değer hata ve riskleri minimize etmek için kullanılmakta olup, bu sistemi kullananlar ise dış denetçiler, iç

denetçiler ve yönetimdir. Bir başka değişle iç denetçiler, denetim faaliyetlerinde iç kontrol sisteminin işleyişini, en iyi şekilde çalışıyor olduğundan emin olmak için incelerler. Bu incelemeyi ise ilgili iç kontrol sisteminin etkinliğini ve verimliliğini, periyodik olarak riskleri değerlendirerek gerçekleştirirler. Söz konusu inceleme sonucu iç kontrol sisteminin yeterliliği, etkinliği ve işleyişiyle ilgili olarak yönetime geri bildirilimde ve önerilerde bulunur. Burada önemli bir nokta ise iç denetçilerin, iç kontrol sisteminin düzenlenmesi ya da uygulanması süreçlerine katılmamasıdır. Denetim mantığı olarak denetçi, denetleyecek olduğu unsurun düzenlenmesi ve uygulanma aşamasında rol oynamamalıdır. İç denetim-iç kontrol ilişkisinde bir diğer boyut ise iç denetim fonksiyonun dış denetim faaliyetleri süreçlerinde iç kontrol çalışmalarına yardımcı olabilmesidir (Abbott ve ark., 2012, s. 6).

Tüm bu açıklamalar neticesinde iç denetim ve iç kontrol arasındaki temel farklılıklar özetlenecek olursa aşağıdaki gibi belirtilebilir :

- İç denetim, organizasyonun iç kontrol verimliliği ve etkililiği amaçlarına ulaşması yolunda bir araçtır.
- Organizasyon için iç kontrol sistemi yönetim sisteminin genelini kapsamaktadır. Ancak iç denetim ayrı bir fonksiyondur ve iç kontrolün bir unsurudur. İç kontrol ise bir sistemdir ve organizasyonun hesap verilebilirliğinin sağlanmasını hedefler.
- İç denetim idari olarak üst yönetime bağlıdır, iç kontrol ise yönetimin tümünün sorumluluğu altındadır.
- İç denetim fonksiyonel olarak bağımsız olup, karar alma ve uygulama mekanizmalarında yer almaz, iç kontrol ise tüm karar alma süreçlerinde rol oynayabilir.

1.4.3 Denetim ve İç Denetim İlişkisi

Çalışmanın geçmiş bölümlerinde tanımları yapılan denetim ve iç denetim kavramları incelendiğinde, genel bir bakış açısıyla benzer kavramlar olarak görünüyor olsa da detaylı olarak ele alındığında birbirinden çok farklı kavramlar olduğu anlaşılabilmektedir.

Ülkemizde teftiş fonksiyonuna kamu sektörü açısından baktığımızda merkezi yönetim bünyesinde 50'den fazla teftiş biriminde 20.000'den fazla denetçinin görev yaptığı görülmektedir (Can, 2013, s. 8). Bu çerçevede pek çok teftiş kurulu oldukça köklü ve saygın kurullar olup görevlerini başarı ile ifa etmektedir. Bununla beraber gelişen ve değişen teknoloji, yeni çalışma süreçleri ve yeni denetim anlayışlarına uyum konusu da önemli ve gerekli bir konudur. Gerek Avrupa Birliği müktesebatına uyum gerek ise de etkin bir kamu mali yönetimi sağlamak açısından yasa koyucu tarafından 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu hazırlanmıştır. Anılan kanun ile iç denetim kavramı ile tanışılmış ve bu çerçevede klasik teftiş anlayışı ile iç denetim arasındaki ilişki, benzerlikler ve farklılıklarda ortaya konulmaya başlamıştır. Konuya ilişkin öne çıkan unsurlar kısaca aşağıdaki gibi belirtilebilir:

- *Pro-aktif yaklaşım*; bilindiği üzere klasik teftiş anlayışında ortaya çıkan bir problem, şikâyet ya da inceleme neticesinde, denetim elemanının görevlendirilerek konuya ilişkin bir değerlendirme yapması geçmiş olayları detaylı bir şekilde inceleyerek nerede hata yapıldığı, ne zaman yapıldığı ve sorumlu kişileri tespitinden bahsedilebilir. Bu tür yaklaşıma örnek "ex-post" bir denetim verilebilir. Örneğin yapılan bir harcamaya ilişkin gelen şikâyet kapsamında, müfettiş görevlendirilir. Ardından ilgili denetim elemanı teftiş faaliyetini gerçekleştireceği yere gider ya da tüm ilgili dokümanları ilgili kurumdan talep eder. Dokumanlar detaylı bir şekilde geriye dönük olarak incelenir. Gerekirse ilgili personel ile görüşmeler yapılarak kayıt altına alınır. Sonuç olarak elde edilen nihai görüş raporlanır, var cezai işleme konu olması gereken personel belirlenir ve izleme aşamasına geçilir. İç denetim faaliyetinde ise durum klasik teftiş anlayışından farklılık gösterir. İç denetim faaliyetlerinde amaç risk yönetimi ve iç kontrol sistemlerinin etkinliğini incelemek ve gelişimi yönünde önerilen sunmaktır. Bir başka deyişle, kurumun hatalarının daha oluşmadan önlenmesini sağlayabilecek olan kontrol ve risk sistemlerinin denetlenmesi ve iyileştirilmesine odaklanır. Bu pro-aktif yaklaşım iç denetim ve klasik teftiş anlayışı arasındaki temel farklılıkların başında gelmektedir.

- *Kapsam*; klasik teftiş anlayışında genel olarak denetim konusu ile ilişkili yasal mevzuatı ihlal eden durumlar incelenir iken iç denetim de finansal, sistem, uygunluk ve bilgi teknolojileri denetimleri gerçekleştirilir.
- *Standartlar*; iç denetim sürecinde iç denetçilerin uymak ile yükümlü olduğu gerek ulusal gerek ise de uluslararası standartlar söz konusudur. Klasik teftiş anlayışında ise genel olarak üstat-yardımcı ilişkisi de denilen ve yardımcının üstat ile gittiği denetimlerden elde ettiği tecrübeleri çerçevesinde bir denetim yolu izlediği değerlendirilebilir.
- *Risk odaklılık*; yukarıda da belirtildiği üzere iç denetimin temel fonksiyonlarından biri de risk yönetim sisteminin etkin olarak çalışıp çalışmadığının değerlendirilmesidir. Bu çerçevede iç denetim fonksiyonu kurum ya da organizasyonun risklerini etkin ve etkili bir şekilde yönetip yönetmediğini ele alarak risk odaklı bir denetimi temel alır. Bununla beraber klasik teftiş anlayışında ise konuya ilişkin yapılan denetimde tüm ilgili belge ve bilgi talep edilerek, düşük risk seviyesindeki risklere ve yüksek önem seviyesindeki riskler ayrımı yapılmaksızın tüm hataların üzerinde detaylı bir şekilde durulur.

Teftiş ve iç denetim arasındaki farklılıklar konusunda bir diğer bakış açısı da dış denetim-iç denetim faaliyetleri kıyaslamalarıdır. Dış denetim, bir denetim faaliyetinin denetlenen organizasyon bünyesi dahilinde olmayan dışarıdan hizmet alımı yoluyla gerçekleştirilen denetimdir. Uzun yıllar boyunca iç denetim, daha ziyade finansal ve idari boyutu ağır basan dış denetim ile karıştırılagelmiştir ancak günümüzde iç denetim farkındalığının da artması ile iç denetim ve dış denetim fonksiyonları arasındaki fark net bir şekilde ortaya konulabilmektedir. Söz konusu farklar aşağıdaki gibi belirtilebilir (IIARF, 2016a, s. 10):

- *Yönetim ile bağ;* dış denetçi yönetim kurulundan faaliyetleri ve fikri anlamda bağımsız iken iç denetçi, denetlenen faaliyetlerden bağımsız olmakla beraber yönetim kurulunun tüm ihtiyaç ve isteklerine cevap vermesi beklenir.
- *Kapsam;* dış denetçi finansal tablolarda yer alan bilgilerin doğruluğuna odaklanır iken iç denetçi, kurumun stratejik amaçlarına yönelik olarak

oluşturulmuş olan kontrollerin değerlendirilmesi bağlamında gelecekteki risk ve olaylara odaklanır. Bir başka deyişle dış denetim geçmişe dönük odak temelli iken iç denetim gelecek dönük odak temellerine sahiptir.

- *Bağımsızlık;* Dış denetçi bağımsız bir konumdadır. Organizasyonun bir çalışanı değildir. İç denetçi ise organizasyonun bir çalışanı veya organizasyon içerisinde bağımsız bir birey olabilir.

2 BÖLÜM
İÇ DENETİM STANDARTLARI, ULUSLARARASI YAPILAR VE ULUSAL MEVZUAT

Çalışmanın ikinci bölümünde öncelikler IIA tarafında oluşturulmuş olan iç denetim standartları, mesleki uygulama çerçeveleri incelenmiştir. Ardından denetim faaliyetleri ile ilişkili uluslararası organizasyonların üzerinde durulmuş ve son olarak denetim ile ilişkili ulusal mevzuat incelenmiştir.

2.1 ULUSLARARASI İÇ DENETİM STANDARTLARI

Denetim faaliyetleri daha önce de belirtildiği gibi küresel olarak birbiriyle etkileşime açık faaliyetlerdir. Özellikle günümüzde ülkeler ekonomik, sosyal veya tarihi nedenlerle çeşitli üst yapılar çatısında ortaklıklar kurabilmektedirler. Farklı alanlarda meydana gelen bu birlikteliklerin denetim faaliyetlerini kapsamayacağı tabii ki düşünülemez. Bir ülkede meydana gelen ekonomik kriz, başka bir ülkeyi etkileyebilir. Bununla beraber ekonomik kriz pek çok alanın olduğu gibi denetim faaliyetleri alanında sorgulanmasını beraberinde getirir. Benzer biçimde iç denetim faaliyetleri de kriz ortamında sorgulanır ve kurum ya da şirket bazında öz değerleme süreçlerine tabii tutulabilir. Ayrıca her ne kadar ülkeden ülkeye, ya da örgütsel kültür anlamında işletmeden işletmeye değişiklikler görülse de risk yönetimine ve iç kontrole gösterilmesi gereken dikkat ortak bir gerekliliktir (Florina ve ark., 2013, s. 1361).

Kuruma ya da işletmeye sunulan iç denetim hizmetinin kalitesi, hesap verilebilirliği ya da güvenilirliğinin ölçülmesi için uluslararası boyutta bazı ilkelere gerek duyulmuştur. Küresel boyutta belirlenecek standartlar ve bu standartlara göre yapılan iç denetim faaliyeti organizasyon yönetim kuruluna ya da ilgili kişilere kıyaslama yapma ve öz değerleme anlamında kolaylık sağlamaktadır. Bu bağlamda iç denetçilerin de söz konusu standart ve ilkeler çerçevesinde yeterliliğini ölçen ve çeşitli uluslararası organizasyonlarca yapılan sertifikasyon ve yeterlilik sınavlarında başarılı olması, iç denetçilerin uluslararası alandaki yeterliliklerinin bir göstergesi olmaktadır. İç denetçilerin bilgi beceri seviyesi kurum özelinden ülke geneline pek çok iyileşmenin tetikleyici unsuru olabilir. İç denetçilerin becerileri ve önerilerinin

yolsuzluk, risk yönetimi ve etik olmayan davranış ya da süreçler üzerinde çok önemli etkileri vardır (Chevers, 2013, s. 54). Ayrıca Uluslararası İç Denetim Standartları organizasyonların yönetim kurulları tarafında iç denetim birimlerini değerlendirmekte de kullanabilirler (IIA, 2015, s. 2). Görüldüğü üzere standartların hem iç denetim biriminin kendi faaliyetlerinde temel önemi söz konusudur hem de birimin bağlı bulunduğu yönetim kurulu içinde iç denetim faaliyetlerinin değerlendirme anlamında kriter belirleyici rolü söz konusudur. IIA, 2024 yılında çıkarmış olduğu "Global İç Denetim Standartları" dokümanı ile en son 2017 de güncellenen iç denetim standartlarında değişikliklere gidilmiştir. 9 Ocak 2024 tarihi itibariyle güncellenmiş olan küresel iç denetim standartları bir yıllık geçiş dönemi neticesinde 9 Ocak 2025 yılı itibariyle geçerlilik kazanacaktır (IIA, 2024a). Yukarıda anlatılanlar ışığında, çalışmanın izleyen kısmında iç denetim faaliyetlerini kapsayan uluslararası standartlar, ulusal mevzuat ve iç kontrol modeli incelenmektedir.

2.1.1 İç Denetçiler Enstitüsü

İç Denetçiler Enstitüsü (IIA) 1941 yılında kurulmuş olup, dünya çapında kabul görmüş, mesleki yeterliliğin küresel sesi olmayı başarmış bir kurumdur (IIA, 2016a). Organizasyon bir anlamda mesleğin hak koruyucusu olarak görev yapmaktadır. Bu anlamda IIA ilgili ülkelerdeki resmî kurumlar, düzenleyici kurumlar, yönetim kurumları, medya organları ve iç denetim paydaşları ile aktif olarak etkileşim halinde bulunmaktadır. Bu etkileşim ile hedeflenen temel konular aşağıdaki gibi belirtilebilir:

- İç denetçilerin rolünün bir diğer deyişle organizasyon içindeki yetki ve sorumluluklarının netleştirilmesi.
- İç denetimin fonksiyonun, organizasyon için yaratmış olduğu katma değeri diğer paydaşlara iletmek ve bilgilendirmek.
- İç denetim faaliyetlerinde profesyonel standartlara ulaşmayı ve o seviyede faaliyetlerin kalitesini korumak ve teşvik etmek.

Bu çalışmalara, IIA'nin Birleşik Devletler'de gerçekleştirdiği çalışmalardan bazıları örnek verilebilir. IIA hak koruyucu (mesleğe destek sağlayıcı) çalışmaları arasında ABD Sermaye Piyasası Kurulu (U.S. Securities and Exchange Commission – SEC) ve ABD Kamu Gözetimi ve Muhasebe Standartları Kurulu (Public Company

Accounting Oversight Board- PCAOB) gibi düzenleyici kurumlar ile iletişim içinde bulunur. ABD yönetiminin yasama bölümü içinde bulunan ve bağımsız bir kurum olan ABD sayıştayının (Walker, 2005) (Government Accountability Office) açıklanmış raporlarına yorum yapmakta, Amerikan kongresinde yasa yapıcılar ile görüşmekte olup, iyi yönetişim ve risk yönetim uygulamaları konusunda IIA'nın görüşlerine başvurulmaktadır.

IIA, iç denetim mesleğinin küresel düzeydeki temsilcisi olarak, benzer çizgideki kurumlar ile beraber iç denetim mesleğinin ve iç denetimin etkili yönetişimdeki rolünü daha fazla paydaşa açıklamaya çalışmaktadır. Benzer çizgideki kurumlara ABD özelinde şu organizasyonlar örnek verilebilir; Ulusal Kurumsal Direktörler Derneği (The National Association of Corporate Directors - NACD, Denetim Kalite Merkezi (The Center for Audit Quality – CAQ), Uluslararası Finansal Yöneticiler (Financial Executives International – FEI), Bilgi Sistemleri Denetimi ve Kontrolü Derneği (Information Systems Audit and Control Association – ISACA) ve Sertifikali Yolsuzluk Araştırmacıları Kurumu (Association of Certified Fraud Examiners – ACFE).

Enstitünün misyonu İç denetim Standartlarına temel olması açısından önem arz etmektedir. Buna göre İç Denetçiler Enstitüsünün misyonu ise üyelerine hizmet etmek ve iç denetim mesleğinin global anlamda ilerlemesine imkan sağlamak olarak tanımlanmıştır (IIA, 2016b, s. 5).

IIA'nın mesleğe hizmet noktasındaki katkıları ise aşağıdaki gibi sıralanabilir :

- Uluslararası düzeyde iç denetim fonksiyonuna ilişkin kabul görmüş standartların belirleyicisi olmak.
- Yeterlilik sertifikaları küresel olarak kabul gören güçlü organizasyonlardan biri olmak.,
- Araştırma ve eğitim hizmetleri sunan ve akademi görevini sağlamak.

Organizasyonun dünya çapında 190 ülkeden 180.000'in üzerinde üyesi bulunmakta olup, üyelerine gerek internet üzerinden gerek ise basılı dokümanlar üzerinden

eğitim, araştırma ve kaynak desteği vermektedir. Eğitim çalışmaları kapsamında, enstitü üniversite öğrencilerinden üst düzey denetim profesyonellerine kadar geniş bir yelpazeye hitap etmektedir. Söz konusu eğitim çalışmalar çeşitli platformlarda sağlanabilmektedir. Halka açık seminerler, internet sitesi üzerinden verilen kişiselleştirilebilir kurslar, e-seminerler, üyelere özel çevrimiçi seminerler, e-çalıştaylar, konferanslar ve IIA CIA Eğitim Sistemi gibi yollar üzerinden eğitim çalışmaları devam etmektedir. Ayrıca IIA üniversitelere yönelik bir çalışmalarda bulunmaktadır. Üniversitelerde denetime yönelik müfredat geliştirme çalışmaları buna örnek verilebilir.

Eğitim çalışmalarının yanında Enstitü bünyesinde araştırma faaliyetlerine de değinilebilir. Enstitü, belirli zaman aralıkları ile küresel ve bölgesel anketler, masa başı tartışmaları, benchmarking çalışmaları gibi araştırma projeleri gerçekleştirmektedir.

Bunun yanında Enstitü bünyesinde kurulan IIA Araştırma Vakfı (IIA Research Foundation – IIARF), kar gütmeyen bir organizasyon olarak pek çok araştırmaya destek vermektedir. Yönetişim, sürdürülebilir gelişme, yolsuzluk tespiti ve yolsuzluktan korunma, Bilgi Teknolojileri ve güvenliği konuları olmak üzere 200'den fazla araştırma raporuna itici kuvvet olarak destek olmuştur. Söz konusu vakfın iç denetim mesleğinin uygulamalarını genel olarak değerlendiren ve açıklayana CBOK (Common Body of Knowledge) isimli küresel projesi de bu alanda çalışma yapan profesyonellere önemli bir kaynak sağlamaktadır.

2.1.2 Uluslararası Mesleki Uygulama Çerçevesi (UMUÇ)

İç denetim faaliyetleri, organizasyonun içinde bulunduğu ülkenin mevzuatı bünyesinde ve kültürel anlamda da benzer şekilde içinde bulunduğu kültürel yapı içinde şekillenmektedir. Söz konusu bölgesel etkiler sadece iç denetim faaliyetleri için değil diğer tüm uluslararası mesleki faaliyetler için de geçerlidir. Örneğin bir muhasebecinin ya da dış denetçinin de gerek ulusal mevzuat gerek ise de kültürel farklılıkları anlamında mesleki farklılıkları söz konusu olabilir. Bu bağlamda dünyada faaliyet göstermekte olan iç denetçilerin kendi yasal ve kültürel kısıtları düşünüldüğünde global anlamda izlemeleri gereken bir standartlar, politika ve

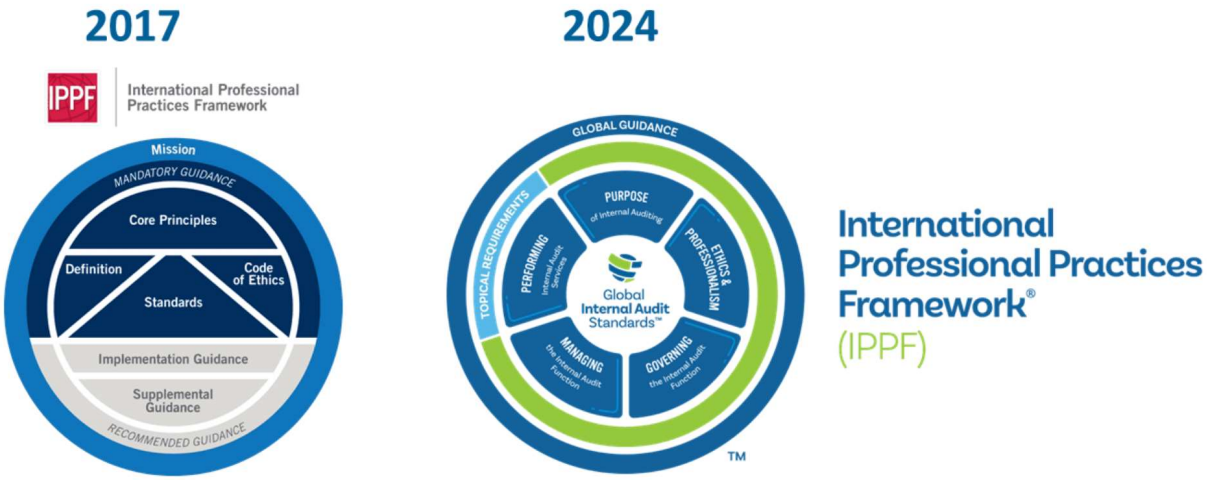
prosedürler paketi oluşturma ihtiyacı hasıl olmuştur. Uluslararası mesleki uygulama çerçevesi bu anlamda IIA'nın iç denetim mesleğinin uygulamasına yönelik kapsayıcı bir rehber olup içerinde hem zorunlu hem de güçlü bir şekilde önerilen kısımları mevcuttur (Pitt, 2014, s. 8). Ayrıca çerçeve sabit bir kapsamda kalamamakta olup sürekli gelişime ve değişime tabidir.

IIA'nın bu çerçevede, UMUÇ oluşturma anlamında attığı adımlar kısaca aşağıdaki gibi belirtilebilir (IIARF, 2016a, s. 14):

- 1947, 1968, 1978 ve 1998 yıllarında sırasıyla iç denetim faaliyetleri sorumluluklar bildirgesinin yayınlanması, etik kurallar bildirgesinin yayınlanması, "Standartlar"ın yayınlanması ve görev gücü belgesinin yayınlanması olarak sıralanabilir.

Tüm bu belirtilen aşamalar neticesinde günümüzde kullanımda olan Uluslararası Mesleki Uygulamalar Çerçevesi (IPPF/UMUÇ) ortaya çıkarılmıştır. Söz konusu çerçeve Uluslararası İç Denetim Standartları Kurulu (Board of International Internal Auditing Standarts) tarafından gerekli görüldüğü kapsamda yenilenmekte ve güncellenmektedir.

UMUÇ'un kendine özgü yapısı ve birleşik süreçleri bünyesindeki tüm rehber belgelerin güncel, konu ile ilişkili ve uluslararası anlamda geçerli ve kabul edilebilir olmasını sağlamaktadır. UMUÇ Gözetim Konseyi (IPPF Oversight Council) söz konusu süreçleri gözden geçirmekte olup, bu çerçevede tüm süreçlerin şeffaf ve güncel gelişmelere uyumlu olmasını sağlamak ile görevlidir. Günümüzde yürürlükte olan UMUÇ 2017 yılında oluşturulmuş olup, 2024 yılı itibariyle güncel versiyon hazırlanmıştır. 2024 UMUÇ güncel versiyonu 9 Ocak 2025 tarihi itibariyle yürürlüğe girecektir. İzleyen kısımda günümüzde yürürlükte olan 2017 çerçevesine değinilecek olup gerekli kısımlarda 2025 yılında yürürlüğe girecek çerçeve ile olan farklar açıklanmaktadır. Yürürlükte olan UMUÇ bünyesinde zorunlu ve kuvvetle tavsiye edilen rehberler olmak üzere iki farklı seviyede bileşen vardır (IIA, 2024a, s. 1).



Şekil 5: Uluslararası Mesleki Uygulamalar Çerçevesi

Şekil-5 de görüldüğü üzere tüm UMUÇ birbiri ile ilişkili bileşen şeklinde bütün olarak değerlendirilmektedir. Öncelikle misyon bileşeni incelenmektedir. İç denetim misyonu şekilde de görüldüğü üzere tüm çerçeveyi kapsar şekilde oluşturulmuştur. Bu durum bilinçli bir şekilde oluşturulmuş olup zorunlu ve tavsiye edilen rehberlerinde üzerinde bir iç denetim misyonunun varlığından bahseder. Bir başka deyişle uygulayıcıların misyonu gerçekleştirmek için bütün çerçeveyi nasıl kullanacağını vurgulamak üzere bilinçli olarak en dış halkaya konumlandırılmıştır. İç denetim misyonu kavramına geçilmeden belki de öncelikle organizasyonlar için misyon kavramı kısaca ele alınmalıdır. Misyon, organizasyonun var oluş sebebini açıklayan, onun varlığının sadece finansal anlamda kazanç sağlamaktan çok daha öte bir konumda olan temel amacıdır (Kılıç, 2010, s. 90). Bu çerçevede organizasyonun hedefine ulaşmada izleyeceği yolu belirler ve organizasyon içi fonksiyonlar için bir rehber niteliği taşır (Kılıç, 2010, s. 91).

İç denetim misyonu, organizasyonun bünyesinde gerçekleştirmeyi istediği tüm hedefleri kapsar. Daha detaylı bir tanım ile iç denetim misyonu; risk yönetimi temelinde, kuruma objektif güvence sağlayarak ve öneri ve iyileştirmeler ile kuruma değer katmak ve değeri korumak olarak belirtilebilir (TİDE, 2015, s. 2). Zorunlu rehber ise geniş bir anlatım ile işin özünü oluşturan konuları kapsamakta olup, günümüzde profesyonel iç denetim mesleki uygulamalarında temel kaynak ve

standartları olarak değer görmektedir (Kara, 2011, s. 51). Bu çerçevede UMUÇ'un ilk olarak zorunlu rehber kısmı ele alındığında, 4 adet ana başlık görülmektedir. Bunlar:

- UMUÇ'ın genel olarak kavramsal çerçevesini belirtilen "Tanım" kısmı.
- Ana Prensipler.
- Etik Kurallar.
- Standartlar, olarak sıralanabilir.

2.1.2.1 Tanım

UMUÇ'un zorunlu rehberinde yer alan ilk kavram tanım kavramıdır. Bu bölümde iç denetimin güncel tanımı belirtilmiş ve iç denetim fonksiyonunun kapsamı kısaca ele alınmıştır. UMUÇ'a göre iç denetim, bir kurumun faaliyetlerini iyileştirmek ve geliştirmek amacıyla ve onlara değer katmak için gerçekleştirilen bağımsız ve tarafsız bir güvence ve danışmanlık faaliyetidir (IIARF, 2016a, s. 15). Bu anlamda tanımda yer alan belirli bazı kavramlar kısaca açıklanmaktadır. Ele alınacak temel konular bağımsızlık ve tarafsızlıktır. Bağımsızlık genel anlamıyla denetçinin yönetim kuruluna direkt olarak raporlama yapabilmesi ve organizasyon bünyesinde tüm iş ve işlemleri denetleyebilmesinin sağlanması olarak özetlenebilir. Diğer bir deyişle iç denetim yöneticisinin yönetim kuruluna direkt erişiminin mümkün olmasıdır. Tarafsızlık, iç denetçinin görevini yaparken ön yargılardan uzak ve çıkar çatışmasından kaçınır bir konumda olmasıdır.

2.1.2.2 Ana Prensipler

Zorunlu rehber bileşenlerinden ikincisi olan Ana Prensipler, iç denetim sürecinde mesleki uygulamalar için ana prensipleri belirtmektedir. Buna göre söz konusu prensiplerden bazıları, dürüstlük, yüksek bilgi, özen, objektiflik, içgörü olarak sıralanabilir. Söz konusu prensiplere, iç denetçilerin tüm denetim, güvence ve danışmanlık faaliyetlerinde uyması ve mesleki ilkelerini benimsemesi beklenmektedir. Bu çerçevede iç denetçilerin yetkinliğinin de üst seviyeye ulaştırılması beklenmektedir.

2.1.2.3 Etik Kuralları

Etik kelimesi güncel Türkçe sözlükte birinci anlamı olarak töre bilimi, ikinci anlamı olarak ise paydaşların izlemesi ya da uzak durması gereken davranışlar bütünü olarak tanımlanmıştır (TDK, 2017). Genel anlamı ile kötülük etmekten kaçınma, iyilik etme, adil davranma gibi anlamlar yüklenmekle beraber; etik, hem oluşturulan yazılı kaynaklar ile hem de insanların çoğunluğu tarafından mutabık kalınan ahlaki ilkeler olarak tanımlanabilir (Yıldız, 2014, s. 265). Günümüzde iş hayatında çalışanlar günlük çalışmalar esnasında bazı kararlar vermek durumunda kalmaktadırlar. Etik bir başka açıdan ele alındığında, özellikle teknolojinin yön vermeye başladığı modern dünyada insanların "en iyisi" için çaba harcamaları ve verdikleri kararlarda ve davranışlarında "en iyiye" ulaşmada takip edebilecekleri standartlar bütünü olarak da tanımlanabilir (Kizza, 2007, s. 23). İç denetim açısından etik kuralları ise izleyen kısımda ele alınmaktadır.

Etik kurallar, zorunlu rehberin bir başka başlığı olup, dokümanda IIA tarafından iç denetim sürecinde sağlanması beklenen temel etik ilkeler açıklanmaktadır. Daha detaylı bir anlatım ile etik kuralları; iç denetim faaliyeti ile ilgili ilke ve davranış tarzlarını tanımlayan davranış kurallarıdır ve iç denetim hizmeti veren herkesi kapsamaktadır (TİDE, 2011, s. 1). Tüm farklı mesleki alanlarda genel kabul gören ve önemi çok büyük olan bir unsur müşteri nezdinde kurum ya da organizasyona duyulan güvendir (IIARF, 2016a, s. 19). Dolayısıyla kurumların etik kurallarına saygılı şekilde yönetilmeleri ve etik ihlallerine karşı gerekli kurum içi tedbirleri almaları, müşterilerin ya da hizmet alanların gözünde kuruma olan güveni doğal olarak artırır. Güven arttıkça da kurumun değeri de paralel şekilde artma eğiliminde olmaktadır. Ayrıca yapılan bir araştırmaca ülkemizdeki kamu iç denetçileri için etik kavramının iç denetim faaliyetlerinde etkili ya da çok etkili olduğu sonucuna varılmıştır (Özdemir, 2011, s. 16). Görüldüğü üzere gerek organizasyonun dış çevresinde yer alan müşteriler gerek ise de içinde yer alan ve örneğimizde iç denetçileri ele alan çalışmada da görüldüğü etik kuralları iç denetim faaliyetlerinde önemli bir yer teşkil etmektedir.

UMUÇ zorunlu rehber içerisinde yer alan bu bölümün Etik Kurallarıyla Tanışma Metni ve Etik Kuralları olmak üzere iki alt başlığı bulunmaktadır. Tanışma metninde etik kuralların amacı belirtilmekte olup, IIA'ya göre etik kuralların amacı iç denetim uygulamalarında etik anlayışını yerleştirmek ve geliştirmektir. Söz konusu anlayışın sağlanması için iki temel kavram ortaya çıkmaktadır. Bunlar, ilkeler ve davranış kurallarıdır. Etik kuralları yukarıda da belirtildiği gibi ilkeler ve davranış kuralları olarak ikiye ayrılmıştır. İç denetçilerin aşağıdaki ilkeleri uygulaması ve benimsemesi gerekli görülmektedir (IIA, 2018b, s. 1).

Yukarıda verilen mesleki ilkelerin yanında daha önce de belirtildiği üzere iç denetçilerce benimsenmesi ve uyulması beklenen davranış kuralları da belirlenmiştir. Söz konusu davranış kuralları esas itibariyle etik ilkelerin, iç denetçinin davranışlarına yansıması anlamında tekrardan değerlendirilmesidir. Davranış kuralları IIA'nın dokümanında dürüstlük, objektiflik, gizlilik, yetkinlik ilkeleri temelinde açıklanmıştır (IIA, 2018b, s. 2) :

Davranış kuralları bir başka anlatım ile etik ilkelerin uygulama noktasında nasıl ele alınacağını açıklayan bir uygulama rehberi olarak da değerlendirilebilir. UMUÇ'un zorunlu rehber kısmının ilk üç bölümü böylece ele alınmış olup dördüncü ve son bölümü olan Standartlar bölümü, çalışmanın temel konularından biri olduğundan ayrıca değerlendirilecektir. UMUÇ'ün yürürlükte olan versiyonunda yukarıda da ele alındığı üzere 6 temel başlık yer almaktadır. 2025 yılında yürürlüğe girecek versiyonunda ise UMUÇ 3 unsurdan oluşmaktadır (IIA, 2024b, pp. 5,6). Bunlar sırasıyla küresel iç denetim standartları, konu temelinde gereklilikler ve küresel rehber olarak belirtilebilir. Gelecek versiyonda da kullanımda olan versiyondakine benzer şekilde zorunlu alan ve tavsiye edilen alanlar yer almaktadır. Küresel iç denetim standartları ve konu temelinde gereklilikler kısımları zorunlu alanda yer almakta iken küresel rehberler ise tavsiye edilen alanda yer almaktadır (IIA, 2024b, s. 5)

2.1.3 Uluslararası İç Denetim Standartları – "Standartlar"

UMUÇ'un zorunlu rehberinin ilk üç bölümü açıklandıktan sonra bu kısımda da zorunlu bölümün son maddesi mesleki standartlara değinilmektedir. Bilindiği gibi uluslararası alanda toplumlar, kültürler ve hatta aynı toplumda farklı zamanlarda çeşitli farklılar söz konusudur. Ayrıca organizasyonlar arasında da yine benzer şekilde hukuki, kültürel, hacim anlamında ve örgütlenme anlamında farklılıklar söz konusu olabilmektedir. Tüm bu kültürel ve organizasyonel farklılıklara rağmen, iç denetim fonksiyonunun ve iç denetçilerin görev ve sorumluluklarını yerine getirmesinde iç denetim standartları çok önemli bir noktadadır. Diğer bir deyişle standartlar iç denetim mesleğinde ve faaliyetlerinde profesyonelleşmenin temel kaynağıdır. Çünkü aşağıda da görülecek olan standartlar; kültürel, toplumsal ve organizasyonel farklılıkların üzerinde bir konumdadır. Standartların amaçları 3 başlıkta beli

- İç denetim uygulamasını olması gerektiği gibi temsil eden temel ilkeleri tanımlamak.
- Katma değerli iç denetim faaliyetlerini teşvik etmeye ve hayata geçirmeye yönelik bir çerçeve sağlamak.
- Performansının değerlendirilmesine uygun bir zemin oluşturmak.
- Gelişmiş kurumsal süreç ve faaliyetleri canlandırmak.

Söz konusu standartlar kendi içinde iki bölümden oluşmaktadır. Bunlardan birincisi standardın temel beyanı diğeri de bahsi geçen beyanı açıklayan, yorumlardır. Temel beyanlar iç denetim fonksiyonunun uygulanabilmesini, etkinliğini değerlendirebilmeyi amaçlayan organizasyonel ve kişisel (iç denetçi) boyutlarında olan kavramlardır. Yorumlar ise söz konusu temel beyanlarda tanımlanan kavramları açıklamaya yarayan destekleyici açıklamalardır. Ayrıca standartlarda belirtilen terimler, tine yine standartların bir parçası olan Terimler Sözlüğü'nde tanımlanmaktadır. Bu durumda bir standardın anlaşılması için standardın temel beyanı değerlendirilmeli ancak sadece bu aşama ile sınırlı kalınmamalı, bunun yanında ilgili standardın yorumu ve terimsel sözlüğünde geçen ilgili terimler de değerlendirilmelidir.

Standartlar; nitelik ve performans standartları olmak üzere iki ayrılmaktadır. Ayrıca nitelik ve performans standartlarını geliştirme amacı ile uygulama standartları adıyla bir standart geliştirilmiştir. Uygulama standartları, güvence (standartlarda A harfi ile gösterilir- Application) veya danışmanlık (standartlarda C harfi ile gösterilir- Consultancy) faaliyetleri çerçevesinde uygulanabilecek gereklilikleri tanımlar. Bu çerçevede öncelikler nitelik ve performans standartlarının tanımı ile uygulama standartlarının kavramsal çerçevesi olan güvence ve danışmanlık hizmetlerinin tanımım yapılmaktadır.

Nitelik standartları, iç denetim fonksiyonu içerinde olan organizasyon ve profesyonellerin niteliklerine ve özelliklerine odaklanan standartlardır. Performans standartları ise iç denetim fonksiyonunun tabiatını açıklar ve iç denetimin performans değerlendirmekte kullanılan kalite kıstaslarını belirler.

Güvence hizmetleri, iç denetçinin objektifliği ile ilgili bir kavramdır. Burada temel anlayış iç denetçinin denetim sürecinde elde ettiği delilleri objektif şekilde değerlendirerek, denetlediği ya da üzerinde çalıştığı her ne konu olursa olsun, görüş ve kanaatini bu objektiflik çerçevesinde oluşturabilmesidir. Güvence hizmeti fonksiyonu doğası gereği genellikler 3 taraflı bir süreçtir. Bunlar süreç sahibi, iç denetçi ve kullanıcı olarak tanımlanabilir. Süreç sahibi; organizasyon ya da organizasyonun bir faaliyet olabileceği gibi kişi ya da grup da olabilir. İç denetçi, değerlendirmeyi gerçekleştiren kişi ya da heyet olarak düşünülebilir. Son olarak kullanıcı ise değerlendirmeyi kullanan taraftır.

Danışmanlık hizmetleri, genelde tavsiye veren kişi konumunda olan iç denetçi ve tavsiye talep eden taraf arasında bir sözleşme ile gerçekleşen ve tavsiye talep eden tarafın belirteceği iş ya da işlemler üzerinde iç denetçinin objektif değerlendirmesinin nihai olarak sunulması hizmetidir.

Standartlar yukarıda da bahsedildiği sürekli gelişen ve değişen küresel ve organizasyonel dinamikler çerçevesinde sürekli gelişen bir yapıya sahiptir. Enstitü 2010 yılından itibaren UMUÇ izleme komitesi adıyla, farklı ülkelerden üyelere sahip biz değerlendirme komitesi de oluşturmuştur (D. Chambers, 2014, s. 214).Tüm iç

denetçiler söz konusu standartlar ile ilgili olarak kendi görüşlerini IIA'ya iletebilmektedir.

2024 yılında yapılan güncelleme ile 2025 yılı Ocak ayından itibaren güncellenmiş iç denetim standartları yürürlüğe girecek olup 5 ana bölümden oluşmaktadır (IIA, 2024c, s. 4). Bunlar sırasıyla; iç denetimin amacı, etik ve profesyonellik, iç denetim fonksiyonunun yönetişimi, iç denetim fonksiyonunun idaresi ve iç denetim hizmetlerinin yürütülmesi olarak belirtilebilir. Ayrıca yeni versiyonda eskisinde farklı olarak nitelik ve performans standartları ayrımı sona erdirilmiş ve bunun yerine "gereklilikler", "uygulamaya ilişkin değerlendirmeler" ve "uygunluğa ilişkin kanıt örnekleri" başlıklarından oluşan bir sınıflandırmaya gidilmiştir (IIA, 2024c, s. 4).

İzleyen kısımda çalışmanın da ana başlıklarından biri olan IIA İç Denetim Standartları (yürürlükte olan 2017 versiyonu), içeriği anlamında incelenmektedir.

2.1.3.1 Amaç, Yetki ve Sorumluluklar

Uluslararası İç Denetçiler Enstitüsü tarafından UMUÇ bağlamında ortaya konulan standartlardan ilki ve 1000 rakamı ile kodlu olup, amaç yetki ve sorumluluklar konusunu ele almaktadır. Söz konusu ilkeye göre; amaç, yetki ve sorumluluklar, iç denetime ilişkin tanımlar, etik kurallar ve standartlar ile uyumlu olan bir yönetmelik hazırlanmalı ve resmi olarak tanımlanmalıdır. Bu çerçevede iç denetim yöneticisi de söz konusu yönetmeliği periyodik olarak gözden geçirmeli ve gerekli gördüğü düzeltmeleri ve güncellemeleri yaparak üst makama onay için sunmalıdır. Yetki ve sorumluluklar netleştirildiği takdirde süreçlerin sorumluları hesap verebilir pozisyona gelmektedir. Hesap verilebilir iç denetim için iç denetimin amacının, organizasyon bünyesindeki yetki ve sorumluluğun net bir şekilde belirlenmesi beklenmektedir. Örneğin risk odaklı bir iç denetim gerçekleştirilecekse, bu süreç işletmenin riskleri ve bu risklerin yönetilmesi üzerine eğilen bir denetim süreci gerçekleştirilmelidir (S. S. Kara, Şakir, 2012). Denetim sürecinin amaç, yetki ve sorumluluğunun da bu bağlamda oluşturulması beklenebilir Ayrıca yine maddede dikkat çekilen bir diğer konu ise iç denetim yöneticisinin organizasyonun en üst organı olan yönetim kuruluna işlevsel bağlılığının tanımlanması konusudur. Gerçekten de iç denetim

fonksiyonun işletmenin tüm diğer karar alma faktörlerinden bağımsız olması gerekmektedir (Florea, 2013, s. 81). Söz konusu bağımsızlık iç denetim yönetmeliğinde net bir şekilde ortaya konulmalıdır.

2.1.3.2 Bağımsızlık ve Objektiflik

Nitelik standartlarının bir diğeri 1100 kodlu Bağımsızlık ve Tarafsızlık standardıdır. İç denetçinin bağımsız olması bu anlamda nasıl sağlanacağı sorusuna cevap vermektedir. Buna göre iç denetçi iç denetim faaliyetindeki sorumluluklarını tarafsız olarak yerine getirme kabiliyetine engel olan tüm şartlardan uzak durmalıdır. Bir diğer açıdan da iç denetim yöneticisi kurumun üst yönetime doğrudan erişebilmelidir.

Bağımsızlık ve objektiflik standardının bazı alt kırımları söz konusudur. Bunlardan ilki kurum içi bağımsızlık kavramıdır. Kurum içi bağımsızlık ilkesine göre iç denetim yöneticisi, kurum bünyesinde, yapacağı faaliyet kapsamındaki sorumluluklarını yerine getirmesine imkân sağlayacak bir üst yönetim kademesine bağlı olmalıdır. Diğer bir deyişle iç denetim yöneticisinin işlevsel olarak yönetim kuruluna raporlama yapması beklenmektedir. İşlevsel raporlama örneği olarak ise yönetim kurulunun aşağıdaki faaliyetleri olarak verilebilir (IIA, 2017, s. 5):

Nitelik Standartlarından 1100 kodlu Bağımsızlık ve Tarafsızlık standardının bir diğer alt kırılımı da bireysel objektiflik kavramıdır. Bireysel objektiflik iç denetçilerin faaliyetlerinde herhangi bir önyargıdan ve çıkar çatışmasından uzak şekilde, tarafsız olarak davranması gerekliliğidir. Çıkar çatışması iç denetçinin gerek kişisel gerek ise de mesleki anlamda birbirine rakip olan çıkarlarının olması durumu olarak tanımlanabilir. Çıkar çatışması iç denetçinin görevini tarafsız şekilde yerine getirmesine engel olacak bir durumdur.

Standardın bir diğer alt kırılımı da Bağımsızlık ve objektifliğin bozulması kavramıdır. Buna göre iç denetçiler gerçekleştirmekte oldukları faaliyete ilişkin herhangi bir neden ile bağımsızlıklarının ya da objektifliklerinin fiilen bozulduğu ya da bozulma ihtimali söz konusu olduğu anda, söz konusu bozulmanın ayrıntılarının ilgili taraflara açıklanması gerekmektedir. Kişisel çıkar çatışması, kapsam sınırlamaları, kayıtlara,

personele ve kurum varlıklarına erişim kısıtlamaları ve fonlama gibi kaynak sınırlamaları kurum içi bağımsızlık ve objektifliğin bozulması durumların örnek verilebilir. Bu sayılan durumların yanında iç denetçinin daha önceden kendisinin sorumlu olduğu bir alanda değerlendirme yapmak ya da son bir içinde kendisinin sorumlu olduğu bir faaliyet çerçevesinde güvence hizmeti vermesi de objektifliğin bozulmasına örnek olarak gösterilebilir.

2.1.3.3 Yeterlilik ve Azami Mesleki Özen ve Dikkat

Dört nitelik standardından üçüncüsü olan yeterlilik ve azami mesleki özen ve dikkat standardı 1200 kodu ile numaralandırmış olup, iç denetçilerin faaliyetleri kapsamında gerçekleştirdikleri görevleri, yeterlilik ve azamî meslekî özen ve dikkat göstererek yerine getirmek ile mükellef olduklarına işaret etmektedir. Yeterlilik gerek iç denetim faaliyeti gerek ise mesleki diğer tüm profesyonel alanlarda olsun benzer bir tanımı kapsamaktadır. Buna göre, sorumluluklar yerine getirmek için gerekli bilgi, beceri ve diğer gerekli vasıfların ilgili kişide bulunması yeterlilik tanımı olarak verilebilir. Kişisel olabileceği ilgili faaliyet anlamında birimde çalışan personel toplu bilgi ve beceri de yeterlilik kapsamına değerlendirilebilir. Söz konusu bilgi ve beceriye sahip olunmadığı düşünülüyorsa konuya ilişkin uzmanlardan gerekli eğitim ve tavsiye alınması gereklidir. Özellikle bilgi teknolojilerine ilişkin konularda iç denetçilerin temel bilgi ve beceriye sahip olması beklenmekle beraber, konunun çok geniş ve teknik olduğu düşünüldüğünde birimde yer alan tüm iç denetçilerin bilgi teknolojileri bilgi ve becerine sahip olması beklenmez (IIA, 2017, s. 7). Çalışmanın uygulama kısmı ve sonuçlar kısmında iç denetçilerin bilgi güvenliğine ilişkin yetkinliklerinin olumlu etkileri ele alınmıştır.

2.1.3.4 Sürekli Mesleki Gelişim

Uluslararası İç Denetçiler Enstitüsünce yayımlanan iç denetim standartları içinde yer alan nitelik standartlarının dördüncü ve sonuncusu, sürekli mesleki gelişim standardıdır. Bu standarda göre iç denetçilerin, mevcut bilgi, beceri ve diğer vasıflarını sürekli mesleki gelişimle artırmaları ve güçlendirmeleri gerekmektedir. Bu çerçevede iç denetim yöneticisi, iç denetim faaliyetinin tüm yönlerini kapsayan bir

kalite güvence ve geliştirme programı hazırlamakla ve bunu devam ettirmekle mükelleftir. Söz konusu program iç denetim faaliyetinin ilgili tanımlara ve standartlara uyup uymadığının ve iç denetçilerin etik kurallarını uygulayıp uygulamadığının değerlendirilmesine imkân sağlamak amacıyla tasarlanır. Kalite güvence program gerek iç gerek ise de dış değerlendirmeleri içermelidir. Söz konusu iç ve dış değerlendirmelerin örnek vermek gerekirse; denetim fonksiyonun sürekli takibi ve periyodik olarak yapılan kurum dışı değerlendirmelerdir (IIA, 2017, s. 9).

Kalite güvence ve geliştirme programının yapısı ve kapsamı ele alındıktan sonar izleyen aşama söz konusu program hakkında raporlama yapılmasıdır. Bu çerçevede iç denetim yöneticisi, uygulanan kalite güvence ve geliştirme programının sonuçlarını üst yönetime ve yönetim kuruluna iletmek zorundadır. Söz konusu raporun ne kadar sürelik periyotlar ile hazırlanacağı, içeriğinin tam olarak hangi konuları kapsayacağı ve raporu ilgililere ulaştırma şekli üst yönetim ve yönetim kurulu ile alınan ortak kararlar doğrultusunda olur.

Konu standarda ilişkin bir diğer alt kırılım da “uygulama standartlarına uygundur” şeklinde bir ibarenin iç denetim faaliyetlerinde kullanılmasın ilişkindir. Buna göre iç denetim yöneticisi ancak kalite güvence ve geliştirme programının sonuçları destekler ise iç denetim faaliyetlerinin uluslararası standartlara uygun olduğunu belirtilebilir. Anılan sonuçlar yukarıda ele alınan iç ve dış değerlendirme sonuçlarından oluşmaktadır. Herhangi bir uygunsuzluk saptandığı durumda ise konu üst yönetimi ve yönetim kuruluna açıklanmak zorundadır.

2.1.3.5 İç Denetim Faaliyetinin Yönetimi

Uluslararası iç denetim standartlarının iki türünden biri olan nitelik standartları yukarıda ele alınmış olup çalışmanın izleyen kısmında ise ikinci tür standart olan performans standartları incelenmektedir. Performans standartları yukarıda da açıklandığı üzere, iç denetim fonksiyonunun tabiatını açıklar ve iç denetimin performans değerlendirmekte kullanılan kalite kıstaslarını belirler. Bu çerçevede ilk performans standardı 2000 kodu ile numaralandırılmış “iç denetim faaliyetinin

yönetimi" standardıdır. İç denetim fonksiyonu kuruluşa değer katmasını sağlayacak etkili bir şekilde yönetilmek durumundadır. Standartta belirtilen etkililikle örnek vermek gerekirse, iç denetim süreçleri ilgili standart ile uyumlu olması gerektiğinden bahsedilebilir. (IIA, 2017, s. 12):

Ayrıca iç denetimin tanımında bahsi geçen kuruma ya da organizasyona değer katan ve risk yönetimi ve iç kontrol süreçlerinin etkinliği ve etkililiğini sağlayan şekilde işleve sahip olması, iç denetim faaliyetinin tarafsız ve uygun güvence sağladığında söz konusu olabilmektedir.

İç denetim faaliyetinin yönetimi isimli standardın yedi adet alt kırılımı vardır. Bunlar planlama, bildirim ve onay, kaynak kullanımı, politika ve prosedürler, eşgüdüm (koordinasyon), üst yönetim ve yönetim kuruluna raporlamalar ve son olarak da iç denetime yönelik dış hizmet sağlayıcı ve kurumsal sorumluluk alt kırılımlarıdır.

2.1.3.6 İşin Niteliği

Standartlar içerisinde yer alan ikinci performans standardı 2100 kodu ile numaralandırılmış olan "işin niteliği" başlıklı standarttır. Anılan standarda göre iç denetim faaliyetinin, kurumun yönetişim, risk yönetimi ve kontrol süreçlerinin değerlendirmesini yapması ve anılan süreçlerin daha iyi bir seviyeye getirilmesine katkı sağlamasının gerekliliği işaret edilmektedir. Ayrıca söz konusu değerlendirme ve katkının sistematik ve disiplinli bir yaklaşım ile gerçekleştirilmesinin önemi vurgulanmaktadır. Yukarıdaki tanımda yer alan yönetişim, risk yönetimi ve kontrol kavramlarını açıklayan alt kırımlar ilgili standartta ele alınmaktadır (IIA, 2017, s. 15).

Ayrıca yönetişimin bilgi teknolojileri boyutu da söz konusudur. Bu çerçevede bilgi teknolojileri yönetişiminin kurumun strateji ve amaçlarını ne ölçüde desteklediği de değerlendirilmelidir.

Yönetişim kavramının ardından değerlendirmeye konu olacak bir diğer unsur da risk yönetimidir. İç denetim birimi, tanımında da belirtildiği üzere risk yönetimi süreçlerinin etkinliğini değerlendirmek ve iyileştirilmesine katkıda bulunmakla

mükelleftir. Söz konusu etkinliği değerlendirme sürecinde, misyon, riskler, risk cevapları gibi kavramların netleştirilmiş olması gerekmektedir (IIA, 2017, s. 16):

İç denetim faaliyeti risk yönetiminin değerlendirilmesine benzer şekilde kontrollerin etkinlik ve verimliliğini de değerlendirmek ve sürekli gelişimi teşvik etmek yoluyla, kurumun etkin kontrollere sahip olmasına yardımcı olmakla sorumlu olmasına işaret eden bir alt kırılımdı da kontrol kavramıdır.

Kontrollerin yeterliliğini ve etkinliğinin varlıklar, stratejik hedefler, etkinlik verimlilik boyutlarıyla ilgili olarak değerlendirilmesi söz konusudur (IIA, 2017, s. 17) :

2.1.3.7 Görev Planlaması

Performans standartların bir diğeri 2200 kod numarası ile görev planlaması standardıdır. İç denetçiler yapacakları görevler için plan hazırlamalıdırlar. Söz konu plan hazırlanırken dikkat edilmesi gereken bazı noktalar vardır. Buna göre görev planı hazırlanırken iç denetçilerin dikkate alması gereken kontrol araçları, riskler, indirgeyici araçlar, geliştirme imkanları vb. konular ele alınmaktadır (IIA, 2017, s. 17)

Görev planlaması standardının bir diğer alt kırımı da görev amaçlarıdır. Bu kırılıma göre amaçlar organizasyonun stratejik hedefleri ile uyumlu olmalı ve yapılan risk ve kontrol değerlendirmelerinin sonuçlarını yansıtır içerikte olmalıdır.

Her bir görev içi belirlenen amaçların karşılanabilmesi için görevin kapsamı da netleştirilmelidir. Bu çerçevede denetim faaliyetinin ilgilerini, maddi varlıklarını, ilgili kayıtlarını ve sistemlerini kapsamalıdır.

Amacı ve kapsamı belirlenen görevin gerçekleşebilmesi için bir diğer unsur ve standardın alt kırılımı da kaynakların kullanımıdır. İç denetçiler görevin kendine has özelliklerini dikkate alarak ayrı zaman ve mevcut kaynak kısıtlarını değerlendirerek, görevin amacınla ulaşabilmesi için uygun ve yeterli kaynağı tespit etmekle mükelleftir.

Son olarak iç denetçiler görev iş program alt kırılımı çerçevesinde faaliyetleri denetim amaçlarına ulaştırabilecek iş programlarını yazılı hale getirerek

hazırlamaktan sorumludur. Söz konusu programların türü içeriği ve şekil şartları önceden belirlenmeli ve üst yönetim ya da yönetim kuruluna onaya sunulmalıdır. Onayın ardından faaliyetler başlamalıdır.

2.1.3.8 Görevin Yapılması

Performans standartlarından 2300 kodu ile numaralandırılmış olan görevin yapılması başlıklı standarda göre, iç denetim faaliyeti kapsamında iç denetçiler belirlenen amaçlara ulaşmak için görevin gerektirdiği yeterli bilgiyi toplamak, bunları analiz etmek ve değerlendirmek, son olarak da kayıt altına almak durumundadır.

Standardın içeriğinde yer alan bilgilerin tespiti ve tanımlanması kavramı ile belirtilmek istenen denetim faaliyeti kapsamında denetim görevi için yeterli, güvenilir, denetim konusu ile ilgili ve amaca ulaşmada faydası olacak bilgileri tespit edilmesi ve tanımlanmasına işaret edilmektedir. Yeterli bilgiden kasıt bilginin gerçekleri yansıtan, uygun ve incelenmesi sonucu ikna edici özelliklere sahip olmasıdır. Güvenilirlik ise denetim kapsamında uygun görev teknikleri ile elde edilen bilginin bir özelliğidir. Bilginin faydalı olması ise kurum ya da organizasyonun amaçlarına ulaşmasında yardımı olabilecek olan bilgiyi işaret eder.

Elde edilen bilgiler ışığında iç denetçiler bir analiz ve değerlendirme süreci gerçekleştirirler. Bir kanaate varır ve bunu kayıtlı hale getirirler. Söz konusu kayıtlar saklanmak zorundadır

2.1.3.9 Sonuçların Raporlanması

Sonuçların raporlaması iç denetçiler için görev sonunda yerine getirmeleri zorunlu olan bir uygulamadır. Raporun içinde denetim neticesinde ele edilen görüşler, bulgulara ilişkin tavsiyeler ve düzeltici işlemlere ilişkin eylem planlarının bulunması gereklidir. Özellikle nihai görüş verirken; söz konusu görüşün üst yönetim, yönetim kurulu ve diğer paydaşların beklentilerinin dikkate alınması ve yeterli, güvenilir, ilgili ve faydalı bilgi ile desteklenmesi gerekmektedir.

Sonuçların raporlamasına ilişkin standardın ilk alt kırılımı raporlama kalitesine ilişkindir. Buna göre raporlamanın kalitesi, raporun doğru, nesnel, açık, özlü, yapıcı, tam ve zamanda sunulmuş olmak gibi özellikleri haiz olması ile değerlendirilebilir (IIA, 2017, s. 21):

Standardın bir diğer kırılımı da raporun ilgililere dağıtımını konu almaktadır Buna göre iç denetim raporu, iç denetim yöneticisi tarafından sonuçlarını etkilediği paydaşlara dağıtılmalıdır.

Ayrıca iç denetim yöneticisi nihai rapor yayınlanmadan önce gözden geçirilmesinden onaylanmasından ve dağıtımın kimlere yapılacağının belirlenmesinden sorumludur. Özellikle kurum dışına iletilecek raporlarına ilişkin eğer yasal mevzuatta bir zorunluluk yoksa, kurumu etkileyecek olası risklerini değerlendirmek için yönetim kurulu ya da hukuk müşaviri ile görüş alışverişi içinde olmalıdır.

Görevin yapılması başlıklı performans standardının son kırılımı da iç denetim faaliyetinin oluşturduğu genel görüşlere ilişkindir. Bir genel görüşün içerisinde kapsam, sınırlamalar, bütünsellik, ilgili ölçütler ve kanaat gibi unsurlar bulunmalıdır (IIA, 2017, s. 23):

2.1.3.10 İlerlemenin Gözlenmesi ve Risklerin Kabulü

Performans standartlarından son iki standart 2500 ve 2600 kod numaraları ile ilerlemenin gözlenmesi ve risklerin kabul edildiğinin iletilmesine ilişkin standartlardır.

Buna göre iç denetim yöneticisi, üst yönetime rapor edilen sonuçların son durumunun gözlenmesinden sorumludur. Söz konusu gözlem işlemi bu iş için kurulan bir sistemin uygulanmasını gerektirmektedir.

Denetim raporunun üst yönetime iletilmesi sonucunda ortaya iki durum çıkar. Birincisi, yönetim raporda yer alan sonuçlara ilişkin bazı tedbirler almayı Kabul eder. İkincisi ise yönetim bu tedbirleri almaz ve ortaya çıkması muhtemel riskleri almayı kabul eder. İşte bu noktada iç denetçi, gerekli tedbirlerin alınıp alınmadığı ya da tedbirleri almayarak riskleri kabul ettiğinden emin olmak için takip sürecini uygular.

Bir diğer önemli husus da üst yönetimin bazen kabul edilmesi uygun olmayan seviyede risk kabul etmesi durumunda iç denetim yöneticisinin ne yapacağı ile ilgilidir. Böyle bir durumda iç denetim yöneticisi konuyu yönetim kurulu seviyesine taşır ve konuya ilişkin yönetim kurulunu bilgilendirir. Eğer konunun çözümlendiği kararına var ise bu durumu yönetim kuruluna bildirir.

2.2 ULUSLARARASI ORGANİZASYONLAR

Çalışmanın bu kısmında denetim ve iç denetim alanında uluslararası alanda etkin faaliyet göstermekte olan ve oluşturdukları standart ve çerçeveler sayesinde denetim ve iç denetim mesleklerini küresel anlamda belirlenmiş standartlara kavuşturan organizasyonlar ele alınacaktır.

2.2.1 COSO (Committe of Sponsoring Organizations) İç Kontrol Modeli

COSO (The Comittee of Sponsoring Organizations) Sponsor Organizasyonlar Komitesi, 1985 yılında Sahte Finansal Raporlamanın önlenmesi üzerine Amerika Birleşik Devletlerinde kurulan Ulusal Komisyona destekleyici olmak amacı ile kurulmuştur (COSO, 2016b). COSO'nun 5 bağımsız kurucusu vardır. Bu kurucular arasında, IIA Uluslararası İç Denetçiler Enstitüsü de yer almaktadır (Türedi, 2014, s. 142). COSO; sahtecilik ile mücadele, kurumsal risk yönetimi ve iç kontrol olmak üzere 3 alanda çalışmalar yürütmektedir (McNally, 2013, s. 2).

2013 yılında güncellenen COSO İç kontrol modeli 17 temel ilke üzerine kurulmuştur (COSO, 2016a, s. 1). Söz konusu 17 ilke 5 bileşen altında yer almakta olup, organizasyonda etkili bir iç kontrol sisteminden söz edebilmek için söz konusu ilkelerin "var olması" ve "işliyor olması" gerekmektedir. Bu açıklamada yer alan "var olmak" kavramı ilgili bileşen ya da ilkenin organizasyonun iç kontrol sistemi dizaynı içinde var olması demek olup, "işliyor olması" kavramı ise çalışmakta olan bir iç kontrol sisteminde söz konusu bileşen ya da ilkenin var olmaya devam etmesini işaret eder (McNally, 2013, s. 5). Söz konusu 5 bileşen arasında risk değerleme ve bilgi ve iletişim bileşenleri ve 17 ilkeye de teknoloji kontrolleri ile iç ve dış iletişimin gerçekleştirilmesi ilkeleri örnek verilebilir (Galligan ve Rau, 2015, s. 3):

COSO iç kontrol modeli kendi başına yeterli bir iç kontrol sistemi oluşturmaya yeterli olmakla beraber diğer başka iç kontrol ve iç denetim modelleri ile de bütünleşmiş biçimde faaliyet gösterebilir. Örneğin üçlü savunma hattı modeli ile COSO iç kontrol modeli bütünleşmiş biçimde kullanılabilir. Yukarıda da belirtildiği üzere COSO iç kontrol modeli en temel anlatım ile risklerini etkili şekilde yönetebilmesi için bir iç kontrol sistemini oluşturma ve bu sistemi oluştururken de ilgili bileşenleri, ilkeleri ve faktörleri ortaya koyma süreçlerini alır. Ancak bu sistemde dikkat edilmesi gereken nokta kurumda söz iç kontrol faaliyetlerinden sorumlu olan kişi ya da birimler ile tam olarak hangi faaliyetleri gerçekleştirecekleri konusunda bazı boşluklar olduğu konusu gündeme gelmiş ve bu konuya ilişkin olarak üçlü savunma hattı modeli ile söz konusu boşlukların doldurulabileceği düşünülmüştür. Söz konusu model ile iç kontrole ilişkin görev sorumluluklar netleştirilmektedir. Modele göre, belirtilen üç savunma hattı aşağıdaki gibi özetlenebilir (Anderson ve Eubanks, 2015, s. 3):

Birinci savunma hattı; iş ve işlemleri gerçekleştirenlerin faaliyetlerine ilişkin risklerin yönetimi ve kurumsal hedeflerden sapmayı önleyici uygulamaları içerir. Diğer bir deyişle doğru risklerin alınması söz konusudur. Bu hatta yönetim kontrolleri ve iç kontrol ölçütleri kullanılabilir.

İkinci savunma hattı; ilk hatta ele alınan risklerin etkili şekilde yönetimi ve kontrolü anlamında gerekli adımların atılıp atılmadığına ilişkin yönetime destek sağlanması sürecidir. İlk hattan bağımsız olmayıp, temel olarak risklerin ele alınışına ilişkin bir yönetim ve gözetim fonksiyonudur. İkinci savuma hattı unsurları arasında finansal kontrol, risk yönetimi, kalite, inceleme ve uygunluk başlıkları yer almaktadır.

Üçüncü savunma hattı; bir ve ikinci hatlardaki çabalar neticesinde üst yönetime ve yönetim kuruluna güvence verilmesi aşamasını içerir. Üçüncü savunma hattı icrai işleri kapsamaz. Bunun sebebi kurumsal bağımsızlığını ve tarafsızlığını koruyabilmektir. Ayrıca bu savunma hattında yönetim kuruluna direkt raporlama yolu açıktır. Üçüncü savunma hattı iç denetim faaliyetlerini kapsar.

COSO iç kontrol modeli ile bütünleşmiş durumda çalışabilen bir diğer sistem de suistimal risk yönetimi sistemidir. Yukarıda da belirtildiği üzere COSO iç kontrol

modelinin 17 adet prensibi ve bu prensipleri bünyesinde barındıran toplam 5 adet bileşeni mevcuttur. Suistimal risk yönetimi işte bu 5 adet bileşen ile tam olarak ilişkilendirilmiş olup bileşen bazında açıklaması aşağıda kısaca açıklanmaktadır (COSO, 2016c, pp. 10-11):

Kontrol çevresi; COSO bileşeni ile ilişkilendirilen suiistimal risk yönetimi birinci ilkesi kapsamında kurum, yönetim kurulu ve üst yönetimin beklentileri ile suistimal risklerinin yönetiminde dikkat edilmesi gereken değerleri içerecek bir suistimal risk yönetimi programı oluşturmalıdır.

Risk yönetimi; bileşeni ile ilişkilendirilen ikinci ilke suistimal risk değerlemesidir. Buna göre kurum, kapsamlı bir risk değerleme faaliyeti gerçekleştirmelidir. Söz konusu faaliyetin amacı ilk olarak suistimal risklerini belirlemek, bu risklerin etki ve ihtimalini hesaplamak ile artı riski azaltacak gerekli eylemleri tanımlamaktır.

Kontrol aktiviteleri; COSO iç kontrol modelinin ikinci bileşeni olan kontrol aktivitelerinin suistimal risk yönetimi sistemi ile ilişkilendirilen prensibi ise suistimal kontrol eylemleridir. Bu ilkeye göre kurum, zamanında belirlenemeyen ya da devam etmekte olan suistimal durumu risklerinin minimize etmek için önleyici ve belirleyici eylemler seçmeli, oluşturmalı ve uygulamaya koymalıdır.

Bilgi ve iletişim; bileşeni ile ilişkilendirilen suistimal yönetim sistemi ilkesi ise suistimal soruşturma ve düzeltici eylem ilkesidir. Buna göre kurum, potansiyel suistimal durumuna ilişkin olarak bilgi sağlama amacıyla bir iletişim süreci başlatır.

İzleme Aktiviteleri; bileşeni ile ilişkilendirilen son suistimal yönetim ilkesi suistimal risk yönetimi izleme aktiviteleri ilkesidir. Bu ilke kapsamında kurum, yukarıda verilen 5 suistimal risk yönetimi ilkesinin var olduğu ve kullanılmakta olduğu konularında değerlendirmeler gerçekleştirir. Bu değerlendirme ile ilgili birimlerin alması gereken düzeltici eylemler ortaya çıkarılır.

2.2.2 Uluslararası Yüksek Denetim Kurumları Teşkilatı (INTOSAI)

Uluslararası yüksek denetim kurumları Örgütü, 1953 yılında dönemin Küba Yüksek Denetim Örgütü başkanı Emilio Fernandez Camus öncülüğünde, Küba'da

gerçekleşen ve 34 ülkenin yüksek denetim örgütünün katılımıyla yapılan birinci INTOSAI kongresinde kurulmuştur. Günümüzde örgütün 192 tam üyesi ve 5 bağlantılı üyesi bulunmaktadır. INTOSAI günümüzde kamu dış denetimi camiasında şemsiye örgüt olarak işlemlerini yürütmektedir. Bu çerçevede 50 yıldan fazla süredir faaliyetlerine devam etmektedir. Örgütün sunduğu gerçekleştirdiği çalışmalar şu şekilde belirtilebilir:

- Bilgi ve tecrübenin paylaşımı ve geliştirilmesinin teşvik edilmesi
- Kamu denetimi faaliyetlerinin dünya genelinde geliştirilmesi,
- Profesyonel kapasitenin iyileştirilmesi gibi konularda kurumsallaşmış bir çerçeve sunmak.

INTOSAI yapısal olarak apolitik, bağımsız ve otonom bir konumdadır. Bununla beraber Birleşmiş Milletler teşkilatının ana organlarından biri olan Birleşmiş Milletler Ekonomik ve Sosyal Konseyinde de özel danışmanlık statüsüne sahip hükümetler dışı bir örgüttür. Örgütün bu çalışma ile doğrudan ilişkili olan kısmı ise yayımlamış olduğu Uluslararası Yüksek Denetim Kurumları Standartları (ISSAI) olarak tanımlanan meslek standartlarıdır. Söz konusu standartlar 4 ana bölümden oluşmakta olup, küresel anlamda yüksek denetim kurumlarının gerçekleştireceği denetimlerin bütünlüğünü ortak bir standart sağlanmasını hedeflemektedir (Sayıştay, 2013, s. 14). ISSAI'den farklı olarak teşkilatın bir de INTOSAI GOV adı verilen "İyi Yönetim Rehberleri" bulunmaktadır. Uluslararası Yüksek Denetim Kurumları Standartları (ISSAI) daha önce de belirtildiği gibi 4 gruptan oluşmaktadır. Birinci grup kurucu ilkeleri kapsamakta olup INTOSAI'nin kurucu ilkelerini temel almaktadır. Bu grupta Lima deklarasyonu adı verilen ve ülkelere etkin görev yapan Yüksek Denetim Kurumlarını kurmaları konusunda çağrıda bulunulmaktadır. İkinci grup Yüksek Kurumlarının İşleyişi için ön koşulları açıklamaktadır. Söz konusu koşullar arasında:

- Bağımsızlık
- Saydamlık
- Hesap Verme Sorumluluğu

- Etik kurallar
- Kalite Kontrolüne yönelik ilkeler bulunmaktadır.

Üçüncü grup ISSAI ise Temel Denetim İlkelerini ele almaktadır. Bu bölümde yer alan ilkeler kamu sektörü denetiminin esaslarına değinmekte olup amaçları şu şekilde sıralanabilir:

- Denetim Kurumlarının gelişimlerini sürekli hale getirmek,
- Uluslararası iş birliğini sağlayarak ortak bir mesleki bilgi birikimini oluşturma yolunda gerekli tedbirlerin alınmasını sağlamaktır.

Dördüncü grupta Denetim Rehberleri incelenmektedir. Esası itibariyle bu bölüm yukarıda belirtilen temel ilke ve esasların gündelik denetim işlemlerine uyarlanmasını sağlamaya yönelik olduğu belirtilebilir.

ISSAI standartlarının yanı sıra yukarıda da belirtildiği üzere teşkilatın bir diğer çalışması da INTOSAI GOV adı verilen INTOSAI İyi Yönetim Rehberleridir. INTOSAI GOV içinde iç denetçileri de yakından ilgilendiren iç kontrol ve risk yönetimi fonksiyonlarına ilişkin birden fazla rehber bulunmaktadır (INTOSAI, 2016a). Bunlardan en iç denetçinin denetim faaliyetlerinde yararlanması da beklenebilecek olan INTOSAI GOV 9100 “Kamu sektörü için İç Kontrol Standartları Rehberi’dir. Anılan rehber COSO modelinin kamu sektörü için uyarlanması sonucu ortaya çıkarılmış ve üye ülke Sayıştaylarına iletilmiştir (Özeren, 2004, s. 1). Ayrıca INTOSAI’nın günümüzün en önemli fonksiyonlarından biri olan bilgi teknolojileri denetimlerine yönelik de farkındalığı artıcı çalışmaları söz konusu olup, bu amaç çerçevesinde bir bilgi teknolojileri çalışma grubu kurulmuştur (INTOSAI, 2016b).

İç kontrol standartları rehberi çalışmanın iç kontrol başlıklı kısmında da ele alınan temel iç kontrol kavramlarını ele almaktadır. Söz konusu rehberde:

- İç Kontrol Tanımı
- İç Kontrol Etkinliğinin Sınırları
- İç Kontrol Unsurları
    - Kontrol Ortamı

  - Risk Değerlendirmesi
  - Kontrol Faaliyetleri
  - Bilgi ve İletişim
  - İzleme
- Roller ve Sorumluluklar başlıkları ele alınmıştır.

Rehberin iç kontrol tanımında ise amaçlar belirtilmiş olup bunlardan bazıları kısaca, faaliyetleri etik, düzenli ve etkin biçimde gerçekleştirmek ile hesap verilebilirliği sağlamak, yasal mevzuata uyumu sağlamak olarak belirtebilir (Akyel, 2010, s. 85). Bu rehber sadece yüksek denetim kurumları denetçileri için değil aynı zamanda gerek dış denetim gerek ise iç denetim faaliyetlerine devam etmekte olan tüm profesyoneller için yararlı bir kaynak teşkil etmektedir.

2.2.3 Amerikan Genel Kabul Görmüş Kamu Denetim Standartları (GAGAS)

Amerikan genel kabul görmüş Kamu denetimi standartları (GAGAS) Amerika Birleşik Devletleri Genel Muhasebe Ofisi (GAO-Government Accountability Office) ofis tarafından yayınlamıştır. GAO'nun Amerika Birleşik Devletler idari yapısı içinde resmi bir yeri bulunur. Daha açık ifade ile GAO ABD yönetiminin yasama fonksiyonu içinde yer almakta olup Amerikan Kongresine dönemsel olarak rapor vermekle yükümlüdür (Uluslararası İç Denetçiler Enstitüsü, 2012). GAO'nun kuruluş yılı 1921 olup görev ve sorumlulukları da zaman içinde çeşitli değişikliklere uğramıştır. İlk kurulduğu yıllarda teşkilatın görevi daha sınırlı tutulmuş olup mali raporlama temelinde faaliyetler gerçekleşmiştir. Ancak zaman içinde gelişen ve farklılaşan kamu ihtiyaçları nedeni ile bir raporlama teşkilatından ziyade danışma organına dönüşmüştür. GAO güncel misyonunu resmi internet sitesinde aşağıdaki gibi açıklamaktadır (GAO, 2016) :

- GAO'nun misyonu Amerikan Kongresi'nin anayasal sorumluluklarını karşılamasında ve Amerikan halkının çıkarları doğrultusunda federal

hükümetin hesap verilebilirliğinin sağlanması ve bu yöndeki performansının artırılması konularında destek sağlamaktır.

Teşkilatın yapısı ele alındıktan sonra GAGAS standartları kısaca incelenecektir. Söz konusu standartlar en son 2011 yılında revizyona uğrayarak son halini almıştır. Aralık 2011 tarihinde yayınlanan Kamu Denetim Standartları (Government Auditing Standards) kitapçığı denetim sektöründeki Amerikan ya da diğer ülkeler bünyesinde profesyoneller için bir referans kaynağı olarak önem arz etmektedir. Bu benzeri kurumların standartlarına erişilebilirlik durumunu konunun bir başka boyutunu oluşturmaktadır. GAGAS ya da benzer bilgi setlerine ulaşabilmek iç denetçinin gerekli donanıma sahip olması gerekmekte olup örneğin GAGAS standartları internete erişime açık halde ilgililerin dikkatine sunulmaktadır (Coderre, 2009).

Söz konusu standartlar 7 ana bölümden oluşmaktadır (GAO, 2016). Bölümler ve kısa açıklamaları aşağıdaki ele alınmaktadır (Office, 2011, s. 14):

1.Bölüm Kamu Denetimi: Kuruluş ve Etik Prensipler

Birinci bölümde GAGAS çerçevesinde uygulanan denetimler hakkında, standartların ortaya çıkısı ve etik prensipler hakkında genel açıklamalar bulunmaktadır. Özellikle denetim, denetçi, denetim organizasyonu gibi kavramlar ayrıntılı şekilde açıklanmıştır. Ulusal ve Uluslararası çerçevede denetim kalitesinin artması ve küresel anlamda ortak bir altyapı oluşması anlamında söz konusu açıklamaların denetim profesyonelleri açısından önemi büyüktür. Bölümün devamında etik ilkeler ele alınmaktadır. Bu aşamada 5 temel ilke denetim sürecinin GAGAS kapsamında gerçekleşebilmesi için öne çıkmaktadır. Bunlar:

- Kamu yararı
- Doğruluk (Dürüstlük)
- Tarafsızlık
- Kamuya ait bilgi, kaynak ve pozisyonların uygun kullanımı
- Profesyonel davranışlar.

Yukarıda yer alan ilkelerden biri olan tarafsızlık iç denetim standartlarında da biri olmakla beraber gerek IIA gerek ise de GAGAS bünyesinde özellikle önyargılardan arınmış bir denetim yapmanın önemine atıflarda bulunulmuştur (Dittonhofer, 2010, s. 8). Çalışmanın temel unsurlarından biri olan bilgi güvenliği çerçevesinde, GAGAS'ın dördüncü etik prensibi olan kamuya ait bilgi, kaynak ve pozisyonların kullanımı önem arz etmektedir. Söz konusu bölümde kamunun bilgi alma hakkı ile bilginin uygun şekilde kullanılması arasındaki dengenin sağlanması konusu ele alınmıştır. Bununla beraber denetim kapsamında yer alan bilginin talep edilmesi ve yine denetim amacı doğrultusunda kullanılmasının gerekliliği vurgulanmıştır.

2.Bölüm Kullanım Standartları ve GAGAS Uygulaması

Bu bölümde denetim kurumlarının GAGAS çerçevesinde gerçekleştirebileceği denetim türleri ele alınmakta olup aşağıdaki şekilde sınıflandırılmıştır.

- Finansal Denetim
- İnceleme Denetimi
- Performans Denetimi

Ayrıca söz konusu bölümde yine denetim profesyonelleri açısında oldukça önemli sayılabilecek bir konu olan GAGAS'ın diğer denetim standartları ile ilişkisi de ele alınmıştır. Örneğin performans denetimlerinde, denetçilerin diğer profesyonel denetim standartları ile beraber GAGAS'ı da kullanabileceğini belirtmiştir. Bu denetim standartları yine GAGAS'ta açıklanmıştır:

- Uluslararası İç Denetim Enstitüsü tarafından oluşturulan İç Denetim Standartları
- Amerikan Değerleme Kurumunun Değerleme Prensipleri Rehberi
- Bilgi Sistemleri Denetim ve Kontrol Kurumu (ISACA) standartları.

3.Bölüm Genel Standartlar

Bu kısımda zihnen bağımsızlık, görünüşte bağımsızlık gibi GAGAS çerçevesinde denetim gerçekleştirecek denetçiler ve denetimin genel standartları ele alınmaktadır.

4. 5. 6. Bölümlerde yukarıda anılan genel standartlar, ilgili denetim özelinde ele alınarak, daha detaylı anlatımı yer almaktadır.

GAGAS'ın son bölümü diğer pek çok standart paketleri gibi raporlama usullerine ayrılmıştır. Raporlama denetim neticesini taşıma ve geçmiş denetimlerin bulgularını takip etmek açısında çok önemli bir aşama olup belirlenen standartlara tam uyum sağlanması raporun ve dolayısıyla denetim sürecinin sağlığı hakkında net bilgiler sağlanması yardımcı olabilmektedir.

2.2.4 A.B.D. Sertifikalı Kamu Muhasebecileri Enstitüsü Standartları (AICPA)

AICPA (The American Institute of Certified Public Accountants) dünyada 143 ülkede faaliyet gösteren, 418.000'den fazla üye sayısı ile küresel anlamda muhasebe alanında faaliyet gösteren en büyük organizasyondur. Enstitü 1887 yılından beri faaliyet göstermektedir. Üyeler endüstriyel, kamu, eğitim ve danışmanlık gibi çok alanda faaliyet göstermektedir. AICPA tarafından oluşturulan standartlar (SAS – Statements on Auditing Standards), Amerika Birleşik Devletleri'nde kar amacı gütmeyen organizasyonlar, kamu kurumları ve benzer pek çok kurumca benimsenmiştir (AICPA, 2016). Bu standart 3 temel grupta incelenmektedir (İSMMO, 2020)s.68). Bunlar;

Tablo 4. AICPA Standartları

1. Genel Standartlar	• Eğitim ve Deneyim Standardı • Bağımsızlık Standardı • Mesleki Özen ve Titizlik Standardı
2. Çalışma Alanı Standartları	• Planlama ve Gözetim Standardı • İç Kontrol Sisteminin İncelenmesi

	• Kanıt Toplama
3.Raporlama Standartları	• Genel Kabul Görmüş Muhasebe İlkelerinde Tutarlılık Standardı • Tam Açıklama Standardı • Görüş Bildirme Standardı

3'lü gruplandırmada bahsi geçen standartlar çalışmanın bu kısmında kısaca incelenmektedir.

1.Genel Standartlar

Genel Kabul Görmüş Denetim Standartlarının ilk kısmı Genel Standartlar olup, bu kısmın içinde denetçilerin kişisel özellikleri ön plana alınmıştır. Kişisel özellik derken, denetçinin davranışları, tecrübesi, mesleki eğitim seviyesi vb. özellikler gibi daha ziyade denetçinin şahsi özelliklerini içerir.

Çalışmanın yukarıda ele alınan bölümlerinde de görülebileceği üzere mesleki yeterlilik ve benzeri konularda farklı organizasyonlarca oluşturulmuş olan standartlar birbirleri ile örtüşmekte olup bu durum iç denetim faaliyetleri arasında koordinasyon sağlamaktadır. Örneğin SAS'ın 65 numaralı standardı iç denetçinin genel iç denetim faaliyeti hakkında yeterli bilgiye sahip olmasını şart koşarken benzer şekilde IIA'nın standartlarında ve GAGAS'ın ilgili standartlarında ilgili maddeler bulunmakta olup söz konusu yeterlilikleri sağlayan iç denetçilerden oluşan iç denetim birimleri arasında izlenen yol anlamında bir koordinasyon söz konusu olabilmektedir (Moeller, 2005, s. 231).

2.Çalışma Alanı Standartları

Genel standartlardan farklı olarak denetim süreci bağlamında daha özele inen standartlardır. Bir başka değişle denetçinin denetim faaliyetlerinde rehberlik eden standartlardır.

- *Planlama ve Gözetim*: Denetim faaliyetlerinde gerek zaman gerek ise insan gücü planlaması yapılması ve var ise yardımcı denetçilere nezaret edilmesi gerekir. Denetim başından sonuna kadar planlı bir şekilde yürütülmelidir. Aksi halde bir noktada başlayan aksama denetimin tüm sürecine tesir ederek, planlanan denetim bitiş tarihinin uzamasına sebep olabilir. Ayrıca denetçi denetim gerçekleştireceği sektör, kurum, organizasyon yapısı ve benzeri konularda detaylı bilgi sahibi olmalıdır. Bu bilgiler ışığında denetçi kendine bir denetim planı hazırlar ve bu doğrultuda denetim faaliyetine devam eder.

- *İç Kontrol Sisteminin İncelenmesi:* Denetim faaliyeti kapsamında denetlenecek kurumun muhasebe iç kontrol sisteminin etkin bir şekilde çalışıp çalışmadığı incelenmelidir. Bunun en temel sebebi denetçinin denetim faaliyetini gerçekleştirirken kurumun hazırladığı finansal tabloları esas alacak olmasıdır. Eğer kurumun iç kontrol sistemi etkin bir şekilde çalışıyorsa denetçi kurumdan aldığı finansal tablolara esas alarak çalışmasına devam eder ancak iç kontrol sistemi güvenilir bulunmaz ise bu durumda denetimin kapsamı hakkında bir revizyon yapılması ya da daha da derinleştirilmesi gibi çeşitli sonuçlar söz konusu olabilmektedir.

- *Kanıt Toplama:* Denetçi yürüttüğü denetim faaliyeti kapsamında hazırlayacağı rapora ve görüşe dayanak oluşturacak kanıtları toplamak durumundadır. Kanıtlar yeterli miktarda ve güvenilir olmak zorundadır. Kanıt miktarı denetlenen kurum ve denetimin konusuna bağlı olarak değişiklik gösterebilir. Örneğin iç kontrol sistemi etkin ve güvenilir şekilde çalışan bir kurumun denetimden elde edilen bir finansal tablo yeterli olurken, iç kontrol sistemi etkin ve güvenilir çalışmayan bir kurumun denetimi için sadece finansal tabloları yeterli

olmayabilir finansal tabloları doğrulayacak daha pek çok kanıta ihtiyaç vardır çünkü bu finansal tablonun oluşmasında temel alınan iç kontrol sistemine yeterli kadar güvenilememektedir.

3.Raporlama Standartları:

Raporlama standartları, denetim faaliyetinin sonucu olan denetim raporlarının, hazırlanışı ile ilgili temel prensipleri kapsar. Denetçiler raporlarını yazarlarken bu kurallara uymak zorundadırlar. Söz konusu raporun tüm ilgililere hitap edeceğinden başka bir değişle geniş bir kitleye hitap edeceğinden rapor standartlarının kesin ve özlü olması diğer standartlara nazaran daha önemlidir (Başpınar, 2005, s. 57).

- *Uyum*: Denetçi denetlemiş olduğu kurumun finansal tabloların genel kabul görmüş muhasebe standartlarına uygun olarak hazırlandığına ilişkin bir görüş bildirmek zorundadır. Bu sebeple denetçi denetim faaliyetini sürdürürken söz konusu ilke ve yasalara uyulup uyulmadığını inceler.

- *Tutarlılık (Devamlılık):* Denetlenen kurumun uygulamakta olduğu genel kabul görmüş muhasebe standartlarında geçmiş yıllara kıyasla bir değişiklik olup olmadığının belirlenerek, bu durumun belirtilmesi gerekir. Geçmiş dönemden güncel döneme değişiklik olmamalıdır. Eğer herhangi bir değişiklik var ise de bu finansal tablolarda dip notlar ile belirtilmelidir.

- *Tam Açıklama*: Finansal tablolarda yer alan bilgiler, geçerli, tarafsız ve güncel olmalıdır. Tablolar tam olarak gerçeği yansıtmalıdır. Denetçi denetim faaliyetini sürdürürken finansal tabloları bu açıdan incelemeli dip notlarını ve açıklamalarını da göz önünde bulundurarak kendilerinden beklenen tam açıklama standardını yerine getirip getirmediği konusunda nihai karara varmalıdır. Eğer bu konuda bir yetersizlik söz konusu ise bunu raporunda belirtmelidir.

- *Görüş Bildirme Standardı:* Denetçi çalışmasının sonunda bir karara varmalıdır ve bunu raporunda açıklamalıdır. Eğer bir karara ulaşılamadıysa bu durum da nedenleri ile beraber raporda açıklanmalıdır. Denetçi ulaştığı netice itibariyle rapor olumlu görüş, olumsuz görüş, şartlı görüş ve görüş bildirmekten kaçınmadır.

2.2.5 Bilgi Sistemleri Denetim ve Kontrol Kurumu (Information Systems Audit and Control Association- ISACA)

Bigi Sistemleri Denetim ve Kontrol Kurumu (ISACA) kâr amacı gütmeyen ve bağımsız bir organizasyondur. Kurumun kuruluşu 1969 yılı olup günümüzde 180 ülkede 100.000'den fazla üyeye sahiptir. İlk Kurum, bilgi teknolojileri liderlerinin bilgi ve teknolojiden sağladıkları faydayı artırmaları ve bunlara ilişkin riskleri yönetme konusunda destek sağlamakta olup, aynı şekilde bilgi güvenliği, güvence, risk yönetimi ve yönetişim konularında çalışan profesyoneller için rehber çerçeveler sağlamaktadır (ISACA, 2014). Bir diğer deyişle ISACA ortaya koymuş olduğu standartlar ile bilgi teknolojileri yönetimi, risk yönetimi ve kontrolleri ile denetimine ilişkin profesyonel gelişim, güvence ve eğitim konularına odaklanmaktadır (Stoel ve ark., 2012, s. 65). ISACA'nın dünya genelinde 200 derneği bulunmaktadır. Kurum Uluslararası İç Denetçiler Enstitüsü'ne benzer şekilde ancak İç Denetim değil bilgi sistemleri denetim ve kontrolü konusunda uluslararası geçerliliği olan çeşitli mesleki çerçeveler ve sertifikasyon hizmeti sunmaktadır. Söz konusu çerçeveler arasında Sertifikalı Bilgi Sistemleri Denetçisi (Certified Information Systems Auditor-CISA), Sertifikalı Bilgi Güvenliği Yöneticisi (Certified Information Security Manager-CISM), Sertifikalı Kurumsal BT Yönetişim Uzmanı (Certified in the Governance of Enterprise IT-CGEIT) and Sertifikalı Risk ve Bilgi Sistemleri Kontrol Uzmanı (Certified in Risk and Information Systems Control-CRISC) sertifikaları sayılabilir. Bununla beraber kurum, sürekli olarak güncellenmekte olan bir çerçeve olan Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri (Control Objectives for Information and related Technology, COBIT) çerçevesini geliştirmiştir ve ilk bilgi ve ilgili teknolojiler için kontrol hedefleri

raporunu 1995 yılında yayınlamıştır (Ayaz, 2011, s. 36). Burada dikkat edilmesi gereken bir unsur da daha ziyade BT temelli olan söz konusu çerçevenin SOx (Sarbanes-Oxley) kanunundan önce oluşturulmuş olduğu ve SOx'un ABD'de kanun olarak yürürlüğe girmesinden sonra pek çok şirket tarafından SOx'a paralel olarak kullanılmaya başlamasıdır (Moeller, 2010, s. 15). Söz konusu çerçeve tüm sektörler ve coğrafi bölgelerdeki kurumların bilgi ve teknolojilerini yönetmelerini ve yönetişimini sağlamalarına imkân sağlama hedefi gütmekte ve BT ve ilgili diğer teknolojilere yönelik olarak detaylı bir kontrol serisi sağlamaktadır (Havelka ve Merhout, 2013, s. 166). Çerçeve kurum bünyesinde genel olarak çevresel ağlar, kurum içi ağlar, sistemler, uygulamalar ve veri tabanlarına odaklanmaktadır (Ramamoorti ve Weidenmier, 2004, s. 374). Özellikle son dönemlerde organizasyonlar ve ilgili yöneticiler aşağıda belirtilen konular için eskiye oranla daha fazla emek ve zaman harcama eğiliminde olup söz konusu (Nicho, 2009, s. 26) başlıklar denetçiler ve hazırlayacakları denetim raporları ve denetim görüşleri içinde benzer şekilde değerlendirilebilir:

- Organizasyonlar ile ilgili verilecek kararların desteklenmesi, temel oluşturması açısından bilginin yüksek kalitede tutulabilmesi,
- Organizasyonun stratejik hedefleri doğrultusunda bilgi teknolojilerinin (BT) etkin kullanımı,
- Teknolojiyi verimli ve güvenilir kullanılması,
- BT ilişkili risklerin kabul edilebilir bir seviyede tutulması,
- BT hizmetlerinin ve ilgili teknolojinin optimal maliyette sürdürülmesinin sağlanması,
- Gelişim haline bulunan ilgili mevzuat, düzenleme ve diğer kaynaklara daya anlaşma ve politikalar çerçevesinde faaliyet sürdürmek.

Özellikle günümüzde başarılı kurumlar BT'nin de organizasyonun diğer temel parçaları gibi benimsenmesinin gerekliliğini anlamışlardır. Özellikle BT'nin daha bilinir hale gelmesi ve gelişen teknolojinin kurumları dijital çözümlere itmesi sonucu

pek çok kontrol çerçevesi söz konusu olmuştur. Söz konusu kontrol çerçeveleri arasında BS7779, CoCo, COSO, FISCAM, GAPP, ITCG, SAC, SSE-CMM, SysTRust ve COBIT örnek verilebilir (Nicho, 2009, s. 29). Bu sebeple COBIT çerçevesi organizasyonların yukarıda belirtilen başlıklar noktasındaki hedeflerine ulaşmada bir yol haritası sunmaktadır. Ayrıca farklı kurumlarda COBIT çerçevesi bileşenlerinin uygulamada çalışıp çalışamayacağı araştırılmış ve örneğin COBIT-5 yönetişim süreçlerinden risk optimizasyonunun ilgili kamu kuruluşunda uygulanabilir olduğu değerlendirilmiştir (Efe, 2016a, s. 17).

COBIT çerçevesi güncel hali ile COBIT-2019 modeli adı altında oluşturulmuştur. Bu çerçevede 6 temel ilkeden söz edilmektedir (ISACA, 2014). Bunlar:

1. Paydaş ihtiyaçlarının karşılanması
2. Kurumun uçtan uca kapsanması
3. Tek bir bütünleşik çerçevenin uygulanması
4. Bütüncül bir yaklaşımın sağlanması
5. Yönetişim ve yönetimin ayrılması

Bu ilkelerin uygulama açısından değerlendirilmesi ise aşağıdaki gibi belirtilebilir:

1. *Paydaş ihtiyaçlarının karşılanması:* Organizasyonlar bilindiği üzere paydaşların faydalarını maksimize etme amacı güderler. Bu bağlamda COBIT 5 çerçevesi BT kullanımı ile söz konusu amaca yönelik gerekli stratejilerin geliştirilmesi konusunda organizasyonlara bir yol haritası sunar. Tahmin edileceği üzere her organizasyonun içinde bulunduğu pazar ya da organizasyon yapısı gibi özellikler sebebi ile hedefleri farklılık gösterebilir. COBIT 5 bu aşamada organizasyonun üst seviye amaçlarını BT ilişkili amaçlara dönüştürüp bunları belirli süreç ve eylemlerle eşleştirir. Özellikle BT yönetişim uygulamalarında COBIT çerçevesinin kullanılması; kurumun, planlama ve organizasyon, uygulama, hizmet sunumu ve destekleme ile

izleme faktörleri anlamında etkin bir yönetişim imkanı sağlar (Ackerman ve ark., 2009, s. 6).

2. *Kurumun baştan uca kapsanması:* COBIT 5, sadece BT fonksiyonuna yönelik bir çerçeve değildir. Organizasyonun tüm fonksiyonlarını kapsar. Bilgi ve bilgi ile bağlantılı teknolojilere, organizasyonda yer alan diğer varlıklara davranıldığı şekilde davranılması gereken varlıklar gibi bakar. Çerçevenin kapsadığı alan kurumun kullanmakta olduğu BT teknolojisi de dahil olmak üzere tüm kurumdur (Hüner, 2014, s. 77). Bir başka deyişle COBIT, sistem teorisinde de açıklanan ve sistemin bütünü oluşturan parçaların birbirleri ile olan ilişkilerinin dikkate alınarak bütüncül bir süreç içinde değerlendirilmesi gereken bir yaklaşımdır (Efe, 2016b, s. 67).

3. *Tek bir bütünleşik çerçevenin uygulanması:* BT ile ilişkili diğer standart ve çerçeveler ile üst seviyede uyuşur, bu anlamda kapsayıcı bir çerçeve sunmaktadır. Bu çerçevede tüm COBIT standartların içermekte olan çeşitli iç denetim yazılımları da iç denetim mesleğinde kullanılmaktadır. Söz konusu yazılımlara sadece COBIT değil diğer uluslararası kabul gören COSO, Sarbanes-Oxley ve benzeri gibi çerçeveler de entegre edilebilmektedir (Tanç, 2009, s. 208).

4. *Bütüncül bir yaklaşım sağlanması:* COBIT'in bu ilkesinde gerçekleştirici kavramı ele alınmaktadır. COBIT çerçevesinde gerçekleştiriciler; organizasyonun amaçlarına ulaşmasına yardımcı olacak herhangi bir unsurdur. Yapılan bir araştırmada denetçiler ve üst yöneticiler için, COBIT çerçevesinin COSO ve BT anlamında yeterli bir güvence sağlamakta olduğu ortaya çıkarılmıştır (Tuttle ve Vandervelde, 2007, s. 251). Ayrıca COBIT sadece COSO ile etkileşim halinde değildir. Örneğin ABD'de hizmet veren bir diğer BT ile ilgili kuruluşu olan Bilgi Teknolojileri Yönetişim Enstitüsü (ITGI); işlem ve kontrol düzeylerinde kuruma BT güvence rehberliği sunan ve COBİT ile ilişkilendirilmiş bir çerçeve geliştirmiştir (Héroux ve Fortin, 2013, s. 190).

Bu bağlamda COBIT çerçevesi organizasyona BT ile ilgili kapsamlı bir yönetim ve yönetişim sisteminin uygulanması için 7 gerçekleştirici unsur tanımlar. Bu gerçekleştiriciler:

- İlkeler, politikalar ve çerçeveler
- Süreçler
- Organizasyon yapıları
- Kültür, etik ve davranış
- Bilgi
- Hizmetler, altyapı ve uygulamalar
- İnsanlar, beceriler ve yeterlikler

Yukarıda verilen 7 geliştiricide de görüldüğü üzere uygulama kapsamı çerçevesinde tüm detaylı unsurlar ele alınmıştır. Bu bağlamda bütüncül yaklaşımın kurumun stratejik hedefleri ile IT hedefleri arasında sağlıklı bir ilişkin kurulabilmesi ve söz konusu ilişkinin düzeyinin ölçümü noktasında gerek icrai faaliyetler gerek ise de BT faaliyetlerinin sorumluluklarını yerine getirme derecelerinin ölçümlenmesi mümkün olmaktadır (Demircioğlu, 2009, s. 74).

COBIT yukarıda da belirtildiği üzere bilgi teknolojileri kontrolleri konusunda kapsamlı ve detaylı bir çerçeve sunmaktadır. Günümüzde gelişen teknolojinin yardımı ile küresel anlamda bilgiye ulaşım kolaylaşmış ancak bilginin korunması da bir o kadar önemli hale gelmiştir. Günümüzde, kimilerine göre BT güvenliği, kontrolleri ve denetimleri teknolojinin kendi inovasyonunun ve uygulamalarının gerisinde kalmıştır (Moorthy, 2011, s. 3536). COBIT çerçevesinin söz konusu BT uygulama, kontrol ve denetim alanlarında geliştirmiş olduğu standartları günümüzde daha da önemli hale gelmektedir. Bu bağlamda COBIT çerçevesinin gücü kendi iş odaklı çerçevesinde ve pragmatik araçları da içeren detaylı kontrol aşamalarında olup, COBIT uygulaması ile kurum neden kurum içi bilginin korunması gerektiği sorusuna cevap alabilmektedir (Frisken, 2015, s. 5).

2.3 ULUSAL MEVZUAT

Ulusal mevzuat başlıklı bölümde iç denetim başta olmak üzere denetim süreçlerinin ülkemizdeki yasal altyapısını belirleyen temel mevzuat incelenecektir.

2.3.1 5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu

Günümüzde kabul göre modern yönetim anlayışları, katılımcılığı ve hesap verilebilirliği ön plana çıkararak paydaş beklentilerini ön plana çıkaran yaklaşımlarını ön plana çıkarmakta ve söz konusu yaklaşım sadece özel sektörde de değil aynı zamanda kamu sektöründe de ağırlığını hissettirmektedir (Güner, 2009, s. 212). Özel sektör başta olmak üzere yaygınlığı artan iç denetim faaliyeti kamu sektöründe de ele alınmaya başlamış ve özellikle Avrupa Birliğinin aday ülkeler için önem verdiği hesap verilebilirlik çerçevesinde yasal düzenleme ihtiyacı ortaya çıkmış ve bu çerçevede 5018 sayılı kanun gündeme gelmiştir (Şahin, 2008, s. 290). Yürürlüğe giriş şekli ile kanun AB müktesebatı ile uyumlu durumda olup, müktesebatın 32 numaralı başlığı olan Finansal Kontrol sistemi ve korunması alt başlıklarından oluşmaktadır (Pehlivanlı, 2008, s. 37). Kanunun amacı kamu kaynaklarının kullanımı ve harcama sürecinde saydamlık, hesap verilebilirlik gibi ilkelerin sağlanmasıdır (Kılıç ve Aktuna, 2015, s. 103).

5018 sayılı Kanun 10.12.2003 tarihinde Türkiye Büyük Millet Meclisinde kabul edilerek, 24.12.2003 tarih ve 25326 sayılı resmi gazete yayımlanmış ve kamu sektörü denetimi alanında reform olarak nitelendirilebilecek bir döneme geçilmiştir (Gönenç, 2011, s. 1). Ayrıca kanun 01.01.20105 tarihinden itibaren geçerli olmakla beraber 81/c maddesi kapsamında 1050 sayılı Muhasebe-i Umumiye Kanunu'nu da yürürlükten kaldırmaktadır. Bu aşamada belirtilmesi gerekir ki 5018 sayılı kanun 2003 yılında Resmi Gazete yayınlanmakla beraber 2006 yılı başında yürürlüğe girebilmiştir (Güler, 2010, s. 152). Ayrıca 2007-2013 dönemini kapsayan Dokuzuncu Beş Yıllık Kalkınma Planı'nda, kamusal hizmet sunumunda, hesap verilebilirlik ilkesinin esas olduğu belirtilmiş ve kamu harcamalarında etkinliği, şeffaflığı ve hesap verilebilirliği artırmayı hedefleyen 5018 sayılı Kanunun tüm kapsamı ile hayata geçirileceği ifade edilmiştir (Kaplan, 2009, s. 97).

Çalışmanın bu kısmında kanunun kapsam yönünden getirdiği yenilikler ile kanunda iç kontrol ve iç denetime ilişkin bölümler incelenmektedir.

Yapılan bu düzenlemelerle daha önceden 5018 Sayılı kanundan önce yüğrükte olan 1050 sayılı Muhasebe-i Umumiye Kanununa tabi olmayan RTÜK, TRT, TÜBİTAK, Türk Dil Kurumu, TSE, Milli Prodüktivite Merkezi, MTA, Toplu Konut İdaresi Başkanlığı, Milli Piyango İdaresi Genel Müdürlüğü, SPK, Kamu İhale Kurumu, BDDK, Rekabet Kurumu gibi kurum ve kuruluşlar mali yönetim ve denetim bakımından 5018 sayılı Kanun hükümlerine tabi olmuşlardır.

Ayrıca yürürlükten kalkan 1050 sayılı Genel Muhasebe Kanunu'nu kapsamında hazırlanan genel ve katma bütçesi uygulamasından vazgeçilmiş ve bütçeler uluslararası standartlar çerçevesinde yeniden ele alınmış ve kategorize edilmiştir (Özkan, 2008, s. 49). Özetle bu kanun ile kamu harcamamalarının yapılması aşamasına gerekli sorumluluk ve denetim alanlarında önemli değişiklikler meydana gelmiştir . 5018 sayılı Kanun genel yönetim çerçevesindeki kamu kurumlarında iç denetim birimlerinin kurulmasını gerektirmektedir (Gökoğlan, 2010, s. 38). Denetim alanındaki en dikkat çeken yeniliklerden biri de doğal olarak iç denetim kavramının kamu idarelerine entegre edilmesi konusu olmuştur. Bu çerçevede entegre edilen iç denetim fonksiyonu, bir birime değil ancak üst yöneticiye bağlı şahıslara diğer bir deyişle iç denetçilere verilmiştir .

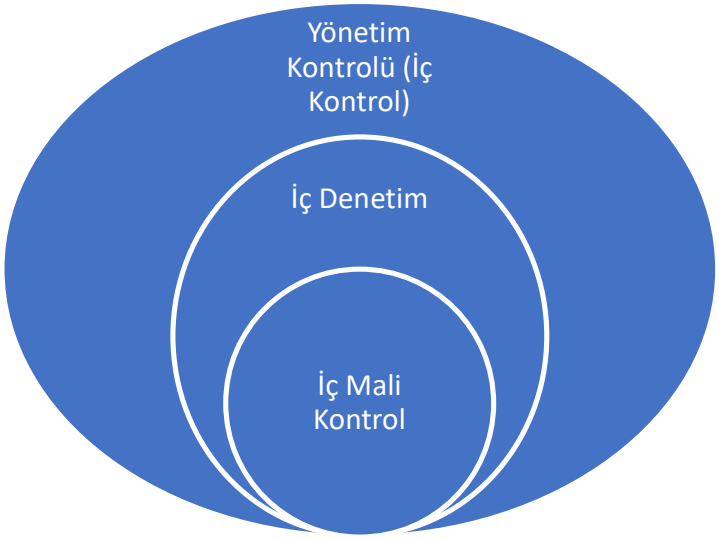
İç denetime Kanun'da 55.- 68. maddeler arasında atıfta bulunulmaktadır. Söz konusu maddelerde iç denetim ve iç kontrole ilişkin tanımlar ve açıklamalar yapılmıştır.

İlgili maddede iç kontrol kavramının tanımı yapılmış ve iç denetiminde bu tanım içinde idare tarafından oluşturulan organizasyon, yöntem ve süreçle beraber yer aldığı belirtilmiştir. İzleyen kısımda ise iç denetime ilişkin standartların belirlenmesinde yetkili kurum olarak İç Denetim Koordinasyon Kurulu'nun sorumlu olduğu açıklanmıştır.

Md.57 ise kontrol yapısı ve işleyişi başlığı altında kamu idarelerinin mali yönetim ve kontrol sistemlerinin içeriği ve bileşenleri açıklanmıştır. İç denetimin de harcama

birimleri, muhasebe ve mali hizmetler ile ön mali kontrol ile kamu idarelerinin mali yönetim ve kontrol sistemlerinin bir parçası olduğu belirtirmiştir. Ayrıca ilgili idarelerin ve diğer üst yöneticiler tarafından görev yetki ve sorumluluklar ele alınarak yeterli ve etkili bir kontrol sisteminin oluşturulmasının gerekliliği ele alınmıştır.

Anılan Kanunun 63.maddesinde doğrudan iç denetimin yapmıştır. Madde 63'te verilen tanıma ilişkin olarak, iç denetimin tanımından ziyade ilgili maddede sadece iç denetimin görevlerinin sayılmakta olduğu yönünde eleştiriler söz konusu olmuştur (Baykara, 2013, s. 99). Eleştiriler dikkate alınmakla beraber ilgili madde ele alındığında; tanımda, özellikle Uluslararası İç Denetçiler Enstitüsü tarafında oluşturan iç denetim tanımının temel alındığı görülmektedir. Tanımdan da anlaşılacağı üzere iç denetim, bağımsız ve nesnel güvence sağlama ve danışmanlık faaliyetidir. Bu faaliyet ister kamu idaresi olsun ister özel sektör kuruluşu olsun organizasyonun çalışmalarına değer katmayı hedefler. Bir organizasyonun çalışmalarına değer katmak için ise iç denetim organizasyonun kaynaklarının ekonomiklik, etkililik ve verimlilik esaslarına göre yönetilip yönetilmediğini değerlendirir. Yine aynı maddede iç denetim fonksiyonunun sadece iç denetçiler tarafından gerçekleştirilebileceği ve kamu idarelerinde kurulacak iç denetim birimlerinin organizasyon şemasındaki yeri ve hacmi ve alınması gereken uygun görüşe yer verilmiştir. 5018 sayılı kanunun kamu mali denetiminde yeni yaklaşım bir Şekil-6 yardımı ile de ele alınabilir (Gönülaçar, 2008, s. 2) :



Şekil 6: Mali Denetim

Şekilde de görüldüğü üzere 5018 sayılı kanun kapsamında planlanan yeni yaklaşımda iç denetim kurumun iç mali kontrol sistemini kapsayacak şekilde belirlenmiş olup yönetim iç kontrol sistemi bu iki unsuru kapsamaktadır.

Madde 64'te ise yıllık iç denetim programının hazırlanma ve onay aşamaları ile iç denetçilerin görevleri ele alınmıştır. Bu kapsamda kamu idarelerinde görevli iç denetçilerin görevleri açık ve net bir şekilde kanunda açıklanmıştır. Bununla beraber kanunun aynı maddesinde iç denetçinin yukarıda belirtilen görevlerini ne şekilde yerine getireceği, bağımsızlığı, faaliyetlerinin raporlanması ve iletimine ilişkin açıklayıcı bilgiler yer almaktadır. İç denetçiler, görevlerinde bağımsızdırlar. Bu çerçevede ve iç denetçilere asli görevleri dışında hiçbir görev verilememektedir. Rapor sunma noktasında ise iç denetçiler, raporlarını doğrudan üst yöneticiye sunarlar. İç denetim raporları en geç iki ay içinde İç Denetim Koordinasyon Kuruluna gönderilir.

Görüldüğü üzere md 64. sonuç olarak iç denetçilerin görevlerini yedi başlık altında toplamış olup, görev bağımsızlığı ve hazırlanan raporların üst yöneticiye sunumu ve ardından İç Denetim Koordinasyon Kurumu ile olan ilişki belirlenmiştir.

İzleyen madde kamu idarelerinde iç denetçi olarak atanacak kişilerin taşıması gereken şartlar, sertifikasyon süreçleri ve ilgili yasal süreçler ele alınmıştır.

Kamu idarelerine iç denetçi olarak atanacaklara ilişkin şartlar net bir şekilde belirtilmiştir. Kanunun 65.maddesi iç denetçi olarak atanacakların niteliklerini ve atanma sürecini detaylı bir şekilde açıklamaktadır. Unutulmamalıdır ki bu nitelikler ve süreç kamu kurumlarına ilişkin yapılacak iç denetçi atamalarını kapsamaktadır. Özel sektör kuruluşları kendi talep ettikleri nitelikleri ve atama süreçlerini kendi kurumsal yapılarına göre belirleyebilirler. Ayrıca anılan maddeye dayanılarak, İç Denetçilerin Çalışma Usul ve Esasları Hakkında Yönetmelik İDKK tarafından hazırlanmış olup Maliye Bakanlığı'nın teklifi üzerine Bakanlar Kurulunca çıkarılmış olup, Resmi Gazete'nin 12.07.2006 tarih ve 26226 sayılı nüshasında yayımlanmıştır (Soylu, 2010, s. 149). Anılan yönetmelikle kapsamında iç denetçilerin; kamu

idareleri temelinde personel sayıları, taşımaları gereken nitelikleri, atanmaları, çalışma usul ve esasları, sertifikasyon süreçleri ve diğer ilgili hususlar düzenlenmiştir (Soylu, 2010, s. 149).

Kanunda son olarak 66. ve 67. maddelerde İç Denetim Koordinasyon Kurulu hakkında bilgi verilmiş olup. Söz konusu kurulun üye sayısı, üyelerin kim tarafından ve hangi kurumlardan atanacağı, ne kadar süreyle görev yapacakları gibi iç işleyiş ile ilgili konulara açıklık getirilmektedir. Kanunun 68.maddesinde ise hukukilik denetimine ilişkin esaslar belirtilmiştir (Kuluçlu, 2008, s. 19). Bu madde ile beraber kanunun iç denetim ve diğer denetimlere olan yaklaşımının ele alınması tamamlanmıştır.

Yukarıda da belirtildiği üzere özel sektörde ülkemizin gündemine 1994 yılından itibaren girmeye başlayan iç denetim kavramı, kamu sektöründe ise anılan kanun ile beraber ülkemiz gündemine girmeye başlamıştır (Okur, 2010, s. 577). İç denetim mesleğine ilişkin gelişmelerden en önemlilerinden biri olan 5018 sayılı kanunun yürürlüğe girmesi süreci neticesinde yapılan çalışmalarda söz konusu gelişmenin ülkemizdeki iç denetçi sayısını artırdığı sonucuna varılmıştır (TİDE, 2010, s. 92). Anılan kanunun yürürlüğe girmesi ile ortaya çıkan bir başka değişim de yönetim sorumluluğuna ilişkindir. Buna göre kamu kaynağının etkili, ekonomik ve verimli kullanılması noktasında sorumlu olan ve hesabını verecek olanlar, ilgili kurumların harcama yetkilisi konumunda olan kişiler olacaklardır (Gönülaçar, 2012, s. 11).

Kanunun iç denetim ile kısımları açıklandıktan sonra son olarak incelenecek konu dış denetim kavramıdır. Kanunda dış denetimin tanımı verilmiş olup, bu fonksiyonun Sayıştay tarafından yerine getirileceği belirtilmiştir (Tufan, 2012, s. 10). Buna göre genel bir tabirle Sayıştay denetiminin kamu idarelerinin finansal faaliyet, karar ve işlemlerinin; kanunlara uyumluluğunun incelenmesi ve elde edilen raporun TBMM'ye sunulması sürecidir (Parlak, 2014, s. 8).

Ayrıca dış denetim; kamu idaresi hesapları ve bunlara ilişkin belgeler esas alınarak, malî tabloların güvenilirliği ve doğruluğuna ilişkin malî denetimi ile kamu idarelerinin gelir, gider ve mallarına ilişkin malî işlemlerinin kanunlara ve diğer hukuki

düzenlemelere uygun olup olmadığının tespiti, gerçekleştirilmesi ile kamu kaynaklarının etkili, ekonomik ve verimli olarak kullanılıp kullanılmadığının belirlenmesi, faaliyet sonuçlarının ölçülmesi ve performans bakımından değerlendirilmesi yoluyla gerçekleşir.

2.3.2 Sayıştay Kanunu

6085 sayılı Sayıştay Kanunu Türkiye Büyük Millet Meclisinde 03.12.2010 tarihinde kabul edilerek 27790 sayı ve 19.12.2010 tarihli resmî gazete yayımlanmıştır. Kamu harcamaları devletin ekonomik hayatın bir parçası olması nedeni ile küresel bağlamda çoğu ülkede söz konusu harcamaların çeşitli kriterlere uygun yapılmasını sağlamak amacıyla Sayıştaylar kurulmuştur.

Sayıştay denetimi kavramsal olarak, kamu idarelerinin ilgili ülkenin parlamentosu adına bağımsız denetim elemanlarınca denetlenmesi ve ilgili finansal tabloların doğruluğunun ve uygunluğunun araştırılması ile yönetimin verimliliği, etkinliği ve ekonomikliği hakkında görüş bildirmesidir (Önder, 2012, s. 199). Bu çerçevede kamu harcamaları başlığı altında kamu bünyesinde faaliyet gösteren işletmelerin, fonların ve benzeri kuruluşların işlem ve faaliyetleri Sayıştayların denetim evrenleri içinde görülmektedir.

Çalışmada bir önceki başlıkta incelenen 5018 sayılı kanun ve Sayıştay Kanunu ile kamu harcamalarının kontrol ve denetimine ilişkin kapsamın genişletilme çabalarıyla yeni bir sistem oluşturulmaya çalışılmaktadır (Önder, 2012, s. 199).

2.3.3 6102 Sayılı Türk Ticaret Kanunu

Türk Ticaret Kanunu 13.01.2011 tarihinde Türkiye Büyük Millet Meclisinde kabul edilerek 27846 sayı ve 14.02.2011 tarihli Resmî Gazete yayımlanmıştır. Söz konusu kanunun iç denetimin çerçevesinde incelenmesinin başlıca nedenlerinden biri gerek iç denetim gerek ise dış denetim çerçevesinde incelenen finansal tablolar ve diğer finansal işlemlerin adı geçen kanun çerçevesinde yapılan işlemlere ilişkin oluşturulduğu belirtilebilir. İç denetim açısından ele alındığında ise TTK ile iç denetim, finans sektörünün yanı sıra diğer sermaye şirketleri açısından da ihtiyaçtan

doğan bir zorunluluk haline gelmiş bulunmaktadır ve söz konusu açıklamalar kanunun 366. ve 375. maddelerinde yer almaktadır (Yereli, 2013, s. 42).

Kanunun 88. Maddesinde ise Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumunun yetkisi başlığı altında oluşturulacak finansal tabloların uyması gereken özellikler açıklanmıştır (Bezirci, 2010, s. 587). Dolayısıyla söz konusu uygulama gelişmiş ülkelerde olduğu ülkemizde de artık vergi amaçlı muhasebeden ziyade bilgi amaçlı muhasebenin hedeflendiğinin bir göstergesi olarak değerlendirilebilir (Yanık, 2010, s. 95). Kanunun 397. maddesinde belirtildiği üzere denetime tabi şirketlerin finansal tablolarının denetimine ilişkin olarak, görevli denetçinin temel alacağı standartlar Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumunca hazırlanan standartlar olmalıdır. Özellikle çalışmanın geçmiş bölümlerinde ele alınan bilgilerin yeterliliği ve tutarlılığı çerçevesinde söz konusu kanun maddesi ortaya bir standart ve gereklilik koymuştur.

3 BÖLÜM
BİLGİ GÜVENLİĞİ VE İÇ DENETİM

Çalışmanın önceki bölümlerinde de ele alındığı üzere iç denetim fonksiyonu; organizasyonun, çeşitli açılardan denetiminden sorumlu bir fonksiyondur. Küresel mesleki yaklaşımlarda bilgi teknolojilerinin inkâr edilemez yükselişi klasik ve geleneksel prosedürlerin tekrar gözden geçirilmesine neden olmaktadır. Örneğin IIA, artık iç denetçilerin bilgi teknolojilerinin (BT) kurumlarda nasıl uygulandığı ve uygulanması gerektiği ile önem arz eden BT riskleri, kontrolleri ve BT temelli denetim tekniklerini konusunda yeterli bilgisi olmasını şart koşmaktadır (Weidenmier ve Ramamoorti, 2006, s. 206). IIA'nın uluslararası kabul gören İç Denetim Sertifikası'nın (CIA - Certified Internal Auditor) 3 aşamalı olarak gerçekleştirilen sınavında en kapsamlı olan 3. aşamasında BT ve BT güvenliği konularına oldukça ağırlık verilmektedir. İşte bu noktada günümüz şartlarının gerektirdiği en önemli alanlardan biri de Bilgi Güvenliği Yönetim Sistemleri (BGYS) alanıdır. Hem bilgi sistemleri (information systems) hem de iç denetim fonksiyonları bilgi güvenliği kavramı ile iç içe durumda bulunmaktadır (Steinbart ve ark., 2012, s. 229). Covid-19 küresel pandemisinde salgının yayılımını yavaşlatmak için hükümetler insanları evlerinden çalışmaya teşvik etti ve organizasyonları çalışanları için uzaktan çalışma imkânı sunmasıyla, çalışanlar bilgi güvenliği alanında pek çok tehdide maruz kaldılar (Kotak ve ark., 2023, s. 2). Teknolojinin hızlı gelişimi ve yaşanan beklenmedik küresel salgın ve onun getirdiği uzaktan çalışma ortamı bilgi güvenliğinin önemini bir kez daha gösterdi.

3.1 BİLGİ GÜVENLİĞİ VE İLGİLİ KAVRAMLAR

Ülkemizde ve dünyada gittikçe daha önemli bir hale gelmekte olan bilgi güvenliği konusu çalışmanın bu aşamasında incelenecek ve iç denetim fonksiyonu ile olan ilişkisi ve bu ilişki çerçevesinde iç denetçinin görev ve sorumlulukları ele alınmaktadır.

3.1.1 Bilgi ve Bilgi Güvenliği

Türk Dil Kurumu güncel sözlüğüne göre bilgi, gerçek ve ilkeler bütünü, malumat, vukuf gibi farklı kavramlar ile tanımlanmaktadır (TDK, 2017). Çalışmada ele alınmakta olan BGYS konusu ile ilişkili bilgi ise yukarıdaki tanımlar ışığında organizasyonun stratejik hedefleri doğrultusunda gerçekleştirdiği iş ve işlemler çerçevesinde elde ettiği verilerin tümü olarak tanımlanabilir. Stratejik hedefler doğrultusunda elde edilen bilgilere ilişkin bazı riskler de söz konusu olabilir. Örneğin söz konusu bilgilere ilişkin olarak, tarafsız olmayan metotlar ile bilgi toplaması ya da gerçek durumu yansıtmayan bilgilerin varlığı gibi bilgi kalitesini düşürebilecek türden durumlara bilgi riski denilmektedir (Tanç, 2009, s. 73). Kurum bu riskleri karşılayabilecek gerekli kontrol ve denetim sistemlerini hayata geçirmelidir. Organizasyon elde edilen bilgileri, tüm süreçlerinin etkililiğini ve gelişimini sağlamak hedefi ile birleştirir (Köklü, 1996, s. 262). Ancak dikkat edilmelidir ki genel anlamda bilgi ele alınırken organizasyonlarda ve özellikle BGYS'de ele alınan bilgi kavramı daha teknik düzeyde incelenebilmektedir. Bu çerçevede BGYS incelemesinde bilgi derken daha ziyade organizasyon özelinde bir tanım oluşturulabilir. Yukarıda bilgiye ilişkin TDK Türkçe sözlüğünde verilen açıklamaya ek olarak bilgi aynı zamanda organizasyon içinde diğer varlıklar gibi önem taşıyan ve korunması gereken bir varlıktır. Bununla beraber bilgi organizasyon içinde farklı türlere sahiptir, bunlar:

- Yazılı halde bulunan bilgi,
- Elektronik haldeki bilgi,
- Organizasyonel videolarda paylaşılan bilgi,
- Kurum içi çalışanlar arasında sözel olarak aktarılan bilgi,
- Organizasyon bünyesinde bulunanların özlük bilgileridir.

Yukarıda bilginin organizasyonun bir varlığı olduğu belirtilmiştir bu çerçevede varlık kavramının da bu aşamada ele alınması gerekebilir. Geniş bir tanım ile varlık; organizasyon için değeri bulunan her şeydir. Bilgi varlığı ise bilginin güvenliğini

etkileyen tüm varlıklardır. Bu çerçevede organizasyon bünyesinde yer alan varlıklar aşağıdaki gibi sıralanabilir (TSE, 2015a, s. 14):

- Finansal Değerler (Kasa, banka, alınan çekler hesapları vb.)
- Üretilen mal ve hizmetler
- Organizasyon çalışanları
- Organizasyon yazılımları (bilgisayarlarda kullanılan işletim sistemleri, var ise uygulamalar ve organizasyonun hedeflerine ulaşmasında kullanılan tüm yazılımlar)
- Donanımlar (yazılım varlıkları ile ilişkili tüm donanım parçaları, bilgisayarlar, sunucular vb.)
- Haberleşme aygıtları (tüm telefon, hatlar, kablolar ve modemler)
- Kurumun yazılı kültürüne ilişkin tüm dokümantasyon (toplantı tutanakları, sözleşmeler vb.)
- Kurumun piyasadaki algısı, imajı ve prestiji.

Bilginin bir kurumdaki önemini anlamak için bir diğer bakış açısında bilgi tayfı kavramıdır. Buna göre bilgi, verilerden oluşmaktadır. Toplanan bilginin bütünü ise bilgi birikimi kavramını meydana getirir. Veri (Data) kısaca; nesneler, olaylar kurumlar hakkındaki ilk ya da ham bilgidir. Nicel ya da nitel olabilir. Bilgi (Information) ise verinin işlenmesi ve anlamlandırılması sonucu elde edilir. Bilgi birikimi (Knowledge) ise bilgi tayfının en üst değerdeki unsurudur. Söz konusu bilgi tayfı izleyen Şekil 7'deki gibi özetlenebilir (Buchanan ve Gibb, 2007, s. 161):

Şekil 7: Bilgi Tayfı

Bilgi güvenliği kavramı ise yukarıda belirtilmiş olan varlık türlerinden biri olan bilgi varlığının herhangi bir yetki ya da izin alınmadan, erişilmesini, kullanılmasını, üzerinde değişiklik yapılmasını, gizli yönlerinin açığa çıkarılmasını, yok edilmesini ya da zarar verilmesini önlemek olarak tanımlanabilir. Bilgi güvenliği gerek bilginin temelini oluşturan veri kavramını, gerek ise de bilginin toplanması sonucu oluşan bilgi birikimi kavramlarını da kapsamaktadır. Tüm bu kavramlar bilginin oluşum aşamaları olarak değerlendirilebilir. Bilgi güvenliği kısaca gizlilik, bütünlük ve kullanılabilirlik (erişilebilirlik) olmak üzere üç ana bileşenden meydana gelmektedir (TSE, 2015a, s. 14):

- Gizlilik; bilginin yetkisiz kişilere kapalı olması durumudur,
- Bütünlük; programların, verilerin ve sistemlerin yetkisiz kişilerce değiştirilmesi ya da bozulmasına karşın korunması ya da korunmuş olması durumudur.
- Kullanılabilirlik; bilginin her ihtiyaç duyulduğunda erişilebilir ve kullanıma elverişli olması durumudur.

Verilen bu üç bileşenden herhangi biri zarar gördüğü takdirde güvenlik zafiyeti açığa çıkar. İşte bilgi güvenliği bu çerçevede kurum ya da organizasyondaki işlerin sürekliliğinin sağlanabilmesi, faaliyetlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelmesi beklenen faydanın maksimize edilmesi noktasında bilginin geniş çaplı tehditlerden korunmasını sağlar.

Bilgi kavramının incelenmesinin ardından diğer temel kavramlar da bilgi teknolojileri (BT) ve BT denetimi kavramlarıdır.

3.1.2 Bilgi Teknolojileri (BT)

Teknoloji kavramı; güncel Türkçe sözlükte, bir alanda kullanılan ara-gereçler ve bunlara ilişkin uygulamalar şeklinde tanımlanmıştır (TDK). Bilgi teknolojileri de bu çerçevede bilgi üzerine onun sağlanması, kullanılması, analiz edilmesi ve buna benzer tüm unsurların uygulanmasına yönelik araç ve süreçleri kapsayan bir uygulama bilgisi olarak tanımlanabilir. Özellikle günümüzde bu tür bilgi

teknolojilerine kurumun bünyesinde bulunan donanım, yazılım ve bilgi varlıklarına ilişkin diğer tüm ilgili teknolojiler örnek verilebilir. Bunların arasında veri tabanı sürücüleri, kurumun kullanmakta olduğu yazılımlar yer alabilmektedir.

IIA Standartları Belgesinde yer alan Terimler Sözlüğüne göre ise BT ve BT kontrolleri; uygulamalar, bilgiler, altyapı ve inşalar gibi bilgi teknolojileri altyapısında üzerinde sağladığı genel ve teknik kontroller yanında işin idaresi ve yönetişimini destekleyen kontroller olarak tanımlanmıştır (IIA, 2017, s. 24). BT bu çerçevede söz konusu yazılım ve donanım unsurlarının tasarlanması, geliştirilmesi, kullanımı, yönetimi ve incelenmesi faaliyetlerinin tümünü kapsamaktadır. BT'nin temel noktalarından biri de bilgi transferini konu edinmesidir. Tüm BT işlemlerinin temelinde bilginin alınıp verilmesi olarak özetlenebilir.

BT, günümüzde gerek işletmelerin ile gerek ise de ülkelerin birbirleri ile rekabetlerinde üstünlük belirleyen temel kriterlerden biri haline gelmiş bilgi teknolojileri endeksleri ile ülkeler arası sıralamalar oluşturulmuştur. Örneğin Birleşmiş Milletler bünyesinde özel bir ajans olarak yer alan ITU (Internatiaonl Telecomication Union) oluşturmuş olduğu ICT (bilgi ve iletişim teknolojileri) gelişmişlik sıralamasını yayımlamakta, ülkelerin ICT gelişmişlik düzeyleri bu sıralamadan izlenebilmektedir (ITU, 2018). BT, günümüzde en değerli kaynaklar olarak nitelenen petrol ve altının yerini almaya başlamakta ve ülkeler kalkınma stratejilerini BT stratejileri üzerine kurmaya yönelmektedir (Aydın, 2007, s. 296). Hatta eski soğuk savaş dönemlerinde ortaya çıkan silaha dayalı çeşitli üstünlük kurma çabaları yerine artık BT teknolojileri üzerinden ülkelerin çeşitli kurumlarına müdahale etme kapasitesi ön plana çıkmaya başlamaktadır. Bugün pek çok ülke bir diğer ülkenin kendi BT sistemlerine kötü niyetli müdahalede bulunduğu iddiasını ileri sürebilmektedir. Ayrıca BT alanındaki uygulamaların, gelişmekte olan ülkelerin ekonomik gelişmeye sağlayacağı katkının diğer uygulamaların yapacağı katkıdan çok daha fazla olacağı anlaşılmaktadır (Aydın, 2007, s. 311). Bilgi ve iletişim teknolojilerinin kullanımı ile yeni pazarlar girebilmeyi mümkün kılmak, rekabetçiliği artırmak, bilgiye ulaşımı sağlamak gibi katkılar örnek verilebilir (Atay ve ark., 2016, s. 1103). Bununla beraber bilgi ve iletişim sektörüne olan ilgi de sürekli artış

içindedir. Örneğin ülkemizde 2010-2014 yılları arasında istihdamın endüstriler ölçeğinde gelişim oranlarına bakıldığında bilgi ve iletişim sektörünün büyüme yüzdesi %77 oran ile gayrimenkul faaliyetleri sektörü ardından ikinci en fazla büyüyen sektör olmuştur (Esen ve Atay, 2017, s. 76). Görüldüğü üzere gerek küresel anlamda gerek ise de yurtiçi sektörel anlamda BT sürekli olarak gelişmekte ve öne çıkmaktadır.

BT, organizasyon bünyesinde iç denetim fonksiyonu içinde de ele alınabilir. İç denetim faaliyetleri anlamında da BT, önemli bir unsur olarak yer almaktadır. Gerek denetim uygulamalarında kullanılan denetim yazılımlar, bilgisayarlı denetim teknikleri gerek ise de denetim faaliyetlerinin evrenini oluşturan iş ve işlemlerde giderek artan BT ağırlığı, iç denetim faaliyetleri açısından BT'nin artık kaçınılmaz bir unsuru olduğu görülebilmektedir. İç denetçiler ana operasyonlarında, analitik incelemelerinde ya da testlerinde BT'den faydalanırlar (Salehi, 2011, s. 6178). İç denetçilere düşenin veri gelişmeler ışığında BT teknolojilerindeki gelişmeleri takip etmek ve denetim kalitesini artırabilecek olası BT tekniklerini denetim faaliyetlerine uyarlayabilmektir.

3.1.3 BT Denetimi

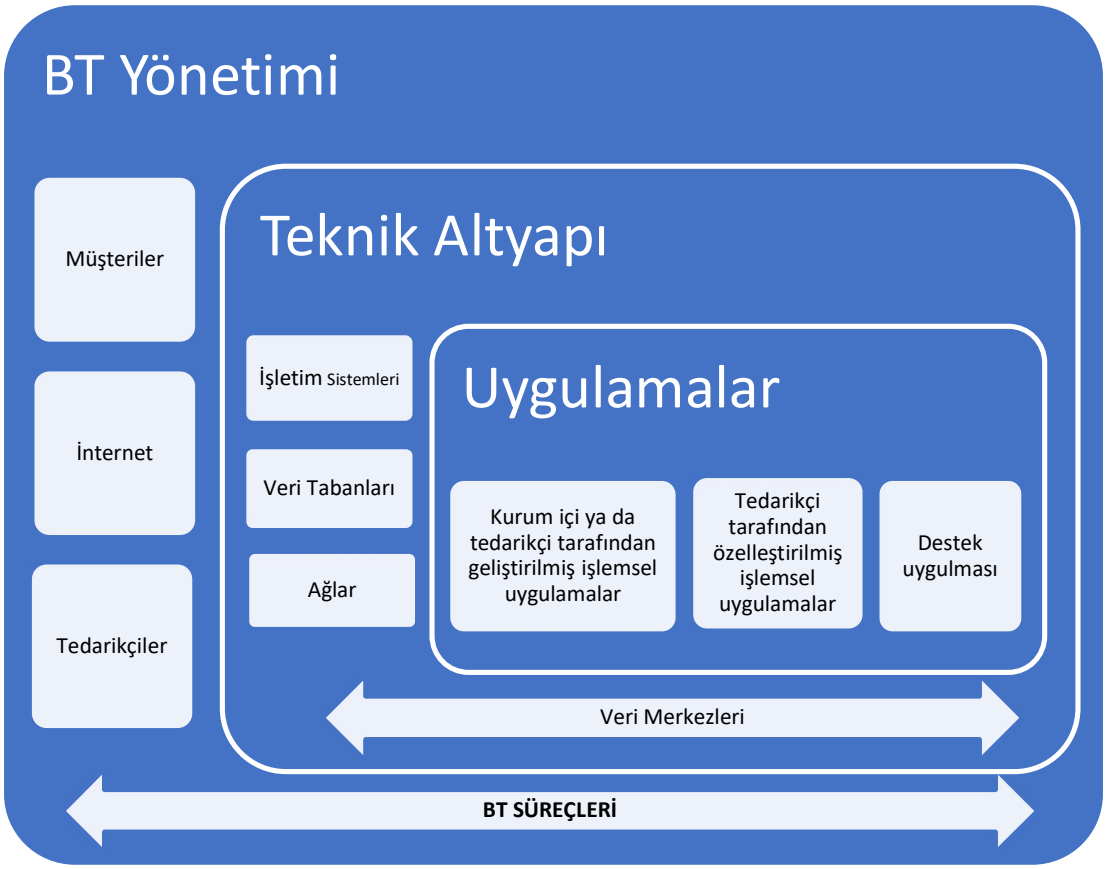
Gerek bugünün iş koşullarındaki teknolojik değişim, gerek denetim mesleğinde ortaya çıkan değişim ihtiyaçları, günümüzde farklı türde denetim faaliyetlerinin gerçekleştirilmesi noktasında bir anlamda gereklilik oluşturmaktadır. Özellikle internetin yaygınlaşması ile bilgiye kolay erişim, kurumların şeffaflığının önemli bir hale gelmesi, kamu çıkarları doğrultusunda oluşturula çeşitli standartlar ve bu standartlara uyum çerçevesinde geliştirilmesi gereken yasal mevzuat tüm bu değişimlere örnek verilebilir. 2019 yılında ortaya çıkan Covid-19 pandemisinde çalışanların evden çalışma koşullarına geçmesi ile organizasyonların bilgi teknolojilerine olan ihtiyacı bu süreçte kullanmakta oldukları bilgi varlıklarının korunması konusu daha da önemli hale gelmiştir (Humaidi ve Shahrom, 2023, s. 208). Hatta teknoloji artık öyle bir noktaya gelmiştir ki sanallaştırma ve bulut bilişim gibi kavramlar ortaya çıkmış ve bu kavramlar çerçevesinde ilgili kişi ya da kurumun sahibi olmadığı donanım, yazılım ya da ağlara gerek kişisel gerek ise kurumsal

bilgilerin emanet edilmesi gündeme gelmektedir (Ersoy, 2012, s. 4). Özellikle standart ve mevzuatta yapılacak değişikliklerde artık BT unsurlarının da dikkate alınması kaçınılmaz bir hal almaktadır. Bununla beraber söz konusu gelişmeler sadece özel sektör temelinde düşünülmemelidir. Günümüzde meydana gelen teknolojik gelişmelerden sadece özel sektör değil aynı zamanda kamu sektörü de etkilenmektedir. Bu çerçevede kamu sektöründe BT'de meydana gelen bu tür gelişmeler bir sorun olarak görülebilmekte geleneksel yönetim anlayışı unsurları bu tür gelişmelere karşı gereken reaksiyonu verememektedir (Öktem ve Aydın, 2005, s. 261). Dolayısıyla kamu sektöründe de bir dönüşüm ihtiyacı ortaya çıkmıştır. Geleneksel devlet modelinin gelişen teknoloji uygulamalarına yönelik olarak ihtiyacı karşılayamaz hale gelmesi sonucu, ileri teknoloji uygulamalarına dayanan ve e-devlet (elektronik devlet) modeli olarak isimlendirilen yeni bir yapı ortaya çıkmıştır. Ancak bu dönüşümün, sadece kamu kurumlarının internet sitelerini oluşturmak ve bazı hizmetleri buradan sağlamak yoluyla gerçekleşmesi beklenmemeli, bununla beraber ilgili tüm kamu görevlerinin düşünce, davranış, iş süreçlerinin yeni sisteme göre algısı, diğer paydaşlar ile paylaşım gibi kapsayıcı olması gerekmektedir (Öktem ve Aydın, 2005, s. 274). Tüm bu gelişmeler karşısında gerek özel gerek ise de kamu kurumların BT bileşenleri anlamında bazı sorularına cevap alma ihtiyaçları söz konusudur. Örneğin kurum, yazılım sistemlerinin kesintisiz olarak çalışma kabiliyetinin olup olmadığı, deprem ya da benzeri bir doğal afet neticesinde iş sürekliliğinin sağlanabilip sağlanamayacağı, kurum hedeflerine ulaşmada yardımcı olabilecek ihtiyaçlarını karşılayabilecek teknolojinin kullanılıp kullanılmadığı, BT sisteminin optimize edilip edilmediği, sistem kontrollerinin etkin şekilde işleyip işlemediği gibi sorulara cevap alma ihtiyacı duyabilmektedir. Tüm bunlarla beraber kurumların cevaplanmasını beklediği en temel sorulardan biri de bilgilerin güvenliğidir. Söz konusu güvenlik bilginin gerek fiziksel gerek ise yazılımsal güvenliğini kapsayabilmektedir.

BT denetimleri bu anlamda, bilgi sistemleri yönetimi süreçleri ile otomasyona dahil edilmiş ya da edilmemiş süreçleri, anılan süreçler arasındaki ara birimleri ve konuya ilişkin inceleme ve değerlendirmeyi kapsayan denetimler olarak tanımlanabilir (Aktolun, 2002, s. 13). BT denetimi bir başka deyişle bilgi varlıklarına atfedilen

risklerin belirlenmesi ve söz konusu risklere yönelik oluşturulacak aksiyonlara ilişkin gerekli kontrollerin oluşturulmasını içeren bir denetim türüdür. Bu çerçevede bilgi teknolojileri kullanımı söz konusu olan tüm kurumlar için mutlak bir gereklilik haline gelmektedir. Yapılan bazı çalışmalarda da iç denetim faaliyetinin BT denetimine ayırdığı zamanının giderek arttığı görülmektedir. Buna göre içerinde ABD ve İngiltere'nin de olduğu bazı ülkelerde 2003, 2006 ve 2009 yıllarını kapsayan bir araştırmada toplan iç denetim faaliyeti içinde BT denetimi için harcanan zaman oranının sırasıyla %7.97, %10.61 ve %13,40 olduğu görülmüştür (Abdolmohammadi ve Boss, 2010, s. 149). Burada görülen oranlar küçük gibi görünse de çalışmanın en on 2009 yılı verileni kapsadığı ve artış hızı ve süre dikkate alındığında BT denetimlerinin ileride iç denetim faaliyetinin belki de en büyük oranda zaman ayrılan unsuru olacağı tahmin edilebilmektedir.

BT denetiminin uygulama aşaması ele alındığında ise, öncelikle iç denetim açısından hangi IIA Standardı ile ilgili olduğu tanımlanabilir. Buna göre Standartların 2110.A2 başlıklı maddesinde iç denetim faaliyetinin, hangi kapsamda değerlendirmesi gerektiğinin altını çizmektedir (IIA, 2017, s. 15). Bu çerçevede BT denetimi gerek bütünleşik denetim içerisinde; sistem denetimi, performans denetimi, mali denetim ve uygunluk denetimlerinin içerisinde yer alarak, gerek ise de tekil denetim olarak güvenlik denetimi kapsamında müstakil olarak gerçekleştirilebilir (İDDK, 2014, s. 14). Bütünleşik denetimler için BT kontrol ortamının ilgili denetim faaliyeti çerçevesinde değerlendirilmesi öngörülmektedir. Müstakil BT denetiminde ise yapılan denetim faaliyeti yukarıda belirtilen denetim türlerine girdi sağlayabileceği gibi, sadece BT süreçlerinin denetimi noktasında kurumun risk ve kontrol ortamının değerlendirilmesi de söz konusu olabilir. Bir kurumun BT süreçleri bir şekil yardımı ile aşağıdaki gibi ele alınabilir:



Şekil 8: BT Süreçleri
Kaynak: (Coates ve ark., 2013, s. 9)

Şekil-8'de de görüldüğü üzere BT süreçleri; uygulamalar, teknik altyapı ve BT yönetimi olmak üzere üç ana başlıktan oluşmaktadır. BT yönetimi kısaca BT hizmet ve tesislerinin idarecileri, ilgili politika ve prosedür ve süreçler olarak tanımlanabilir (Coates ve ark., 2013, s. 10). Teknik altyapı ise işletim sistemleri, veri tabanları ve ağlardan oluşan ve uygulamaları kapsar şekilde ilgili katmanlardan oluşan bir kümedir. Son olarak uygulamalar ticari ya da hizmet işlemleri ile ilişkili belirli görevlerin yerine getirilmesini sağlayan elektronik programlar olup; işlemsel uygulamalara defteri kebir kayıtları ya da envanter kayıtları, destek uygulamalarına da eposta programları ya da elektronik belge görüntüleme yazılımları örnek verilebilir (Coates ve ark., 2013, s. 12).

BT denetiminin gerçekleştirilme aşamasında ise diğer denetim türlerinden farklı bir yol izlenmemektedir. Denetçi ilgili BT denetimini planlar, denetim konusu

kapsamındaki kontrolleri tanımlar, söz konusu kontrollerin işlemsel verimliliğini test eder, bir sonuca ulaşır ve bu sonuçları da test ederek süreci tamamlamaktadır (Coates ve ark., 2013, s. 17).

Bir diğer ifade ile BT denetim metodolojisi, kurumsal ve denetim hedeflerine uygun bir şekilde planlama, saha çalışması, raporlama ve izleme aşamalarından oluşmaktadır (İDDK, 2014, s. 24). Kurum hedefleri doğrultusunda belirlenen denetim hedefi çerçevesinde planlama aşamasında risk değerleme ve kapsam belirleme süreci gerçekleştirilir dolayısıyla söz konusu süreç denetim aşamasını kapsamaktadır. Söz konusu metodoloji, süreç ve aşamalar Şekil 9'da özetlenmektedir:

Şekil 9: BT Denetim Metodolojisi
Kaynak: (İDDK, 2014, s. 25)

Görüldüğü üzere BT denetimi diğer denetim türlerinden metodoloji olarak çok farklılık göstermemekle beraber kapsam anlamında teknoloji boyutu ağır basabilen bir denetim türüdür. Tüm bunlara ek olarak denetçiler, BT denetimine ilişkin gerekli dikkati ve yoğunluğu vermelidir ancak bu denetimde odaklanılan riskler eski tarihli kalmış ya da gelişen teknoloji neticesinde artık bir risk olmaktan çıkmış olabilir işte

denetçiler bu noktada BT denetimi gerçekleştirirken odaklandıkları BT risklerine dikkat etmeli tüm yoğunluklarını ve enerjilerini bu risklere ayırarak Kurumun bütüncül stratejik hedefleri doğrultusunda faaliyetlerini gerçekleştirme noktasında bir eksiklik ortaya çıkarmamalıdırlar (Hill, 2011, s. 57). BT denetimleri kurumlarda gerek ayrı bir denetim olarak gerek ise de genel denetimin içinde gerçekleştirilebilir (Jackson, 2012, s. 42). BT'nin kendine has bir uzmanlık gerektirmesi nedeni ile kurumlar belirli iç denetçilerini BT üzerine özel bir eğitim almalarını teşvik edebilir. BT denetimin geleceği ise literatürde ele alınan konulardan birisidir. Buna göre teknolojinin sürekli gelişimi, mobil cihazlar ve bulut teknolojileri gibi sürekli ve hızlı gelişen unsurları ile beraber, tahmin edilebilir ki BT denetimini gelecekte de çok önemli bir konumda olacaktır. BT denetçisine düşen ise yeni ortaya çıkan risklerin bir adım önünde olmak ve bu risklere karşılık gerekli önlemlerin alınmasını sağlamaktır (Ibrahim, 2014, s. 21).

3.2 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) ve İlgili Kavramlar

Çalışmanın izleyen kısmında ISO/IEC 27001 Bilgi Güvenliği Yönetimi Sistemi (BGYS) detaylı bir şekilde ele alınacak olup, öncelikler söz konusu sistemi meydana getiren ilgili organizasyonlar kısaca açıklanacak ardından da sistem bütünsel olarak incelenmektedir.

3.2.1 ISO/IEC Ortak Komitesi

ISO/IEC Ortak komitesi adından da anlaşılabileceği üzere iki farklı organizasyonun ortak bir amaç uğruna bir araya gelerek oluşturdukları bir yapıdır.

ISO (International Organization for Standartization – Uluslararası Standardizasyon Örgütü), 1946 yılında 25 ülkeden gelen katılımcıların Londra'da İnşaat Mühendisleri Enstitüsü'nde bir araya gelerek endüstriyel standartlar noktasında uluslararası koordinasyonun ve söz konusu endüstriyel standartların birleştirilmesi kararı

vermeleri kurulma sürecine girmiş olup tam olarak 23 Şubat 1947 tarihinde resmi olarak çalışmalarına başlamıştır. Verilen tarihten günümüze örgüt teknoloji ve sanayinin pek çok alanında 21607 adet standart yayımlamıştır (ISO, 2017b, s. 1). Örgütün bugün 16 ülke ve 779 teknik organdan üyeleri bulunmaktadır. Örgütün en temel felsefesi eski yunanca “isos” anlamına gelen eşitlik kavramıdır. Hangi ülkede olursa hangi dilde olursa olsun eşit standartların yerleştirilmesi hedeflenmektedir.

IEC (Uluslararası Elektroteknik Komisyonu), kar amacı gütmeyen yarı-resmi bir organizasyondur (IEC, 2017a, s. 1). IEC’nin bugün 171 ülkede faaliyet göstermekte olup, ilgili endüstrilerden 20.000 uzman, test ve araştırma laboratuvarını bünyesinde bulundurur ayrıca IEC, 9000 adet standardı kataloğunda oluşturmuş bulunmaktadır (IEC, 2017b, s. 5).

TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri standardı, diğer ISO/IEC 27000 ailesi standartları gibi organizasyonun bilgi varlıklarının güvende tutulması konusunda organizasyona yardım etmeyi hedeflemektedir (ISO, 2017a). 2700 standart ailesi ise “ISO/IEC Joint Tecnical Committee” tarafından oluşturulan 20 alt komiteden biri olan ISO/IEC JTC 1/SC 27 Bilgi Teknolojileri güvenliği alt komitesinin çalışmaları çerçevesinde oluşturulmuştur (IEC, 2014, s. 2). ISO/IEC ortak teknik komitesi birbirinden bağımsız iki adet organizasyon olan ISO yani Uluslararası Standardizasyon Örgütü (International Organisation for Standarts) ile IEC yani Uluslararası Elektroteknik Komisyonu’nun (International Electrotechnical Commission) bir araya gelerek oluşturdukları bir komitedir. Söz konusu komitede bir araya gelen uzmanlar, çalışma hayatı ve tüketici ihtiyaçları konusunda dünya çağında kabul gören standartlar geliştirmektedirler. Ayrıca anılan standartlar uluslararası uygulanabilirlik ve sürdürebilir kalkınma yönünde organizasyonlara destek vermektedir. Söz konusu ortak teknik komitenin vizyonu ve misyonu aşağıdaki gibi özetlenebilir (IEC, 2014, s. 2):

ISO/IEC JTC’nin vizyonu; dünya genelinde bir araya gelen uzmanların iş ve tüketim dünyasında yer alacak BİT standartlarını oluşturacakları bir standart geliştirme çevresi olarak tanımlanabilir. Misyonu ise, BİT’i standartlaştırılmasında tek ve kapsamlı bir standartlaştırma süreci oluşturmaktır.

ISO/IEC JTC komitesi çalışmalarını gerçekleştirirken temel alanlara odaklanmaktadır (IEC, 2014, s. 3):

- Bilgi ve iletişim teknolojileri (BİT) sistemleri ve araçlarının tasarımı ve geliştirilmesi,
- BİT ürünlerinin ve sistemlerinin performans ve kalitesi,
- BİT sistemleri e programlarının güvenliği,
- BİT ürünleri ve sistemlerinin karşılıklı işlerliği,
- Konsolide edilmiş araçlar ve çevre,
- Birbiriyle uyumlu BİT ilgili kavramları,
- Kullanıcı dostu ve ergonomik olarak tasarlanmış kullanıcı arayüzleri,
- Bilgi teknolojilerinin sürdürülebilirliği.

Komite anılan alanlara odaklanırken 6 temel prensip çerçevesine çalışmalarını devam ettirmektedir. Bunlardan ilki, iş dünyası benzeri yaklaşım olarak belirtilen maliyet etkinliğini temel alan, market odaklı sonuçları hedefleyen bir politikadır. İkinci prensip JTC'nin belirlenmiş küresel ihtiyaçlar çerçevesinde geniş bir yelpazede kaliteli ürün ve hizmetler sunmasıdır. Bir diğer prensibe göre JTC küresel anlamda ürünlerini güncel tutacak ve bunları hizmetleri ile beraber kullanımlarını teşvik edecektir. Dördüncü prensibe göre JTC dünyada geçerli olan uluslararası ticaret kavramları çerçevesinde kullanıcılarının çok kültürlü ihtiyaçlarını karşılayacaktır. Beşinci prensipte JTC'nin diğer organizasyonların çalışmalarını dikkate aldığı ve söz konusu bilgi teknolojileri çalışmalarının gelişmesinde ortak katkı sağlamaya hazır olacağı belirtilmektedir. Altıncı ve son prensipte JTC'nin teknik uzmanları kendine çekerek onlara standart geliştirebilecekleri bir ortam yaratacağı kabul edilmiştir. İlgili organizasyonlar ve ortak komite incelendikten sonra izleyen kısımda bilgi güvenliği yönetim sistemi ve ISO/IEC 27001 standartı açıklanmaktadır.

3.2.2 Bilgi Güvenliği Yönetim Sistemi

Yönetim sistemi kavramı günümüzde oldukça çok kullanılan temel bilgi teknolojileri kavramlardan biridir. Bilgi güvenliği yönetim sistemleri kavramı üzerinde durulurken, öncelikle yönetim sistemi kavramının da açıklanması yerinde olur. Yönetim sistemi;

organizasyonun temel ilkelerini, işleyiş prensiplerini, prosedürlerini, faaliyetlerini, iş ve işlemlerini yönetmeye ve sürekli gelişimini sağlamaya yönelik kanıtlanmış bir çerçevededir (TSE, 2015a, s. 4).

Yönetim sistemleri organizasyonların stratejik hedeflere ulaşma doğrultusunda politikalarını oluşturmak ve bu politikaları uygulamaya koymak amacı ile kullanılabilir. Söz konusu politikaların uygulamaya konulabilmesi için ise organizasyonun kurumsal yapısı, ölçme ve değerlendirme teknikleri, sistematik süreçler ve ilgili süreçlerin sürekli iyileştirme politikaları üzerine bina edilmiş amaç ve hedefler belirlenmesi gerekmektedir. Burada temel olarak dikkat edilmesi konu, yönetim sisteminde yukarıda da bahsedildiği gibi sistematik süreçlerin ve diğer ilgili tüm bileşenlerin izlenmesi neticesinde elde edebileceğimiz ölçülebilen bir kaynak oluşması ve bu kaynağında yönetilebilmesinin sağlamasıdır.

Yönetim sistemi bazı unsurları bulunmaktadır bunlar aşağıdaki gibi sıralanabilir:

- Politika unsuru,
- Planlama unsuru,
- Uyarlama unsuru,
- Performans değerlendirme,
- Sürekli iyileştirme unsuru,
- Yönetim tarafından gerçekleştirilen gözden geçirme süreci.

Yukarıda belirtilen unsurlara ilişkin olarak politika unsurunda dikkat edilmesi gereken nokta kararlılık ve uygulama ilkelerinin belirlenmesidir. Planlama unsurunda ise sistemin oluşturan bileşenlerin genel anlamda ihtiyaçlarının, girdilerinin vb. faktörlerinin ortaya konulması söz konusudur. Uyarlama unsurunda konuya ilişkin olarak kurum içi ya da dışı eğitimler ile farkındalık oluşturulması beklenmektedir. Bir diğer unsur olan performans değerlendirmesinde, iş ve işlemlerin denetimi, izleme ve ölçme teknikleri ile takibi ve ortaya çıkan uygunsuzlukların değerlendirilmesi temel alınmaktadır. Sürekli geliştirme ve yönetimin gözden geçirmesi unsurlarında ise düzeltici faaliyet ve sürekli geliştirme yolu ile sürekli iyileştirmenin sağlanması ve söz konusu sürecin yönetim tarafından

düzenli aralıklarla değerlendirilmesi belirtilmektedir. Yönetim sistemlerine Elektronik Belge Yönetimi Sistemi (EBYS) veya Bilgi Güvenliği Yönetim Sistemi (BGYS) gibi yönetim sistemleri örnek verilebilir. EBYS, ne kısa tanımı ile bir organizasyonda ilgili birimlerin faaliyetlerini yerine getirirken ortaya çıkarılan belgelerin, üretimlerinden imhalarına kadar süreç içerisindeki yönetiminin elektronik ortamda sağlanmasına olanak veren bir bilgi yönetim sistemidir (Önaçan ve ark., 2012, s. 5). EBYS'nin uygulanması ilgili organizasyonda diğer tüm dönüşümlerde olduğu üzere bir direnç ile karşılaşabilir. Ancak unutulmamalıdır ki EBYS'nin ilgili organizasyona önemli faydaları olmaktadır. Söz konusu faydalar kısaca aşağıdaki gibi belirtilebilir (Önaçan ve ark., 2012, s. 17):

- Bilginin ilgili karar vericilere önceden belirlenen iş akışı yardımı ile sistematik biçimde iletilebilmesi,
- Fiziki anlamda dokümantasyon yükünün hafifletmesi ve verimli çalışma ortamı oluşturması,
- Bilginin standardize edilmesi ve belirli güvenlik şartlarında saklanması,
- Belgenin hızlı bir şekilde ulaşımının sağlanabilmesi.

Bu çerçevede BGYS aşağıdaki gibi tanımlanabilir (TSE, 2015a, s. 5):

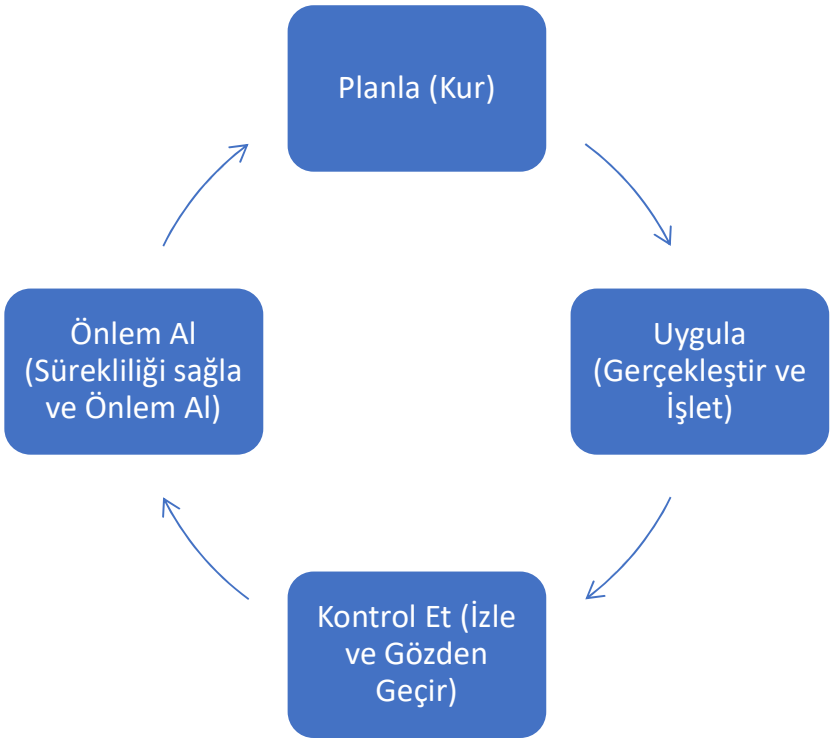
Organizasyonun fiziki ve elektronik bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini korumak için organizasyonel kademeler içerisinde en üst seviyeden en alt seviyeye kadar her aşamada uygulayacağı iş odaklı yönetim yaklaşımıdır. Aynı zamanda BGYS, toplam yönetim sisteminin, iş riski yaklaşımı çerçevesinde bilgi güvenliğini oluşturan, uyarlayan, çalıştıran, izleyen, gözden geçiren, koruyan ve geliştiren bileşenidir. Bu bileşen oluşturulurken, organizasyonun iş gereksinimleri, hedefleri, güvenlik gereksinimleri, süreçleri ve organizasyonun büyüklüğü ve yapısı önemli rol oynamakta olup, BGYS'nin şekillenmesinde etkili unsurlardır.

Yukarıda verilen bilgiler ışığında BGYS hakkında bazı çıkarımlar aşağıdaki gibi sıralanabilir:

- BGYS yukarıda da açıklandığı üzere sadece bilgi teknolojileri (BT) departmanının sorumluluğunda değildir, organizasyonun tüm kademelerini etkiler. Bu farklı kademelerde çalışan tüm personelin işlerini gerçekleştirirken bilgi güvenliği prensiplerine uygun davranmaları beklenmektedir.
- Belirli bir tarihte uygulanacak ve tamamlanınca rafa kaldırılacak bir uygulamadan ziyade bir organizasyon kültürü olarak ucu açık bir zaman aralığında uygulanması hedeflenir. Organizasyonun iş yapma tarzını şekillendiren bir uygulamadır ve aynı zamanda sürekli bir gelişim sürecidir.
- BGYS sistemi gerçek hayatta uygulanmalıdır, bir başka deyişle uygulamalar sadece kâğıt üzerinde kalmamalıdır.
- BGYS bir ürün hizmet vb. şeklinde ele alınmamalıdır. Bu bir farkındalıktır ve tüm organizasyon kademelerinde bu farkındalığın sağlanması gerekmektedir. Organizasyonda BGYS bilincinin oluşması sürekli bir gelişim süreci olarak değerlendirilir.

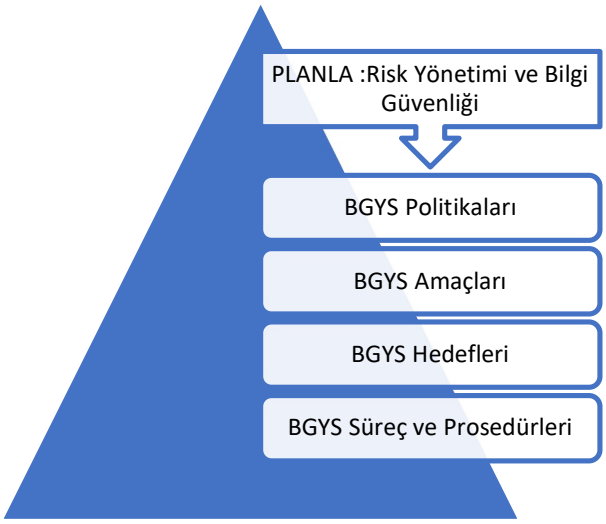
BGYS sürecinin bir kurum ya da organizasyona uygulanmasında kısaca PUKÖ modeli denilen ve daha açık tanımıyla planla, uygula, kontrol et ve önlem al deyimlerinin baş harflerinden oluşan modelden bahsedilebilir.

PUKÖ modeli tüm sistemi kapsayacak şekilde ele alındığında aşağıdaki şekil ile özetlenebilir (TSE, 2006, s. 2):



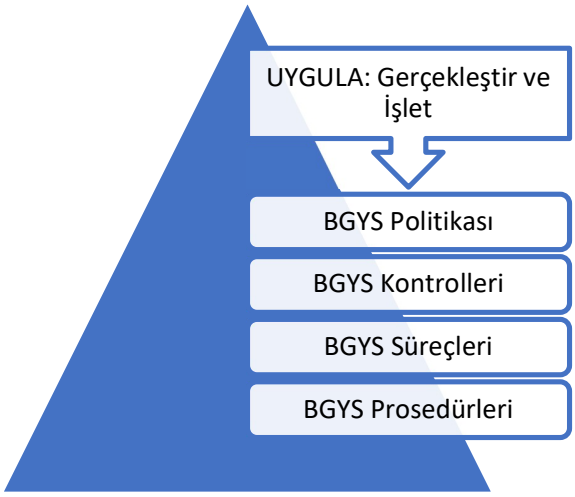
Şekil 10: PUKO Modeli

Şekil-10'da görüldüğü üzere PUKÖ modelinin ilk aşaması planlama yani BGYS'nin kurulması sürecidir. Bu aşamada ilgili kurum, gerekli risk analizleri sonucu ve stratejik hedefleri doğrultusunda bir bilgi güvenliği yönetim sistemi hedef, amaç, politika ve prosedürler bütünü oluşturmalıdır.



Şekil 11: BGYS Planlama

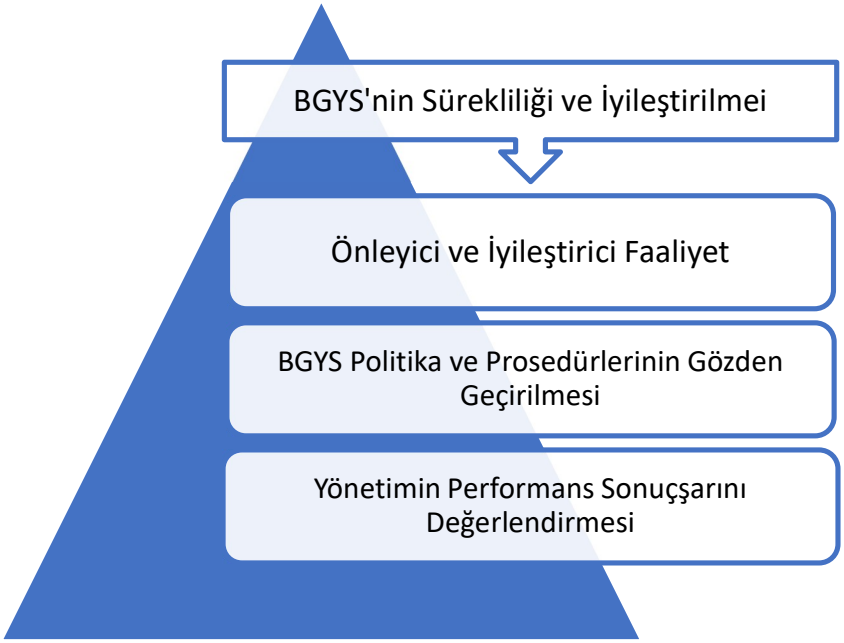
Şekil-11'de özetlenen PUKÖ modelinin planlama aşamasının ardından BGYS modelinin uygulama safhası söz konusu olmaktadır. Bu aşama bir diğer anlatım ile modelin gerçekleştirilmesi ve işletilmesi aşamasıdır. Planlama aşamasında belirlenmiş olan BGYS prosedürleri, süreçleri, kontrol ve politikaları hayata geçirilmesi modelin uygulama safhasında söz konusu olmaktadır. Konu safha aşağıdaki şekil yardımı ile açıklanmaktadır:



Şekil 12: BGYS Uygula

Uygulama aşamasını ardından ise Kontrol safhası modelde yerini almaktadır. Kontrol safhasında halihazırda planlanmış ve uygulamaya alınarak işletilmeye başlanmış BGYS'nin politika ve amaçları doğrultusunda sistemin izlenmesi ve gözden geçirilmesi söz konusu olmaktadır. Özellikle BGYS'nin önceden belirlenmiş uygulama performansının izlenerek, performans ölçümünün mümkün olduğu alanlarda gerekli ölçümlerin yapılarak, sonuçlarının değerlendirilmesi için ilgili düzeydeki yönetim kademesine iletilmesi gerekmektedir.

PUKO modelinin son basamağı olan önlem al safhasında BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi amaçlanmaktadır. Bir önceki basamakta yönetime sunulan performans değerlendirme sonuçları doğrultusunda ve sonuçların değerlendirilmesi neticesinde, BGYS'nin ilgili kurum ya da organizasyon için oluşturulmuş kapsamı, politika ve prosedürleri ile hedeflerinin yeniden değerlendirilmesi ve bu amaç doğrultusunda gerekli olan önleyici ve iyileştirici faaliyetlerin hayata geçirilmesi söz konusu olmaktadır. PUKÖ modelinin son basamağı olan "önlem al" safhası aşağıdaki şekil yardımı ile özetlenmektedir:



Şekil 13: BGYS Önlem Al

3.2.3 Türk Standartları Enstitüsü (TSE) ve Standardın Türk Standardı Olarak Kabulü

ISO/IEC 27001 standardı ISO tarafından 14 Ekim 2005 tarihinde yayınlanmış ve ISO/IEC 27000 standart ailesin içinde yerini almıştır. Ülkemizde ISO tarafından oluşturulan söz konusu standart esas alınarak TSE bilgi teknolojileri ve iletişim ihtisas grubunca hazırlanmış ve TSE teknik kurulunun 2 Mart 2006 tarihli toplanasında Türk standardı olarak kabul edilmiş ve adı da "TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri" adıyla yayınlanmıştır. Ardından ISO tarafından anılan standarda güncellemeler yapılmış ve revize standart Ekim 2013 "ISO/IEC 27001:2013" olarak yayınlanmıştır.

3.2.4 ISO/IEC 27001 Standardı

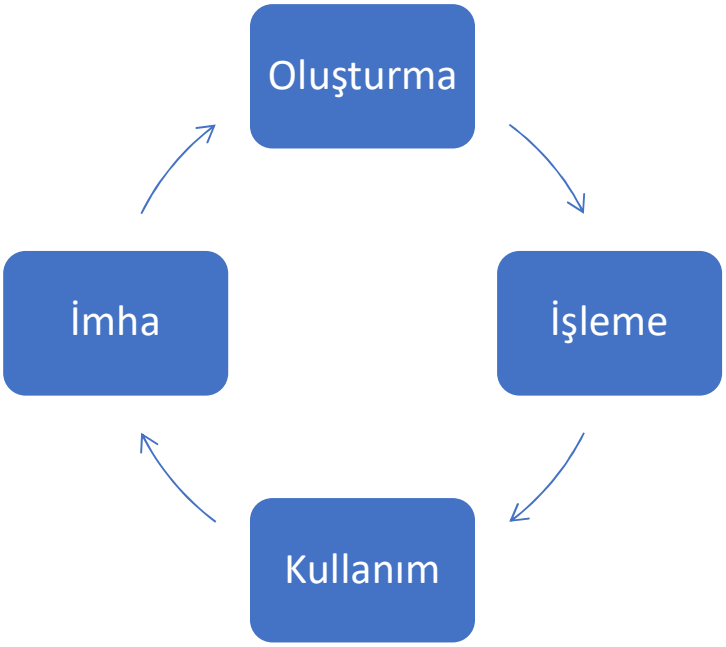
Türk standardı olarak da kabul edilme süreci yukarıda anlatılan TS ISO/IEC 27001 standardı, bir bilgi güvenliği ve yönetim sistemini kurmak, geliştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model oluşturmak amacıyla oluşturulan bir bilgi güvenlik yönetim standardıdır.

Söz konusu ISO standartları arasından ISO/IEC 27001 ve ISO/IEC 27002 diğer bileşenler arasında en temel standartlardır. ISO 27002, BGYS'nin planlanmasını, gerçekleştirilmesini, iyileştirmelerini ve devamlılığı için uygulanacak işlemleri ve kontrolleri içerirken, ISO 27001'de BGYS'nin belgelendirilmesi için gereken standartlar yer alır. Bir diğer deyişle ISO/IEC 27002 bilgi güvenliği yönetimi için uygulama prensipleri standardıdır ve bilgi güvenliğini başlatan, gerçekleştiren ve sürekliliğini sağlayan kişilerin kullanımı için bilgi güvenliği yönetimi ile ilgili tavsiyeler içerir. ISO 27001 standardı ise yukarıda verildiği üzere kurumsal bilgi güvenliğinin sağlanmasına yönelik bir standarttır.

ISO 27001 kurumsal bilgi güvenliğinin bir kurumda nasıl uygulanabileceğini açıklayan bir standart olup sadece sistem güvenliğinden değil bilgi güvenliğinden de bahsetmektedir. Bu noktada organizasyonların hangi sebeplerden dolayı güvenlik sistemi oluşturmak istedikleri, bir diğer deyişle organizasyonların güvenlik

gereksinimlerinin kaynakları da ele alınmalıdır. Organizasyonların güvenlik kaynakları risk değerlemesi, yasal gereksinimler ve iş gereksinimleri olmak üzere üç ana başlık altında toplanabilir (TSE, 2015a, s. 8):

Bilgi güvenliğinin öznesi olan bilginin ve bilgi sistemlerinin tanımı ve incelenmesi yukarıdaki bölümlerde yapılmıştı. Bu noktada bilgi güvenliğinin bilgi ve bilgi sistemleri doğal yaşam döngülerindeki tüm aşamalarında önemli olacağının ve dikkate alınması gerektiğinin önemi vurgulanmalıdır. Bilginin doğal yaşam döngüsü, bilginin oluşturulması, işlenmesi, kullanımı ve imhası şeklinde tamamlanır (Newfoundland, 2017).

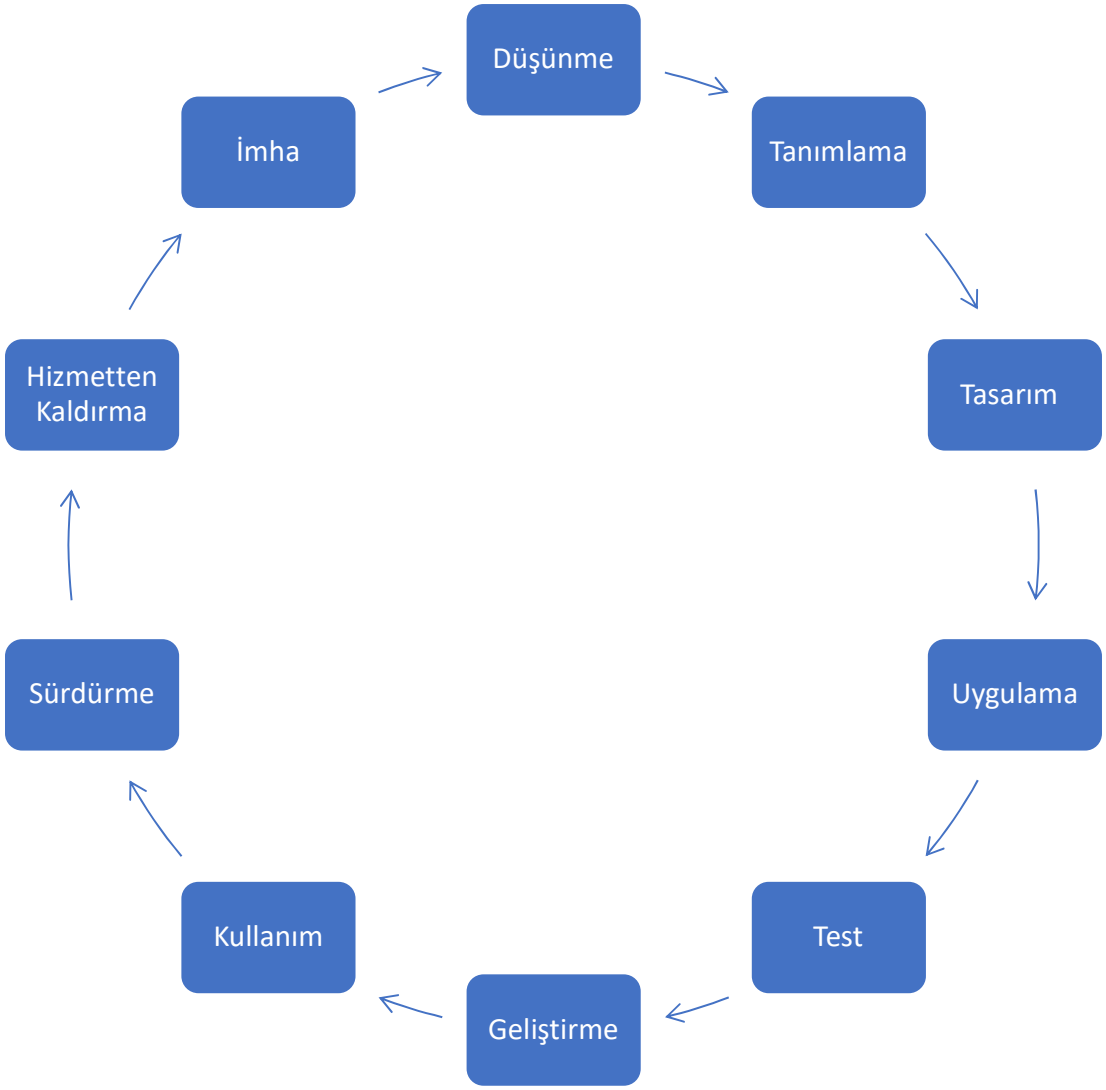


Şekil 14: Bilginin Hayat Döngüsü

Söz konusu yaşam döngüsü boyunca bilginin varlık değeri ve ona karşı oluşan risklerde değişiklikler görülebilir. Bu çerçevede bilgi güvenliği her kademede değerini korumaya devam eder.

Bilginin yaşam döngüsünün yanı sıra bilgi sistemlerinin de doğal yaşam döngüsünden bahsedilebilir. Bilgi sistemleri hayat döngüsü öncelikler sistemi düşünme ile başlar ardından, tanımlama, tasarım, uygulama, test, geliştirme,

kullanım, sürdürme, hizmetten kaldırma ve en sonunda imha aşaması ile son bulur (EATC, 2018).



Şekil 15: Bilgi Sistemleri Hayat Döngüsü

Bilgi sistemleri hayat döngüsünde de bilginin hayat döngüsününkine benzer şekilde bilgi güvenliği her aşamada önem arz etmektedir.

3.3 ISO 27001:2013 STANDARDI VE İÇ DENETİM

Bir kurumda ya da organizasyonda görevli iç denetçiler, bünyesinde bulundukları yapının en kısa tanımı ile risk ve iç kontrol sistemlerinin etkinliği ve etkililiğini değerlendirmektedir. Bu çerçevede yapılan işlemler, standartlar ve prosedürler çalışmalarının geçmiş bölümlerinde ele alınmıştır. Bilindiği üzere bilgi, kurumun tüm sistemlerinin ve dolayısıyla iç denetçinin denetlemekle yükümlü olduğu alanların ana girdisidir. Finansal rakamlardan iç kontrol listelerine, risk organizasyon prosedürler dokümanına kadar tüm bu alanların ana girdisi bilgidir. Bilgi olmadan bu anılan dokümanların sağlanması mümkün görünmemektedir. İşte bu noktada bilginin ne şekilde elde edildiği, korunup korunmadığı, ilgili kurumda bilgi güvenliğine ilişkin prosedürlerin oluşturulup oluşturulmadığı ya da kurumun ilgili bir BGYS sertifikasına sahip olup olmadığı gibi konuların değerlendirilmesi ihtiyacı hasıl olmaktadır. Dolayısıyla iç denetçinin bilgi güvenliği farkındalığının yüksek olması, kurum çalışanlarının da bilgi güvenliği farkındalığını yükseltecek bir faktör olabilir. İç denetim birimi gerek kurumun iç yapısında yer alan bir organ olması gerek ise de denetim ve rehberlik faaliyetini üstlenmesi sebebi ile kurum çalışanlarının bilgi güvenliği farkındalığını yükseltmesine yardımcı olarak en önemli unsurlardan biri olarak değerlendirilebilir. Çalışmanın izleyen bölümünde kurum iç denetim fonksiyonunun ISO/IEC 27001 standardı ilgili kriterleri çerçevesinde üstlenebileceği görev ve sorumluluklar incelenmektedir. İç denetim fonksiyonu, içinde bulunduğu kurum ya da organizasyona yönelik bir ISO/IEC 27001:2013 standardı çerçevesinde bir bilgi güvenliği denetimi yapmayı amaçlıyor ise öncelikle belirtilen standardın içeriğine hâkim olması beklenmektedir. Standardın en güncel versiyonu olan 2013 versiyonu toplam 10 maddeden ve “referans kontrol hedefleri ve kontroller” başlıklı ekten oluşan bir bütündür. Aynı standardın bir eski modeli olan 2005 versiyonunda ise 8 madde ve 3 ek bulunmaktadır (TSE, 2006, s. 4). ISO/IEC 27001:2013 standardı uluslararası kabul görmüş bir standart olup, ilgili organizasyonun ihtiyaçlarını karşılayacak bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekleri ortaya koyar (TSE, 2013, s. 1). ISO 27001 standardı en son 2022 yılında güncellenmiş ve 25 Ekim 2022

tarihinde yayımlanarak son halini almıştır. Yeni versiyon standardın uygulamaya geçiş sürecine ilişkin olarak Uluslararası Akreditasyon Forumu (IAF) tarafından bir rehber yayınlanmış olup anılan sürecin 31.10.2025 tarihine kadar tamamlanması gerektiği belirtmiştir (IAF, 2023, s. 8). İçerik anlamında da 2022 versiyon ile 2013 versiyonu arasında ortaya çıkan değişiklikler ISO/IEC 27001:2022 standart dokümanında tablo yardımı ile açıklanmıştır (ISO/IEC, 2022, pp. 143-149). Buna göre uygulanacak kontrol sayıları 114 adetten 93 adete indirilmiş olup 14 olan bölüm sayısı da 4 bölümüne düşürülmüştür. Çalışmanın izleyen kısmında anılan standardın ilgili maddelerinde yer alan ana unsurlar incelenecek ve iç denetim fonksiyonunun ISO 27001 standardına uyum kapsamında Bilgi Güvenliği Yönetim Sistemleri (BGYS) iç tetkiki sürecinde söz konusu unsurlara yönelik alabileceği aksiyonların neler olabileceği değerlendirilmektedir.

3.3.1 Denetlenecek Kurumun İç ve Dış Çevresi

BGYS iç tetkiki gerçekleştirilecek kurumun iç ve dış çevresini oluşturan faktörlerin ortaya konulması ve anlaşılması, kurumun risklerini belirlerken içsel ve dışsal tüm unsurların göz önünde bulundurulmasını sağlar. BGYS iç tetkik süreci prosedürlerine göre iç çevre, kurumun içsel risklerinin yönetimini etkileyebilecek tüm unsurları kapsar. Bu unsurlar aşağıdaki gibi sıralanabilir (TSE, 2015b, s. 28)

- Kurum strateji, hedef ve politikaları,
- Kurumsal yapı, görev dağılımı ve kurum kültürü,
- Kurumun prosedürleri, rehber ve standartları,
- Kurum bünyesinde faaliyet gösteren bilgi sistemleri, bilgi akış diyagramları ve resmi ya da gayri resmi karar alma süreçleri,
- Kurum bünyesindeki tüm kaynaklar, örneğin çalışanlar, teknolojik durum, sermaye, zaman vb.
- İç paydaşların bilgi güvenliğinin önemi üzerindeki algısı.

Görüldüğü üzere iç çevre tamamen kurumun kontrolü altında olan ve üzerinde değişiklik ya da iyileştirme yapabileceği alanları kapsamaktadır. Bununla beraber dış çevre ise tamamen kurumun kontrolünde olamayabilir. Dış çevre, uluslararası

ve ulusal mevzuat ve sosyo-kültürel yapı ile politik ve ekonomik ortamın tamamını kapsar.

Bir BGYS denetiminde kapsam, yukarıda ortaya konuların iç ve dış unsurlar ışığında değerlendirilir. Denetimi yapan ve denetlenen tarafların net bir şekilde belirlenmesi de gereklidir. Örneğin denetim yapacak taraf iç denetim birimi ilen denetlenen taraf ise kurumun bilgi teknolojileri departmanı olabilir. Tarafların net bir şekilde ortaya konulmasının ardından tarafların beklenti ve ihtiyaçları netleştirilmelidir. Bu beklenti ve ihtiyaçlar yasal mevzuattan doğabileceği gibi denetim olurundan ya da denetim işi sözleşmesinden de doğabilir. Örneğin üst yönetim iç denetim birimine bir olur ile bilgi teknolojileri departmanının ISO 27001 standardı çerçevesinde yeterli olup olmadığına ilişkin bir denetim faaliyeti gerçekleştirmesini isteyebilir. Bu çerçevede yukarda verilenlere ek olarak kapsam benzer kurumlarda gerçekleşmekte olan faaliyetlerin dikkate alınması sonucu da şekillenebilir.

3.3.2 Liderlik

İç denetçi, BGYS faaliyetlerine ilişkin çalışmalarını devam ettirirken dikkate alması gereken bir diğer unsur liderlik hakkındadır. BGYS'de üst yönetim sorumluluğu demek, kurum ya da organizasyon üst yönetiminin BGYS'ye olan bağlılığı, BGYS politikası oluşturulup oluşturulmadığı ve kurumsal görev dağılımı ile yetki ve sorumlulukların dağıtılıp dağıtılmadığının değerlendirilmesidir. BGYS'ye olan bağlılık birden çok unsura ilişkin gerekli adımların üst yönetim tarafından atılmış olması demektir. Bunlar (TSE, 2013, s. 2):

- Kurum ya da organizasyonun daha önceden belirlenmiş olan stratejik hedefleri ile BGYS politika ve hedeflerinin konsolide edilmesi,
- Tüm iş süreçlerinin BGYS çerçevesinde gözden geçirilmesi ve uyumlu hale getirilmesi,
- Organizasyonel kaynakların BGYS için ulaşılabilir olmasını sağlamak,
- Tüm çalışanların BGYS'ye olan farkındalığını geliştirmek ve etkin bir şekilde sürdürülebilmesi için onları cesaretlendirmek,
- Tüm BGYS süreçlerinde sürekli iyileştirme faaliyetlerini desteklemektir.

Diğer tüm farklı strateji uygulama süreçlerinde olduğu gibi BGYS uygulama sürecinde de bazı engeller ortaya çıkabilir. Unutulmamalıdır ki, başarılı bir stratejik uygulama yönetimi, üst yönetim başta olmak üzere tüm çalışanların bu hedefe odaklanması ile ortaya çıkmaktadır ve uygulama süreci tüm çalışan ve yöneticiler tarafından benimsenmeli, başarılı uygulama örnekleri aynı hataların tekrarından kaçınılması anlamında paylaşılmalıdır (Kılıç ve Aktuna, 2015, s. 133). Liderlik unsurunun BGYS'te bağlılık safhasının ardından gelen kavram politika kavramıdır. Kurumun BGYS politikası şekil ve içerik anlamında bazı özellikleri taşımalıdır. Örneğin şekil anlamında BGYS yazılı olarak hazırlanmış olmalı, organizasyon çapında bu doküman duyurulmuş olmalı ve tüm ilgililerin bu dokümana kolaylıkla ulaşabilmeleri sağlanmalıdır. İçerik anlamında ise BGYS politikası (TSE, 2015a, s. 23):

- Kurum ya da organizasyonun hem stratejik hem de BGYS amaçlarına uygun olmalıdır,
- BGYS'nin sürekli iyileştirilmesi ve ilgili şartların sağlanacağına yönelik bir taahhüt içermelidir.

Son olarak üst yönetim başlığının son aşaması da kurumsal roller, sorumluluklar ve yetkiler konusudur. Organizasyon içinde BGYS ile ilişkili olan tüm pozisyonların belirlenerek, uygun görülen kişilerin bu pozisyonlara atanması ve bu pozisyonlar için görev tanımları hazırlanarak yetki ve sorumluluklarının netleştirilmesi gerekmektedir. İlgili BGYS kadrosu, BGYS şartlarının kurum içinde uygulanmasını sağlamalı ve bu konuda gerçekleşmekte olan performansı rapor haline üst yönetime iletmelidir.

3.3.3 Planlama

Kurum ya da organizasyon içinde BGYS'de belirtilen şartlara uyumun sağlanabilmesi için ortaya bir plan konulmalıdır. Söz konusu plan detaylı ve kapsayıcı bir şekilde hazırlanmalıdır. Özellikle BGYS amacı ve bu amaca ulaşmak için neler yapılacağı ve hangi kaynakların gerekli olacağı, söz konusu çalışmalarda kimlerin sorumlu olacağı, hangi tarihte tamamlaması gerektiği ve süreç sonuncunda

elde edilen çıktıların nasıl gözden geçirileceği net bir şekilde plan kapsamı içinde yer almalıdır. BGYS amaçları plan kapsamında ilk sırada yer almakta olup, BGYS politikası çerçevesinde ve uyumlu bir şekilde belirlenmelidir. Ayrıca tüm kuruma bu hedefler duyurulmalıdır. İç denetçi bir BGYS planı incelerken yukarıda anlatınla kapsam özelliklerinin oluşturulup oluşturulmadığını değerlendirilmelidir. Planlama aşamasında yer alan belki de en önemli unsurun risk değerleme ve işleme faaliyetleridir. Buna göre kurum risk kriterini belirlemeli bu çerçevede bilgi güvenliği risklerini ortaya çıkarmalı ve onları analiz etmeli, söz konusu risklere ilişkin gerekli kontrol faaliyetlerini oluşturmalıdır (TSE, 2013, s. 4).

3.3.4 Destek

BGYS'nin destek boyutu 5 farklı alanda incelenmekte olup iç denetçi denetim planı çerçevesinde gerekli gördüğü alanlarda daha detaylı çalışma gerçekleştirebilir. Söz konusu 5 alan kaynaklar, yetkinlik, farkındalık iletişim ve dokümantasyondur (TSE, 2013, s. 6). BGYS'de konu edilen organizasyona ilişkin olarak gerek insan kaynakları ki bunların içinde personel eğitim ve geliştirme faaliyetleri ve farkındalık eğitimleri sayılabilir, gerek fiziki çevre (kurumun fiziki yapısı altyapısı vb.) gerek ise de kurum ya da organizasyonun tüm iletişim ve bilişim altyapısı ve teknolojileridir. Kaynaklar özellikle BGYS sürecinde net bir şekilde ortaya koyulmalıdır. Net bir şekilde envanteri sağlanan kaynaklar kurumun kendinden ya da çevresel faktörlerden kaynaklanan değişim ihtiyacının takibinde ve bu doğrultuda faaliyetlerin sürdürülebilirliği açısından önem arz etmektedir.

Bir diğer alan iletişimdir. İletişim iç ve dış iletişim olmak üzere sağlanan bilgi alışverişinin kurum içi ya da kurum dışı kaynaklı olması bakımından ikiye ayrılır. İletişim desteğinde bazı prosedürlerin net bir şekilde tanımlanması gerekmektedir. Bunlar, iletişim konusunun ne olduğu, iletişimin tarafları ve zamanı ile iletişimi etkileyen faktörlerdir (TSE, 2015a, s. 31).

Destek başlığının bir diğer alt alanı ise dokümantasyondur. Dokümantasyon ilgili BGYS standardının kurum içinde olmasının gerektirdiği yazılı prosedürlerdir. Prosedürlerin yazılı olmasından kasıt söz konusu dokümanın fiziki bir ortamda

muhafaza edilmesi olarak açıklanabilir. Yukarıda belirtildiği üzere ilgili standardın gerektirdiğinin yanı sıra kurum ya da organizasyonun da BGYS'nin etkin bir şekilde işlemesini sağlamak için oluşturduğu bazı prosedürler de söz konusu olabilir. İç denetçi tüm bu dokümanları da göz önünde bulundurmalıdır.

Yetkinlik ve farkındalık ise son iki alt başlığı tanımlamaktadır. Yetkinlik BGYS performansını ya da başarısını etkileyen insan faktörünün ne derece ilgili sürece katkı yapabildiğinin ölçülme süreci olarak özetlenebilir. İlgili çalışanların konuya ilişkin eğitimler ve tecrübe paylaşımları ile yetkinliklerinin arttırılması gerekmektedir.

Farkındalık kurumdaki tüm ilgililerin bilgi güvenliği prosedürleri ile söz konusu prosedürlerdeki görev sorumlulukları ilişkin olarak yeterli düzeye bilgi sahibi olması olarak özetlenebilir. Kurum bünyesindeki ilgili kişilere çalışanlar ve kurum ile iş yapan diğer paydaşlar örnek verilebilir. Daha detaylı bir anlatım ile söz konusu paydaşların aşağıdaki konularda yeterli düzeyde bilgi sahibi olmaları beklenir (TSE, 2013, s. 5):

- BGYS politika ve prosedürleri
- BGYS'nin kurum faaliyetlerine olan katkısı
- Çalışanların BGYS'den kaynaklı görev ve sorumlulukları

3.3.5 Operasyon

Operasyon aşaması kısaca tanılamak gerekir ise; operasyon, ilgili standart çerçevesinde BGYS'nin gereklerinin sağlanması amacı ile ilgili proseslerin en başından bir diğer deyişle planlama aşamasından başlayarak uygulama ve kontrol altında tutulmasıdır (TSE, 2015a, s. 35). Kurum bünyesinde ilgili birimleri ortaya çıkabilecek olası sorunları tahmin ve takip edebilmek amacıyla ilgili risk analizi süreçlerini hayata geçirmeli risk kütükleri tutularak gerekli önlemler alınmalıdır (TSE, 2013, s. 7).

3.3.6 Performans Değerlendirme

Performans değerleme konusu, özellikle diğer tüm farklı alanlardaki performans analizlerine benzer şekilde ilgili sürecin etkinliği ve etkililiğinin analizini içermektedir. BGYS performans değerlendirmesinde de bu açıklamaya paralel olarak, bilgi güvenliği politikalarının ve bilgi güvenliği yönetim sisteminin etkinliğinin incelenmesi söz konusu olmaktadır.

Performans değerleme BGYS çerçevesinde üç başlık altında ele alınabilir. Bunlar; izleme, ölçme ve değerlendirme aşaması; iç tetkik ve son olarak yönetim değerlemesidir (TSE, 2013, s. 8). İzleme, ölçme ve değerlendirme sürecinde öncelikle tam olarak hangi sürecin ya da kontrol unsurunun ele alınacağı belirlenmelidir. Örneğin kurumun zararlı yazılımlara karşı uygulanmakta olan kontrol süreçleri ya da kurumun fiziki varlıkların kurum dışına çıkarılması sürecinde uygulanması gereken prosedürler gibi performans değerlemesinde bulunulacak süreç açık olarak belirlenmelidir. Süreç belirlenmesinden sonra izlenecek yöntem ve uygulanacak ölçme ve değerlendirme yöntemleri belirlenmelidir. Bu çerçevede izleme ve ölçmenin kurumun hangi çalışanlar tarafından gerçekleştirileceği, uygulama zamanı ve sonuçların değerlendirmesine ilişkin detaylarında netleştirilmesi beklenmektedir.

Performans değerleme aşamasının ikinci alt başlığı iç tetkik kavramıdır. İç tetkik kavramına çalışmanın izleyin kısmında geniş olarak yer verilmektedir.

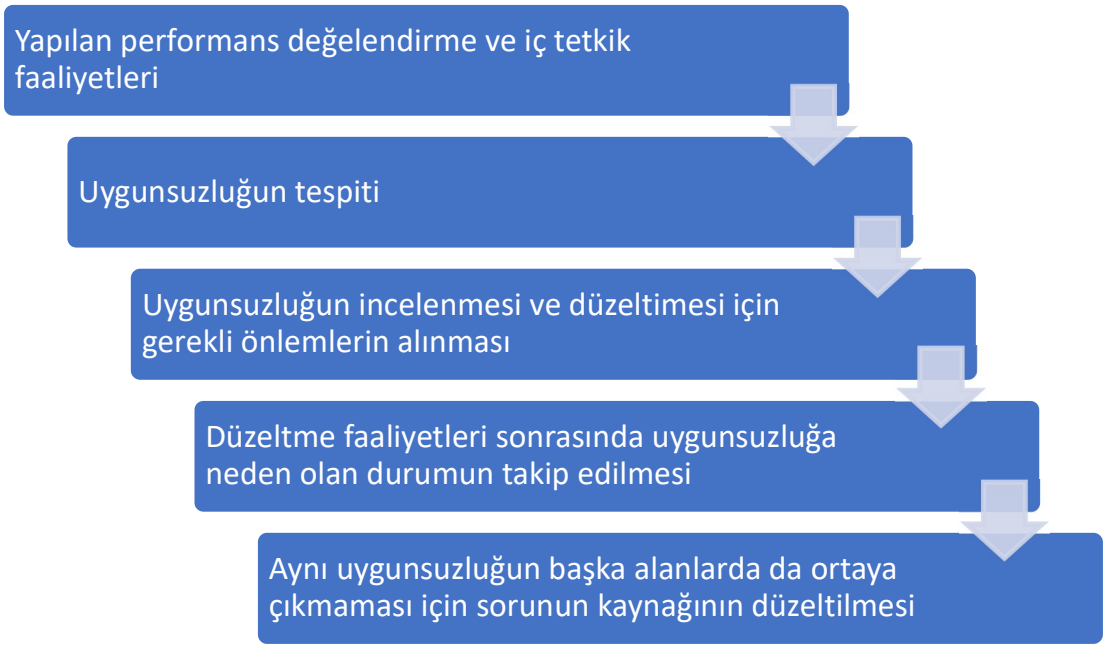
Performans değerlemenin üçüncü başlığı da yönetim değerlemesidir. Bu süreç, kurum ya da organizasyonun üst yönetimin belirli zaman aralıkları ile kurumun BGYS yeterliliğini, uygun bir şekilde uyarlanıp, uygulamada etkinliğin sağlanıp sağlanmadığını incelemesini kapsamaktadır. Üst yönetim bu değerlemeyi yaparken öncelikle geçmiş dönem değerlemelerinde ortaya çıkarılan eksikliklerin giderilip giderilmediğini inceler. İzleyen adımda BGYS standartlarında ve BGYS'ye ilişkin kurum için politika ve prosedürlerde herhangi bir değişiklik olup olmadığını gözden geçirir. Ardından üst yönetim eldeki diğer verileri değerlendirir. Söz konusu veriler; izleme ve ölçme faaliyeti neticesinde elde edilen sonuçlar, iç tetkik sonuçları, kurum

içi ve kurum dışı paydaşların BGYS çerçevesindeki geri bildirimleri, risk analizi sonucu elde edilen risk unsurları olarak belirtilebilir.

Üst yönetimin değerleme faaliyeti sonucunda ortaya kurumun BGYS'nin etkin bir şekilde uygulayabilmesi için ihtiyacı olan kaynakları, finansal gereksinimleri, kontrol faaliyetlerinin etkinliğine ilişkin sonuçlar elde edilebilir.

3.3.7 İyileştirme

İyileştirme, yapılan performans değerlemeleri ve iç tetkik faaliyetleri sonucunda elde edilen bulguların ve bu bulguları doğuran uygunsuzlukların giderilmesi yönünde atılan adımları kapsamaktadır. İyileştirme faaliyetleri, uygunsuzluğun tespiti ve düzeltici faaliyet ile sürekli iyileştirme olmak üzere iki başlık altında toplanabilir. İlk olarak uygunsuzluğun tespiti ve düzeltici faaliyet süreci ele alınacak olup, söz konusu faaliyetin süreci Şekil-16 yardımı ile açıklanabilir (TSE, 2013, s. 9):



Şekil 16: BGYS İyileştirme

Şekil-16'da görüleceği üzere uygunsuzluk ve düzeltici faaliyet aşaması daha ziyade sorunun tespitinin ardından onu düzeltmeye ilişkin gerekli faaliyetlerin gerçekleştirilmesine yönelik bir yaklaşımdır. Uygunsuzluk ilgili tetkik faaliyeti sonucu

ortaya çıkarılır. Ardından söz konusu uygunsuzluk ilgili BGYS standardı ya da kurum BGYS politika ve prosedürleri kapsamında incelenir. Ele alınana uygunsuzluğa ilişkin olarak yapılan inceleme sonucunda gerekli düzeltici faaliyet gerçekleştirilir ve bu faaliyetin sonuçları gözlemlenir. Son aşamada da aynı tür uygunsuzluğun diğer başka süreçlerde de yaşanmaması için sorunun kaynağının düzeltilmesine yönelik daha geniş kapsamlı bir düzeltici faaliyet aşamasına geçilir. İyileştirmenin bir diğer boyutu da sürekli iyileştirmedir. Sürekli iyileştirme adından da anlaşılacağı üzere, ortaya çıkarılan bireysel bulgulara yönelik değil sistemin genel işleyişine ilişkin olarak kesintisiz bir iyileştirme faaliyeti olarak tanımlanabilir. Sürekli iyileştirme faaliyetinde kurum ya da organizasyonda kabul edilen ilgili BGYS standardı çerçevesinde bu BGYS'nin uygunluğu doğruluğu ve etkinliğine ilişkin kapsamı bir iyileştirme faaliyeti söz konusudur.

3.4 BGYS İÇ TETKİKİ VE AŞAMALARI

Bilgi Güvenliği ve Yönetim Sistemleri çerçevesinde iç denetçi nasıl bir görev ve sorumluluk alanı kapsamında hareket etmelidir? Bu soruya verilecek cevaplar belki de günümüz iç denetim anlayışının sınırlarının çizilmesine yardımcı olabilecektir.

Bilindiği üzere en kısa tanımı ile iç denetim organizasyondaki risk yönetimi ve iç kontrol sistemlerinin etkin ve etkili bir şekilde çalışıp çalışmadığını belirleme ve ortaya çıkarılan eksikliklerin giderilmesi yönünde faaliyet göstermektedir. Ayrıca iç denetim faaliyeti; Uluslararası İç Denetim Standartlarına göre, bilgi sistemlerini de kapsayan çeşitli kontrollerin yeterliliğini ve etkinliğini değerlendirmektedir (TİDE, 2012b, s. 16). Söz konusu değerlendirmenin kapsam alanları;

- Yasal Mevzuata ve ilgili yazılı dokümanlara uyum,
- Faaliyet ve kontrollerin etkinlik ve verimliliği,
- Organizasyon varlıklarının korunması ve,
- Finansal ve Operasyonel bilgilerin güvenilirliğidir (Adiloğlu, 2010, s. 66).

Görüldüğü üzere finansal ve operasyonel bilgilerin güvenilirliği konusu iç denetim fonksiyonun değerlendirilmesi kapsamında ele alınan ana konulardan birisidir. Bu

çerçevede BGYS iç tetkik faaliyeti ile iç denetim fonksiyonunun bilgi güvenliği ile ilgili olarak üzerine düşen görev ve sorumluluklar çalışmanın izleyen bölümünde incelenmektedir.

3.4.1 BGYS İÇ TETKİKİ

Çalışmanın bu bölümünde öncelikle BGYS İç Tetkik faaliyeti çerçevesinde tanımlar, tetkik aşamaları, hazırlık süreci, tetkikin uygulanması ve raporlama konuları ele alınacaktır.

3.4.1.1 İç Tetkik ve İlgili Kavramlar

Tetkik kavramı, tetkik delili elde etmek ve ilgili alanda belirlenen kriterlerin karşılanma durumunu objektif olarak değerlendirmek için yapılan sistematik, bağımsız ve yazılı bilgi haline getirilmiş süreçler bütünü olarak tanımlanabilir (TSE, 2015b, s. 73). Tanımadan da anlaşılacağı üzere tetkik kavramı diğer denetim kavramları ile benzer şekilde önceden belirlenmiş olan kriterlerin karşılanma derecesi ile ilgilenmektedir. Tetkik kriterleri, organizasyonun politikaları, prosedürleri ve benzeri koşullar seti olarak düşünülebilir. Söz konusu kriterler ile bağlantılı olan ve doğrulaması sağlanabilen tüm kayıt, beyan ve bilgilere ise tetkik delilleri denir. Tetkik kriterleri içerisinde bir faaliyetin ya da durumun gerçekliğini veya varlığını kanıtlayan verilere ise objektif delil denir. Belirtildiği üzere objektif delil; deney, gözlem ve tarafsız ölçümler ile sağlanmalıdır. Bu çerçevede objektif delillerin duygu ve önyargılardan etkilenmemesi gerektiği, gözlem ölçme ve muayene yolları ile elde edilebilecek olması bir diğer deyiş ile sayılabilir ölçülebilir olması gerektiği, mümkün ise belgelendirilmiş olması gerektiği ve son olarak da doğrulanabilir olması gerektiği düşünülebilir.

Tetkik programı kavramına gelindiğinde ise yine diğer denetim süreçlerine benzer şekilde program, belirli bir zaman dilimi için planlanan ve özel amaca yönelik olan bir veya birden çok sayıdaki tetkik faaliyetlerinin belirlenmesi olarak açıklanabilir. Tetkik planı ise tetkik için gerçekleştirilmesi planlanan faaliyetlerin belirlenmesidir.

Söz konusu tetkik programı ve planı kapsamında gerçekleşecek tetkikin kısıtları ve genişliğine ise tetkik kapsamı denilmektedir.

İç Tetkik faaliyetine ilişkin diğer kavramlar aşağıdaki gibi tanımlanabilir (TSE, 2015b, s. 73):

Tetkik bulguları; tetkik faaliyeti neticesine ortaya çıkan sonuçlar olarak açıklanabilir. Bu sonuçlar diğer denetim türlerinde de söz konusu olduğu önceden belirlenmiş olan prosedürler ile tetkik neticesinde elde edilen delillerin karşılaştırılması ve değerlendirilmesini kapsamaktadır.

Tetkik sonucu; tetkik faaliyeti kapsamında belirlenen amaçlar ile elde edilen tetkik bulgularının değerlendirilmesinin ardından tetkiki gerçekleştirilen ekip tarafından tetkik edilen tarafa sunulan faaliyet sonucudur.

Yeterlilik ve uygunluk; tetkik faaliyeti kapsamında belirlenen hedeflere ulaşılabilmesi anlamında sahip olunan bilgi ve becerilerin kullanılmasına yeterlilik denir. Bununla beraber BGYS kapsamında belirtilen şartların yerine getirilip getirilmemesi durumunu da uygunluk/uygunsuzluk durumu denir.

3.4.1.2 İç Tetkik Faaliyetinde İlgili Kişiler

İç tetkik faaliyetinin bir diğer boyutu da faaliyeti gerçekleştirecek ya da gerçekleşmesinde rol alabilecek ilgili kişilerdir. Bu çerçevede konu kapsamındaki roller tetkikçi, teknik uzman, gözlemci, rehber ve tetkik ekibi olarak özetlenebilir (TSE, 2015b, s. 74).

İç tetkik faaliyeti diğer tüm denetim türlerinde olduğu gibi çeşitli ilkelere dayanır. Bu ilkeler arasında bütünlük, adil temsil, profesyonel özen, gizlilik, delile dayalı yaklaşım ve bağımsızlık ilkeleri sayılabilir. Bu noktada yukarıda belirtilen ilkeler çerçevesinde tetkikçi de bazı özellikleri haiz olmalıdır:

- Tarafsızlık: İç tetkikçi, tetkik faaliyetini gerçekleştirirken bağımsız olmalı, tetkik edilen taraf ile arasında asla bir çıkar ilişkisi yaratacak etkileşimde bulunmamalıdır.

- Güncellik: İç tetkikçi, çalışmalarında özellikle belirlenen iç tetkik kriterlerinin oluşturulması anlamında, ilgili BGYS standartlarında ve dünyada ortaya çıkan diğer ilgili bilgi güvenliği ve yönetimi ilkelerinde meydana gelen değişim ve gelişimleri yakından takip etmelidir.
- Yapıcılık: Çalışmanın ilk bölümlerinde de bahsedildiği gibi günümüzde denetim cezalandırıcı rolünden ziyade rehberlik ve yol gösterici, iyileştirici bir özelliğe kavuşmaya başlamıştır. Bu çerçevede iç tetkikçi de kendisinden çekinilen, ceza vermek için fırsat kollayan bir konumdan ziyade, bulgularının yardımı ile ilgili kurumun BGYS alanında daha ileriye gidebilmesi, bu doğrultuda kuruma yol gösterilmesi gibi yapıcı konumda olmalıdır.
- Tetkikçinin diğer özellikleri ise aşağıdaki gibi sıralanabilir:
    - Pratiklik, dakiklik,
    - Profesyonellik,
    - Sabırlı olmak,
    - İlgili taraflara karşı anlayışlı ve nazik olmak,
    - Faaliyete başlamadan önce ilgili tüm konularda hazırlıklı olmak.

Tetkik ekibinin kendi içinde de bir görev dağılımı söz konusu olabilir. Diğer denetim faaliyetlerine benzer şekilde bir tetkik ekibi lideri ve tetkik ekibi görevlilerinden söz edilebilir. Tetkik lideri genel tabiri ile tetkikin yönetiminden sorumlu olmaktadır. Daha detaylı bir şekilde belirtilecek olursa tetkik lideri, tetkikin programının oluşturulmasından buna bağlı olarak zaman yönetiminin gerçekleştirilmesi, prosedürlerin oluşturulması ve buna uyumun sağlanması, tetkik gizliliğine riayet edilmesi, tetkike ilişkin gelinen noktayı belirtme amacıyla ara değerlendirilmelerin yapılması ve bulguların derlenme, raporun hazırlanma ve sonucun bildirilmesi kısımlarını kapsayan raporlama aşamalarını yönetmek ile yetkilidir.

Tetkik liderinin yukarıda belirtilen görev ve sorumlulukları yanında heyetin diğer üyelerinin de bazı ve görev sorumlulukları söz konusudur. Öncelikler tahmin edileceği üzere tetkik görevlerinin tetkikin her aşamasında tetkik liderine destek vermekle sorumludurlar. Bunun yanında tetkik görevlilerinin; tetkike hazırlık yapmak, tetkik zamanına uyum göstermek, tetkik liderinin verdiği görevleri

zamanında ve tam olarak yerine getirmek, tetkikin gizliliğini devam ettirmek ve bu konuda gerekli özeni göstermek, yeterli tetkik delili toplamak ve onları tetkik lideri ve ekip ile paylaşmak gibi sorumlulukları söz konusudur.

Tetkikçi ve tetkik ekibi bir iç tetkik faaliyetinin tetkik eden tarafı iken, doğal olarak diğer tarafta da tetkik edilen kurum ya da organizasyon bulunmaktadır. Tetkik edilen taraf olarak tanımlanan bu kişi ya da kurumunda bazı görev ve sorumlulukları bulunmaktadır. Öncelikle tetkik edilen taraf hesap verilebilirliğin bir organizasyonun en güçlü yanlarından biri olduğunu en üst yönetimden aşağı doğru tüm kademelerde bu bilincin yerleşmesinde etkin bir eğitim faaliyeti içinde olmalıdır. Bu çerçeve de tetkik edilen tarafın; tetkik ekibinin sorularına yeterli ve zamanında cevap verme, tetkik ekibine tetkike hazırlık aşamasında talep edilen konularda yardımda bulunma, organizasyon içinde ilgili bölüm ve faaliyetleri açıklama, iletişim noktasında olabildiğince açık olmak ve faaliyet sonucu raporlanan eksiklerin giderilmesi amacıyla olabildiğince hızlı ve etkin çalışılması konularında sorumlulukları söz konusudur.

3.4.2 İÇ TETKİK FAALİYETİNİN AŞAMALARI

İç tetkik faaliyeti daha önce de belirtildiği üzere tetkik faaliyetinin iki türünden biridir. Diğer tetkik türüne ise dış tetkik denilmektedir. Dış tetkik ise kendi içinde ikiye ayrılmaktadır. Tetkikin hangi tarafça gerçekleştirdiğine göre bu kırılım tanımlanmaktadır. Eğer tetkik bir belgelendirme kuruluşu tarafından gerçekleştiriliyorsa üçüncü taraf, müşteri ya da tedarikçinin tetkiki olarak gerçekleşiyorsa ise 2.taraf tetkiki olarak açıklanabilir. Kurum için tetkik ise tanımı itibarıyla da birinci taraf tetkiki olarak değerlendirilebilir.

İç tetkik faaliyetinin aşamaları diğer denetim süreçlerinde benzer şekilde oluşturulmuştur. Öncelikle iç tetkik prosedürlerinin oluşturulması gerekmektedir. İzleyen aşamada plan hazırlanır ve tetkike ilişkin tüm prosedürler ve kriterler değerlendirilir. Tetkik faaliyetine ilişkin zaman planlaması yapılır, bu plan tetkik edilecek tarafın iş ve işlemlerine ilişkin yeterli bilgi alınarak ve geçmiş dönemde neticelenen iç tetkik raporları dikkate alınarak düzenlenir. İzleyen süreçte tetkik

heyeti oluşturularak faaliyete başlanır. İç tetkik faaliyetlerinin aşamalarına aşağıda kısaca değinilmektedir.

3.4.2.1 Planlama

İç tetkik faaliyetinin ilk aşaması olan planlama aşamasında, iç tetkik lideri daha önceden bilgisi dahilinde olan tetkik programı çerçevesine gerçekleştireceği iç tetkik faaliyetinin zamanına ilişkin bir plan oluşturur. İç tetkik hazırlığı aşamasından önce gelen bu aşamada gerçekleşecek tetkikin başlama zamanı, tahmini olarak ne kadar sürede tamamlanması planlandığı ve diğer ilgili zamansal kısıtlar değerlendirilir. Tüm bu değerlendirmeler için tetik eden tarafın katkısı yanında tetkik edilen tarafın da katkısı gerekmektedir.

Tetkik edilen taraf ile ilk temasını kuran tetkik heyeti, kurumun tetkike ilişkin olarak uygunluk durumunu verilen tarihler için sorar. Karşı taraftan gelen uygunluk durumu cevabına göre de tetkikin planlanan tarihlerde gerçekleştirilip gerçekleştirilemeyeceği ortaya çıkmış olur.

Uygunluk durumunun teyidinin ardından iç tetkik lideri, tetkike ilişkin zaman programını oluşturur. Tetkikin tahminen kaç gün süreceği, sorulan sorulara ilişkin olarak karşı tarafın cevaplaması için tahminen ne kadar zaman ayrılacağı gibi konularda planlama gerçekleştirilir.

Planlama aşaması zaman kısıtlarının değerlendirilmesi ile beraber bir sonraki aşama olan iç tetkik hazırlık aşamasına geçilmesi uygun olur.

3.4.2.2 Hazırlık

İç tetkik planlama aşamasının ardından, faaliyetin ikinci aşamasın olan hazırlık aşamasına geçilir. Hazırlık aşamasında ilk olarak tetkik ile ilişki dokümanların gözden geçirilmesi gerekmektedir. Söz konusu belgeler arasında aşağıdaki dokümanlar sayılabilir (TSE, 2015b, s. 77):

- Eğer gerçekleşmişse ilgili kurum ya da organizasyonda geçmiş dönemlerde gerçekleşmiş iç tetkik faaliyetleri sonuncunda oluşturulan nihai iş tetkik raporları,
- Tetkik edilecek tarafa ait eğer kurumun tamamı ise kurumsal doküman ve prosedürleri içerecek belgeler, eğer kurumun içinde bir birim ya da bölüm ise bu bölümü ilgilendiren prosedürler ve dokümanlar,
- İç tetkik faaliyetinin esasını oluşturan ilgili standarda ait doküman,
- İç tetkiki gerçekleştiren organizasyonun prosedürleri gereği kullanması gereken tüm dokümanlar.

Yukarıdaki maddelerde adı geçen ilgili standart, BGYS iç tetkik faaliyeti çerçevesinde ISO 27001:2013 standardıdır. Söz konusu standart çalışmanın daha önceki kısımlarında da ele alındığı üzere 10 ana madde ve bir ekten oluşan bir bütündür. İç tetkik faaliyetinde işte bu maddeler ve ekinde yer alan referans kontrol hedefleri ve kontroller incelenir ve gözden geçirilir. Anılan standardın ekinde yer alan kontroller aslında ISO 27002:13 standardının 5.den 18.e kadar olan maddelerden oluşturulmuştur (TSE, 2013, s. 10). ISO 27002:13 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği İçin Uygulama Kodu isimli standart, 18 maddeden oluşan ve iç tetkik faaliyetine temel teşkil edebilecek bilgi güvenliği uygulama kodlarını içeren bir kurallar bütünüdür. Söz konusu 18 maddeden 14'ü güvenlik kontrol maddesi olup toplamda 35 ana güvenlik kategorisini ve 114 kontrolü içermektedir.

Tetkik ekibi gözden geçirmesi gereken belgeleri tamamlayarak, iç tetkike ilişkin soru listelerinin hazırlanması için söz konusu dokümanları detaylı olarak inceler ve değerlendirir. Bu değerlendirme sonrasında iç tetkik soru listeleri hazırlanır. Soru listelerinde diğer denetim faaliyetlerinde de temel izlenmekte olan yol olan hali hazırda kurumda izlenmekte olan prosesler ve uygulamalar ile kurumun tabii olduğu mevzuat ya da prosedürler ile alınmak istenen sertifikanın gereklerinin karşılaştırılmasına yönelik sorular soru listelerin esasını oluşturur. Örneğin "dokümante edilmiş bir BGYS sistemi kurumunuzda mevcut mudur" sorusu iç tetkik faaliyeti çerçevesinde soru listelerinde yer alabilir. Yukarıda da belirtildiği bu soru listelerinin oluşturulması için belli bir hazırlık süreci gerekmektedir. Bununla beraber

soru listelerinin hazırlanmış ve uygulanmakta olması tetkik ekibine bazı faydalar sağlar. Söz konusu faydalar aşağıda belirtilmektedir (TSE, 2015b, s. 78):

- Öncelikle tetkik heyetinde bu şekilde bir dokümanın hazır olması, tetkik sonunda oluşturulacak olan nihai rapora esas teşkil eder,
- Listenin hazırlanması aşamasında yukarıda da belirtildiği üzere belirli derecede bir belge taraması gerektirdiğinden dolayı, tetkik ekibini iç tetkik faaliyetine hazırlamış olur,
- Tetkik faaliyetinin zaman boyutuna ilişkin olarak belirli bir plan çerçevesinde devam etmesini sağlar,
- Soruların tetkik edilen tarafa açık bir şekilde iletilmesi, tetkikçiye olan güveni artırır ve tetkik amaçlarının sorular üzerinden açık ve net bir şekilde görülmesini sağlar,
- Son olarak da elde edilen soru listesi, ileriki iç tetkikler için bir rehber niteliği taşır, özellikle yeni iç tetkik görevlileri için soru listesinin oluşturulmasında yardımcı belge olarak değerlendirilebilir.

Belirtildiği üzere iç tetkik soru listelerinin gerek iç tetkik heyeti gerek ise de tetkik edilen taraf açışından olumlu yönleri bulunmaktadır. Bununla beraber iç tetkik soru listelerinin belirli özellikleri haiz olması beklenmektedir. Özellikle ilgili standart şartına, kurum içi proses şartlarına, kurum faaliyetlerinde kurumun uymakla yükümlü olduğu yasal mevzuata, kurumun kuruluş amaçlarına uygun sorular oluşturulmalıdır.

Çoğu süreçte olduğu üzere iç tetkik soru listelerinin değerlendirme aşamasında da çeşitli riskler ve yanlış uygulamalar görülebilir. Özellikle soru listelerinin tik atılmalı ya da evet hayırlı seçenekli sorular şeklinde olması, dokümanın dikkatli bir şekilde cevaplandırılmayarak, daha ziyade kutucuklara tik atılarak geçilmesi ya da evet-hayır seçeneklerinin işaretlenmesi şeklinde yüzeysel değerlendirilmesine neden olabilir (TSE, 2015b, s. 78).

3.4.2.3 Uygulama

İç tetkik faaliyetinin planlama ve hazırlık aşamalarının ardından uygulama aşaması söz konusu olmaktadır. Uygulama çok kısa bir şekilde belirtilecek olursa, iç tetkik açılış toplantısıyla başlayan izleyen süreçte tetkik faaliyeti ile devam eden ve nihayetinde kapanış toplantısı ile tamamlanan bir süreçtir.

Şekil 17: Tetkik Faaliyeti

Açılış toplantısı diğer denetim türlerinde de olduğu gibi sürecin ilk ve karşılıklı güveninin temini açısından belki de en önemli adımlarından biridir. Çünkü açılış toplantısında öncelikle tetkik eden ve edilen taraflar birbirleri ile tanışma imkânı bulurlar ve karşılıklı görüş alışverişinde bulunabilirler. Tanışma safhasının yanında açılış toplantısında tetkik edilen taraf tetkikin izleyeceği program ve prosedürler hakkında bilgilendirilir. Tetkik ekibinin kurum içinde kimlerle ile iletişim haline olacağı netleştirilir. Gerek iç tetkik gerek ise diğer denetim türlerinde denetim iletişim kanallarının net bir şekilde belirlenmesi, tetkik ya da ilgili denetim faaliyetinin sağlıklı yürüyebilmesi açısından çok önemlidir. Tetkik heyeti ortaya çıkan soruların tam olarak hangi bölüme iletilmesi gerektiğini öngöremeyebilir, bu konuda belirlenen bir iletişim kişisinin yardımı ile söz konusu sorular ilgili bölüme ya da birime iletilebilir. Sorulan sorulara tetkik edilen tarafından verilen cevaplar ya da talep edilen bilgi ve belge de yine aynı yol üzerinden tetkik heyetine iletilebilir.

İç tetkik açılış toplantısında yukarıda değinilen konularından haricinde diğer bazı konuların da netleştirilmesinde ya da tarafların bilgilendirilmesinde fayda görülmektedir. Örneğin iç tetkik ekibi öncelikler tetkik esnasında yararlanacakları bilgi ve belgenin kendilerine temin edilebileceğinin teyidini tetkik edilen taraftan almalıdır. Aksi takdirde iç tetkik tamamlanamama riskiyle karşı karşıya kalabilir. İç tetkik heyetine, faaliyetlerinde yardımcı olması beklenen iç tetkik rehberlerinin görevlendirilmesi ve görev tanımlarının netleştirilmesi gerekmektedir. Tetkik heyeti

gerçekleştireceği tetkik hakkında tetkik edilen tarafa işleyiş ile ilgili konularda detaylı bilgi vermelidir. Bu konular aşağıdaki gibi belirtilebilir (TSE, 2015b, s. 79);

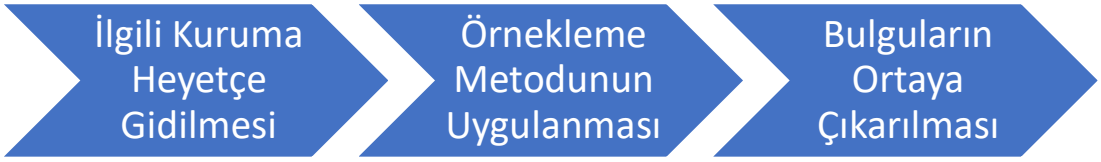
- Uygulanacak metotlar,
- Uyulması gereken ilkeler,
- Tetkik faaliyetinin nasıl sonlandırılacağı,
- Karşılıklı iletişim yollarının netleştirilmesi,

İletişim konusunun önemi tetkik heyeti açısından çok net bir şekilde anlaşılmalıdır. İletişim tüm denetim faaliyetlerinde esas unsurlardan biri olarak değerlendirilebilir. Bu konuda ortaya çıkabilecek bir aksaklık tüm faaliyetin doğru olmayan bir zemine oturmasına neden olabilir. Bu çerçevede tetkiki gerçekleştiren kişiler karşı taraf ile sağlıklı bir iletişim kurmayı sağlayacak tutum ve davranışlar geliştirmelidirler.

İç tetkikçiler, iletişim noktasında öncelikle tetkik edilen tarafa her zaman nazik ve anlayışlı olmalıdır. Nezaket bir zayıflık olarak algılanmamalıdır. Çalışmanın ilk bölümünde de değinilen klasik teftiş anlayışının iletişim algısındaki sert ve cezalandırıcı tavrın yerine günümüz denetim anlayışında iletişimin sağlıklı temeller üzerine kurulması açısından faydalı olabileceği düşünülmemektedir. Nazik ve anlayışlı olmak iç tetkikçilerin kararlı ve sorgulayıcı olmasının önüne bir engel değildir. Aksine konusunda hâkim bir tetkikçi sorularını kararlı bir şekilde karşı tarafa iletilebilmelidir. Faaliyetleri kişisel boyuta taşımadan tamamen işe odaklı bir şekilde gerekli çalışmalarını sürdürmelidir. Bu çalışmalarda da en önemli etken muhakeme sürecinin çok dikkatli ve detaylı şekilde gerçekleştirilmesidir.

İletişim açısında iç tetkikçinin ya da tetkik edilen tarafın kaçınması gereken temel kavramlar söz konusudur. Özellikle karşı tarafa karşı nezaketten uzak bir şekilde saldırgan davranmak, gereğinden fazla ısrarcı olmak, karşı tarafın görüşlerine gereken değeri vermemek, ben merkezci bir yaklaşım benimsemek, kişilerin kutsallarına ya da siyasi görüşlerine ilişkin olumsuz bir yaklaşım sergilemek, ortaya sorun çıkarabilecek ve rekabet temelinde yer alan spor ve ya benzer konulara değinmek, tetkik eden ve edilen taraflar arasında oluşacak iletişime zarar verecek tutum ve davranışlardır (TSE, 2015b, s. 82).

Açılış toplantısı ve ilk iletişimin kurulmasının ardından iç tetkik heyeti saha denetimine başlama aşamasına geçer. Saha tetkiki, iç tetkik faaliyetinin asıl amaçlarından biri olan tetkik bulgularını ortaya çıkarılmasına yönelik olarak, seçilen örneklem çerçevesinde ilgili kurum ya da organizasyona gidilerek gerekli çalışmaların yapılması olarak açıklanabilir.



Şekil 18: Saha Tetkiki

İlgili kuruma heyetçe gidilmesi aşamasında, iç tetkik heyeti ilgili kurumun görevlendirdiği rehber ile birlikte, iç tetkik faaliyeti süresince görmek istediği konulara ilişkin olarak sırayla çalışmalarına başlar. Üzerinde daha derinlemesine durulmasını gerek gördüğü konularda incelemelerini yoğunlaştırırken, herhangi sorun teşkil etmediğini düşündüğü konuları ise bir diğerine geçmek üzere tamamlar. Daha önce de belirtildiği üzere temel yaklaşım belirlenen standartlara ve kriterlere ilişkin bir uygunsuzluk bulmayı amaçlamak değil, yapıcı ve rehberlik sağlayıcı bir tutum içinde bulunmalıdır. İç tetkik heyeti faaliyetine başlamak için ilgili organizasyona ulaştığında halihazırda belirlenmiş bir örneklemi söz konusu olmalıdır. Çünkü tetkiklerde tüm denetim evrenini kontrol edilmesi gerek personel gerek ise de işlem ve zaman boyutları açısından oldukça zordur. Bunun yerine iç tetkik lideri, tetkik ekibinin yardımı ile denetim evreninden bütünü temsil edecek şekilde bir örneklem seçer bu örneklem üzerinden iç tetkik faaliyetini gerçekleştirir.

Uygulama aşamasının bir diğer bölümü de bulguların ortaya çıkarılmasıdır. Bulguların ortaya çıkarılması aşağıdaki tabloda yer alan 4 yol üzerinden gerçekleşebilir (TSE, 2015b, s. 80):

Şekil 19: Bulguların Ortaya Çıkarılması

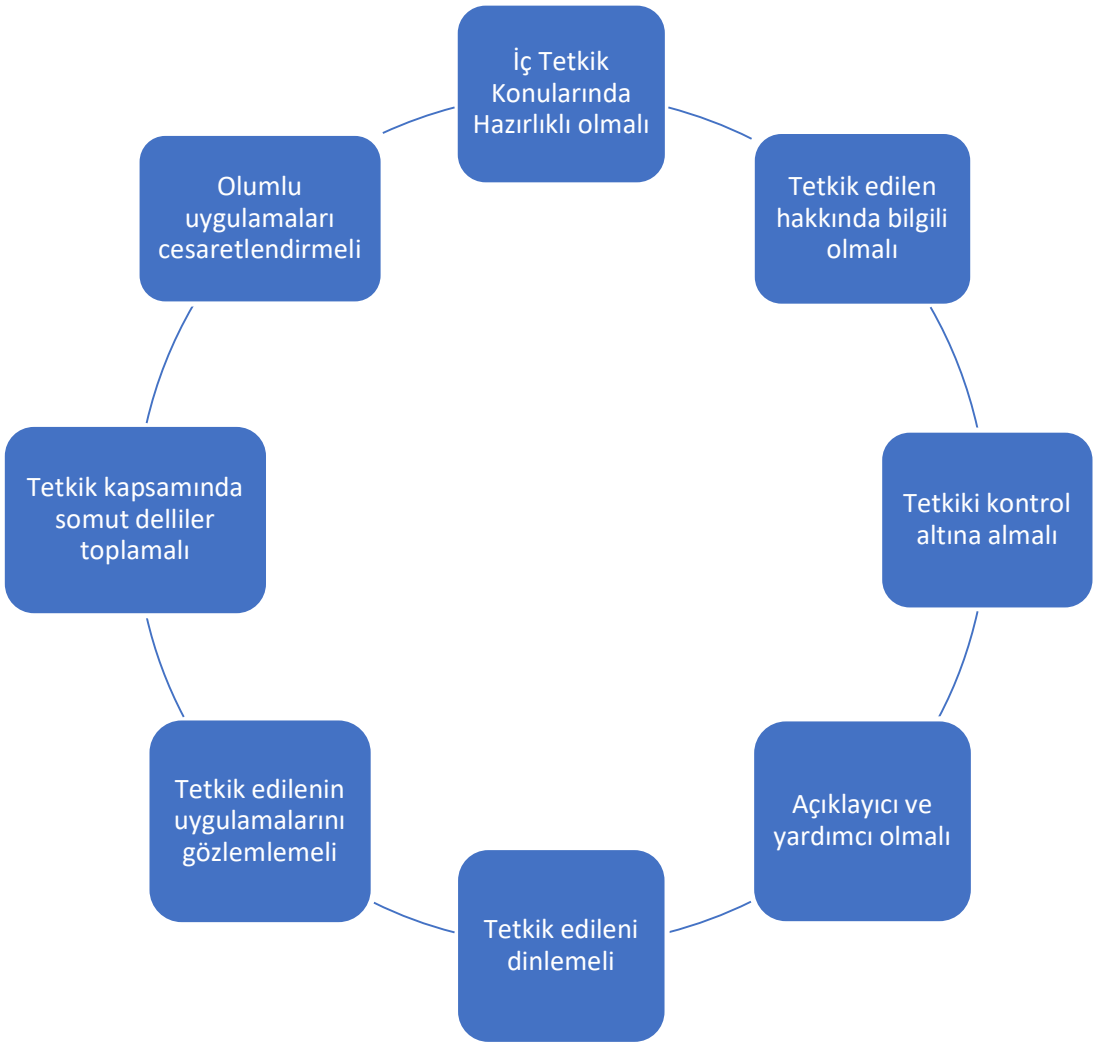
Şekil-19'da görüldüğü üzere iç tetkik uygulama sürecinin dört farklı ayağı bulunmaktadır. Bunlar yüz yüze görüşme, dosya ve işlemlerin incelenmesi, altyapı ve iş ortamının incelenmesi ve diğer iletişim yollarıdır.

Yüz yüze görüşme diğer bir deyişle karşılıklı görüşme iç tetkik ekibinin tetkik faaliyeti kapsamında, kendilerine en uygun ve açık cevabı verebileceğine inandıkları ve tetkiki gerçekleştirdikleri konulara hâkim olabilecek uygun düzeydeki kişiler ile gerçekleştirecekleri mülakatlardır. Klasik teftiş anlayışından farklı olarak müfettişin ifade almasından farklı olarak burada ilgili kişiye yapılan görüşmenin neticesi paylaşılır ve beraber gözden geçirilir. Görüşmede öncelikler kişinin ilgili konu hakkında yapacağı tarif dinlenir ve konu ile ilgili net sorular sorulur, soruların dolaylı değil doğrudan olması önemlidir. Görüşme yeri ve saati anlamında ise öncelikle mesai saatleri içinde ve ilgili kişinin çalışma alanında yapılması karşı tarafın daha rahat hissetmesini sağlamaktadır. Görüşme sonunda tutulan notlar karşı taraf ile paylaşılır. Görüşme esnasında karşı tarafa sorulacak sorulara ilişkin olarak dikkat edilmesi gereken noktalardan bazıları arasında; konulu sorular, genişletici sorular, kanaat soruları ve araştırma soruları belirtilebilir (TSE, 2015b, s. 83).

Konulu sorular, tetkik edilen kurumda yapılmakta olan bir faaliyete ilişkin açıklayıcı bilgi talep edilmesidir. Örneğin, bilgisayar kullanıcı şifreleme sürecini nasıl yapıyorsunuz şeklinde bir soru sorulabilir.

İç tetkik uygulamasının bir diğer aşaması da dosya ve işlemler ile altyapı ve iş ortamlarının incelenmesidir. Bu bağlamda iç tetkik heyeti, tetkik faaliyetinin gerçekleşmekte olduğu kurum ya da organizasyon bünyesinde konu ile alakalı tüm dokümanları ve kayıtları incelemelidir. İlgili personelin iş ortamını, belirtilen prosedürlere uyulup uyulmadığını, bir diğer deyişle belirlenen prosedürlerin kâğıt üzerinde kalıp kalmadığı değerlendirilmelidir. Dolayısıyla iç tetkik faaliyetinin uygulama safhasında iç tetkik heyetine düşen soru listelerinin de yardımı ile tüm iş ortamını ve altyapıyı incelemek, bilgi ve belgeyi incelemek, gerekli durumlarda not tutarak objektif delillere ulaşmaya çalışmaktır.

İç tetkik heyeti ne yapmalıdır sorusuna kısaca aşağıdaki yanıt verilebilir (TSE, 2015b, s. 82):



Şekil 20: İç Tetkikçilerin Yetkinliği

Şekil-20'de belirtildiği üzere iç tetkik heyeti özetle; hazırlıklı, bilgili, kontrollü, yardımcı, dinleyici, gözlemci, delil toplayıcı ve cesaretlendirici olmalı ve bu doğrultuda hareket ederek başarılı bir iç tetkik faaliyeti gerçekleştirmelidir.

İç tetkikin uygulama safhasının bir diğer önemli unsuru da tetkik delillerinin toplanması ve olası uygunsuzlukların ortaya çıkarılmasıdır. Tetkik delillerinin tanımı ve açıklamasına çalışmanın önceki bölümlerinde incelenmiştir. Tetkik delillerinin toplanmasına ilişkin olarak ise iç tetkik heyetinin üzerine düşen bazı sorumluluklar bulunmaktadır. Öncelikle iç denetim faaliyetlerinde gerekli inceleme çalışmalarının yapılması aşamasında da benzer şekilde olduğu üzere tetkikçiler gerek gözlem

gerek ise de sorularına ilişkin olarak söz konusu kurum ya da organizasyonun çalışanlarından yardım almalıdır. İletişimde yaşanan aksamaların tetkikin gidişatını olumsuz etkilemesine izin verilmemelidir. Tüm deliller detaylarıyla birlikte kayıt altına alınmalıdır. Uygunsuzluğun kaynağı ve neden ortaya çıktığı konusunda detaylı inceleme yapılmalıdır. Delillerin detaylı bir şekilde kayıt altına alınmasına tetkik notları oluşturulması süreci denir. Tetkik notları, iç denetim uygulamalarında değinilen çalışma kağıtlarına benzer. Bu notlar açık bir şekilde okunabilir ve teyit edilebilir olması halinde devam eden tetkik faaliyetlerine yardımcı belge olarak kullanılabileceği gibi tetkikin ilerleyen aşamalarında ya da ileri de gerçekleşecek başka denetim çalışmalarında da yardımcı belge olarak değerlendirilebilir. Bu noktada tetkik delillerinin detaylı bir şekilde kaydedilmesi kavramının bir örnekle ile ele alınması yerinde olacaktır.

Örneğin kötü niyetli bir yazılım saldırısı sonucu zarar gören bir donanımın halihazırda kullanılmaya devam edildiği tespit edilmiş ve bu konuda tetkik delili toplanması gereği doğmuştur. Öncelikler kötü niyetli yazılım bulaşan donanıma ilişkin gerek tetkik edilen tarafın verdiği bilgiler gerek ise donanım üzerinde yazılı halde bulunan marka, isim, seri numarası ve demirbaş numarası gibi bilgiler açık bir şekilde kayıt altına alınmalıdır. Ardından söz konusu duruma ilişkin tetkik edilen tarafa ait prosedürler ve bu prosedürlere ait alt belge ve evrakların sayı ve numaraları not alınmalıdır. Son olarak da donanımı kullanmakta olan personelin bilgileri kayıt altına alınır. Görüldüğü üzere delilin objektif olarak tutulabilmesi için ilgili tüm detaylar net bir şekilde kayıt altına alınmalıdır.

Tetkikin raporlama ve takip aşamasından önceki son safhası uygunsuzlukları belirleme safhasıdır. Uygunsuzluklar, tetkik delillerinin tetkik kriterleri temel alınarak değerlendirilmesi ve var ise ortaya çıkan farklılıkların kayıt altına alınması süreci olarak özetlenebilir. Bu süreçte gerçekleştirilen değerlendirme faaliyeti tetkik kriterlerinin tüm standart şartlarını, kurum ya da organizasyonun işlem proseslerini, faaliyetlerini ve saha gözlemlerini kapsayabilir. Bu kapsam iç tetkik faaliyetinin amacına göre belirlenir. Örneğin sadece yazılım güvenliğine yönelik bir iç tetkik faaliyeti gerçekleştirilecekse bu durumda ilgili standardın yazılıma ilişkin maddeleri,

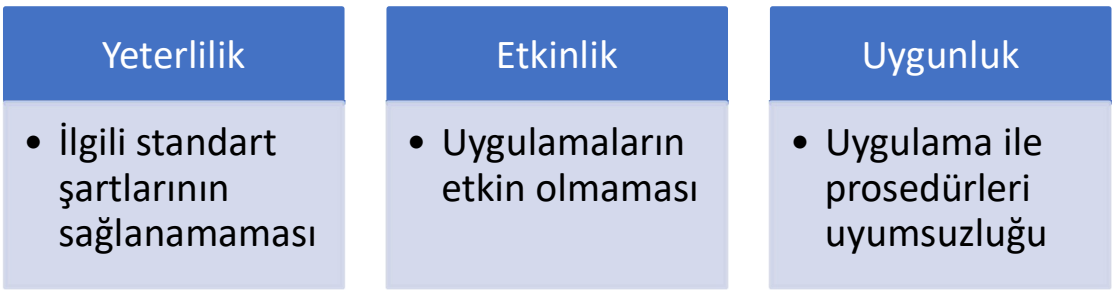
ilgili kurumun yazılım güvenliğine ilişkin prosedürleri, yine benzer şekilde iş ve işlemleri ve son olarak da saha gözlemleri bu iç tetkikin kapsamını oluşturur. Söz konusu değerlendirmeler sonucu uygunsuzluğu belirtir bulgular ortaya çıkar ve bu bulgulara tetkik bulguları adı verilir. Tetkik bulguları, yukarıda da belirtilmiş olan tetkik kriterlerine olan uygunluğu ya da uygunsuzluğu temel almalıdır. Uygunsuzluk söz konusu olan bir durumda bu uygunsuzluğun tüm destekleyici bilgi ve belgesi de kayıt altın alınmalıdır. Ayrıca oluşturulacak raporda kullanılmak üzere anılan bulguların önem dereceleri ve alınması gereken aksiyonların aciliyetine göre bulgular arası derecelendirme de yapılmalıdır. Ortaya çıkarılan bulgularda yer verilen uygunsuzlukların, tanımlanması aşamasında bazı noktalara önem verilmelidir. Bunlar aşağıdaki gibi sıralanabilir (TSE, 2015b, s. 87):

- Uygunsuzluğun tam ve net olarak ifade edilmesi,
- Tespitin açıklanması ve uygunsuzluk olarak tanımlanmasına neden olan unsurların belirtilmesi,
- Tespitin tam olarak kurum ya da organizasyonun hangi bölümünde ve hangi tarihlerde tespit edilmesi,
- Ortaya çıkan bulguya ilişkin ne gibi bir düzeltici işlemin uygulamasının önerilmekte olduğu,
- Ve önerilen düzeltici işlem ya da işlemler ile ne gibi düzeltici aksiyon alınmış olacağının,

Belirtilmesi gerekmektedir. Ortaya çıkarılan bulgularsa dayanak teşkil eden uygunsuzluklar çeşitli nedenlerden kaynaklanabilir. Bu dayanaklara (TSE, 2015b, s. 85),

- Standardın şartlarına uymama,
- Yasal mevzuatın gereklerine uymama,
- Kurum ya da organizasyonun kendi oluşturmuş olduğu şartlara uymama,
- İç tetkikin gerçekleştirilmesini talep eden müşterinin belirlemiş olduğu şartlara uymama,

Gibi örnekler verilebilir. Bununla beraber uygunsuzlukların kaynaklarına göre sınıflandırılmasının yanında içerik anlamında da sınıflandırılması söz konusu olabilir (TSE, 2015b, s. 85):



Şekil 21: Uygunsuzluk Türleri

Şekil-21'de Görüldüğü üzere uygunsuzluklar 3 temel açıdan sınıflandırılmaktadır. Yeterlilik iç tetkik faaliyetinin gerçekleşmekte olduğu asıl amaç olan ilgili standartlara uyumun sağlanması anlamında ortaya çıkarılan bulguları işaret etmektedir. Etkinlik ise halihazırda ve günlük düzeyde devam etmek olan uygulamaların hedeflenen kriterlere uyup uymadığının değerlendirilmesidir. Son olarak uygunluk ise iç denetim faaliyetinin türlerinden biri olan uyum denetimi ile benzerlik göstermektedir. Kurum ya da organizasyonda halihazırda uygulanmakta olan prosedürlerin, ilgili mevzuata ya da standart şartlarına uyumlu olup olmadığı bu tür uygunsuzlukların işaret etmiş olduğu alanlardır.

3.4.2.4 Raporlama ve İzleme

Raporlama süreci, iç tetkik faaliyetinin sona erme aşamasında ele alınmakta olan bir çalışmadır. Raporlama tetkik faaliyetinin sonunda nihai rapor olarak hazırlamakla beraber, tetkik faaliyeti devam ederken de tetkik gelişimine ilişkin ara raporlar düzenlenebilmektedir. Söz konusu toplantılara ara değerleme toplantısı denilmektedir. İç tetkik faaliyeti açısından zorunlu olmasa da çalışmada o noktaya kadar gelinmiş süre içerisinde karşılaşılan uygunsuzlukların değerlendirilmesi açısından önem arz etmektedir. Uygunsuzlukların bu şekilde ara süreçlerde gözden geçirilmesi, olası yanlış anlaşılmalardan kaçınılmasını sağlamakla beraber tetkik edilen tarafa, tetkik heyetinin içinde bulunduğu bazı yanlış anlaşılmaları düzeltme

imkânı sağlar. Bu şekilde belki de ileride ortaya çıkabilecek büyük problemler daha ileri boyuta yönlenmeden sonlandırılmış olur.

İç tetkik kapanış toplantısından önce iç tetkik ekibi iç tetkik raporunun hazırlaması için bir araya gelir. Bu genel gözden geçirme faaliyetinde iç tetkik heyeti üyelerinin elde ettikleri tetkik bulguları ile kriterler bir kez daha gözden geçirilir ve uygunsuzluklara ilişkin heyetçe mutabakat sağlanır. Tetkik sonuçları üzerinde mutabakata varıldıktan sonra var ise bulgulara ilişkin tavsiyeler netleştirilir.

Bulgular ve var ise tavsiyeler netleştikten sonra tetkik ekip liderinin öncülüğünde iç tetkik raporu hazırlanır ve hazırlanan rapor gözden geçirilir. İç tetkik faaliyet raporu oluşturulduğunda rapor içeriğinde, iç denetim raporlarında da benzer şekilde olduğu üzere, tetkik faaliyeti süresince tetkik edilen kurum ya da organizasyon bünyesinde görüşülen kişiler, tetkikin içeriğine ilişkin hazırlanmış olan tetkik programı, tetkikisin bir standart çerçevesinde yapılıyorsa standarda ilişkin ya da müşteri için yapılıyorsa müşterinin talebine ilişkin hazırlanan soru listeleri ve uygunsuzlukların sıralandığı bulguları içeren kısım ile beraber rapor bütün halini alır (TSE, 2015b, s. 87).

Kapanış toplantısı için karşılıklı uygun görülen bir tarih belirlenir ve tetkik edilen kurum ya da organizasyon bünyesinde kapanış toplantısı gerçekleştirilir. Kapanış toplantısında yine tüm iç tetkik sürecinde olduğu gibi tetkik heyeti anlayışlı ve nazik bir tavır ve üslup içine olmalıdır. Açılış konuşmasını tetkik lideri gerçekleştirir ve ardından elde ettikleri bulguları tetkik edilen tarafa açıklar. İç tetkik faaliyetinin sonucunu ve bundan sonra yapılacak işlemleri net ve detaylı bir şekilde karşı tarafa iletir. Tetkik edilen tarafta elde edilen bulgulara ya da tam olarak anlaşılamayan konuşarak ilişkin tetkik heyetine sorular ya da destekleyici bilgi ve belge iletir. Tüm konular üzerinde anlaşıldığında toplantı sonra erer.

Kapanış toplantısının tamamlanması ile iç tetkik faaliyetinin saha çalışması sonra erer ve bu aşamadan sonra ortaya çıkarılan bulguların izleme süreci başlar.

Yukarıda da belirtildiği üzere ortaya çıkarılan bulguların düzeltilmesi yönünde iç tetkik heyeti, raporunda çeşitli tavsiyeler sunmaktadır. Bu tavsiyeler ortaya çıkarılan bir uygunsuzluğun giderilmesini amaçlamaktadır. Tetkik edilen taraf ellerine ulaşan

iç tetkik raporunda yer alan eksikler ve onlara ilişkin tavsiyeler ışığında gerekli aksiyonu almakla mükelleftir. İşte tüm bu aksiyonlar ve süreç sonunda elde edilen aşama iç tetkik heyetinin izleme faaliyetlerinde değerlendirilmektedir. Bu izleme faaliyeti periyodik olarak yapılabileceği gibi yıllık olarak da yapılabilir. İç tetkik heyeti, yaptığı izleme faaliyeti neticesinde söz konusu uygunsuzluğun giderildiğini düşünüyorsa, iç tetkik izleme raporundan söz konusu bulguyu düşürür. Eğer söz konusu henüz giderilmediğini düşünüyor ise bu durumda raporunda ilgili bulguyu açık olarak korumaya devam eder.

3.5 CUMHURBAŞKANLIĞI DİJİTAL DÖNÜŞÜM OFİSİ BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ

06.07.2019 tarih ve 30823 sayılı Resmî Gazete'de yayımlanan, 2019/12 sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri genelgesi ile gün geçtikçe dijitalleşen bilginin korunması ve güvenli bir ortamda saklanması ve sağlıklı bir biçimde kullanılması gibi temel konular ele alınmıştır.

Söz konusu genelge yirmi bir madde içermekte olup özetle (CBDDO, 2019, s. 2);

- Kritik bilgilerin depolanmasına,
- Güvenli bir ağ oluşturma ve kullanımı,
- Bulut depolama yönetimlerine yönelik düzenleme,
- Sosyal medya kullanımı,
- Siber tehditler ve alınması gereken önlemleri,
- Taşınabilir cihazların güvenliği,
- Eposta ve haberleşmeye ilişkin alınması gereken tedbirler,

Ve benzeri pek çok konuya ilişkin temel politikalar belirlenmiştir. Tüm kamu idareleri ile kritik altyapı hizmeti sağlayan organizasyonların söz konusu genelgede belirtilen konulara ilişkin gerekli önlemleri alması beklenmektedir.

Belirtilen temel kavramlara ilişkin T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) yayınlamış olduğu "Bilgi ve İletişim Güvenliği Rehberi" ile rehberin içerdiği konulara ilişkin uyumlu hale gelinmesinde temel rol oynamaktadır. CBDDO tarafından yayımlanan iki temel doküman olan "Rehber" ve "Denetim Rehber"i incelenmektedir.

3.5.1 BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ

2019/12 sayılı genelgenin çıkması ile CBDDO tarafından söz konusu genelgenin gereklerini yerine getirilmesini sağlayacak rehber hazırlama çalışmalarını yürütmüş ve 10.07.2020 tarihinde 2020/1.0 numaralı Bilgi ve İletişim Güvenliği Rehberi (Rehber) sürümü CBDDO internet sitesinde yayımlanmıştır. Doküman gelişime açık

olduğundan gerekli görüldüğünde güncellenmesi söz konusu olmaktadır. Söz konusu rehbere göre temel amaç ilgili kurumun bilgi güvenliği risklerinin belirlenerek, söz konusu risklere yönelik aksiyonların alınarak riskin etkisinin azaltılması ve bilgi güvenliğinin temel kavramları olan gizlilik, bütünlük ve erişilebilirliğin olumsuz yönde etkilendiği durumlarda milli güvenliği ve kamu düzeninin bozulması sonuçlarını doğurabilecek kritik bilgi ya da verinin güvenliğinin sağlanması amacıyla asgari güvenlik tedbirlerinin alınması ve söz konusu tedbirlerin uygulanması için gerekli süreçlerin oluşturulmasıdır (CBDDO, 2020, s. 11).

Anılan rehbere göre on iki temel hedef belirlenmiştir. Bu hedefler arasında; ürün kullanımında yerli ve milli ürünlerin kullanımının tercih edilmesi, rehberde belirtilen güvenlik tedbirlerinin derecelendirilerek ve ilgili varlık grupları ile ilişkilendirilerek uygulanması, güvenlik tedbirlerinin uygulanma süreçlerinin izlenmesi ve uygulanıp uygulanmadığının denetlenmesi, güvenlik tedbirlerinin ürün ve teknolojik bakımdan her hangi bir marka ya da teknolojiye bağımlı olmamasının sağlanması, tedbirlerin tüm kurum ve kuruluşlar bakımından uygulanabilir olması sayıların. Rehberin kendi içeriğine yönelik hedefleri arasında ise; sürdürülebilir olması, gelişen ve değişen şartlara yönelik olarak güncellenebilmesi, içeriğinin ve yapısının özgün olması, içeriğinin hem bu rehberi uygulayacak hem de bu rehbere göre denetimi gerçekleştirecek denetçilere yönelik olması ve anlaşılabilir olması ve son olarak da gerek ulusal gerek ise de küresel anlamda kabul görmüş bilgi güvenliği standartlarına uyumlu olması şeklinde belirtilebilir.

Rehber verilen hedeflerin yanında bu hedeflerin gerçekleştirilmesine yönelik olarak kurum ve kuruluşlara 24 aylık bir uyum planı önermektedir (CBDDO, 2020, s. 13). Buna göre rehberin uygulanma kararı alınmasından itibaren ilk altı aya kadar olan süreçte kurumun varlık gruplarının belirlenmesi, bu grupların kritiklik derecelendirmelerinin yapılması, mevcut durum ile olması gereken arasında bir boşluk analizi yapılması ve bu analize göre bir yol haritasının belirlenmesi gerektiği belirtilmektedir. Belirlenen yol haritasına göre altıncı aydan on sekizinci aya kadar olan sürede daha önceden derecelendirilmiş olan tedbirlerden birinci seviye olanlara ilişkin çalışmaların tamamlanması, on sekiz ile yirmi birinci aylar arasında ise ikinci

seviye tedbirlere ilişkin çalışmaların tamamlanması beklenmektedir. Son olarak da yirmi birinci aydan yirmi dördüncü aya kadar olan süreçte de üçüncü seviye tedbirlerin tamamlanması gerektiği belirtilmektedir. Rehberin uygulama süreci sonrasında denetim aşaması da uygulamada önemli bir rol oynamaktadır.

3.5.2 BİLGİ VE İLETİŞİM GÜVENLİĞİ DENETİM REHBERİ

Tedbirlerin uygulanması ve rehberin hayata geçirilmesine ilişkin olarak gerçekleştirilen boşluk analizlerinde ortaya çıkan eksikliklerin ve planlanan yol haritasının, belirlenen doğrultuda ilerleyip ilerlemediğinin izlenmesi amacıyla denetim sürecinin de dikkate alınması gerekmektedir. CBDDO Bilgi ve İletişim Güvenliği Denetim Rehberi (Denetim Rehberi) 2021/1.0 sürün numarası ile 10.10.2021 tarihinde CBDDO resmi internet sitesinde yayımlanmıştır. Denetim rehberi, ilgili kurum ve kuruluşlara denetim faaliyetlerine ilişkin olarak yol göstermek amacıyla hazırlanmış olup, bilgi ve iletişim güvenliği alanında yapılan denetim faaliyetlerinin sürekliliğine ve yeterli bir güvence seviyesinde yülütülmesini hedeflemektedir (CBDDO, 2020, s. iv). Denetim rehberine göre ilgili kurumlar denetim süreçlerini; planlama, uygulama, değişiklikleri yönetme, kontrol etme ve önleme alma aşamalarını kapsayacak biçimde gerçekleştirmelidir.

Bilgi güvenliği ve iç denetim ilişkisi özellikle Denetim Rehberi'nde bir kez daha gözlemlenebilmektedir. Buna göre rehber kapsamındaki tüm kurumlarda denetim faaliyetlerinin öncelikli olarak iç denetim birimlerinde görevli iç denetçilerce gerçekleştirilmesinin esas olduğu belirtilmiştir (CBDDO, 2021, s. 11). Ayrıca denetimi gerçekleştirecek denetçilerin ISO/IEC 27001 Baş denetçi sertifikasını ya da CISA sertifikalarını haiz olması beklenmekte olup, kamu kurum ve kuruluşlarında ise yukarıda verilen şartların birini haiz olup ya da iç tetkik veya iç denetim faaliyetlerini daha önce gerçekleştirmiş personelden oluşturulması gerektiği belirtilmiştir.

Denetim rehberinin uygulanma aşamasında denetçinin temel olarak inceleyeceği iki ana alandan bahsedilebilir. Bunlardan birincisi "Rehber Uygulama Sürecinin Etkinliği" diğeri ise varlık gruplarına uygulanmakta olan tedbirlerin etkinliğine yönelik

denetim unsurlarıdır (CBDDO, 2021, s. 29). Söz konusu 2 ana unsur başlığı altında sekiz yüz adete yakın güvenlik tedbiri yer almaktadır. Denetim sürecinde söz konusu güvenlik tedbirlerinin değerlendirilmesi ve uygulanıp uygulanmadığına göre yapılması gerekenler belirlenecektir.

4 BÖLÜM
İÇ DENETİMİN BİLGİ GÜVENLİĞİNE KATKISI: BİR ALAN ARAŞTIRMASI

Tezin bu bölümünde iç denetim ve bilgi güvenliği arasındaki ilişkiye yönelik olarak gerçekleştirilen araştırmanın amacı, önemi ve kapsamı ele alınmaktadır. Ardından araştırmanın metodolojisi açıklanmaktadır. Bu kısımda veri toplama aracı ve süreci, örneklem ve kullanılan istatistiksel teknikler açıklanmaktadır. Kapsam, yöntem ve uygulama süreçlerinin açıklanmasının ardından elde edilen verilerin analizi sonucu ortaya çıkan bulgular değerlendirilmektedir.

4.1 ARAŞTIRMANIN AMACI VE ÖNEMİ

Bu bölümde öncelikle araştırmanın amacı ve kapsamının ortaya konulmasının ardından önceki çalışmalar ve çalışmanın önemine değinilmektedir. Model ve araştırmaya ait hipotezlerin açıklanmasının ardından da araştırmanın kısıtlarına yer verilmektedir.

4.1.1 Araştırmanın Amacı

Araştırmanın temel amacı ülkemizde faaliyetlerine devam etmekte olan iç denetim profesyonellerinin, çalışmakta oldukları kurumlardaki iç denetim ve bilgi güvenliği fonksiyonlarının arasındaki ilişkinin niteliğine yönelik algılarının araştırılmasıdır. Bu kapsamda iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin niteliğini etkileyen faktörlerin araştırılması amaçlanmaktadır. Bununla beraber bilgi güvenliği ve iç denetim fonksiyonunun birlikte çalışması durumunda bilgi güvenliği etkinliği ya da iç denetimin sağladığı katma değer gibi elde edilecek potansiyel faydaların incelenmesi amaçlanmıştır.

4.1.2 Önceki Çalışmalar Ve Araştırmanın Önemi

Bu araştırmada ülkemizde faaliyetlerine devam etmekte olan iç denetim profesyonellerinin, iç denetimin bilgi güvenliği ilişkisine yönelik algıları ve söz konusu ilişkinin kurumun bilgi güvenliği faaliyetlerine katkısı değerlendirilmiştir. İç denetim ve bilgi güvenliği fonksiyonları organizasyonun bilgi kaynaklarının etkili bir şekilde yüksek seviyede bir ortak amaç taşırlar. Bu ortak amaç altında her iki fonksiyonun birbiriyle olan ilişkisi ve iş birlikleri söz konusu olmaktadır. COBIT-5 çerçevesi ve söz konusu çerçevenin 2019 yılında geliştirilmiş olan güncel versiyonu olan COBIT-2019 çerçevesinde, "bilgi ve teknoloji kurumsal çerçevesi" kapsamında iç denetim ekiplerinin sunmuş olduğu yıllık beyan yoluyla bilgi ve teknoloji yönetimi açısından yönetim kuruluna bilgi sağlamış olmaktadır (ISACA, 2019, s. 54). Ayrıca yine COBIT-2019 çerçevesine göre; iç denetim fonksiyonu, bilgi ve teknoloji kurumsal çerçevesinin yeterliliği ve etkinliği konusunda yönetim ve denetim komitesine güvence sağlamakla görevlidir (ISACA, 2019, s. 54). Görüldüğü üzere görev kapsamı gereği iç denetimin, bilgi güvenliği ile doğrudan bir ilişkisi söz konusudur.

İç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişki sürekli ve gelişmeye açık bir kapsamla devam etmektedir. Ancak bu seviyede yakın iş birliği içinde bulunan söz konusu fonksiyonlar arasındaki ilişkiye yönelik literatürde çok sayıda çalışma yer almamaktadır. Sınırlı sayıdaki çalışmalardan birinde (Donathan, 2012, s. 27) iç denetim ve bilgi teknolojileri fonksiyonları arasında iyi bir iş ilişkisi geliştirilmesinin ve sürdürülmesinin önemi savunulmaktadır. Anılan iki fonksiyon arasındaki ilişkiye ilişkin bir diğer çalışma da Steinbart ve arkadaşlarının (Steinbart ve ark., 2012, s. 241), denetçi ve bilgi güvenliği uzmanlarıyla gerçekleştirdiği derinlemesine mülakatlardır. Buna göre bazı organizasyonlarda bu iki birim arasında saygı ve iş birliği olduğu ancak bazılarında ise güvensizlik ve anlaşmazlığın görüldüğü belirtilmiştir. Bahsi geçen çalışmanın kısıtı, derinlemesine mülakatların sadece bir sektörde ve yalnızca dört kuruluşta yapılmış olması, diğer bir deyişle sınırlı bir alanın incelenmiş olmasıdır. Steinbart ve arkadaşları (2013, s. 79) izleyen dönemdeki çalışmaları ile söz konusu sınırlı alanı daha da genişletebilmek için anket yöntemi ile yeni bir araştırma gerçekleştirmişlerdir. Bu araştırma neticesinde 25 katılımcı

kuruluş sayısına ulaşılarak bir önceki çalışmada söz konusu olan 4 kuruluş sayısının yarattığı kısıtın giderilmesi hedeflenmiş olup çalışma sonucunda özetle; bilgi güvenliği uzmanlarının iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin kalitesine dair algıları ile iç denetimin bilgi güvenliği incelemesinden elde edilen katma değer ile organizasyonun bilgi güvenliği faaliyetlerinin genel etkinliğine dair algıları arasında pozitifi bir ilişki bulunmuştur. Ayrıca anılan çalışmada gelecek dönemler için yapılmasının uygun olacağı değerlendirilen araştırma önerisinde, ölçeğin bu kez bilgi güvenliği uzmanlarına değil de iç denetçilere uygulanarak, iç denetçilerin bu iki fonksiyon arasındaki algılarının ölçülmesine değinilmiştir. Steinbart ve arkadaşları (2015, s. 7) izleyen çalışmalarında iç denetçilerin algılarına yönelik bir araştırma yapmış ve 43 katılımcıya uygulanan internet tabanlı anket ile çalışmayı tamamlamıştır. Bahsi geçen araştırmada iç denetçilerin algılarının bir önceki çalışmada uygulama yapılan bilgi güvenliği uzmanları ile uyumlu olduğu görülmüştür. Aynı yazarların (2018, s. 21) üç yıl sonraki çalışmalarında da söz konusu iki fonksiyon arasındaki ilişkiye yönelik olarak İç denetim fonksiyonunun organizasyonun diğer fonksiyonları ile olan ilişkisinin, iç denetimin gerçekleştirdiği denetimin kalitesi ve iç denetim fonksiyonunun organizasyona değer katması açısından önemli bir faktör olduğu değerlendirilmektedir. Araştırma konusuna ilişkin yerli literatürde ise Kurnaz ve Dindaroğlu'nun (2016, s. 60) çalışmasında Ege bölgesinde yer alan organizasyonlardaki iç denetçi ve bilgi güvenliği uzmanları ile görüşmeler gerçekleştirilmiş ve iç denetim ve bilgi güvenliği arasındaki ilişkinin olumlu olması durumunda, organizasyonlara çeşitli faydalar sağlanacağı değerlendirilmiştir.

Bir kontrol faaliyetinin; onu tasarlayan, yöneten ya da sorumluluğuna alan kişi ya da bölümden ayrı bir birim tarafından denetlenmesi gerektiği iç denetim standartlarının temel kavramlarından biridir (IIA, 2017, s. 6). Bu çerçevede bilgi güvenliği kontrollerinin de onu tasarlayan, sahiplenen ya da sorumluluğunu alan bölümden ayrı bir birim olan iç denetim birimince periyodik olarak izlenmelidir. Bu bağlamda iç denetim, kuruluşun bilgi güvenliği faaliyetlerinin etkin bir şekilde devam ettirilmesine katkı sağlayabilir. İç Denetçiler Enstitüsü'nün oluşturduğu ve küresel anlamda genel kabul görmüş olan iç denetim standartlarında iç denetçilerin bilgi güvenliğine ilişkin

temel kavramları anlayabilecek ve kontrol eksikliğini fark edebilecek düzeyde bilgi güvenliği donanımının olması gerektiği belirtilmiştir. İşte bu sorumluluk iç denetim ve organizasyonel bir fonksiyon olarak bilgi güvenliği faaliyetlerinin arasında sürekli bir etkileşim ve ilişki olmasına neden olmaktadır. Yukarıda da belirtiği gibi iki fonksiyon arasındaki ilişkiye yönelik Steinbart ve arkadaşlarının 2013 yılında gerçekleştirdiği çalışmadan farklı olarak, ölçeğin bu kez iç denetçilere uygulanması ve daha büyük bir örnekleme ulaşılması söz konusu olmuştur.

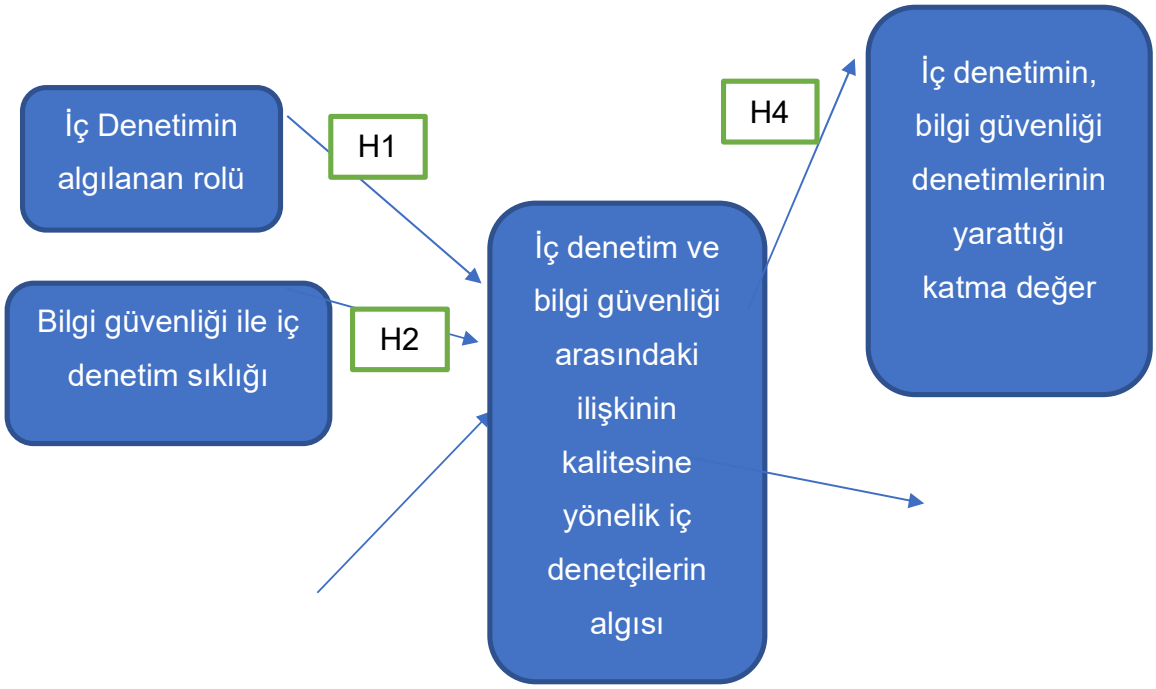
4.1.3 Araştırmanın Modeli ve Hipotezleri

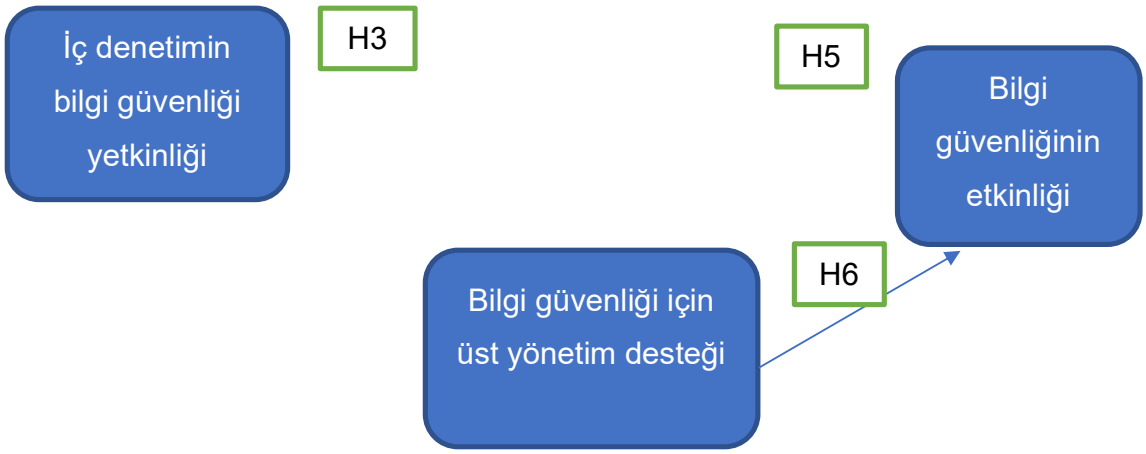
İç denetim ve bilgi güvenliği fonksiyonlarına ilişkin araştırmalar son dönemde daha sık yapılmakta olsa da iki fonksiyonun davranışsal boyutlarına ilişkin araştırmalar görece daha azdır. COBIT 5 ve COBIT 2019 çerçeveleriyle birlikte bilgi güvenliği süreçlerinin davranışsal boyutları bir diğer anlatımla bilgi güvenliği fonksiyonunun diğer paydaşlar ile olan davranışsal uyumu ya da uyumsuzluğu ele alınmaya başlanmıştır. COBIT çerçevesine göre her ne kadar organizasyonel süreçler en iyi şekilde planlanıp tasarlansa da; süreçlerin ilgili paydaşları, her hangi bir nedenle süreçlerdeki faaliyetleri tasarlanan şekilde gerçekleştiremezlerse ve dolayısıyla ortaya bir uyumsuzluk çıkarsa sürecin amaçlanan çıktıları elde edilemeyecektir (ISACA., 2012, s. 80). Bununla beraber, fonksiyonel yapısı her ne kadar en iyi örneğe göre tasarlanmış olsa da kişisel uyumsuzluklar, motivasyon eksikliği vb. sebeplerden dolayı kurumsal bilgi teknolojileri doğru bir şekilde yönetilemez (ISACA., 2012, s. 80). Fonksiyonlar arası ilişkinin işletmeyi etkileyen sonuçlar doğurmasına benzer olarak denetim sürecinde denetim ve denetlenen arasındaki iyi bir ilişki denetimin başarısını ve verimliliğini artırırken, kötü bir ilişki (örneğin denetlenenin bir bilgiyi saklaması) denetim sürecinin sağlıklı bir şekilde işlemesini engelleyebilir (Steinbart ve ark., 2013, s. 67). Denetçi denetlenen ilişkisinin niteliği, denetçinin denetlenenle olan tecrübesi (daha önceki dönemlerde de beraber denetim süreci gerçekleştirip gerçekleştirmediği) gibi faktörler de denetim kalitesini etkilemektedir (Stoel ve ark., 2012, s. 75). Denetçi-denetlenen ilişkisinde özü itibariyle karışık ve normalden yüksek bir gerginlik seviyesinde ilerleyen bir süreç söz konusu olabilmektedir. Bilgi güvenliği ve organizasyonun diğer fonksiyonların arasındaki ilişkinin de bilgi güvenliği ve bilgi teknolojileri konularının oldukça teknik

konular olması nedeniyle farklı bir karmaşıklık seviyesinde olduğu değerlendirilebilir. Dolayısıyla bilgi güvenliği ve diğer ilgili paydaşlar arasındaki ilişki neticesinde ortaya çıkması planlanan karşılıklı faydanın da her zaman tam olarak sağlanamadığı belirtilmektedir (Anderson, 2012, s. 44). Gerek denetim gerek ise de bilgi güvenliği fonksiyonlarına ilişkin kendi içlerindeki karmaşıklığının yanında organizasyonel yapıda birbirleriyle olan ilişkilerine ilişkin, iç denetçilerin algılarına yönelik olarak yapılan çalışmalar düşük katılımcı sayısı ile yapılan araştırılmalardır. Örneğin Steinbart ve arkadaşlarının çalışmasında (2015, s. 7) 43 katılımcı, Kurnaz ve Dindaroğlu'nun çalışmasında (2016, s. 58) ise 20 katılımcı yer almaktadır. Bu tez çalışması ile önceki çalışmalardan oldukça fazla bir örneklem sayısı olan 272 katılımcı sayısına ulaşılmıştır. Ülkemizde iç denetim profesyonellerinin anılan iki fonksiyon arasındaki ilişkiye yönelik algıları aşağıdaki iki araştırma sorusu ile incelenmektedir.

Araştırma Sorusu 1: İç denetim ve bilgi güvenliği arasındaki ilişkinin niteliğini, iç denetim fonksiyonunun hangi özellikleri etkilemektedir?

Araştırma Sorusu 2: İç denetim ve bilgi güvenliği arasındaki ilişkinin niteliği, iç denetimin bilgi güvenliği denetimleri neticesinde ortaya çıkan katma değere ve organizasyonun bilgi güvenliği yönetiminin genel etkinliğine ilişkin algılarını nasıl etkilemektedir?





Şekil 22: Araştırma Modeli

Araştırma sorularını incelemek için kullanılacak model Şekil-22'de gösterilmektedir. Modelin açıklaması ve ilgili faktörler ve hipotezler aşağıda sırasıyla açıklanmaktadır.

4.1.3.1 İç Denetim ve Bilgi Güvenliği Arasındaki İlişkinin Kalitesine Etki Eden Faktörler

Şekil-22'de iç denetim ve bilgi güvenliği arasındaki ilişkininin kalitesine etki ettiği varsayılan faktörler; (1) iç denetimin algılanan rolü, (2) iç denetimin bilgi güvenliği bilgisi ve uzmanlığı ve (3) iç denetimin bilgi güvenliği fonksiyonu ile etkileşim sıklığı diğer bir deyiş ile iç denetimin bilgi güvenliği denetimleri sıklığı olarak belirtilmektedir.

4.1.3.1.1 İç Denetçilerin İç Denetimi Konumlandırdıkları Rol

Çalışmanın önceki bölümlerinde de değinildiği üzere organizasyondaki ortak amaç doğrultusunda bölümler arası iş birliğinin olumlu sonuçlar doğurması söz konusu iken yanlış anlaşılma ve çeşitli uyuşmazlıklar organizasyon için çatışma kaynağı olarak öne çıkmaktadır. İç denetim ve bilgi güvenliği fonksiyonlarının da organizasyon içindeki ortak amacı kuruluşun kaynaklarını korumaktır (Steinbart ve ark., 2013, s. 69). İç denetimin görevleri, Uluslararası İç Denetçiler Enstitüsü tarafından hazırlanan ve küresel boyutta kabul görmüş temel kaynak olan İç Denetim Standartları'na göre; bir organizasyonun faaliyetlerini geliştirmek, söz konusu faaliyetlerine değer katmak, bu hedeflere ulaşırken objektif ve bağımsız

olmak, güvence vermek ve danışmanlık yapmaktır (IIA, 2018a, s. 1). Tanımdan da görüldüğü üzere denetim süreci ve sonunda güvence vermek faaliyetinin yanında iç denetime danışmanlık faaliyeti de verilmiştir. Denetim anlayışı çalışmanın kavramsal çerçevesinin açıklandığı önceki bölümlerinde de belirtildiği üzere geleneksel teftiş anlayışından modern denetim anlayışına doğru gelişim sergilemektedir. Buna göre denetim fonksiyonu; bulgu bulup, söz konusu bulgulara ilişkin izleme takibini gerçekleştiren bir fonksiyon olmaktan öte, yönetime danışmanlık faaliyeti sağlayan, sorunların köküne inen ve kök nedenlerini bularak, sorun büyümeden gerekli eylemlerin alınması yönünde yönetime ya da denetlenene yol gösterme faaliyeti sunan bir fonksiyon haline evrilmektedir. Üzerinde sürekli denetimin baskısını hisseden denetlenenin, bu anlayış yerine kendisiyle beraber sorunların çözümüne yardım eden, kök nedenleri araştıran ve çözümlere yönelik fikirler sunan bir denetim anlayışını tercih edeceği ve bu anlayış kapsamında denetim bölümü ile daha sağlıklı ve iyi ilişkiler kurabileceği düşünülebilir. Steinbart ve arkadaşlarının (2012, s. 235) çalışmasında bilgi güvenliği yöneticisinin iç denetimin rolünün kuralları uygulayan ve takip eden fonksiyondan çok bir danışman ya da yardımcı olarak algıladığı bir organizasyonda, iç denetim ve bilgi güvenliği fonksiyonları arasında olumlu bir ilişki bulunduğu belirtilmiştir. Çalışmamızda ise faktörün bilgi güvenliği profesyonelleri açısından değil iç denetçilerin algılarına yönelik incelenmesi aşağıdaki hipotezi ortaya çıkarmaktadır:

H1: İç denetçilerin; iç denetim fonksiyonunu mevzuatın uygulayıcısı rolünden ziyade danışmanlık rolü olarak algılamaları durumunda, iç denetim ve bilgi güvenliği arasındaki ilişkiye dair algıları daha olumludur.

4.1.3.1.2 İç Denetim ve Bilgi güvenliği Arasındaki Etkileşim (İç Denetimce Gerçekleştirilen Bilgi Güvenliği Denetimlerinin Sıklığı)

İç denetim bölümünün organizasyonda bilgi güvenliği denetimi yapma sıklığı, süreç içinde bilgi güvenliği uzmanlarıyla daha fazla etkileşim içinde olmalarını, tarafların birbirlerini daha iyi anlamasını sağlayabilir. Özellikle ilk kez yapılan denetimlerde denetlenen taraf için süreç bir bilinmezlik olarak algılanabilir. Denetçilerin hal ve

tavırlarından, denetim konularına kadar pek çok etken denetlenen için bir kaygı unsuru olabilir. Böyle bir ortamda ise denetlenen sorulan soruları geçiştirme, talep edilen belgeleri sunarken endişe duyma gibi denetçi-denetlenen ilişkini zedeleyebilecek durumlar söz konusu olabilir. Yapılan bir çalışmada iç denetim ve bilgi güvenliği fonksiyonların sık sık etkileşime girdiği bir organizasyonda iki tarafında karşılıklı bir güven oluşturduğu tespit edilmiştir (Steinbart ve ark., 2013, s. 70). Bu çerçevede oluşturulan ikinci hipotez aşağıdaki gibidir:

H2: İç denetçilerin; iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin niteliğine dair algıları, iç denetimin gerçekleştirdiği bilgi güvenliği denetimlerinin sıklığına dair algılarıyla pozitif ilişkilidir.

4.1.3.1.3 İç Denetçinin Bilgi Güvenliği Yetkinliği

IIA tarafından yayımlanmış olan İç Denetim Standartlarının 1210. maddesine göre iç denetçinin kişisel olarak sorumluluklarını etkili bir biçimde yerine getirebilmesi için gerekli bilgi beceri ve vasıfları haiz olması gerekmekte ve bununla beraber iç denetim fonksiyonu da toplu olarak kendi sorumluluklarını yerine getirmek için gerekli bilgi, beceri ve diğer vasıfları haiz olmak veya bunları edinmek için gerekenleri yapmak durumundadır (IIA, 2017, s. 7). Denetlenen tarafında, denetime gelen denetçinin temel konularda eksikliğinin hissedilmesi denetim faaliyetinin ilerleyişi açısından olumsuz bir durum yaratmaktadır. Denetlenenin, denetçi yetersiz görmesi vereceği cevapları ve alacağı aksiyonları etkileyebilecek olup iki fonksiyon arasındaki denetim süreci ilişkisi olumsuz etkilenebilir. Benzer şekilde iç denetçilerin de kendilerini denetim konularında eksik hissetmesi denetim sürecine olumsuz yansıyabilir. Bu doğrultuda 3. Hipotez aşağıdaki gibi önerilebilir:

H3: İç denetçilerin; iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin niteliğine dair algıları, iç denetçinin bilgi güvenliği hakkındaki yetkinliğine dair algılarıyla pozitif ilişkilidir.

4.1.3.2 İç Denetim ve Bilgi Güvenliği Arasındaki İyi İlişkinin Faydaları

Araştırma sorusu 1, yukarıda verilen ilk üç hipotezi kapsamaktaydı. Birinci araştırma sorusu ile iç denetim ve bilgi güvenliği arasındaki ilişki etkileyebilecek faktörler incelenmeye çalışılmıştır. İzleyen bölümde ise ikinci araştırma soruna yönelik olarak 2 hipotez oluşturulmaktadır. Söz konusu ilişkinin organizasyona sağladığı bir faydanın olup olmayacağına odaklanılmaktadır.

4.1.3.2.1 İç Denetimin Sağladığı Algılanan Katma Değer

İç denetim uygulamalarına yönelik olarak IIA tarafından geliştirilen Uluslararası Mesleki Uygulamalar Çerçevesi'ne göre iç denetimin misyonu içinde organizasyonel değeri korumak ve geliştirmek ifadesi yer almaktadır (TİDE, 2015, s. 1). Dolayısıyla iç denetimden organizasyonun değerini artırmaya yönelik faaliyetler yapması beklendiği yukarıdaki ifadeden anlaşılabilir. Söz konusu beklenti iç denetimin organizasyonun çeşitli fonksiyonlarının başarılı bir şekilde faaliyet göstermesinin sağlanması olarak da açıklanabilir. Bu çerçevede iç denetim bilgi güvenliği fonksiyonları arasındaki ilişki özelinde iyi bir ilişkinin bilgi güvenliği politikalarını uygulama ve bunlara uyum aşamasındaki sorunların çözülmesi anlamında yardımcı olacağı ifade edilmektedir (Steinbart ve ark., 2012, s. 237). Böylece sağlıklı işleyen bir bilgi güvenliği fonksiyonu ile bilginin korunması başarılmış olacak ve organizasyona katma değer sağlanabilmektedir. Bir diğer deyişle iç denetim ve bilgi güvenliği arasındaki ilişkinin niteliği, bilgi güvenliği fonksiyonunun sağlıklı çalışması, bilginin korunması ve var ise eksiklerin giderilerek bilgi güvenliği faaliyetinin iyileştirilmesi ve geliştirilmesi ile ilişkili olmaktadır. Bu çerçevede dördüncü hipotez aşağıda belirtilmektedir:

H4: İç denetim ve bilgi güvenliği arasındaki ilişkinin niteliği, iç denetçilerin, içinde bulundukları iç denetim fonksiyonunun organizasyona sağladığı katma değere dair algılarıyla pozitif ilişkilidir.

4.1.3.2.2 Algılanan Bilgi Güvenliği Etkinliği

Denetim ve bilgi güvenliği arasındaki ilişkinin sağlık bir şekilde yürümesi, denetim süreçlerinin verimli bir şekilde gerçekleşmesi ve elde edilen bulguların kök

nedenlerine inilerek temelinden çözülebilmesi, organizasyonda yer alan bilginin, bilgi güvenliğinin 3 temel unsuru olan gizlilik, bütünlük ve erişilebilirlik ilkelerine maksimum uyum sağlanması ile elde edilebildiğini göstermektedir. Örneğin ISO 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasını almış bir kurumun kendi iç denetim biriminin yıllık olarak bilgi güvenliği denetimi gerçekleştirilmesi gerekmektedir. Alınan bir sertifika gerek kuruma gerek ise de iç denetim ve bilgi güvenliğine birimlerine karşılıklı sorumluluk yüklemekte ve iki fonksiyon arasındaki ilişkinin niteliğine göre sertifikasyon süreci devam edebilmekte ya da başarısız olarak sona ermektedir. Bu çerçevede de iki fonksiyon arasındaki uyumun bilgi güvenliğinin etkinliğini artırdığı öne sürülebilir. Böylece 5. Hipotez aşağıdaki gibidir:

H5: İç denetim ve bilgi sistemleri fonksiyonları arasındaki ilişkinin algılanan niteliği; iç denetçilerin, bilgi güvenliği etkinliğine olan algılarıyla pozitif ilişkilidir.

4.1.3.3 Üst Yönetim Desteği

Üst yönetim bir yön verici olarak organizasyonun ilgili birimlerine ait faaliyetlerde rol almalıdır. Bu katılım icrai değil yukarıda da belirtildiği üzere yön verici olmalıdır. Yapılan bir çalışmada üst yönetimin bilgi güvenliğine yönelik yaklaşımının iç denetim ve bilgi güvenliği fonksiyonlarının, beraber çalışma derecelerini etkilediği görülmüştür (Steinbart ve ark., 2012, s. 240). Bu kapsamda 6. hipotez aşağıdaki şekilde oluşturulmuştur:

H6: Üst yönetimin bilgi güvenliğine yönelik desteğinin algılanan niteliği; iç denetçilerin, bilgi güvenliği etkinliğine olan algılarıyla pozitif ilişkilidir.

4.1.4 Araştırmanın Kısıtları

Araştırmanın kısıtları ele alındığından özellikle anketlerin iç denetçilere ulaştırılması ve fiziki çıktılar üzerinden anketlerin büyük bir kısmının tamamlanması planlanırken özellikle küresel pandemi döneminde ve hemen sonrasındaki dönemde yüz yüze iletişimde zorluklar yaşandığından, eposta aracılığıyla katılımcılara ulaşılmıştır. Özellikle pandemi döneminde yaşanan stres ve diğer olumsuzluklar, yüksek üye

sayısına sahip meslek örgütlerince üyelerine eposta yolu ile iletilen anketlere geri dönüşlerin düşük olmasına neden olmuştur.

4.2 METODOLOJİ

Tez çalışmasının bu kısmında öncelikle veri toplama aracı olarak anket hakkında bilgi verilecek olup ardından yöntemin ele alınacağı veri toplama süreci ve örneklem bölümü yer almaktadır. Ardından da kullanılan istatistiksel teknikler ve veri gerçekleştirilen veri analizi incelenmektedir.

4.2.1 Veri Toplama Aracı

Çalışma kapsamında iç denetçilerin algılarını ölçmek için Steinbart ve arkadaşları (2013, s. 86) tarafından geliştirilmiş olan ölçek yazarlardan izin alınarak kullanılmıştır. İngilizce dilindeki anket karşılıklı çeviri yoluyla Türkçe'ye çevrilmiştir. Ölçek aracılığıyla, görüş ve değerlendirmeler için toplamda 7 boyut ve 30 maddeden elde edilen veriler 5'li Likert derecelendirme ölçeği ile sayısallaştırılmıştır. Buna göre 30 maddenin ilgili boyutlara göre dağılımı aşağıda verilmektedir:

- İç denetimin algılanan rolü: 3 madde,
- İç denetim biriminin bilgi güvenliği yetkinliği: 2 madde,
- Üst yönetimin bilgi güvenliğine yönelik desteğinin algılanan niteliği: 6 madde,
- İç denetim ve bilgi güvenliği arasındaki ilişkinin algılanan niteliği: 3 madde,
- İç denetim fonksiyonunun bilgi güvenliği denetimleriyle kuruma sağladığı katma değer: 5 madde,
- Bilgi güvenliği faaliyetlerinin başarısı: 3 madde,
- Bilgi güvenliği denetimlerinin sıklığı: 8 madde.

4.2.2 Veri Toplama Süreci Ve Örneklem

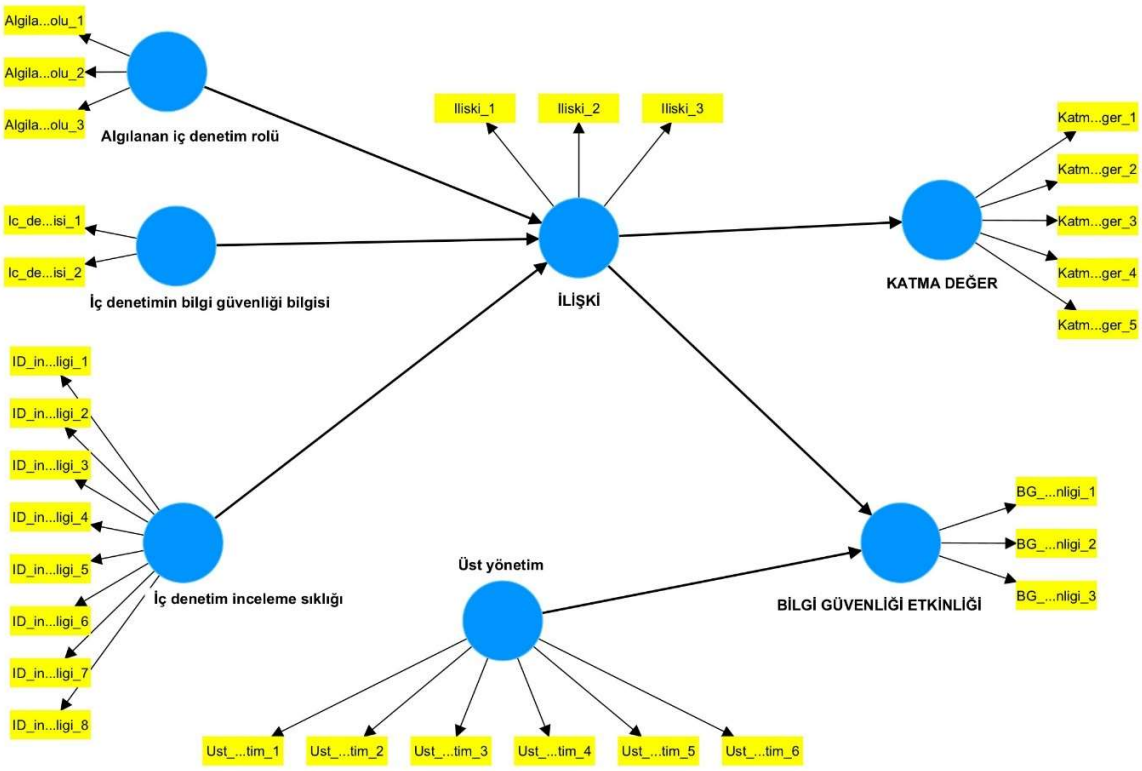
Çalışmada alan araştırması, Türkiye'deki kamu ve özel sektörde görev yapan iç denetçiler ve iç denetim birimi yöneticilerine yönelik olarak 13.03.2020 ve 15.06.2021 tarihleri arasında gerçekleştirilmiştir. Bu kapsamda gerek internet tabanlı anket üzerinden ve gerek ise de fiziki anket dokümanı yardımı ile TİDE, KİDDER gibi meslek derneklerine ulaşılarak üyelerine anketin eposta yoluyla iletilmesi sağlanmıştır. Söz konusu derneklere ve üye sayıları dikkate alındığında

yaklaşık ikibin kişilik bir iç denetçi evreninden bahsedilebilmektedir. İç denetçilere iletilen bu anketlere 272 adet geçerli dönüş alınmıştır. Böylece 272 iç denetim profesyonelinden oluşan bir örneklem elde edilmiştir.

Araştırmada örnekleme ilişkin demografik bilgileri içeren tablo, izleyen bölümlerde yer almaktadır. Söz konusu tabloda, cinsiyet, yaş, eğitim durumu, iş tecrübesi, sertifika sahipliği vb. demografik unsurlar incelenmiştir.

4.2.3 Kullanılan İstatistiksel Teknikler Ve Veri Analizi

Mevcut çalışmada iç denetim fonksiyonunun hangi özelliklerinin iç denetim ile bilgi güvenliği arasındaki ilişkinin niteliğini etkilediğini, bunun yanı sıra iç denetim ile bilgi güvenliği fonksiyonları arasındaki ilişkinin niteliği, iç denetimin bilgi güvenliğini incelemesinden sağlanan değeri ve kuruluşun bilgi güvenliğinin genel etkinliği hakkındaki algıyı nasıl etkilediğini tespit edebilmek için Kısmi En Küçük Kareler (KEKK) regresyon (Partial Least Square Regression; PLS-R) yöntemi kullanılarak Yapısal Eşitlik Modeli (YEM) (Structural Equation Modeling-SEM) oluşturulmuştur (Şekil.23). Bunun için SmartPLS *ver.* 4.0.9.6 (SmartPLS GmbH, Boenningstedt, Germany) paket programından yararlanılmıştır.



Şekil 23: Araştırma çalışmasının birincil ve ikincil hipotezleri doğrultusundaki yapısal eşitlik modeli

Mevcut yapısal eşitlik modeline ilişkin Normed fit indeksi ve sRMSE gibi uyum iyiliği istatistiklerinin yanı sıra değişken grupları arasındaki mevcut birlikteliklerin açıklanmasında her bir bileşeni oluşturan soruların yansıtıcı (reflektif) modele göre faktör yükleri hesaplanmıştır. Söz konusu madde yüklerinden hiçbiri 0,50'den düşük olmadığı için herhangi bir maddenin göz ardı edilmesi ihtimal dışı tutulmuştur. Elde edilen modele ilişkin güvenirlik göstergelerinden Cronbach alpha (iç tutarlılık katsayısı) ve toplam (composite) güvenirlik katsayılarının yanı sıra geçerlik göstergesi olarak ortalama varyans açıklama miktarı (AVE) da ayrıca hesaplanmıştır.

Bir sonraki aşamada iç denetim fonksiyonları ve bilgi güvenliği konusunda katılımcıların her bir bileşenden elde etmiş oldukları puanlar arasındaki korelasyon katsayıları elde edilmiştir. Akabinde mevcut YEM için değişken çiftleri arasındaki

direkt ve indirekt etkilere ait yol (yol (path)) katsayıları, güven aralıkları, t-istatistikleri ve p-değerleri hesaplandı. $p<0,05$ için sonuçlar istatistiksel olarak anlamlı kabul edilmiştir.

İç denetim fonksiyonları ve bilgi güvenliği konusunda katılımcıların her bir bileşenden elde etmiş oldukları ortalama puanlara ait tanımlayıcı istatistikler ortalama ± standart sapma biçiminde gösterilmiştir. Katılımcıların diğer sosyo-ekonomik özellikleri ve iç denetim konusundaki deneyimlerine yönelik sorulara vermiş oldukları yanıtlar ise sayı ve yüzde (%) biçiminde frekans dağılımı olarak gösterilmiştir.

İç denetim fonksiyonları ve bilgi güvenliği konusunda katılımcıların her bir bileşenden elde etmiş oldukları puanların normale yakın dağılıp dağılmadığı Kolmogorov-Smirnov testi ile varyansların homojenliği varsayımının sağlanıp sağlanmadığı ise Levene testi ile incelenmiştir.

Gruplar arasında iç denetim fonksiyonları ve bilgi güvenliği konusunda katılımcıların her bir bileşenden elde etmiş oldukları puanlar yönünden farkların önemliliği; bağımsız grup sayısı iki olduğunda Mann Whitney U testi ile ikiden fazla bağımsız grup arasındaki farkların önemliliği ise Kruskal Wallis testi ile incelenmiştir. Kruskal Wallis test istatistiği sonuçlarının önemli bulunması durumunda ise Dunn-Bonferroni çoklu karşılaştırma testi kullanılarak farka neden olan durum(lar) tespit edilmiştir.

Söz konusu verilerin analizinde IBM SPSS Statistics *ver.* 25 (IBM Corporation, Armonk, NY, US) paket program kullanılmış olup $p<0,05$ için sonuçlar istatistiksel olarak anlamlı kabul edilmiştir.

4.3 ARAŞTIRMA BULGULARI VE TARTIŞMA

İzleyen bölümünde öncelikle çalışmanın katılımcılarının sosyo-demografik bilgileri ve yönlendirilen sorulara ilişkin frekans dağılımını içeren bulgular incelenmektedir. Ardından yukarıda belirtilmiş olan istatistiksel yöntemler ile veriler analiz edilmiş ve sonuçları değerlendirilmiştir.

4.3.1 BULGULAR

Mevcut çalışmada 93'ü (%34,2) kadın, 179'u (%65,8) erkek olmak üzere toplam 272 katılımcı yer almaktadır. Katılımcıların 34'ü (%12,5) 30 yaş altındayken 130'u (%47,8) 30-39 yaşları arasında, 81'i (%29,8) 40-49 yaşları arasında, 27'si (%9,9) ile 49 yaş üzerinde yer almaktadır. Katılımcıların 124'ü (%45,6) lisans mezunu iken 130'u (%47,8) yüksek lisans, 18'i (%6,6) ise doktora düzeyinde öğrenime sahiptir.

Katılımcıların 50'sinin (%18,4) şu anki işyerlerinde iç denetim alanında çalışma süresi 2 yıl ve altında iken 96'sında (%35,3) 3-6 yıl arasında, 83'ünde (%30,5) 7-10 yıl arasında olup 43 kişide (%15,8) 11 yıl ve üzerindedir.

Katılımcıların 24'ünün (%8,8) kariyerleri boyunca iç denetim alanındaki çalışma süresi 2 yıl ve altında iken 76'sında (%28,0) 3-6 yıl arasında, 104'ünde (%38,2) 7-10 yıl arasında olup 68 kişide (%25,0) 11 yıl ve üzerinde yer almaktadır.

Aşağıdaki tabloda çalışmaya dahil edilen katılımcıların sosyo-demografik özelliklerine ait frekans dağılımları gösterilmiştir.

Tablo 5: Çalışmaya Dahil Edilen Katılımcıların Sosyo-demografik Özellikleri

	Sayı	**Yüzde**
Yaş		
<30 yıl	34	12,5
30-39 yıl	130	47,8
40-49 yıl	81	29,8
>49 yıl	27	9,9
Cinsiyet		
Kadın	93	34,2
Erkek	179	65,8
Öğrenim durumu		
Lisans	124	45,6
Yüksek lisans	130	47,8
Doktora	18	6,6

Şu anki işyerinde iç denetim alanındaki çalışma süresi		
≤2 yıl	50	18,4
3-6 yıl	96	35,3
7-10 yıl	83	30,5
≥11 yıl	43	15,8
Kariyeri boyunca iç denetim alanındaki çalışma süresi		
≤2 yıl	24	8,8
3-6 yıl	76	28,0
7-10 yıl	104	38,2
≥11 yıl	68	25,0

Katılımcıların 170'i (%62,5) kamu iç denetim sertifikasına sahiptir. 120 katılımcının (%44,1) iç denetçiler enstitüsü veya diğer uluslararası organizasyonlar tarafından verilen herhangi bir sertifikası bulunmazken 76 katılımcı (%27,9) CIA, 57 katılımcı (%21,0) CGAP, 53 katılımcı (%19,5) ise CISA sahibidir. 17 katılımcının (%6,2) ise diğer münferit sertifikalara sahip olduğu gözlenmiştir.

Katılımcıların 116'sı (%42,6) özel, 146'sı (%53,7) kamu, 5'i (%1,8) dernek veya vakıf, 5'i ise (%1,8) diğer sektörlerde çalışmaktadır.

32 katılımcı (%11,8) çalışmakta olduğu organizasyonda herhangi bir bilgi güvenliği politikasının uygulanmadığını belirtirken 24 katılımcı (%8,8) konu hakkında bilgisinin olmadığını 216 katılımcı ise (%79,4) çalışmakta olduğu organizasyonda herhangi bir bilgi güvenliği politikasının uygulandığını belirtmiştir. Çalışmakta olduğu organizasyonda herhangi bir bilgi güvenliği politikasının uygulandığını belirtenler içerisinde 136 kişi (%63,0) TS ISO / IEC 27001 Bilgi Güvenliği Yönetim Sistemi, 114 kişi (%52,8) Kurum içinde oluşturulmuş politika ve prosedürler uygulandığını, 4 kişi (%1,8) ise diğer uygulamaların olduğunu belirtmişti.

211 kişi (%77,6) bilgi güvenliğine ilişkin organizasyon içi ya da dışı herhangi bir eğitim veya konferansa katılım sağlamış olduğunu belirtirken, katılımcılardan 132'si

(%48,5) çalıştıkları organizasyonda herhangi bir bilgi güvenliği tehdidi ile karşılaşmış olduklarını belirtti.

Tablo 6'da katılımcıların diğer sorulara vermiş oldukları yanıtlar yönünden frekans dağılımı yer almaktadır.

Tablo 6: Katılımcıların Diğer Sorulara Vermiş Oldukları Yanıtlar Yönünden Frekans Dağılımı

	Sayı	**Yüzde**
Kamu iç denetçi sertifikası		
Yok	102	37,5
Var	170	62,5
İç denetçiler enstitüsü veya diğer uluslararası organizasyonlar tarafından verilen sertifikaları		
Yok	120	44,1
Certified Internal Auditor (CIA)	76	27,9
Certified Government Auditing Professional (CGAP)	57	21,0
Certified Information Systems Auditor (CISA)	53	19,5
Diğer	17	6,2
Çalıştığı organizasyonun içinde bulunduğu sektör		
Özel	116	42,6
Kamu	146	53,7
Vakıf-Dernek	5	1,8
Diğer	5	1,8
Çalışmakta olduğu organizasyonda bilgi güvenliği politikası		
Uygulanmıyor	32	11,8
Bilgisi yok	24	8,8
Uygulanıyor	216	79,4
TS ISO / IEC 27001 Bilgi Güvenliği Yönetim Sistemi	136	63,0
Kurum içinde oluşturulmuş politika ve prosedürler	114	52,8
Diğer	4	1,8

Bilgi güvenliğine ilişkin organizasyon içi ya da dışı herhangi bir eğitim veya konferansa katılım	211	77,6
Çalıştığı organizasyonda herhangi bir bilgi güvenliği tehdidi ile karşılaşma	132	48,5

Tablo 7'de ise iç denetim fonksiyonları ve bilgi güvenliği konusunda katılımcılara yöneltilen her bir soruya verilen yanıtlara ait frekans dağılımı verilmiştir.

Tablo 7: İç Denetim Fonksiyonları Ve Bilgi Güvenliği Konusunda Katılımcılara Yöneltilen Her Bir Soruya Verilen Yanıtlara Ait Frekans Dağılımı

	Hiç katılmıyorum		**Katılmıyorum**		**Kısmen katılıyorum**		**Katılıyorum**		**Kesinlikle katılıyorum**	
	Sayı	*Yüzde*	*Sayı*	*Yüzde*	*Sayı*	*Yüzde*	*Sayı*	*Yüzde*	*Sayı*	*Yüzde*
Algılanan iç denetim rolü 1	6	2,2	16	5,9	51	18,8	93	34,2	106	39,0
Algılanan iç denetim rolü 2	16	5,9	30	11,0	52	19,1	93	34,2	81	29,8
Algılanan iç denetim rolü 3	4	1,5	12	4,4	49	18,0	102	37,5	105	38,6
İç denetimin BG bilgisi 1	7	2,6	18	6,6	67	24,6	94	34,6	86	31,6
İç denetimin BG bilgisi 2	7	2,6	17	6,3	66	24,3	92	33,8	90	33,1
İD inceleme sıklığı 1	38	14,0	43	15,8	71	26,1	68	25,0	52	19,1
İD inceleme sıklığı 2	31	11,4	40	14,7	53	19,5	78	28,7	70	25,7
İD inceleme sıklığı 3	38	14,0	27	9,9	65	23,9	78	28,7	64	23,5
İD inceleme sıklığı 4	32	11,8	33	12,1	63	23,2	76	27,9	68	25,0
İD inceleme sıklığı 5	31	11,4	36	13,2	53	19,5	76	27,9	76	27,9
İD inceleme sıklığı 6	30	11,0	33	12,1	64	23,5	69	25,4	76	27,9
İD inceleme sıklığı 7	30	11,0	38	14,0	68	25,0	72	26,5	64	23,5
İD inceleme sıklığı 8	29	10,7	35	12,9	64	23,5	73	26,8	71	26,1
İlişki 1	33	12,1	100	36,8	35	12,9	53	19,5	51	18,8
İlişki 2	2	0,7	47	17,3	79	29,0	79	29,0	65	23,9
İlişki 3	1	0,4	19	7,0	64	23,5	111	40,8	77	28,3

İD: İç denetim, BG: Bilgi güvenliği.

Tablo 7. Devamı

	Hiç katılmıyorum		Katılmıyorum		Kısmen katılıyorum		Katılıyorum		Kesinlikle katılıyorum	
	Sayı	*Yüzde*	*Sayı*	*Yüzde*	*Sayı*	*Yüzde*	*Sayı*	*Yüzde*	*Sayı*	*Yüzde*
Üst yönetim 1	6	2,2	22	8,1	62	22,8	100	36,8	82	30,1
Üst yönetim 2	7	2,6	37	13,6	73	26,8	80	29,4	75	27,6
Üst yönetim 3	5	1,8	13	4,8	51	18,8	115	42,3	88	32,4
Üst yönetim 4	2	0,7	33	12,1	60	22,1	100	36,8	77	28,3
Üst yönetim 5	4	1,5	35	12,9	54	19,9	88	32,4	91	33,5
Üst yönetim 6	6	2,2	26	9,6	55	20,2	99	36,4	86	31,6
Katma değer 1	3	1,1	14	5,1	43	15,8	122	44,9	90	33,1
Katma değer 2	3	1,1	12	4,4	38	14,0	125	46,0	94	34,6
Katma değer 3	4	1,5	31	11,4	77	28,3	88	32,4	72	26,5
Katma değer 4	2	0,7	4	1,5	56	20,6	118	43,4	92	33,8
Katma değer 5	2	0,7	4	1,5	41	15,1	111	40,8	114	41,9
BG etkinliği 1	6	2,2	36	13,2	65	23,9	95	34,9	70	25,7
BG etkinliği 2	5	1,8	16	5,9	63	23,2	109	40,1	79	29,0
BG etkinliği 3	5	1,8	44	16,2	82	30,1	69	25,4	72	26,5

İD: İç denetim, BG: Bilgi güvenliği.

Tablo.8'de ise iç denetim fonksiyonları ve bilgi güvenliği konusunda katılımcılara yöneltilen sorulara ait her bir bileşenden elde edilen puanlara ilişkin tanımlayıcı istatistikler gösterilmiştir.

Tablo 8: İç Denetim Fonksiyonları Ve Bilgi Güvenliği Konusunda Katılımcılara Yöneltilen Sorulara Ait Her Bir Bileşenden Elde Edilen Puanlar

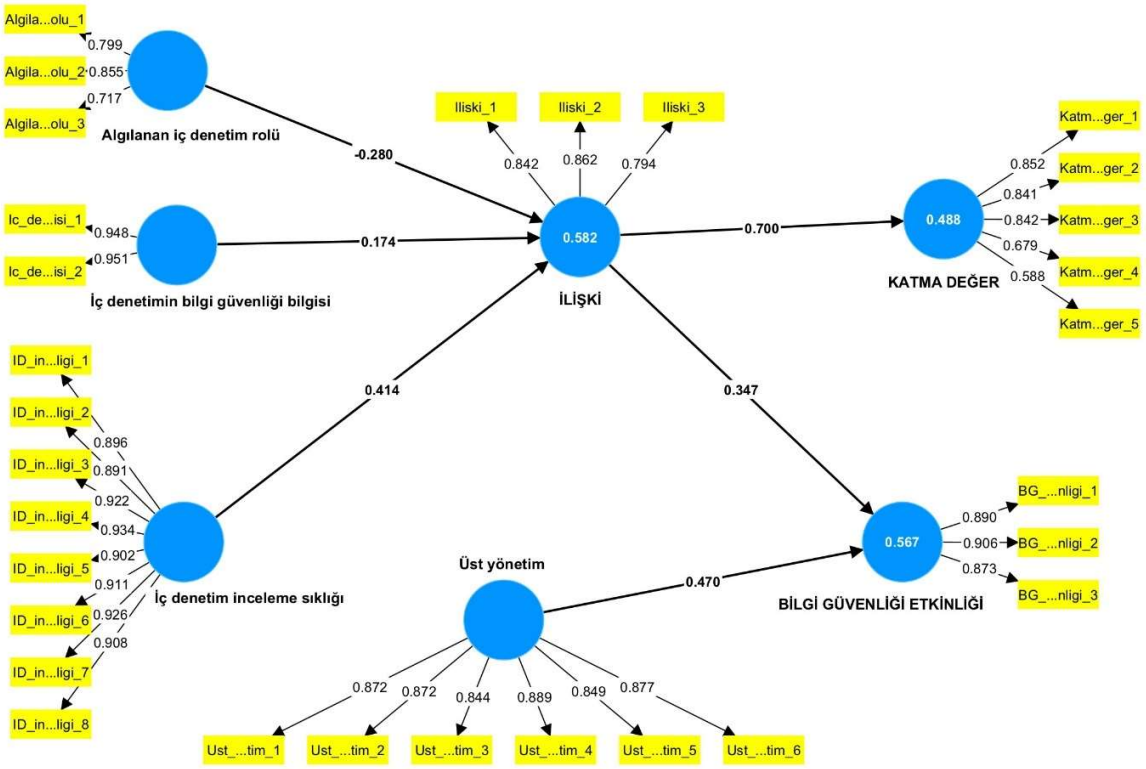
	Ortalama	Std.Sapma	Minimum	25.yüzdelik	Medyan	75.yüzdelik	Maksimum
Algılanan iç denetim rolü	3,93	0,83	1,00	3,33	4,00	4,67	5,00
İç denetimin bilgi güvenliği bilgisi	3,87	0,97	1,00	3,00	4,00	5,00	5,00
İç denetim inceleme sıklığı	3,40	1,19	1,00	2,63	3,50	4,25	5,00
Üst yönetim	3,83	0,89	1,50	3,33	3,83	4,50	5,00
İlişki	3,48	0,92	1,67	2,67	3,33	4,33	5,00
Katma değer	4,03	0,68	2,00	3,60	4,00	4,55	5,00
Bilgi güvenliği etkinliği	3,72	0,92	1,33	3,00	3,67	4,33	5,00

4.3.2 ANALİZ VE DEĞERLENDİRME

Yapılan istatistiksel analiz neticesinde Kestirim yapılan YEM'e ait Normed fit indeksi (NFI) 0,803 olup mevcut veri setinin elde edilen modele oldukça yüksek uyum sağladığı gözlenmiştir. (X^2=1572,712 ve p<0,0001). Ayrıca mevcut modele ait standartlaştırılmış RMSE düzeyi de referans değer olan 0,08'in üzerinde olup (sRMSE=0,106) yine mevcut veri seti ile uyumlu olduğu görülmüştür.

Kısmi en küçük kareler (KEKK) yöntemi uygulanarak elde edilen yapısal eşitlik modeli (YEM) sonucunda iç denetim fonksiyonları ve bilgi güvenliği konusunda katılımcılara yöneltilen her bir sorunun bağlı bulunduğu bileşeni oldukça iyi yansıttığı görülmüştür. Her bir bileşene ilişkin maddelere ait faktör yükleri 0,588 ile 0,951 arasında değişmektedir. Söz konusu madde yüklerinden hiçbiri 0,50'den düşük olmadığı için herhangi bir maddenin göz ardı edilmesi ihtimal dışı tutulmuştur.

Belirtilen sonuçlar model üzerinde de aşağıdaki şekilde gösterilmektedir (Şekil.24). Ayrıca izleyen tabloda (Tablo.9) ilgili maddelerin bağlı bulundukları bileşene ait faktör yükleri gösterilmiştir.



Şekil 24: Kısmi En Küçük Kareler Yöntemine Göre Elde Edilen Yapısal Eşitlik Model Analizi Sonuçları

Tablo 9: İç Denetim Fonksiyonları Ve Bilgi Güvenliği Konusunda Katılımcılara Yöneltilen Her Bir Sorunun Bağlı Bulunduğu Bileşenlere Ait Faktör Yükleri

	Algılanan iç denetim rolü	**İç denetimin bilgi güvenliği bilgisi**	**İç denetim inceleme sıklığı**	**Üst yönetim**	**İlişki**	**Katma değer**	**Bilgi güvenliği etkinliği**
Algılanan İD rolü 1	0,799						
Algılanan İD rolü 2	0,855						
Algılanan İD rolü 3	0,717						
İD BG bilgisi 1		0,948					
İD BG bilgisi 2		0,951					
İD inceleme sıklığı 1			0,896				
İD inceleme sıklığı 2			0,891				
İD inceleme sıklığı 3			0,922				

İD inceleme sıklığı 4	0,934			
İD inceleme sıklığı 5	0,902			
İD inceleme sıklığı 6	0,911			
İD inceleme sıklığı 7	0,926			
İD inceleme sıklığı 8	0,908			
Üst yönetim 1		0,872		
Üst yönetim 2		0,872		
Üst yönetim 3		0,844		
Üst yönetim 4		0,889		
Üst yönetim 5		0,849		
Üst yönetim 6		0,877		
İlişki 1			0,842	
İlişki 2			0,862	
İlişki 3			0,794	
Katma değer 1				0,852
Katma değer 2				0,841
Katma değer 3				0,842
Katma değer 4				0,679
Katma değer 5				0,588
BG etkinliği 1				0,890
BG etkinliği 2				0,906
BG etkinliği 3				0,873

İD: İç denetim, BG: Bilgi güvenliği.

Bileşenlere ait Cronbach alfa iç tutarlılık katsayılarının 0,703 ile 0,971 arasında değiştiği gözlenmiştir. Kompozit (bileşik) güvenirlik düzeylerinin ise rho-a katsayısına

göre 0,724 ile 0,972 arasında yer almakta olup; rho-c katsayısına göre ise de 0,834 ile 0,975 arasında değiştiği görülmektedir. Son olarak her bir bileşeni oluşturan soruların mevcut bileşen içerisindeki ortalama varyans açıklama miktarlarının ise 0,628 ile 0,902 arasında değiştiği gözlenmiştir. Buna göre hangi kriter açısından bakılırsa mevcut bileşenlere ait güvenirlik düzeylerinin istatistiksel açıdan kabul edilebilir derecede yüksek olduğu söylenebilmektedir.

Tablo 10: İç denetim fonksiyonları ve bilgi güvenliği konusunda katılımcıların her bir bileşenden elde etmiş oldukları puanlar arasındaki korelasyon katsayıları

	Cronbach alfa	**Toplam güvenirlik (ρ-a)**	**Toplam güvenirlik (ρ-c)**	**Ortalama varyans açıklama miktarı (AVE)**
Algılanan İD rolü	0,703	0,724	0,834	0,628
İD BG bilgisi	0,892	0,892	0,949	0,902
İD inceleme sıklığı	0,971	0,972	0,975	0,831
Üst yönetim	0,934	0,934	0,948	0,752
İlişki	0,778	0,778	0,871	0,693
Katma değer	0,825	0,863	0,876	0,590
BG etkinliği	0,868	0,868	0,919	0,792

İD: İç denetim, BG: Bilgi güvenliği.

Yapılan korelasyon analizi sonucunda algılanan iç denetim rolünden elde edilen ortalama puanlar ile sırasıyla; iç denetim bilgi güvenliği bilgisi, iç denetim inceleme sıklığı, üst yönetim, ilişki, katma değer ve bilgi güvenliği etkinliği bileşenlerinden elde edilen ortalama puanlar arasında istatistiksel olarak anlamlı ve ters yönlü korelasyonlar mevcuttur ($p<0,05$).

Öte yandan iç denetim bilgi güvenliği bilgisi ortalama puanları ile sırasıyla; iç denetim inceleme sıklığı, üst yönetim, ilişki, katma değer ve bilgi güvenliği etkinliği bileşenlerinden elde edilen ortalama puanlar arasında istatistiksel olarak anlamlı ve aynı yönlü korelasyonlar mevcuttur ($p<0,05$).

İç denetim inceleme sıklığı ortalama puanları ile sırasıyla; üst yönetim, ilişki, katma değer ve bilgi güvenliği etkinliği bileşenlerinden elde edilen ortalama puanlar arasında da istatistiksel olarak anlamlı ve aynı yönlü korelasyonlar yer almaktadır (p<0,05).

Benzer şekilde üst yönetim ortalama puanları ile sırasıyla; ilişki, katma değer ve bilgi güvenliği etkinliği bileşenlerinden elde edilen ortalama puanlar arasında da istatistiksel olarak anlamlı ve aynı yönlü korelasyonlar söz konusudur (p<0,05).

Son olarak ilişki, katma değer ve bilgi güvenliği etkinliği bileşenlerinden elde edilen ortalama puanların birbirleri arasında da istatistiksel olarak anlamlı ve aynı yönlü korelasyonlar görülmüştür (p<0,05).

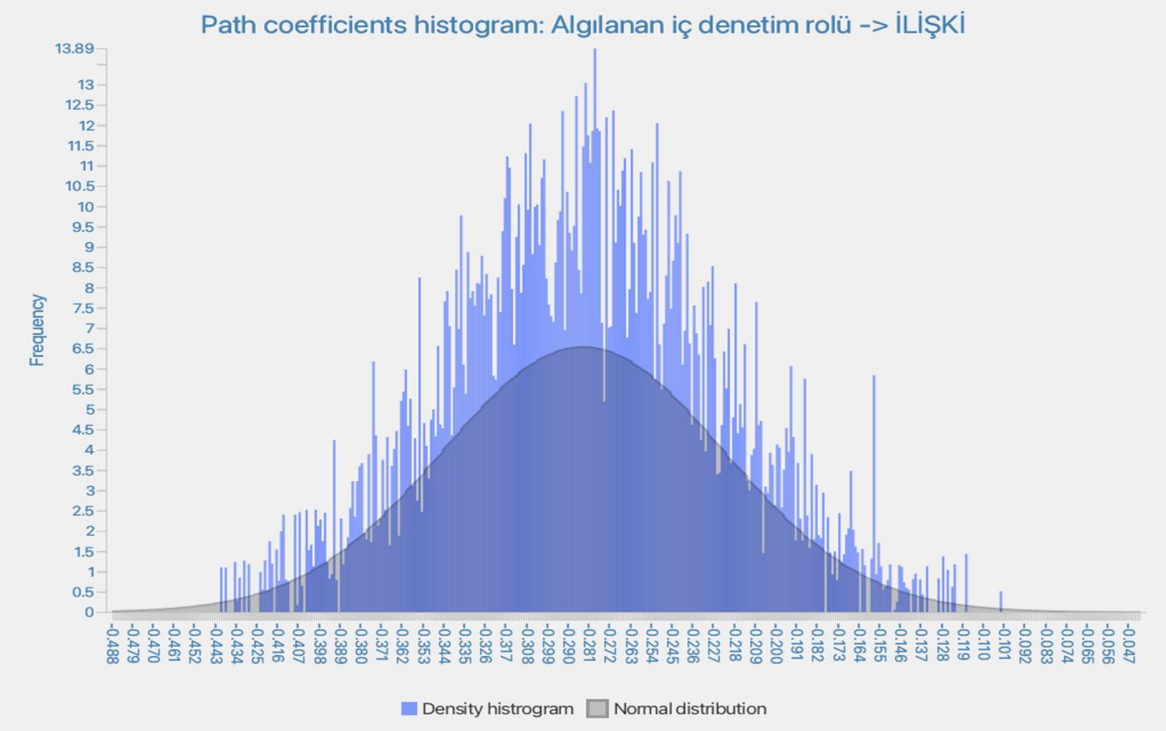
Tablo 11: İç denetim fonksiyonları ve bilgi güvenliği konusunda katılımcıların her bir bileşenden elde etmiş oldukları puanlar arasındaki korelasyon katsayıları

	Algılanan iç denetim rolü	**İç denetimin bilgi güvenliği bilgisi**	**İç denetim inceleme sıklığı**	**Üst yönetim**	**İlişki**	**Katma değer**
İD BG bilgisi	-0,653					
İD inceleme sıklığı	-0,616	0,694				
Üst yönetim	-0,653	0,703	0,726			
İlişki	-0,649	0,644	0,707	0,701		
Katma değer	-0,692	0,671	0,727	0,730	0,700	
BG etkinliği	-0,605	0,562	0,683	0,713	0,677	0,667

İD: İç denetim, BG: Bilgi güvenliği.

Algılanan iç denetim rolünün ilişki bileşeni üzerinde istatistiksel olarak anlamlı ve ters yönlü etkisi görülmüştür [İz (path) katsayısı =-0,280; %95 Güven Aralığı:-0,404 ila -0,164 arası ve p<0,001]. Böylece algılanan iç denetim rolü ortalama puanlarına ait standart sapmadaki her bir birimlik artış ilişki bileşeni ortalama puanlarına ait standart sapmada 0,280 birimlik azalmaya neden olmaktadır. Mevcut modele ait etki büyüklüğü (f^2=0,099) görece düşük olmakla birlikte VIF düzeyi (1,916) makul seviyelerde olup araştırma çalışmasına ait *1. hipotez kabul edilmiştir*.

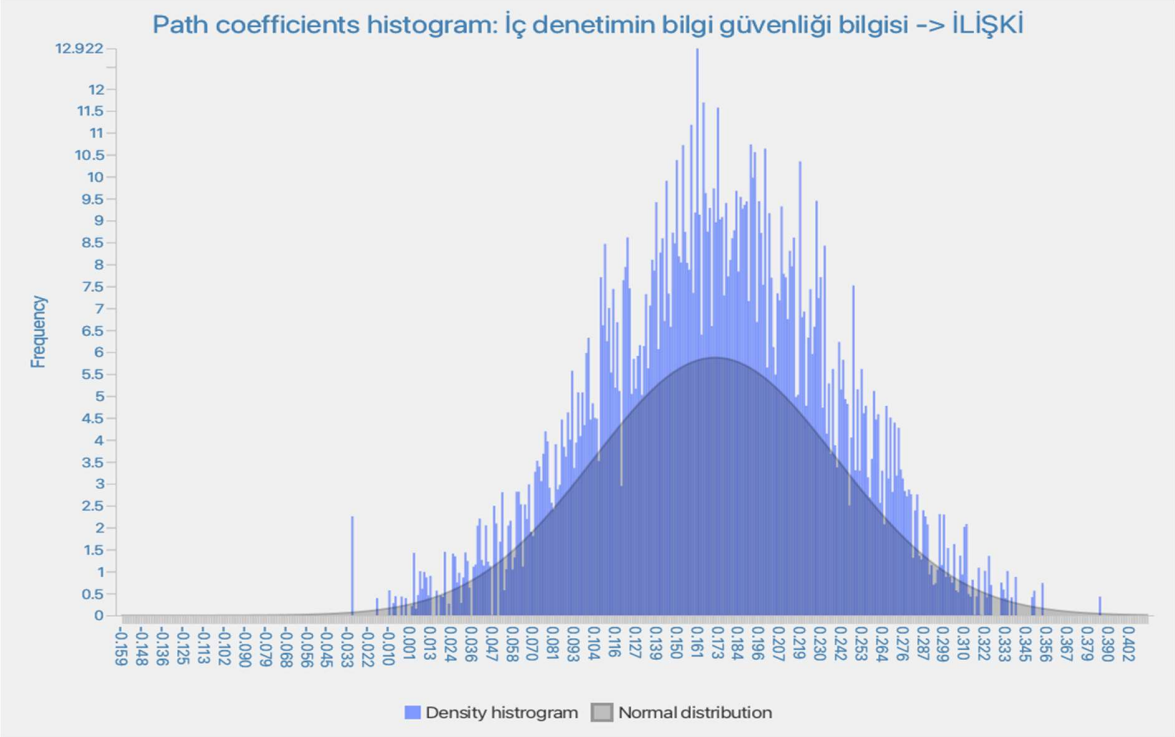
Aşağıdaki şekilde değişken çiftleri arasındaki mevcut birlikteliği açıklamada her bir olguya ait yol (path) katsayılarına ilişkin frekans dağılımı histogram olarak verilmiştir. Mevcut grafik görece normale yakın olup şişkin bir dağılım göstermektedir.



Şekil 25: Algılanan iç denetim rolünün ilişki bileşeni üzerindeki etkisinin incelendiği (her bir katılımcıdan elde edilen) yol (path) katsayılarına ait frekans dağılımı ve histogram

İç denetimin bilgi güvenliği bilgisinin ilişki bileşeni üzerinde istatistiksel olarak anlamlı ve aynı yönlü etkisi görülmüştür [Yol (path) katsayısı= 0,174; %95 Güven Aralığı: 0,033 – 0,301 ve p=0,010]. Böylece iç denetimin bilgi güvenliği bilgisi ortalama puanlarına ait standart sapmadaki her bir birimlik artış ilişki bileşeni ortalama puanlarına ait standart sapmada 0,174 birimlik artışa neden olmaktadır. Mevcut modele ait etki büyüklüğü (f^2=0,032) oldukça düşük olmakla birlikte VIF düzeyi (2,293) makul seviyelerde olup araştırma çalışmasına ait *2.hipotez kabul edilmiştir*.

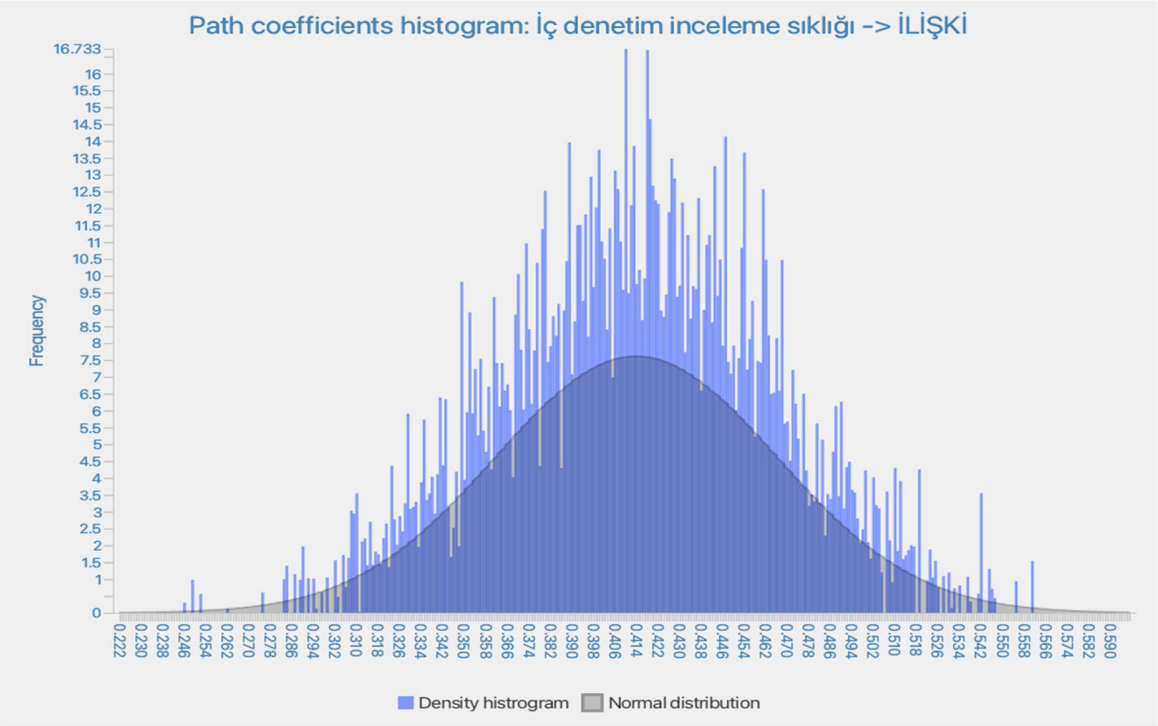
Aşağıdaki şekilde değişken çiftleri arasındaki mevcut birlikteliği açıklamada her bir olguya ait yol (path) katsayılarına ilişkin frekans dağılımı histogram olarak verilmiştir. Mevcut grafik görece sağdan çarpık olup şişkin bir dağılım göstermektedir.



Şekil 26: İç denetimin bilgi güvenliği bilgisinin ilişki bileşeni üzerindeki etkisinin incelendiği (her bir katılımcıdan elde edilen) yol (path) katsayılarına ait frekans dağılımı ve histogram

İç denetim inceleme sıklığının da ilişki bileşeni üzerinde istatistiksel olarak anlamlı ve aynı yönlü etkisi görülmüştür [Yol (path) katsayısı= 0,414; %95 Güven Aralığı: 0,309 – 0,514 ve p<0,001]. Böylece iç denetim inceleme sıklığı ortalama puanlarına ait standart sapmadaki her bir birimlik artış ilişki bileşeni ortalama puanlarına ait standart sapmada 0,414 birimlik artışa neden olmaktadır. Mevcut modele ait etki büyüklüğü (f^2=0,195) kabul edilebilir düzeyde olmakla birlikte VIF düzeyi (2,120) makul seviyelerde olup araştırma çalışmasına ait *3.hipotez kabul edilmiştir*.

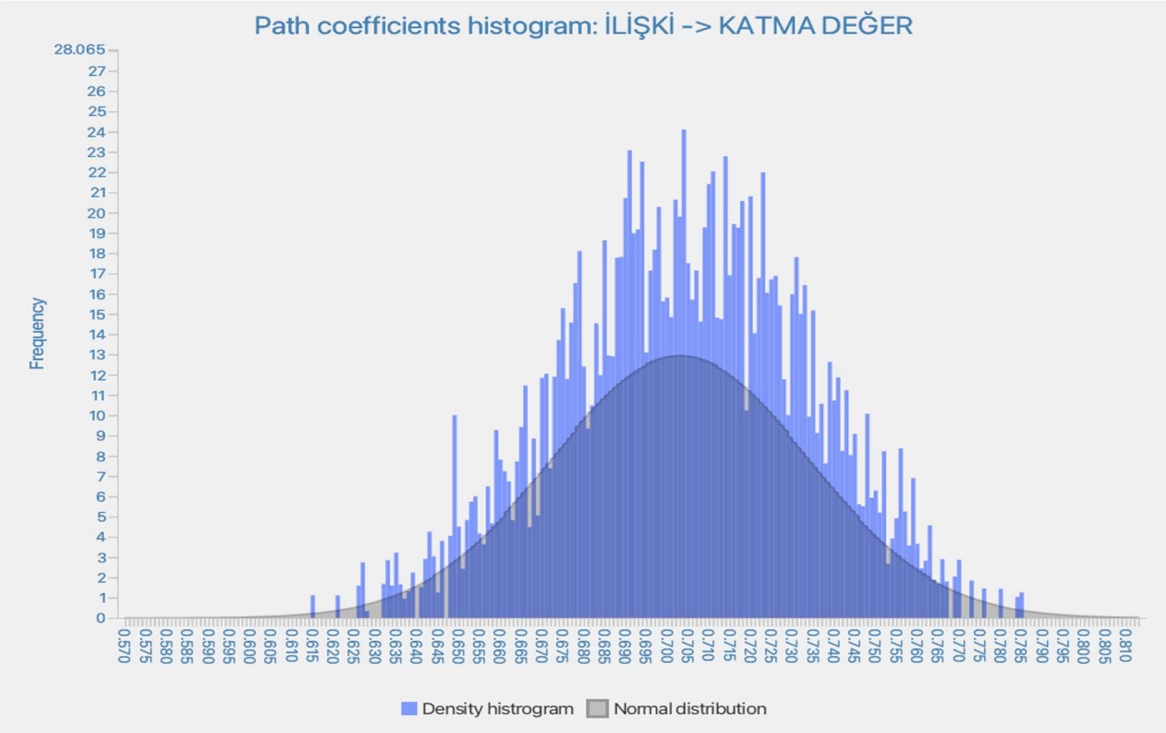
Aşağıdaki şekilde değişken çiftleri arasındaki mevcut birlikteliği açıklamada her bir olguya ait yol (path) katsayılarına ilişkin frekans dağılımı histogram olarak verilmiştir. Mevcut grafik görece normale yakın olup şişkin bir dağılım göstermektedir.



Şekil 27: İç denetim inceleme sıklığının ilişki bileşeni üzerindeki etkisinin incelendiği (her bir katılımcıdan elde edilen) yol (path) katsayılarına ait frekans dağılımı ve histogram

Algılanan iç denetim rolü, iç denetimin bilgi güvenliği bilgisi ve iç denetim inceleme sıklığı bir arada değerlendirildiğinde ilişki bileşenine ait toplam değişimin (varyansın) 0,582'sinin açıklayabildiği görülmüştür. Mevcut bileşenler içerisinde en fazla belirleyici olan iç denetim inceleme sıklığı olup en düşük belirleyiciliğe sahip olan iç denetimin bilgi güvenliği bileşeni idi. İlişki alt boyutunun katma değer alt boyutu üzerinde istatistiksel olarak anlamlı ve aynı yönlü etkisi görülmüştür [İz (path) katsayısı= 0,700; %95 Güven Aralığı: 0,640 – 0,760 ve $p<0,001$]. Başka bir ifade ile ilişki ortalama puanlarına ait standart sapmadaki her bir birimlik artış katma değer ortalama puanlarına ait standart sapmada 0,700 birimlik artışa neden olmaktadır. Mevcut modele ait etki büyüklüğü (f^2=0,960) mükemmele yakın olmakla birlikte VIF düzeyi (1,000) makul seviyelerde olup araştırma çalışmasına ait 4.hipotez kabul edilmiştir.

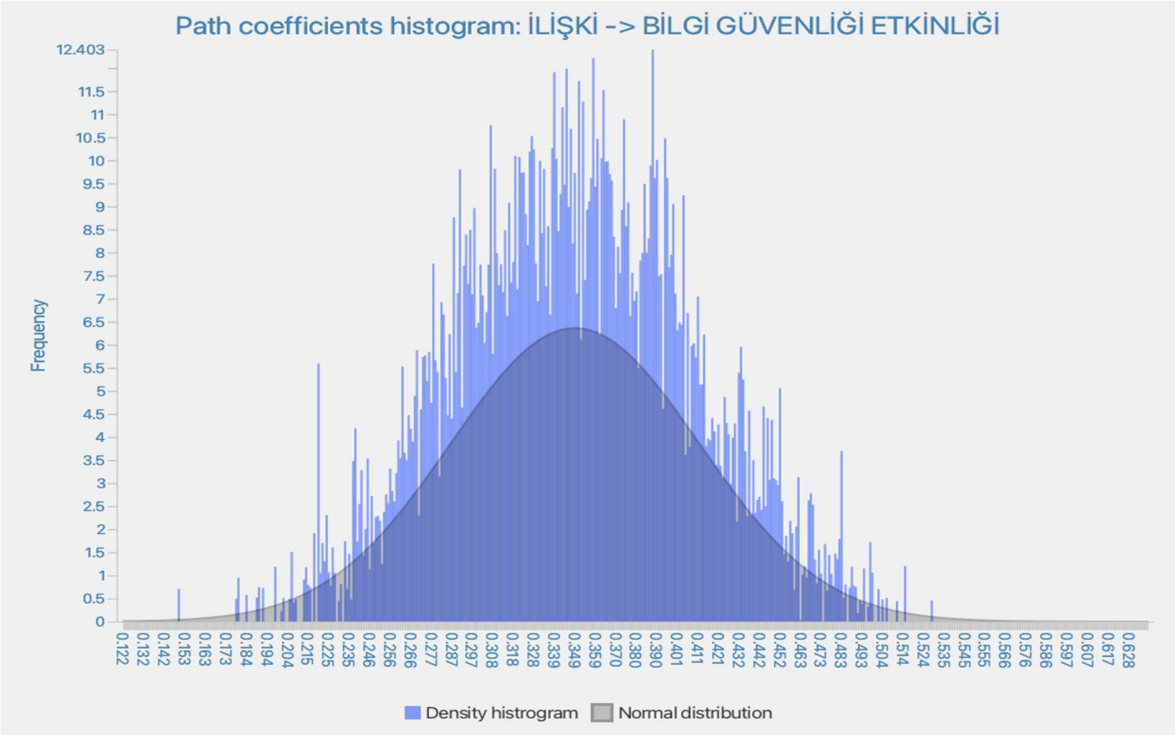
Aşağıdaki şekilde değişken çiftleri arasındaki mevcut birlikteliği açıklamada her bir olguya ait yol (path) katsayılarına ilişkin frekans dağılımı histogram olarak verilmiştir. Mevcut grafik görece normale yakın olup hafif şişkin bir dağılım göstermektedir.



Şekil 28: İlişki bileşeninin katma değer bileşeni üzerindeki etkisinin incelendiği (her bir katılımcıdan elde edilen) yol (path) katsayılarına ait frekans dağılımı ve histogram

Algılanan iç denetim rolü, iç denetimin bilgi güvenliği bilgisi ve iç denetim inceleme sıklığının katma değer alt boyutu üzerindeki ilişki bileşenine bağlı indirekt etkileri ile ilişkinin direkt etkilerinin katma değer bileşenine ait toplam değişimin (varyansın) 0,488'ini açıklayabildiği görülmüştür. İlişki bileşeninin bilgi güvenliği etkinliği üzerinde istatistiksel olarak anlamlı ve aynı yönlü etkisi görülmüştür [İz (path) katsayısı= 0,347; %95 Güven Aralığı: 0,227 – 0,474 ve $p<0,001$]. Başka bir ifade ile ilişki ortalama puanlarına ait standart sapmadaki her bir birimlik artış bilgi güvenliği etkinliği ortalama puanlarına ait standart sapmada 0,347 birimlik artışa neden olmaktadır. Mevcut modele ait etki büyüklüğü (f^2=0,143) görece düşük olmakla birlikte VIF düzeyi (1,965) makul seviyelerde olup araştırma çalışmasına ait *5.hipotez kabul edilmiştir*.

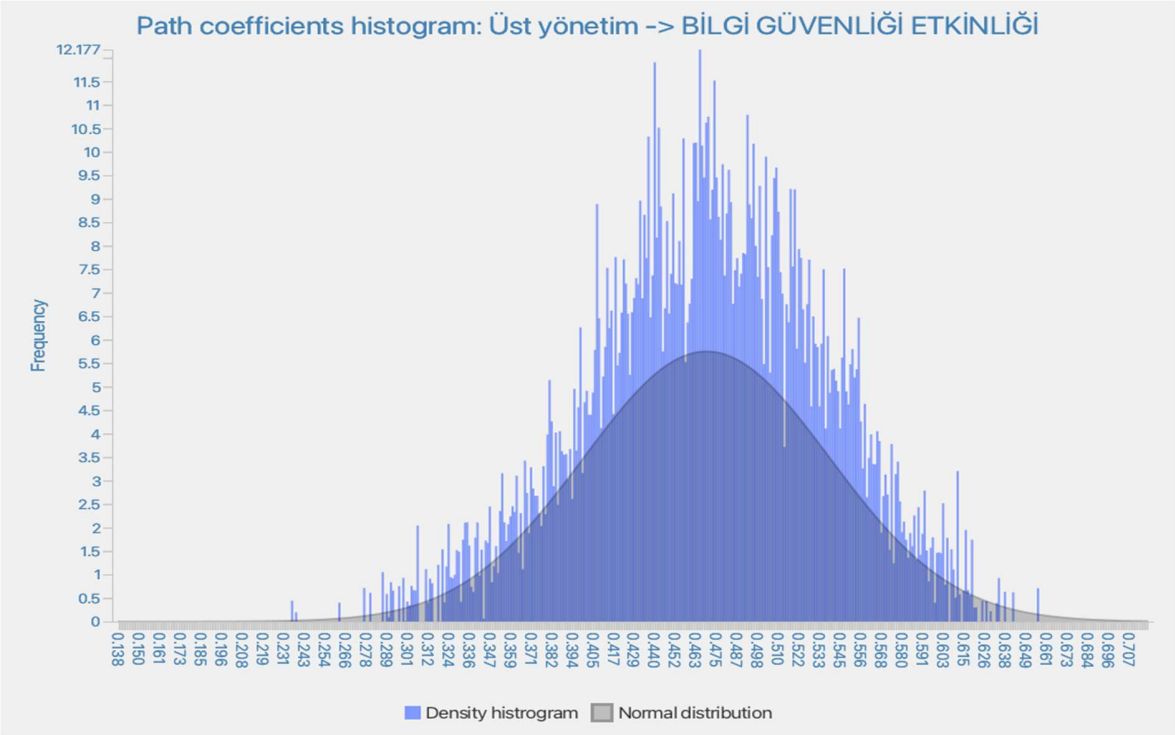
Aşağıdaki şekilde değişken çiftleri arasındaki mevcut birlikteliği açıklamada her bir olguya ait yol (path) katsayılarına ilişkin frekans dağılımı histogram olarak verilmiştir. Mevcut grafik görece soldan çarpık olup şişkin bir dağılım göstermektedir.



Şekil 29: İlişki bileşeninin bilgi güvenliği etkinliği bileşeni üzerindeki etkisinin incelendiği (her bir katılımcıdan elde edilen) yol (path) katsayılarına ait frekans dağılımı ve histogram

Üst yönetim bileşeninin bilgi güvenliği etkinliği üzerinde istatistiksel olarak anlamlı ve aynı yönlü etkisi görülmüştür [İz (path) katsayısı= 0,470; %95 Güven Aralığı: 0,325 – 0,600 ve p<0,001]. Başka bir ifade ile üst yönetim ortalama puanlarına ait standart sapmadaki her bir birimlik artış bilgi güvenliği etkinliği ortalama puanlarına ait standart sapmada 0,470 birimlik artışa neden olmaktadır. Mevcut modele ait etki büyüklüğü (f^2=0,262) kabul edilebilir düzeyde olmakla birlikte VIF düzeyi (1,965) makul seviyelerde olup araştırma çalışmasına ait *6.hipotez kabul edilmiştir.*

Aşağıdaki şekilde değişken çiftleri arasındaki mevcut birlikteliği açıklamada her bir olguya ait yol (path) katsayılarına ilişkin frekans dağılımı histogram olarak verilmiştir. Mevcut grafik görece sağdan çarpık olup şişkin bir dağılım göstermektedir.



Şekil 30: Üst yönetim bileşeninin bilgi güvenliği etkinliği bileşeni üzerindeki etkisinin incelendiği (her bir katılımcıdan elde edilen) yol (path) katsayılarına ait frekans dağılımı ve histogram

Algılanan iç denetim rolü, iç denetimin bilgi güvenliği bilgisi ve iç denetim inceleme sıklığının bilgi güvenliği etkinliği alt boyutu üzerindeki ilişki bileşenine bağlı indirekt etkileri ile ilişki ve üst yönetim bileşenlerinin direkt etkilerinin bilgi güvenliği etkinliğine ait toplam değişimin (varyansın) 0,567'sini açıklayabildiği görülmüştür. Öte yandan direkt etkiler incelendiğinde bilgi güvenliği etkinliğindeki değişimi tahmin etmede üst yönetim bileşeninin ilişki bileşeninden daha fazla belirleyiciliğe sahip olduğu görülmüştür.

Aşağıdaki tabloda mevcut YEM için direkt etkilere ait yol (path) katsayıları, güven aralıkları ve t-istatistikleri yer almaktadır.

Tablo 12: Mevcut YEM için değişken çiftleri arasındaki direkt etkilere ait iz (path) katsayıları, güven aralıkları, t-istatistikleri ve p-değerleri

	İz (path) katsayısı	**Güven Aralığı**		**t istatistiği**	**p- değeri**
		Alt sınır	*Üst sınır*		
Algılanan iç denetim rolü-> İLİŞKİ	-0,280	-0,404	-0,164	4,593	**<0,001**
Üst yönetim-> BİLGİ GÜVENLİĞİ ETKİNLİĞİ	0,470	0,325	0,600	6,776	**<0,001**
İLİŞKİ-> BİLGİ GÜVENLİĞİ ETKİNLİĞİ	0,347	0,227	0,474	5,540	**<0,001**
İLİŞKİ-> KATMA DEĞER	0,700	0,640	0,760	22,707	**<0,001**
İç denetim inceleme sıklığı-> İLİŞKİ	0,414	0,309	0,514	7,899	**<0,001**
İç denetimin bilgi güvenliği bilgisi-> İLİŞKİ	0,174	0,033	0,301	2,563	**0,010**

Algılanan iç denetim rolünün ilişki bileşenine bağlı olarak bilgi güvenliği etkinliği üzerindeki ters yönlü dolaylı etkisi istatistiksel olarak anlamlı bulunmuştur [İz (path) katsayısı= -0,097; %95 Güven Aralığı: -0,163 – -0,047 ve p<0,001]. Söz konusu etki görece zayıf olup ilişki bileşenine bağlı olarak algılanan iç denetim rolü ortalama puanlarına ait standart sapmadaki her bir birimlik artışın bilgi güvenliği etkinliği ortalama puanlarına ait standart sapmada 0,097 birimlik azalmaya neden olduğu görülmüştür.

Algılanan iç denetim rolünün ilişki bileşenine bağlı olarak katma değer üzerindeki ters yönlü dolaylı etkisi de istatistiksel olarak anlamlı bulunmuştur [İz (path) katsayısı= -0,196; %95 Güven Aralığı: -0,289 – -0,113 ve p<0,001]. Başka bir ifade ile ilişki bileşenine bağlı olarak algılanan iç denetim rolü ortalama puanlarına ait standart sapmadaki her bir birimlik artışın katma değer ortalama puanlarına ait standart sapmada 0,196 birimlik azalmaya neden olduğu görülmüştür.

İç denetimin bilgi güvenliği bilgisinin ilişki bileşenine bağlı olarak bilgi güvenliği etkinliği üzerindeki aynı yönlü dolaylı etkisi istatistiksel olarak anlamlı bulunmuştur [İz (path) katsayısı= 0,060; %95 Güven Aralığı: 0,012 – 0,109 ve p=0,013]. Söz konusu etki görece zayıf olup ilişki bileşenine bağlı olarak algılanan iç denetimin bilgi güvenliği bilgisi ortalama puanlarına ait standart sapmadaki her bir birimlik artışın bilgi güvenliği etkinliği ortalama puanlarına ait standart sapmada 0,060 birimlik artışa neden olduğu görülmüştür.

İç denetimin bilgi güvenliği bilgisinin ilişki bileşenine bağlı olarak katma değer üzerindeki aynı yönlü dolaylı etkisi istatistiksel olarak anlamlı bulunmuştur [İz (path) katsayısı= 0,122; %95 Güven Aralığı: 0,023 – 0,211 ve p=0,011]. Söz konusu etki görece zayıf olup ilişki bileşenine bağlı olarak algılanan iç denetimin bilgi güvenliği bilgisi ortalama puanlarına ait standart sapmadaki her bir birimlik katma değer ortalama puanlarına ait standart sapmada 0,122 birimlik artışa neden olduğu görülmüştür.

İç denetim inceleme sıklığının ilişki bileşenine bağlı olarak bilgi güvenliği etkinliği üzerindeki aynı yönlü dolaylı etkisi istatistiksel olarak anlamlı bulunmuştur [İz (path) katsayısı= 0,144; %95 Güven Aralığı: 0,082 – 0,219 ve p<0,001]. Başka bir ifade ile ilişki bileşenine bağlı olarak iç denetim inceleme sıklığı ortalama puanlarına ait standart

sapmadaki her bir birimlik artışın bilgi güvenliği etkinliği ortalama puanlarına ait standart sapmada 0,144 birimlik artışa neden olduğu görülmüştür.

İç denetim inceleme sıklığının ilişki bileşenine bağlı olarak katma değer üzerindeki aynı yönlü dolaylı etkisi istatistiksel olarak anlamlı bulunmuştur [İz (path) katsayısı= 0,290; %95 Güven Aralığı: 0,209 – 0,375 ve p<0,001]. Başka bir ifade ile ilişki bileşenine bağlı olarak iç denetim inceleme sıklığı ortalama puanlarına ait standart sapmadaki her bir birimlik artışın katma değer ortalama puanlarına ait standart sapmada 0,290 birimlik artışa neden olduğu görülmüştür.

Tablo 13: Mevcut YEM için değişken çiftleri arasındaki indirekt etkilere ait iz (path) katsayıları, güven aralıkları, t-istatistikleri ve p-değerleri

	İz (path) katsayısı	Güven Aralığı		t istatistiği	p-değeri
		Alt sınır	*Üst sınır*		
Algılanan iç denetim rolü-> BİLGİ GÜVENLİĞİ ETKİNLİĞİ	-0,097	-0,163	-0,047	3,291	**<0,001**
Algılanan iç denetim rolü-> KATMA DEĞER	-0,196	-0,289	-0,113	4,395	**<0,001**
İç denetimin bilgi güvenliği bilgisi-> BİLGİ GÜVENLİĞİ ETKİNLİĞİ	0,060	0,012	0,109	2,487	**0,013**
İç denetimin bilgi güvenliği bilgisi-> KATMA DEĞER	0,122	0,023	0,211	2,543	**0,011**
İç denetim inceleme sıklığı-> BİLGİ GÜVENLİĞİ ETKİNLİĞİ	0,144	0,082	0,219	4,091	**<0,001**
İç denetim inceleme sıklığı-> KATMA DEĞER	0,290	0,209	0,375	6,845	**<0,001**

Mevcut YEM analizi sonucunda elde edilen iz (path) katsayıları dikkate alınarak "*post-hoc power*" analizi yapıldığında 1.senaryo için (α=0,01 ve 1-β=0,80 kabul edildiğinde) en az 332 katılımcıya, 2.senaryo için (α=0,05 ve 1-β=0,80 kabul edildiğinde) en az 205 katılımcıya, 3.senaryo için (α=0,01 ve 1-β=0,90 kabul edildiğinde) en az 430 katılımcıya, 4.senaryo için ise (α=0,05 ve 1-β=0,90 kabul edildiğinde) en az 283 katılımcıya gereksinim olduğu görülmüştür. Mevcut hesaplamalara göre α=0,05 olarak alındığında çalışmanın gücünün %80'den fazla ve %90'a çok yakın olduğu gözlenmiştir. Dolayısı ile mevcut bulguların önemliliğinin incelenmesinde katılımcı sayısının yeterli olduğu görülmektedir.

Tablo 14: Mevcut YEM analizi sonucunda elde edilen yol (path) katsayıları dikkate alınarak yapılan post-hoc power analizi hesaplamaları

	İz (path) katsayısı	**α = 0.01 1-β = 0.80**	**α = 0.05 1-β = 0.80**	**α = 0.01 1-β = 0.90**	**α = 0.05 1-β = 0.90**
Algılanan iç denetim rolü-> İLİŞKİ	-0,280	128	79	166	109
Üst yönetim-> BİLGİ GÜVENLİĞİ ETKİNLİĞİ	0,470	46	28	59	39
İLİŞKİ-> BİLGİ GÜVENLİĞİ ETKİNLİĞİ	0,347	84	52	108	72
İLİŞKİ-> KATMA DEĞER	0,700	21	13	27	18
İç denetim inceleme sıklığı-> İLİŞKİ	0,414	59	37	77	51
İç denetimin bilgi güvenliği bilgisi-> İLİŞKİ	0,174	332	205	430	283

40 yaş altı katılımcılara göre 40 yaş ve üzeri katılımcıların sırasıyla; algılanan iç denetim rolü, iç denetimin bilgi güvenliği bilgisi, iç denetim inceleme sıklığı, üst yönetim, ilişki, katma değer ve bilgi güvenliği etkinliği ortalama puanları istatistiksel anlamlı olarak daha düşüktür (p<0,001).

Tablo 15: Katılımcıların yaşlarına göre iç denetim fonksiyonları ve bilgi güvenliği konusundaki her bir bileşenden elde etmiş oldukları puanlar yönünden yapılan karşılaştırmalar

	<40 yaş (n=164)	**≥40 yaş (n=108)**	**p-değeri †**
Algılanan iç denetim rolü	4,15±0,80	3,60±0,76	**<0,001**
İç denetimin bilgi güvenliği bilgisi	4,07±0,87	3,57±1,04	**<0,001**
İç denetim inceleme sıklığı	3,73±1,12	2,89±1,12	**<0,001**
Üst yönetim	4,02±0,86	3,54±0,87	**<0,001**
İlişki	3,75±0,93	3,07±0,75	**<0,001**
Katma değer	4,15±0,69	3,84±0,62	**<0,001**
Bilgi güvenliği etkinliği	3,89±0,95	3,46±0,82	**<0,001**

Tanımlayıcı istatistikler; ortalama ± standart sapma biçiminde gösterildi. † Mann Whitney U testi.

Kadınlara göre erkeklerin sırasıyla; iç denetim inceleme sıklığı ve ilişki bileşenlerinden elde etmiş oldukları ortalama puanları istatistiksel anlamlı olarak daha düşüktür (p=0,022 ve p=0,044). Cinsiyete göre diğer bileşenlerden elde edilen ortalama puanlar yönünden istatistiksel olarak anlamlı herhangi bir farklılık tespit edilmemiştir(p>0,05).

Tablo 16: Katılımcıların cinsiyetlerine göre iç denetim fonksiyonları ve bilgi güvenliği konusundaki her bir bileşenden elde etmiş oldukları puanlar yönünden yapılan karşılaştırmalar

	Kadın (n=93)	**Erkek (n=179)**	**p-değeri †**
Algılanan iç denetim rolü	4,06±0,76	3,87±0,85	0,066

İç denetimin bilgi güvenliği bilgisi	3,96±0,87	3,83±1,02	0,433
İç denetim inceleme sıklığı	3,61±1,15	3,29±1,20	**0,022**
Üst yönetim	3,99±0,78	3,74±0,94	0,051
İlişki	3,62±0,90	3,41±0,93	**0,044**
Katma değer	4,09±0,64	3,99±0,70	0,196
Bilgi güvenliği etkinliği	3,79±0,92	3,68±0,92	0,360

Tanımlayıcı istatistikler; ortalama ± standart sapma biçiminde gösterildi. † Mann Whitney U testi.

Lisans mezunu katılımcılara göre lisans üstü mezunu olan katılımcıların sırasıyla; iç denetimin bilgi güvenliği bilgisi ve katma değer bileşenlerinden elde etmiş oldukları ortalama puanlar istatistiksel anlamlı olarak daha yüksektir (p=0,047 ve p=0,049). Öğrenim durumuna göre diğer bileşenlerden elde edilen ortalama puanlar yönünden istatistiksel olarak anlamlı herhangi bir farklılık tespit edilmemiştir (p>0,05).

Tablo 17: Katılımcıların öğrenim durumlarına göre iç denetim fonksiyonları ve bilgi güvenliği konusundaki her bir bileşenden elde etmiş oldukları puanlar yönünden yapılan karşılaştırmalar

	Lisans (n=124)	**Lisans üstü (n=148)**	**p-değeri †**
Algılanan iç denetim rolü	3,83±0,79	4,02±0,85	0,050
İç denetimin bilgi güvenliği bilgisi	3,78±0,86	3,95±1,05	**0,047**
İç denetim inceleme sıklığı	3,30±1,03	3,48±1,31	0,116
Üst yönetim	3,76±0,75	3,88±1,00	0,108
İlişki	3,38±0,77	3,56±1,03	0,368
Katma değer	3,93±0,61	4,11±0,73	**0,049**
Bilgi güvenliği etkinliği	3,61±0,83	3,81±0,99	0,060

Tanımlayıcı istatistikler; ortalama ± standart sapma biçiminde gösterildi. † Mann Whitney U testi.

Şu anki işyerlerinde 6 yıl ve daha kısa süredir iç denetim alanında çalışanlara göre şu anki işyerlerinde 7 yıl ve daha uzun süredir iç denetim alanında çalışanların sırasıyla; iç denetim inceleme sıklığı, üst yönetim ve bilgi güvenliği etkinliği ortalama puanları

istatistiksel anlamlı olarak daha yüksektir (p=0,035; p=0,018 ve p=0,017). Gruplar arasında diğer bileşenlerden elde edilen ortalama puanlar yönünden ise istatistiksel olarak anlamlı herhangi bir farklılık tespit edilmemiştir (p>0,05).

Tablo 18: Katılımcıların şu anki işyerlerinde iç denetim alanındaki çalışma sürelerine göre iç denetim fonksiyonları ve bilgi güvenliği konusundaki her bir bileşenden elde etmiş oldukları puanlar yönünden yapılan karşılaştırmalar

	≤6 yıl (n=146)	**≥7 yıl (n=126)**	**p-değeri †**
Algılanan iç denetim rolü	3,92±0,79	3,95±0,87	0,694
İç denetimin bilgi güvenliği bilgisi	3,78±0,95	3,98±0,99	0,069
İç denetim inceleme sıklığı	3,28±1,15	3,54±1,23	**0,035**
Üst yönetim	3,72±0,85	3,96±0,93	**0,018**
İlişki	3,41±0,81	3,56±1,04	0,540
Katma değer	3,96±0,62	4,10±0,74	0,072
Bilgi güvenliği etkinliği	3,58±0,93	3,88±0,89	**0,017**

Tanımlayıcı istatistikler; ortalama ± standart sapma biçiminde gösterildi. † Mann Whitney U testi.

Kariyeri boyunca toplam 6 yıl ve daha kısa süredir iç denetim alanında çalışanlara göre kariyeri boyunca toplam 7 yıl ve daha uzun süredir iç denetim alanında çalışanların sırasıyla; üst yönetim ve bilgi güvenliği etkinliği ortalama puanları istatistiksel anlamlı olarak daha yüksektir (p=0,034 ve p=0,019). Gruplar arasında diğer bileşenlerden elde edilen ortalama puanlar yönünden ise istatistiksel olarak anlamlı herhangi bir farklılık tespit edilmemiştir (p>0,05).

Tablo 19: Katılımcıların kariyerleri boyunca iç denetim alanındaki toplam çalışma sürelerine göre iç denetim fonksiyonları ve bilgi güvenliği konusundaki her bir bileşenden elde etmiş oldukları puanlar yönünden yapılan karşılaştırmalar

	≤6 yıl (n=100)	**≥7 yıl (n=172)**	**p-değeri †**
Algılanan iç denetim rolü	3,90±0,81	3,95±0,84	0,665
İç denetimin bilgi güvenliği bilgisi	3,80±0,89	3,92±1,01	0,157
İç denetim inceleme sıklığı	3,26±1,14	3,48±1,22	0,071

Üst yönetim	3,71±0,82	3,90±0,93	**0,034**
İlişki	3,39±0,84	3,53±0,97	0,489
Katma değer	3,93±0,65	4,08±0,69	0,080
Bilgi güvenliği etkinliği	3,54±0,94	3,83±0,90	**0,019**

Tanımlayıcı istatistikler; ortalama ± standart sapma biçiminde gösterildi. † Mann Whitney U testi.

Kamu iç denetçi sertifikasına sahip olmayan katılımcılara göre kamu iç denetçi sertifikasına sahip olan katılımcıların sırasıyla; üst yönetim, ilişki, katma değer ve bilgi güvenliği etkinliği ortalama puanları istatistiksel anlamlı olarak daha yüksektir ($p<0,01$). Gruplar arasında diğer bileşenlerden elde edilen ortalama puanlar yönünden ise istatistiksel olarak anlamlı herhangi bir farklılık tespit edilmemiştir ($p>0,05$).

Tablo 20: Katılımcıların kamu iç denetçi sertifikasına sahip olup olmama durumlarına göre iç denetim fonksiyonları ve bilgi güvenliği konusundaki her bir bileşenden elde etmiş oldukları puanlar yönünden yapılan karşılaştırmalar

	Yok (n=102)	**Var (n=170)**	**p-değeri †**
Algılanan iç denetim rolü	3,83±0,71	4,00±0,88	0,057
İç denetimin bilgi güvenliği bilgisi	3,78±0,93	3,93±0,99	0,176
İç denetim inceleme sıklığı	3,27±1,04	3,48±1,27	0,077
Üst yönetim	3,68±0,77	3,92±0,95	**0,009**
İlişki	3,20±0,69	3,65±1,00	**<0,001**
Katma değer	3,87±0,63	4,12±0,69	**0,009**
Bilgi güvenliği etkinliği	3,43±0,85	3,89±0,93	**<0,001**

Tanımlayıcı istatistikler; ortalama ± standart sapma biçiminde gösterildi. † Mann Whitney U testi.

İç denetçiler enstitüsü veya diğer uluslararası organizasyonlar tarafından verilen sertifikalardan herhangi birine sahip olmayan gruba göre iç denetçiler enstitüsü veya diğer uluslararası organizasyonlar tarafından verilen en az bir sertifikaya sahip olan katılımcıların sırasıyla; algılanan iç denetim rolü, iç denetimin bilgi güvenliği bilgisi, iç denetim inceleme sıklığı, üst yönetim, ilişki, katma değer ve bilgi güvenliği etkinliği ortalama puanları istatistiksel anlamlı olarak daha yüksektir ($p<0,01$).

Tablo 21: Katılımcıların iç denetçiler enstitüsü veya diğer uluslararası organizasyonlar tarafından verilen sertifikalara sahip olup olmama durumlarına göre iç denetim fonksiyonları ve bilgi güvenliği konusundaki her bir bileşenden elde etmiş oldukları puanlar yönünden yapılan karşılaştırmalar

	Yok (n=120)	Var (n=152)	p-değeri †
Algılanan iç denetim rolü	3,79±0,74	4,04±0,88	**0,005**
İç denetimin bilgi güvenliği bilgisi	3,65±0,94	4,05±0,96	**<0,001**
İç denetim inceleme sıklığı	3,07±1,15	3,66±1,17	**<0,001**
Üst yönetim	3,58±0,84	4,03±0,89	**<0,001**
İlişki	3,16±0,72	3,73±0,99	**<0,001**
Katma değer	3,90±0,59	4,13±0,73	**0,004**
Bilgi güvenliği etkinliği	3,44±0,84	3,94±0,93	**<0,001**

Tanımlayıcı istatistikler; ortalama ± standart sapma biçiminde gösterildi. † Mann Whitney U testi.

Kamu sektöründe çalışan katılımcılar ile kamu dışı sektörlerde çalışan katılımcılar arasında sırasıyla; algılanan iç denetim rolü, iç denetimin bilgi güvenliği bilgisi, iç denetim inceleme sıklığı, üst yönetim, ilişki, katma değer ve bilgi güvenliği etkinliği ortalama puanları yönünden istatistiksel olarak anlamlı herhangi bir farklılık tespit edilmedi (p>0,05).

Tablo 22: Katılımcıların çalıştığı organizasyonun içinde bulunduğu sektörlere göre iç denetim fonksiyonları ve bilgi güvenliği konusundaki her bir bileşenden elde etmiş oldukları puanlar yönünden yapılan karşılaştırmalar

	Kamu dışı (n=126)	Kamu (n=146)	p-değeri †
Algılanan iç denetim rolü	3,98±0,73	3,89±0,90	0,343
İç denetimin bilgi güvenliği bilgisi	3,99±0,86	3,77±1,05	0,087
İç denetim inceleme sıklığı	3,46±0,96	3,35±1,36	0,810
Üst yönetim	3,94±0,73	3,74±1,00	0,144
İlişki	3,44±0,77	3,51±1,04	0,999
Katma değer	3,98±0,62	4,06±0,73	0,437

Bilgi güvenliği etkinliği	3,68±0,84	3,75±0,99	0,482

Tanımlayıcı istatistikler; ortalama ± standart sapma biçiminde gösterildi. † Mann Whitney U testi.

Katılımcıların çalışmakta olduğu organizasyonda bilgi güvenliği politikası uygulamalarına göre üst yönetim ortalama puanlarında istatistiksel olarak anlamlı farklılık olup (p=0,009) söz konusu farka neden olan durum; herhangi bir politika uygulanmayan gruba göre en az bir politika uygulanan grubun puanlarının daha yüksek olmasıdır (p=0,007). Katılımcıların çalışmakta olduğu organizasyonda bilgi güvenliği politikası uygulamalarına göre bilgi güvenliği etkinliği ortalama puanlarında da istatistiksel olarak anlamlı farklılık olup (p=0,014) söz konusu farka neden olan durum; herhangi bir politika uygulanmayan gruba göre en az bir politika uygulanan grubun puanlarının daha yüksek olmasıdır (p=0,011). Gruplar arasında diğer bileşenlerden elde edilen ortalama puanlar yönünden ise istatistiksel olarak anlamlı herhangi bir farklılık tespit edilmemiştir (p>0,05).

Tablo 23: Katılımcıların çalışmakta olduğu organizasyonda bilgi güvenliği politikası uygulamalarına göre iç denetim fonksiyonları ve bilgi güvenliği konusundaki her bir bileşenden elde etmiş oldukları puanlar yönünden yapılan karşılaştırmalar

	Uygulanmıyor (n=32)	Bilgisi yok (n=24)	Uygulanıyor (n=216)	p-değeri †
Algılanan iç denetim rolü	3,74±0,63	3,96±0,85	3,96±0,85	0,229
İç denetimin bilgi güvenliği bilgisi	3,61±0,94	3,75±1,08	3,93±0,96	0,156
İç denetim inceleme sıklığı	2,94±1,17	3,36±1,28	3,47±1,18	0,071
Üst yönetim	3,34±0,88	3,83±0,99	3,90±0,86	**0,009**
İlişki	3,27±0,82	3,49±1,02	3,51±0,93	0,558
Katma değer	3,84±0,65	4,06±0,68	4,05±0,68	0,397
Bilgi güvenliği etkinliği	3,26±0,95	3,79±0,90	3,78±0,91	**0,014**

Tanımlayıcı istatistikler; ortalama ± standart sapma biçiminde gösterildi. † Kruskal Wallis testi. a: Uygulanmıyor yanıtını veren grup ile uygulanıyor yanıtını veren grup arasındaki fark istatistiksel olarak anlamlı (p<0,05).

Bilgi güvenliğine ilişkin organizasyon içi ya da dışı herhangi bir eğitim veya konferansa katılmayan gruba göre organizasyon içi ya da dışı herhangi bir eğitim veya konferansa katılan grubun sırasıyla; algılanan iç denetim rolü, iç denetimin bilgi güvenliği bilgisi ve iç denetim inceleme sıklığı ortalama puanları istatistiksel anlamlı olarak daha yüksektir (p=0,030; p=0,020 ve p=0,015). Öte yandan gruplar arasında sırasıyla; üst yönetim, ilişki, katma değer ve bilgi güvenliği etkinliği ortalama puanları yönünden istatistiksel olarak anlamlı herhangi bir farklılık tespit edilmedi (p>0,05).

Tablo 24: Katılımcıların bilgi güvenliğine ilişkin organizasyon içi ya da dışı herhangi bir eğitim veya konferansa katılıp katılmama durumlarına göre iç denetim fonksiyonları ve bilgi güvenliği konusundaki her bir bileşenden elde etmiş oldukları puanlar yönünden yapılan karşılaştırmalar

	Hayır (n=61)	**Evet (n=211)**	**p-değeri †**
Algılanan iç denetim rolü	3,70±0,89	4,00±0,80	**0,030**
İç denetimin bilgi güvenliği bilgisi	3,59±1,09	3,95±0,92	**0,020**
İç denetim inceleme sıklığı	3,05±1,29	3,50±1,15	**0,015**
Üst yönetim	3,62±0,99	3,89±0,85	0,077
İlişki	3,34±0,91	3,52±0,93	0,263
Katma değer	3,88±0,73	4,07±0,66	0,090
Bilgi güvenliği etkinliği	3,54±0,93	3,77±0,92	0,087

Tanımlayıcı istatistikler; ortalama ± standart sapma biçiminde gösterildi. † Mann Whitney U testi.

Katılımcıların çalıştıkları organizasyonda herhangi bir bilgi güvenliği tehdidi ile karşılaşıp karşılaşmama durumuna göre sırasıyla; algılanan iç denetim rolü, iç denetimin bilgi güvenliği bilgisi, iç denetim inceleme sıklığı, üst yönetim, ilişki, katma değer ve bilgi güvenliği etkinliği ortalama puanlarında istatistiksel olarak anlamlı herhangi bir değişim görülmemiştir (p>0,05).

Tablo 25: Katılımcıların çalıştıkları organizasyonda herhangi bir bilgi güvenliği tehdidi ile karşılaşıp karşılaşmama durumuna göre iç denetim fonksiyonları ve bilgi güvenliği konusundaki her bir bileşenden elde etmiş oldukları puanlar yönünden yapılan karşılaştırmalar

	Hayır (n=140)	Evet (n=132)	p-değeri †
Algılanan iç denetim rolü	3,92±0,82	3,94±0,83	0,619
İç denetimin bilgi güvenliği bilgisi	3,89±0,93	3,86±1,01	0,876
İç denetim inceleme sıklığı	3,44±1,11	3,36±1,28	0,855
Üst yönetim	3,85±0,83	3,81±0,96	0,907
İlişki	3,48±0,88	3,48±0,98	0,906
Katma değer	4,03±0,63	4,02±0,73	0,955
Bilgi güvenliği etkinliği	3,76±0,89	3,67±0,97	0,456

Tanımlayıcı istatistikler; ortalama ± standart sapma biçiminde gösterildi. † Mann Whitney U testi.

Çalışma kapsamında gerçekleştirilen istatistiksel analiz neticesinde 6 hipoteze ilişkin sonuçların özeti Tablo.26'da sunulmaktadır.

Tablo 26: Hipotez Testi Sonuçları

Hipotezler	Sonuçlar
H1: İç denetçilerin; iç denetim fonksiyonunu mevzuatın uygulayıcısı rolünden ziyade danışmanlık rolü olarak algılamaları durumunda, iç denetim ve bilgi güvenliği arasındaki ilişkiye dair algıları daha olumludur.	Desteklendi
H2: İç denetçilerin; iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin niteliğine dair algıları, iç denetimin gerçekleştirdiği bilgi güvenliği denetimlerinin sıklığına dair algılarıyla pozitif ilişkilidir.	Desteklendi
H3: İç denetçilerin; iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin niteliğine dair algıları, iç denetçinin bilgi güvenliği hakkındaki yetkinliğine dair algılarıyla pozitif ilişkilidir.	Desteklendi
H4: İç denetim ve bilgi güvenliği arasındaki ilişkinin niteliği, iç denetçilerin, içinde bulundukları iç denetim fonksiyonunun	Desteklendi

organizasyona sağladığı katma değere dair algılarıyla pozitif ilişkilidir.	
H5: İç denetim ve bilgi sistemleri fonksiyonları arasındaki ilişkinin algılanan niteliği; iç denetçilerin, bilgi güvenliği etkinliğine olan algılarıyla pozitif ilişkilidir.	Desteklendi
H6: Üst yönetimin bilgi güvenliğine yönelik desteğinin algılanan niteliği; iç denetçilerin, bilgi güvenliği etkinliğine olan algılarıyla pozitif ilişkilidir.	Desteklendi

SONUÇ VE ÖNERİLER

Çalışmanın son kısmında alan araştırmasında elde edilen bulgular tartışılmaktadır. Ardından çalışmanın kısıtlarına ve gelecek araştırmalara, son olarak da iç denetim yöneticileri ve iç denetçilere yönelik önerilere değinilmektedir.

GENEL SONUÇ

Bu tez çalışmasının amacı, organizasyonlarda faaliyetlerini yürütmekte olan iç denetim ve bilgi güvenliği fonksiyonlarının birbirleriyle olan ilişkilerini etkileyen faktörlerin belirlenmesi, bu bağlamda söz konusu ilişkinin niteliğinin iç denetim fonksiyonunun algılanan değerine ve bilgi güvenliği fonksiyonun başarısına olan etkisini incelemektir.

Çalışmanın uygulama bölümünden önceki bölümlerinde öncelikle denetim ile ilişkili kavramlara yer verilmiş olup. Kontrol, iç kontrol, teftiş ve teftiş anlayışının geçmiş bugüne kadar ki değişimi ele alınmıştır. Ardından denetim türleri bu türlerin kendi aralarındaki farklılıkları, iç denetim kavramı, iç denetimin özellikleri, iç denetim-iç kontrol ilişkisi, iç denetim-teftiş ilişkisi incelenmiştir. İzleyen kısımda iç denetim uygulamalarının temel kaynağını oluşturan Uluslararası Mesleki Uygulama Çerçevesi, Uluslararası İç Denetim Standartları (IIA, 2017) ve İç Denetçiler Enstitüsü (IIA, 2016a) yapıları incelenmiştir. Sonraki bölümde denetim ve bilgi güvenliği ile ilişkili uluslararası ve ulusal mevzuat iç denetim ve bilgi güvenliği açısından incelenmiştir. Son olarak bilgi, bilgi güvenliği, ISA 27001 standardı, BGYS İç tetkik faaliyetleri ve Cumhurbaşkanlığı Dijital Dönüşüm Ofisi rehberleri süreçleri açıklanmıştır. Kavramsal çerçevenin incelemesinin ardından tezin uygulama aşamasında geçilmiştir.

Çalışmanın dördüncü bölümü olan uygulama aşamasında; öncelikle araştırmanın amacı ve önemi açıklanmıştır. Ardından araştırma modeli ve hipotezler hakkında bilgi verilmiştir. İzleyen bölümde araştırma kısıtları incelenmiştir. Metodoloji bölümünde ise veri toplama aracı hakkında bilgi verilmiş olup veri toplama süreci ve örneklem açıklanmıştır. Veri analizi ve kullanılan istatistiksel tekniklere de değinilerek araştırma bulguları bölümüne geçilmiştir. İzleyen aşamada ise

bulguların analizi ve değerlendirilmesi ile çalışmanın uygulama bölümü tamamlanmıştır.

Tez çalışmasının uygulama bölümünde yapılan istatiksel analizler sonucunda hipotez testlerine ilişkin sonuçlar aşağıda incelenmektedir. Çalışmanın ilk hipotezi, iç denetim fonksiyonunun mevzuatın uygulayıcısı rolünden ziyade danışmanlık rolüne yöneldiğinde, iç denetçilerin iç denetim ve bilgi güvenliği arasındaki ilişkinin niteliğine dair algılarının daha olumlu olduğudur. Yapılan istatistiki analizlerde birinci hipotezin desteklendiği belirlenmiştir. Bu çerçevede iç denetçiler, sadece mevzuatı uygulayıp, elde edilen bulguları takip etme görevlerini değil, ortak amaçlar kapsamında yönetime ya da talep eden bölümlere danışmanlık faaliyeti de sağlamaları, iç denetçilerin bilgi güvenliği ile olan ilişkilerinin daha iyi olması arasında pozitif ilişki ortaya çıkmaktadır. Bir başka deyişle iç denetim ve bilgi güvenliği arasındaki ilişkinin, iç denetçilerin klasik denetim anlayışı yerine danışmanlık ya da yol gösterici faaliyetlere ağırlık verdiğinde daha iyi bir noktaya geleceği ortaya çıkmaktadır. Bu kapsamda eksiklikleri bulup raporlayan ve söz konusu eksiklerin giderilememesi durumunda çeşitli müeyyidelerin uygulanması öneren bir denetim anlayışında denetlenen taraf, denetleyen taraf ile olabildiğince düşük düzeyde iletişim kurmaya çalışacak, talep edilen belgeleri sunacak ve belki de ileride bir ceza almamak için bazı bilgi ve belgeyi denetleyen tarafa sunmaktan imtina edebilecektir. Oysa denetleyen tarafın ceza verme amaçlı değil hataların kök nedenini bulup yerinde düzeltme anlayışı ile yapacağı bir denetim faaliyetinde denetlenen taraf çözümün bir parçası olma güdüsü ile denetim sürecine olumlu katkı sağlayabilecektir.

Çalışmanın ikinci hipotezinde ise iç denetçilerin; iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin niteliğine dair algılarının, iç denetimin gerçekleştirdiği bilgi güvenliği denetimlerinin sıklığına dair algılarıyla pozitif ilişkili olduğu test edilmiş ve yapılan istatistiksel analiz sonucunda hipotez kabul edilmiştir. Buna göre bilgi güvenliği denetimlerinin yapılma sıklığı; iç denetçilerin bilgi güvenliğinden sorumlu personel ile daha fazla etkileşim içinde olmalarına neden olmaktadır. Özellikle ilk kez yapılan denetimlerde denetlenen taraf için denetim süreci bir bilinmezlik olarak algılanabilir. Gerek denetim sürecinin

aşamaları gerek ise de iç denetçilerin hal ve tavırları denetlenen için bir kaygı unsuru olarak ortaya çıkabilecektir. Bu tür bir denetim ilişkisinde sağlıklı iletişimin sağlanamaması gibi denetim sürecine zarar verebilecek sonuçlar ortaya çıkabilir. İşte bu aşamada iç denetim birimi ile bilgi güvenliği uzmanlarının daha sık etkileşime girdiği bir denetim sürecinde iki tarafın da karşı tarafa ilişkin kaygıları azalacak ve iki fonksiyon arasında daha iyi bir ilişki kurulabilecektir.

Üçüncü hipotezde ise iç denetçilerin; iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin niteliğine dair algıları, iç denetçinin bilgi güvenliği hakkındaki yetkinliğine dair algılarıyla pozitif ilişkili olduğu test edilmiş ve gerçekleştirilen analiz sonucunda hipotez kabul edilmiştir. Denetim sürecinde denetlenen taraf, iç denetçinin bilgi güvenliğine ilişkin temel unsurlarda yetersiz olduğunu düşündüğünde sürece katkısı olumsuz olarak etkilenir. Denetleyen tarafın da kendini bilgi güvenliği konularında eksik hissetmesi denetim sürecine olumsuz yansıyacaktır. Özellikle sorunların kök nedenine inememe, teknik kavramların fazlalığı nedeniyle denetlenenin cevaplarını değerlendirememe gibi sorunlar ortaya çıkabilecek ve denetim süreci olumsuz etkilenecektir. Denetim sürecindeki bu olumsuzluk iki fonksiyon arasındaki ilişkiye de olumsuz anlamda etki edecektir.

Çalışmanın dördüncü hipotezinde iç denetim ve bilgi güvenliği arasındaki ilişkinin niteliğinin; iç denetçilerin, içinde bulundukları iç denetim fonksiyonunun organizasyona sağladığı katma değere dair algılarıyla pozitif ilişkili olduğu test edilmiş olup, hipotez kabul edilmiştir. İşletmedeki iç denetim fonksiyonun organizasyonel değerin artırılması, korunması ve geliştirilmesi gibi bir misyonu bulunmaktadır. İç denetim biriminin düzenli ve etkili bilgi güvenliği denetimleri ve bilgi güvenliği sorumluları ile olan iyi ilişkisi neticesinde işletmenin bilgi güvenliği politikalarını uygulama ve bunlara uyum konusundaki yetkinliğini artırma konularında gelişme sağlanacaktır. Söz konusu gelişme sonucunda etkin bir bilgi güvenliği politikası izlenmiş olacak ve bilginin korunması hedefi gerçekleşmiş olacak ve dolayısıyla işletmeye katma değer sağlanmış olacaktır.

Beşinci hipotezde, iç denetim ve bilgi sistemleri fonksiyonları arasındaki ilişkinin algılanan niteliğinin; iç denetçilerin, bilgi güvenliği etkinliğine olan algılarıyla

pozitif ilişkili olduğu test edilmiş ve yapılan istatistiksel analizler sonucunda kabul edilmiştir. Denetim ve bilgi güvenliği arasındaki iyi bir ilişki, denetim süreçlerinin sağlıklı bir şekilde yürütülmesi ve organizasyonda yer alan bilginin, bilgi güvenliğinin 3 temel unsuru olan gizlilik, bütünlük ve erişilebilirlik ilkelerine maksimum uyum sağlanması ile elde edilebilmektedir. Başarılı bir şekilde yürütülen bilgi güvenliği denetim faaliyetleri, gerek bilgi güvenliği politikalarının eksiksiz şekilde takip edilebilmesi gerek ise de bilgi güvenliği ilkelerine uyumlu olunmasını sağlamaktadır.

Altıncı ve son hipotezde ise üst yönetimin bilgi güvenliğine yönelik desteğinin algılanan niteliğinin; iç denetçilerin, bilgi güvenliği etkinliğine olan algılarıyla pozitif ilişkili olduğu test edilmiş olup, hipotez kabul edilmiştir. Bilgi güvenliğine ilişkin sorumluluk sadece bilgi güvenliğinden sorumlu kişilerde değil tüm işletme çalışanlarındadır. Özellikle üst yönetim yol gösterici ve politikalara yön veren bir pozisyonda olduğundan üst yönetimin bilgi güvenliği farkındalığı tüm bilgi güvenliği süreçlerine etki etmektedir. Bu kapsamda gerek farkındalık eğitimleri gerek ise de ayrılan kaynaklar ile üst yönetim bilgi güvenliğine destek vermektedir.

Demografik özelliklere göre yapılan analizlerde ise 40 yaş altı katılımcılara göre 40 yaş üstü katılımcılara iç denetimin rolünün klasik denetim anlayışı olan mevzuata uyum ve eksiklikleri belirleme olarak görüldüğü, tam tersi 40 yaş altı iç denetçilerde ise iç denetimin danışmanlık rolünün daha fazla benimsenmeye başlandığı görülmüştür.

Yaş noktasında 40 yaş altı ve üstü gruplarda istatistiksel olarak anlamlı olan bir başka farklılık da 40 yaş üstü grup için iç denetçilerin bilgi güvenliği yetkinliğinin, iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkiyi olumlu olarak etkileyeceği konusuna 40 yaş altı gruba göre daha az katılmalarıdır. Buna göre daha genç iç denetçilerin özellikle bilgi güvenli alanındaki yetkinliklerine daha fazla önem vermekte oldukları söylenebilir. Cinsiyet anlamında hipotezlerde yer verilen bileşenlere yönelik algıları kapsamında kadın ve erkek katılımcılar arasında genel olarak bir farklılık ortaya çıkmamıştır. Eğitim düzeyi açısından bakıldığında ise lisans mezunu olan iç denetçilere göre lisans üstü mezunu alan

iç denetçilerin, bilgi güvenliği konusunda yetkinliklerinin artırılması konusuna daha olumlu yaklaştıkları görülmüştür. Çalışmaya katılan iç denetçilerin kamu iç denetim sertifikasına sahiplik bakımından anılan sertifikaya sahip olanların olmayanlara göre özellikle iç denetim ve bilgi güvenliği arasındaki iyi ilişkinin gerek iç denetimin faaliyetleri sonucu işletmeye kattığı katma değerin daha fazla olması gerek ise de işletmedeki bilgi güvenliği etkinliğini artırdığına yönelik algılarının daha olumlu olduğu görülmüştür. Uluslararası organizasyonlarca verilen iç denetim sertifikalarına sahip iç denetçilerin de benzer şekilde bilgi güvenliği etkinliği ve iç denetimin işletmeye sağladığı katma değerin, iç denetim ve bilgi güvenliği fonksiyonları arasındaki olumlu ilişki ile beraber artacağı konusunda sertifika sahibi olmayan iç denetçilere göre daha olumlu yaklaştığı ortaya çıkmıştır.

Kamu sektörü ve kamu dışı sektörlerde çalışan ayrımına göre iç denetçilerin hipotezlerde yer alan bileşenler kapsamında algılarında istatistiksel olarak anlamlı bir farklılık gözlenmemiştir. Çalışmaya katılan iç denetçilerin çalıştıkları kuruluşlarda herhangi bir bilgi güvenliği tehdidi yaşayanlar ve yaşamayanlar olmak üzere gruplandıklarında da hipotezlerde yer alan bileşenler kapsamında algılarında istatistiksel olarak anlamlı bir farklılık gözlenmemiştir.

Bilgi güvenliğine ilişkin işletme içi ya da dışı herhangi bir eğitim veya konferansa katılmayan katılan iç denetçiler, katılmayanlara göre özellikle iç denetimin algılanan rolünün daha çok danışmanlık rolüne evrilmesi, iç denetimin bilgi güvenliği yetkinliğinin artırılması ve yapılacak bilgi güvenliği denetimlerinin sıklaştırılması konularındaki algılarında istatistiksel olarak anlamlı bir farklılık söz konusu olup, anılan bileşenlere daha olumlu yaklaştıkları gözlenmiştir.

YÖNETİCİLERE ÖNERİLER

Çalışmanın bu bölümünde araştırmada elde edilen sonuçlar neticesinde iç denetim profesyonellerine ve yöneticilerine öneriler sunulmaktadır. İç denetim faaliyetlerinin katma değeri ve bilgi güvenliğinin etkinliğine ilişkin iç denetçi algıları ile iç denetim ve bilgi güvenliği arasındaki algılanan ilişkinin niteliği arasında

pozitif yönlü ilişki bize temel olarak organizasyonun değerini koruma ve ona katma değer sağlama görevine ilişkin ipuçları sunmaktadır.

Öncelikle çalışmanın ilk kısmında incelenen yönetim ve organizasyon kavramları kapsamında, iç denetim yöneticisinin içinde bulunduğu organizasyonun yapısını, bilen örgüt yapısından öğrenen örgüt yapısına kadar uzanan yelpaze içinde yönetim anlayışının hangi noktada olduğunu değerlendirmesi beklenmelidir. Ayrıca mikro ve makro çevresel faktörler de bu süreçte dikkate alınmalıdır. Böylece çalışmanın sonuç kısmında ortaya çıkmış olan, organizasyon içinde fonksiyonlar arası ilişkinin iyileştirilmesinde atılacak adımların da başarılı bir değerlendirilmesi yapılabilir. Başka bir deyişle iç denetim yöneticisi bu çalışmanın sonuçlarına göre alınabilecek aksiyonları belirlerken, öncelikle içinde bulunduğu organizasyonun yapısını çalışmanın 1. bölümü bağlamında değerlendirmelidir.

Çalışmanın sonuçları kapsamında atılacak adımlar belirlenirken iç denetim yöneticilerince dikkat edilmesi gereken bir diğer konu da organizasyondaki iç kontrol faaliyetlerinin olgunluk düzeyidir. Bir diğer deyişle işletmenin kontrol ortamı, risk değerleme süreçleri, kontrol faaliyetleri, bilgi ve iletişim süreçleri ile izleme faaliyetlerinin etkin olarak çalışmakta olup olmadığı konusunun değerlendirilmesidir. İç denetim faaliyetlerinin amaçlarından birinin de işletmedeki iç kontrol faaliyetlerinin tasarım ve etkinliğini değerlendirmek olduğu çalışmanın ilk bölümlerinde açıklanmıştı. Bu kapsamda iç denetim yöneticisi bilgi güvenliği fonksiyonu ile olan kurum içi ilişkinin iyileştirilmesi hedefine yönelik olarak öncelikle iç kontrol tasarım ve süreçlerinin etkinliğini değerlendirmelidir. Özetle etkin işleyen bir iç kontrol sürecine sahip organizasyonlarda iç denetim ve bilgi güvenliği arasındaki ilişkinin olumlu yönde gelişmesi daha kolay ve hızlı olabilmektedir.

İç denetim ve bilgi güvenliği fonksiyonunun arasındaki ilişkinin niteliğini etkileyen faktörler incelendiğinde, gerek danışmanlığa yönelen iç denetim rolü, gerek iç denetimin bilgi güvenliği ile daha fazla etkileşime girmesi bir diğer deyişle daha fazla sıklıkta bilgi güvenliği denetimi gerçekleştirmesi ve gerekse de iç denetçilerin bilgi güvenliğine dair yetkinliklerinin artırılması konuları öne çıkmaktadır. İç denetçilerin görevlerinin geçmişte olduğu gibi sadece eksikleri

bulup raporlamak değil bununla beraber denetlenen birime; süreçlerin, iş ve işlemlerin nasıl daha verimli ve etkili şekilde yürütülebileceği konusunda da yol gösterici rolü izlemesi sağlanmalıdır. Benzer şekilde klasik teftiş anlayışı ile iç denetim arasındaki yaklaşım farklarının da iki fonksiyon arasındaki ilişkinin geliştirilmesinde önem arz eden bir konu olduğu iç denetim yöneticilerince dikkate alınmalıdır. Bu bağlamda 1. Hipotez kapsamında, özellikle çalışmanın önceki bölümlerinde incelenen uygunluk denetimi, faaliyet denetimi ve iç denetim konularında ele alınan farklılıklar iç denetim yöneticisi için bir rehber olarak değerlendirilebilir. İç denetim görevlendirmelerinde bilgi güvenliği alanlarında iç denetçilere sadece denetim görevleri değil zaman zaman danışmanlık görevleri de atanarak iç denetçilerin bilgi güvenliği faaliyetlerine farklı bir bakış açısı ile bakmaları sağlanabilir. Böylece bilgi güvenliği çalışanları iç denetimin sadece eksik ya da hata bularak bunun izlemesini yapmadığı örneğin bilgi güvenliği süreçlerinin nasıl daha verimli yürütülebileceğine ilişkin ve benzer konularda iş birliği içinde çalışabilecek bir bölüm olduğunu deneyimleyebilir. Dolayısıyla iç denetim ve bilgi güvenliği arasındaki ilişki sadece denetlenen ve denetleyen ilişkisinden farklılaşarak ortak bir hedef için beraber çalışmaya evrilmiş olmaktadır.

İç denetim ve bilgi güvenliği arasındaki ilişkiyi ve dolayısıyla iç denetimin katma değerini ve bilgi güvenliği etkinliğini etkileyen bir diğer unsur da iç denetim ve bilgi güvenliği etkileşim sıklığıdır. Çalışmanın 2. hipotezi ile bilgi güvenliği konularında yapılacak denetimlerdeki sıklık ile anılan iki fonksiyonun arasındaki ilişkinin niteliği arasında pozitif yönlü ilişki olması test edilerek hipotez kabul edilmiştir. Bu kapsamda iç denetim yöneticilerinin özellikle üç yıllık iç denetim planları ve yıllık iç denetim programlarını hazırlanırken özellikle bilgi güvenliği denetimlerine yönelik olarak organizasyonun imkanları dahilinde denetimlere farklı denetim ekiplerinin yılın farklı dönemlerinde denetim gerçekleştirebilecekleri şekilde tasarlanması önerilmektedir. Denetimlerin imkanların el verdiği ölçüde sık periyodlar ile gerçekleştirilmesi de önerilmektedir. Söz konusu denetimlere örnek olarak çalışmanın ilk bölümünde değinilen ara dönem denetimleri verilebilir. Ara dönem denetimleri yıl sonu denetimlerinden farklı olarak yıl sonu mali tablolarının değil ara mali tabloların belirli aralıklarla denetlenmesidir. Ara denetimler yıl sonu

denetimlerinin süresinin kısalmasını sağlar ve bir anlamda önleyici bir denetim türü olarak değerlendirilebilir. Benzer şekilde iç denetim faaliyetleri de ara dönemler şeklinde planlandığında hem yıllık iç denetim faaliyetlerinin sürelerinin kısalması hem de iç denetim ve bilgi güvenliği arasındaki iletişimin sıklaştırılması anlamında önemli olduğu değerlendirilmektedir. Özellikle çalışmanın üçüncü bölümünde detaylı şekilde ele alınmış olan, ISO 27001 sertifikası kapsamındaki iç tetkik faaliyeti yılda en az bir kere bilgi güvenliği denetimini zorunlu kılmaktadır. Benzer şekilde Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi denetimlerinin de yıllık olarak gerçekleştirilmesi gerekli olduğundan, söz konusu denetimlerin alt başlıklarının yıl içinde bölümlendirilerek ara denetimler şeklinde yapılmasının, bilgi güvenliği ve iç denetim fonksiyonları arasındaki etkileşimi artırması ve böylece iki fonksiyon arasındaki ilişkinin niteliğine olumlu etki yapması söz konusu olmaktadır.

Denetim ve bilgi güvenliği arasındaki ilişkinin niteliğini etkileyen diğer bir faktör iç denetimin bilgi güvenliği yetkinliğidir. Çalışmanın 3. hipotezi ile iç denetim bilgi güvenliği yetkinliği ile söz konusu iki fonksiyon arasındaki ilişkinini niteliği arasındaki pozitif yönlü ilişki test edilerek hipotez kabul edilmiştir. Buna göre iç denetim yöneticilerinin gerek hizmet içi eğitimler gerek mesleki sertifikasyon alımını cesaretlendirme gerekse de seminer, konferans vb. etkinliklere katılımın sağlanması yoluyla iç denetçilerin bilgi güvenliği yetkinliklerini artırılması önerilmektedir. Özellikle CISA ya da CIA gibi uluslararası kabul görmüş denetçi sertifikasyon süreçlerinde, ilgili sertifikanın sınavlarına çalışırken elde edilen akademik kazanımın yanında, bir de sertifika alındıktan sonra denetçilerin yıllık olarak tamamlamaları gereken eğitim vb. saat/yıl hedefleri bulunduğundan kazanılan bilginin güncel tutulması sağlanmaktadır. Aksi takdirde elde ettikleri sertifikalar pasif duruma düşmekte ve kullanılamamaktadır. Benzer şekilde ISO 27001 ve Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi kapsamında da bilgi güvenliği denetimi yapacak iç denetçilerin belirli sertifikasyonları haiz olması ya da minimum tecrübe ve yetkinlikte olmasının beklendiği dikkate alınmalıdır.

İç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin algılanan niteliği ile iç denetim bilgi güvenliği denetimlerinin yarattığı katma değer arasında pozitif yönlü ilişkiyi içeren 4. hipotez de test edilerek kabul edilmiştir. Bu çerçevede iç denetim ve bilgi güvenliği yöneticileri açısından ve üst yönetim açısından her iki fonksiyon arasındaki uyuşmazlık, iletişim eksikliği, karşılıklı güven ve anlayış gibi çeşitli alanlardaki sorunların en aza indirilmesi konusunda ortak çaba sağlanması önerilmektedir. İç denetim ve bilgi güvenliği özelinde birbirine güvenen ve birbirini anlayan iki bölüm arasında gerek denetim süreci öncesinde evrak belge talebinde, gerekse de denetim süreci ve sonrasında izleme süreçlerinde daha başarılı denetim faaliyetleri ve gelişim fırsatları ortaya çıkabilecektir. Bu kapsamda söz konusu iki bölüm arasında var olan uyumsuzlukların giderilmesi için kurum içi paydaş toplantıları, isimsiz öneri kutusu, bölüm içi anketler vs. gibi bir bölüm çalışanlarının diğer bölüm çalışanları ile arasındaki ilişkilerine yönelik araştırmalar ve iyileştirmeler yapılması ve sonuçlarına göre gerekli çözüm yollarına başvurulması önerilmektedir.

Bilgi güvenliği ve iç denetim ilişkisinin algılanan niteliği ile pozitif yönlü ilişki içinde bulunan diğer faktör de algılanan bilgi güvenliği etkinliğidir. Test edilerek kabul edilen çalışmanın 5. hipotezine göre iç denetçiler, aralarında iyi bir ilişkin bulunan iç denetim ve bilgi güvenliği fonksiyonlarının organizasyondaki bilgi güvenliği etkinliğini de olumlu yönde etkileyeceğini düşünmektedir. Bu bakış açısında; denetlenen birim olan bilgi güvenliği fonksiyonu ile yapılan etkileşimde gerçekleşen denetimin kalitesi ve bu denetimler neticesinde bilgi güvenliği fonksiyonunun daha da olumlu yönde gelişecek olması, söz konusu algının kaynağı olarak değerlendirilebilmektedir. Bu kapsamda katma değer faktöründe de olduğu her iki fonksiyonu da içeren paydaş toplantıları, çalışanlara yapılacak iyileştirme önerilerine ilişkin anket vb. uygulamaların hayata geçirilmesi önerilmektedir.

Son olarak çalışmada yer alan 6. Hipotezin kabul edilmesi ile üst yönetim desteği ve bilgi güvenliği arasında pozitif yönlü ilişki ortaya çıkarılmıştır. Burada üst yönetimin bilgi güvenliği için yeterli kaynak ayırması önem arz etmektedir. Özellikle gerçekleştirilecek bilgi güvenliği eğitimler, örnek olay canlandırması, bir

canlı senaryo üzerinden farkındalık testleri, sızma testleri gibi özel bilgi güvenliği firmalarınca sağlanan farkındalığı artıcı faaliyetler bu bağlamda önerilmektedir. ISO 27001 BGYS standardı kapsamındaki sertifikasyon süreci ve tetkikler, bir organizasyonu gerek öz değerlemesini yapması gerek ise de bu konuda var olan eksikliklerini düzeltmesi anlamında kolaylaştırıcı rol oynamaktadır. Alınan sertifikanın yıllık olarak organizasyonun iç denetim birimi tarafından periyodik denetime tabi olması ve aynı zamanda TSE denetim ekiplerince de belirli periyotlarla denetlenmesi organizasyondaki bilgi güvenliği farkındalığını üst seviyeye taşıyabilmektedir.

KAYNAKÇA

Abbott, L. J., Parker, S., & Peters, G. F. (2012). Internal Audit Assistance and External Audit Timeliness. *Auditing: A Journal of Practice & Theory*, *31*(4), 3-20. https://doi.org/10.2308/ajpt-10296

Abdolmohammadi, M. J., & Boss, S. R. (2010). Factors associated with IT audits by the internal audit function [Article]. *International Journal of Accounting Information Systems*, *11*(3), 140-151. https://doi.org/10.1016/j.accinf.2010.07.004

Ackerman, M., Rucker, B., Wells, A., Wilson, J., & Wittmann, R. J. U. (2009). IT Strategic Audit Plan. *Journal of Technology Research*, *1*(1), 1-10.

Adiloğlu, B. (2010). *İç Denetim Süreci ve Temel İşletme Faaliyetlerinin Kontrol Prosedürleriyle Değerlendirilmesi: Bir Uygulama* [Doktora Tezi, İstanbul Üniversitesi]. İstanbul.

Adiloğlu, B. (2011). *İç Denetim Süreci ve Kontrol Prosedürleri*. Türkmen Kitabevi.

AICPA. (2016). *About the AICPA*. Erişim tarihi: 02.09.2016 Erişim adresi: http://www.aicpa.org/About/Pages/About.aspx

Akbulut, H. (2010). *Muhasebe Denetiminin Etkinliğini Sağlamada Denetim Komitesinin Rolü: Bağımsız Denetim Firmalarına Yönelik Bir Araştırma* [Doktora Tezi, Afyon Kocatepe Üniversitesi]. Afyonkarahisar.

Akçay, S. (2012). *Kamu Sektörü'nde İç Denetimin Etkinliğinin Ölçülmesi ve Belediyeler Üzerine Bir Uygulama* [Doktora Tezi, Dumlupınar Üniversitesi]. Kütahya.

Akpınar, M. (2011). Denetim Anlayış ve Metodolojisinde Değişimin Adı İç Denetim. *ZKÜ Sosyal Bilimler Dergisi*, *7*(14), 22.

Aktolun, O. (2002). *Bilgi Teknolojileri Denetim Yaklaşımı*. Türkiye Bankalar Birliği. Erişim tarihi: 04.01.2018 Erişim adresi: https://www.tbb.org.tr/Dosyalar/Konferans_Sunumlari/btdy1.ppt

Akyel, R. (2010). Türkiye'de İç Kontrol Kavramı, Unsurları ve Etkinliğinin Değerlendirilmesi. *Yönetim ve Ekonomi*, *17*(1), 16.

Al-Taee, S. H. H., & Flayyih, H. H. (2023). Impact of the electronic internal auditing based on IT governance to reduce auditing risk. *Corporate Governance and Organizational Behavior Review*, *7*(1), 94-100.

Alkan, M. (2015). Hüseyin Hilmi Paşa'nın Rumeli Umumi Müfettişliği (1902-1908). *CBÜ Sosyal Bilimler Dergisi*, *13*(1), 242-255.

Alp, Z. (2012). *Hukuk, Siyaset ve Ekonomi Bağlamında Kamuda Yeni Denetim Sistemi : İç Denetim* (Publication Number 232) Abant İzzet Baysal Üniversitesi]. Bolu.

Altuğ, F. (2000). *Mali Denetim*. Ezgi Kitabevi.

Anderson, D. J., & Eubanks, G. (2015). *Leveraging COSO Across The Three Lines of Defense*. COSO.

Anderson, K. A. (2012). A case for a partnership between information security and records information management. *ISACA Journal*, *2*, 40.

Arslan, M. C. (2013). *İç Denetim ve Türkiye'de Büyükşehir Belediyelerinin İç Denetim Uygulamaları Üzerine Bir Araştırma* [Doktora Tezi, Marmara Üniversitesi]. İstanbul.

Asare, S. K., & Wright, A. (2012). The Effect of Type of Internal Control Report on Users' Confidence in the Accompanying Financial Statement Audit

Report*. *Contemporary Accounting Research*, *29*(1), 152-175. https://doi.org/10.1111/j.1911-3846.2011.01080.x

Atay, O., Nord, J. H., Lee, T.-R., Cetin, F., & Paliszkiewicz, J. (2016). Examining the impact of social technologies on empowerment and economic development. *International Journal of Information Management*, *36(6)*, 1101-1110.

Ayaz, M. (2011). *Bankalarda İç Denetim Yaklaşımları ve Bir Uygulama Örneği* [Doktora Tezi, Marmara Üniversitesi]. İstanbul.

Aydın, M. D. (2007). Kamu hizmetlerinde bilgi teknolojileri uygulamalari: firsat ve tehditler. *Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *25(2)*, 295-322.

Bajary, A. R., Shafie, R., & Ali, A. (2023). COVID-19 pandemic, internal audit function and audit report lag: Evidence from emerging economy. *Cogent Business & Management*, *10*(1), 2178360.

Basku, F. (2009). *Uluslarası İnsan Kaynakları Yönetiminde İç Kontrol Etkinliği, Alstom ve NCR Örneğinde Uygulanması* [Doktora Tezi, Gazi Üniversitesi]. 2009.

Başpınar, A. (2005). Türkiye'de ve Dünyada Denetim Standartlarının Oluşumuna Genel Bir Bakış. *Maliye Dergisi*(12), 28.

Baykara, S. T. (2013). Denetimin ilişkili olduğu disiplinler üzerine bir değerlendirme. *Sayıştay Dergisi*, *Temmuz-Eylül 2013*(90), 22.

Bezirci, M. K., Fehmi. (2010). Türkiye'de Denetimin Tarihsel Gelişimi. *SÜ İİBF Sosyal ve Ekonomik Araştırmalar Dergisi*, 22.

Buchanan, S., & Gibb, F. (2007). The information audit: Role and scope. *International Journal of Information Management*, *27*(3), 159-172. https://doi.org/10.1016/j.ijinfomgt.2007.01.002

Bulut, E. Ç. (2015). Devletin Taşradaki Eli: Umumi Müfettişlikler. *CTAD*, *11*(21), 83-110.

5018 Sayılı Kanun, (2003). http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5018.pdf

BÜMKO. (2015). Kamu İç Kontrol Rehberi. In T. C. M. Bakanlığı (Ed.), (pp. 132).

BÜMKO. (2016). *Mali Yönetim ve Kontrol*. Erişim tarihi: 06.11.2017 Erişim adresi: http://kontrol.bumko.gov.tr/TR,7059/mali-yonetim-ve-kontrol.html

Büyükmirza, H. K. (2008). *Maliyet Muhasebesi ve Yönetim* (12. Baskı ed.). Gazi Kitabevi.

Can, A. (2013). *Yerel Yönetimlerde İç Denetim: İstanbul Su ve Kanalizasyon İdaresi Örneği* Marmara Üniversitesi]. İstanbul.

Can, H. (1999). *Organizasyon ve Yönetim*. Siyasal Kitabevi.

Çatıkkaş, Ö. (2005). *Bankalarda İç Kontrol Sistemi ve İç Denetim Fonksiyonunun Etkililiği* [Doktora Tezi, Marmara Üniversitesi]. İstanbul.

Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi, 1-2 (2019). https://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20190706-12.pdf

CBDDO. (2020). *Bilgi ve İletişim Güvenliği Rehberi*. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

CBDDO. (2021). *Bilgi ve İletişim Güvenliği Denetim Rehberi*. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

Chevers, J. E. e. a. (2013). The Internal Audit Process And Good Governance: Toward A Research Model. *Academy of Business Research Journal*, *1*, 48-58.

Coates, S., Haege, M., Johannessen, R., Lourens, J., & Martinez, L. C. (2013). *Global Teknoloji Denetim Rehberi (GTAG)*. IIA.

Coderre, D. (2009). *Internal Audit: Efficieny Through Automation*. Wiley.

COSO. (2016a). COSO Internal Control - Integrated Framework Principles. In C. Graphic (Ed.), (pp. 1): Committee of Sponsoring Organizations.

COSO. (2016b). *COSO: About Us*. Erişim tarihi: 05.10.216 Erişim adresi: http://www.coso.org/aboutus.htm

COSO. (2016c). *Fraud Risk Management Guide*. Committee of Sponsoring Organizations.

D. Chambers, A. (2014). New guidance on internal audit – an analysis and appraisal of recent developments. *Managerial Auditing Journal*, *29*(2), 196-218. https://doi.org/10.1108/maj-08-2013-0925

Dal, S., & Çalış, Y. E. (2012). Anonim Şirketlerde Bağımsız Denetim ve Bağımsız Denetçi. *Mali Çözüm Dergisi*(Temmuz-Ağustos 2013), 87-106.

Demircioğlu, K. (2009). *Ticari Bankalarda Operasyonel Risk Yönetimi ve Denetimi: Türkiye, Hollanda ve Rusya Uygulaması* [Doktora Tezi, Marmara Üniversitesi]. İstanbul.

Dittonhofer, M. A. v. A. (2010). *Behavioral Dimensions of Internal Auditing: A Practical Guide to Professional Relationships in Internal Auditing* (The Institute of Internal Auditors Research Foundation, Issue.

Donathan, C. (2012). So you want to be an IT auditor: practitioners need a combination of technical and people skills to forge a career in auditing technology. *Internal Auditor*, *69*(5), 25-27.

Duman, Ö. (2008). *Muhasebe Denetimi ve Raporlama*. TESMER.

Dunn, J. (2010). *Financial Reporting And Analysing*. Wiley.

EATC. (2018). Information Life Cycle. In (Vol. 2018): European Association for Technical Communication;.

Efe, A. (2016a). Kamu Yönetiminde COBIT-5 Çerçevesinde Risk Yönetimi. *Uluslararası Eğitim Bilim ve Teknoloji Dergisi*, *2*(1), 18.

Efe, A. (2016b). Strateji Belirlemede Türkiye'de Kalkınma Ajanslari İçin Bütüncül Yaklaşım: Cobit-5 Kapsamında Ulusal Strateji Belgeleri Üzerinde Bir Analiz. *TESAM Akademi Dergisi*, *3*(2), 30.

Erdem, Y. T. (2009). Osmanlı eğitim sisteminde teftiş. *Osmanlı Tarihi Araştırma ve Uygulama Merkezi Dergisi*(26), 55-55.

Ergeneli, A. (2006). *Örgüt ve İnsan*. Hacettepe Üniversitesi.

Ersoy, E. V. (2012). *ISO/IEC 27001 Bilgi Güvenliği Standardı : Tanımlar ve Örnek Uygulamalar*. ODTÜ Yayıncılık.

Esen, Ü. B., & Atay, Ö. (2017). Ekonominin Yeni Yüzü: Yaratıcı Ekonomi [Article]. *The New Face of Economy: Creative Economy.*, *25*(3), 59-80. https://doi.org/10.17233/sosyoekonomi.289441

Ettredge, M. L., Li, C., & Sun, L. (2006). The impact of SOX Section 404 internal control quality assessment on audit delay in the SOX era. *Auditing: A Journal of Practice & Theory*. http://www.aaajournals.org/doi/abs/10.2308/aud.2006.25.2.1

Florea, R. F., Ramona. (2013). Internal Audit and Corporate Governance. *Economy Transdisciplinarity Cognition*, *16*(1), 79-83.

Florina, P. A., Ludovica, B., & Leonica, B. J. (2013). Challenges of internal audit in the current crisis. *The Annals of the University of Oradea, Ser.: Economic Science*, *22*(1), 1354-1362.

Frisken, J. (2015). Leveraging COBIT to Implement Information Security. *COBIT Focus*, 1-6.

Galligan, M. E., & Rau, K. (2015). *COSO in the Cyber Age*. COSO.

GAO. (2016). *About GAO*. U.S. Government Accountability Office. Erişim tarihi: 03.11.2016 Erişim adresi: http://www.gao.gov/about/

Gençoğlu, M. (2012). Erzurum Vilâyeti Maârif Teftişleri (1910). *Cumhuriyet Tarihi Araştırmaları Dergisi*, *8*(16), 151.

Gökalp, B. (2013). *Kamu Yönetiminde İç Denetimin Etkinliğinin Ölçülmesi* [Yüksek Lisans Tezi, Gazi Üniversitesi]. Ankara.

Gökoğlan, K. (2010). *Kamu İç Denetçilerinde Tükenmişlik Sendromu Üzerine Bir Araştırma* [Yüksek Lisans Tezi, Niğde Üniversitesi]. Niğde.

Gönenç, B. G. (2011). *Kamu İdarelerinin İç Denetimi* [Yüksek Lisans Tezi, Marmara Üniversitesi]. İstanbul.

Gönülaçar, Ş. (2008). İç Denetimin Bürokratik Serencamı. *Mali Hukuk Dergisi*, *Haziran 2008*(135), 21.

Gönülaçar, Ş. (2012). Etkili Bir Yolsuzlukla Mücadele İçin Kamu Denetiminde Yeni Bir Kurumsal Yapı Önerisi. *Mali Hukuk Dergisi*, *27*(159), 16.

Güler, C. (2010). Kamuda Yeni Denetim Sistemi: İç Denetim. *Dış Denetim Dergisi*(Temmuz-Ağustos-Eylül 2010), 9.

Günay, N. A. (2009). Osmanlı Taşrasında Bir Yetki Alanı Haremeyn-i Şerifeyn Teftiş Vekâleti Görevi ve Kapsamı. *Ankara Üniversitesi Osmanlı Tarihi Araştırma ve Uygulama Merkezi Dergisi*, *Güz 2009*(26), 11.

Güner, M. F. (2009). Kamu Yönetiminde İç Denetime Geçiş Süreci ve Karşılaşılan Sorunlar Kamu iİç Denetiminin Değişimi Üzerine Bir Araştırma. *Ç. Ü. Sosyal Bilimler Enstitüsü Dergisi*, *18*(2), 19.

Havelka, D., & Merhout, J. W. (2013). Internal information technology audit process quality: Theory development using structured group processes. *International Journal of Accounting Information Systems*, *14*(3), 165-192. https://doi.org/10.1016/j.accinf.2012.12.001

Héroux, S., & Fortin, A. (2013). The Internal Audit Function in Information Technology Governance: A Holistic Perspective. *Journal of Information Systems*, *27*(1), 189-217. https://doi.org/10.2308/isys-50331

Hill, E. (2011). The Relevant IT AUDIT. *Internal Auditor*, *68*(3), 57-61.

Humaidi, N., & Shahrom, M. (2023). Assessing Employees' Cybersecurity Attitude Based on Working and Cybersecurity Threat Experience. *The African Journal of Information Systems*, *15*(3), 3.

Hüner, D. B. (2014). *Bağımsız Denetimde İç Kontrol ve İç Denetimin Rolü* [Yüksek Lisans Tezi, Okan Üniversitesi]. İstanbul.

IAF. (2023). Transition Requirements for ISO/IEC 27001:2022. *International Accreditation Forum* 13.

Ibrahim, N. (2014). It audit 101. *Internal Auditor*, *71*(3), 19-21.

İDDK. (2014). *Kamu Bilgi Teknolojileri Denetimi Rehberi* http://www.idkk.gov.tr/SiteDokumanlari/Mevzuat/Ucuncul%20Duzey%20Mevzuat/KamuBTDenetimiRehberi/KamuBTDenetimiRehberi.pdf

IEC. (2017a). *IEC: About Us*. Erişim tarihi: 02/05/2017 Erişim adresi: http://www.iec.ch/about/profile/

IEC. (2017b). Welcome to the IEC. In IEC (Ed.), (pp. 36). Geneva: IEC.

IEC, I. (2014). Information and Communications Technology ISO/IEC JTC 1: Vision, Mission and Principles. In (pp. 8).

IIA. (2015). İç Denetim Standartları: Neden Önemlidir? In *Tone at the TOP* (Vol. 73): Institute of Internal Auditors.

IIA. (2016a). *About The IIA*. Institute of Internal Auditors. Erişim tarihi: 23/04/2022 Erişim adresi: https://na.theiia.org/about-us/Pages/About-The-Institute-of-Internal-Auditors.aspx

IIA. (2016b). Information on IIA. In: Institute of Internal Auditors.

IIA. (2016c). IT and the integrated audit. In (pp. 70): Institute of Internal Auditors, Inc.

IIA. (2017). *Uluslararası İç Denetim Standartları* (Vol. 1). Türkiye İç Denetim Enstitüsü.

IIA. (2018a). Etik Kuraları. In (Vol. 2018, pp. 2): Türkiye İç Denetim Enstitüsü.

IIA. (2018b). *Standartlar*. T. İ. D. Enstitüsü.

IIA. (2024a). *The Future of IPPF Evolution*. The Institute of Internal Auditors, Inc. Erişim tarihi: 07.06.2024 Erişim adresi: https://www.theiia.org/en/standards/2024-standards/future-of-the-ippf-evolution/

IIA. (2024b). Global Internal Audit Standarts. In (pp. 120): The Institute of Internal Auditors, Inc.

IIA. (2024c). Two-Way Mapping : 2017 Standarts to 2024 Standarts. In (pp. 166): The Institute of Internal Auditors, Inc.

IIARF. (2016a). *SAWYER'S İç Denetçiler İçin Rehber 1.Cilt* (Vol. 1). Türkiye İç Denetim Enstitüsü.

IIARF. (2016b). *SAWYER'S İç Denetçiler İçin Rehber 2.Cilt* (Vol. 2). Türkiye İç Denetim Enstitüsü.

IIARF. (2016c). *SAWYER'S İç Denetçiler İçin Rehber 3.Cilt* (Vol. 3). Türkiye İç Denetim Enstitüsü.

INTOSAI. (2016a). *INTOSAI*. International Organization of Supreme Audit Institutions. Erişim tarihi: 01.11.2016 Erişim adresi: https://www.intosai.org/focus-areas/audit-standards.html

INTOSAI. (2016b). *Working Group on IT Audit*. Erişim tarihi: 11.11.2016 Erişim adresi:

ISACA. (2014). COBIT 5. In (Vol. 2014/1): Information Systems Audit and Control Association.

ISACA. (2019). COBIT 2019 Çerçevesi : Giriş ve Metodoloji. In (Vol. 2019): Information Systems Audit and Control Association.

ISACA. (2012). COBIT 5: A business framework for the governance and management of enterprise IT. In (pp. 11): Information Systems Audit and Control Association.

İSMMO. (2020). *Denetim Standartları* (Vol. 2020). İstanbul Serbest Muhasebeci Mali Müşavirler Odası.

ISO. (2017a). *ISO/IEC 27000 family - Information security management systems*. Erişim tarihi: 01/05/2017 Erişim adresi: https://www.iso.org/isoiec-27001-information-security.html

ISO. (2017b). *ISO: About Us*. Erişim tarihi: 02/05/2017 Erişim adresi: https://www.iso.org/about-us.html

ISO/IEC. (2022). 27001:2022 International Standart. 152.

ITU. (2018). *The ICT Development Index (IDI)*. Erişim tarihi: 12.02.2018 Erişim adresi: http://www.itu.int/net4/ITU-D/idi/2017/index.html

Jackson, R. A. (2012). Facing IT risk head-on: internal audit departments must confront constantly emerging technology threats without losing sight of previous dangers that never go away. (4), 36.

Kapic, J. (2013). Internal Supervision, Internal Control and Internal Audit. *Poslovni Konsultant (Business Consultant)*, 13.

Kaplan, R. (2009). *Türk Kamu Harcama Yönetiminde Hesap Verme Sorumluluğunun İncelenmesi ve Değerlendirilmesi* [Doktora Tezi, Gazi Üniversitesi]. Ankara.

Kara, S. (2011). *İç Denetimde Risk Yönetimi* [Doktora Tezi, Celal Bayar Üniversitesi]. Manisa.

Kara, S. S., Şakir. (2012). Kurumsal Risk Yönetimi Çerçevesinde Rİsk Odaklı İç Denetim ve İMKB Uygulaması. *Muhasebe ve Vergi Uygulamaları Dergisi*, *5*(1), 69-95.

Kara, S. Y., Ayşe N. (2012). İç Denetimde Risk Yönetimi ve İMKB- İmalat Sanayi Sektöründe Bir Uygulama. *Muhasebe ve Finansman Dergisi*, *Nisan-2012*(54), 65-86.

Kaval, H. (2008). *Muhasebe Denetimi* (3.Baskı ed.). Gazi Kitabevi.

Kılıç, M. (1989). İnnovasyon ve İşletmeler [article]. *7/1-2*.

Kılıç, M. (2010). Stratejik Yönetim Sürecinde Değerler, Vizyon ve Misyon Kavramları Arasındaki İlişki [Article]. *Sosyoekonomi Dernegi*, *13*(2), 81-98.

Kılıç, M., & Aktuna, A. (2015). Perceptions on the obstacles of strategy execution: The case of turkish public organizations [Article]. *Hacettepe University, Faculty of Economic & Administrative Sciences.*, *33*(1), 101-136.

Kılıç, M., & Bariş, B. (2010). İhracatçı Türk Firmalarında Personel Sağlama ve Seçme Yöntemleri ve İnovasyon Performansı İlişkisi: Orta Anadolu İhracatçı Birlikleri Örneği. In (Vol. 13, pp. 215-241): Sosyoekonomi Dernegi (Sosyoekonomi Society).

Kincaid, J. K., & Sampias, W. J. (2005). *Certified Government Auditing Professonal Examination Study Guide*.

Kizza, J. M. (2007). *Computer Network Security and Cyber Ethics*. McFarland & Company, Inc.

Koçel, T. (2001). *İşletme Yöneticiliği*. Beta Yayınevi.

Köklü, M. (1996). Etkili Denetim. *Eğitim Yönetimi*, *2*(2), 10.

Korkmaz, Y. (2013). *Uluslararası İç Denetim Standartları Çerçevesinde Türk Bankacılık Sisteminde İç Denetim* [Yüksek Lisans Tezi, Marmara Üniversitesi]. İstanbul.

Kotak, J., Habler, E., Brodt, O., Shabtai, A., & Elovici, Y. (2023). Information Security Threats and Working from Home Culture: Taxonomy, Risk Assessment and Solutions. *Sensors (Basel)*, *23*(8), 4018. https://doi.org/10.3390/s23084018

Kotb, A., Elbardan, H., & Halabi, H. (2020). Mapping of internal audit research: a post-Enron structured literature review. *Accounting, Auditing & Accountability Journal*, *33*(8), 1969-1996. https://doi.org/10.1108/AAAJ-07-2018-3581

Kotler, P., & Armstrong, G. (2012). *Principles of Marketing*.

Kulak, F. (2009). *Merkez Bankalarında İç Kontrol ve İç Denetim: Kavramsal Çerçeve ve Türkiye Cumhuriyet Merkez Bankası'nda İç Kontrol ve İç Denetimin Etkililiği Konununda Bir Değerlendirme* [Doktora Tezi, Marmara Üniversitesi]. İstanbul.

Kuluçlu, E. (2008). Türk Hukuk Sisteminde Normlar Hiyerarşisi ve Sayıştay Denetimine Etkileri. *Sayıştay Dergisi*(71), 20.

Kurnaz, N., & Çetinoğlu, T. (2010). *İç Denetim -Güncel Yaklaşımlar*. Umuttepe Yayımları.

Kurnaz, N., & Dindaroğlu, A. K. (2016). İç denetim ve bilgi güvenliği ilişkisi: Bölgesel bir araştırma. *Bilgi Ekonomisi ve Yönetimi Dergisi*, *10*(1).

Lupu, M. e. a. (2013). Internal audit, risk detection tool for contemporary crisis. *Internal Auditing & Risk Management*, *8*(2), 149-158.

Masli, A., Peters, G. F., Richardson, V. J., & Sanchez, J. M. (2010). Examining the potential benefits of internal control monitoring technology. *Accounting Review*, *85*(3), 1001-1034. https://doi.org/10.2308/accr.2010.85.3.1001

McGill, M. E. S., W. John. (1993). *Unlearning the Organizations*. Elsevier Science Publishing.

McNally, J. S. (2013). The 2013 COSO Framework & SOX Compliance. In (pp. 9): Committee of Sponsoring Organizations.

Memiş, M. Ü. (2006). *İç Denetimin Yönetim Fonksiyonlarının Yerine Getirilmesindeki Rolü: Türkiye'deki Büyük İşletmeler Üzerinde Bir Saha Araştırması* [Doktora Tezi, Çukurova Üniversitesi]. Adana.

Moeller, R. (2005). *Brink's Modern Internal Auditing*. John Wiley & Sons, Inc.

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

Moorthy, M. K. A. (2011). The Impact of Information Technology on Internal Auditing. *African Journal of Business Management*, *5*(9), 17.

Munsif, V., Raghunandan, K., & Rama, D. V. (2012). Internal Control Reporting and Audit Report Lags: Further Evidence. *Auditing: A Journal of Practice & Theory*, *31*(3), 203-218. https://doi.org/10.2308/ajpt-50190

Newfoundland, M. U. o. (2017). *What Is Information Management?* Erişim tarihi: 20.09.2017 Erişim adresi: https://www.mun.ca/cio/imp/whatisim.php

Nicho, M. (2009). Information technology audit: systems alignment and effectiveness measures. *aut.researchgateway.ac.nz*.

Nurdoğan, A. (2009). II. Abdülhamid Döneminde Rumeli'de Maarifin Teftişi. *Osmanlı Tarihi Araştırma ve Uygulama Merkezi Dergisi*(26), 193-193.

Office, U. S. G. A. (2011). *Government Auditing Standarts 2011 Revision*.

Oğuz, M. (2006). *II. Abdülhamid'e Yerel Yönetimlerde (Sivas, Canik Sancağı) Yapılan Yolsuzluklarla İlgili Sunulan Bir Lahiya* (Publication Number 3) [Master, Ankara, Üniversitesi,]. Ankara Türkiye.

Öktem, M. K., & Aydın, M. D. (2005). *Information Technologies and Transformation of Turkish Public Administration*. Hacettepe Üniversitesi.

Okur, Y. (2010). Türkiye'de Teftiş ve İç Denetim: Kavramlar, Beklentiler ve Hayatla Yüzleşme. *Maliye Dergisi*, *Ocak-Haziran 2010*(158), 17.

Ölmez, A. (2012). Askerî teftîş komisyonu'nun kuruluşu ve faaliyetleri. In. İstanbul Üniversitesi.

Önaçan, M. B. K., Medeni, T. D., & Özkanli, Ö. (2012). Elektronik belge yönetim sistemi (ebys)'nin faydalari ve kurum bünyesinde ebys yapılandırmaya yönelik bir yol haritasi. *Sayıştay Dergisi*(85), 1.

Önder, Ö. T., İrfan. (2012). Denetim Anlayışının Değişimi: Yeni Sayıştay Kanunu Üzerine Değerlendirmeler. *Uluslararası Yönetim İktisat ve İşletme Dergisi*, *8*(12), 18.

Orth, D., & Schuldis, P. M. (2021). Organizational learning and unlearning capabilities for resilience during COVID-19. *The Learning Organization*, *28*(6), 509-522. https://doi.org/10.1108/TLO-07-2020-0130

Özdemir, S. (2011). İç Denetim Etiği ve Kamu İç Denetçileri Tarafından Algılanışı. *Akdeniz Üniversitesi Uluslararası Alanya İşletme Fakültesi Dergisi*, *3*(2), 19.

Özeren, B. (2004). *INTOSAI - Kamu Kesimi İç Kontrol Standartları Rehberi*.

Özkan, Y. (2008). *5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu Kapsamsında İç Denetimin Değerlendirilmesi ve Öneriler* [Doktora Tezi, Marmara Üniversitesi]. İstanbul.

Palmer, L. A. (2008). Considering Bias in Government Audit Reports: Factors That Influence the Judgments of Internal Government Auditors. *Journal of Business Communication*, *45*(3), 265-285. https://doi.org/10.1177/0021943608317521

Parlak, M. P., Z. (2014). Sayıştay Denetçilerinin Denetimle İlgili Algıları, Beklentileri ve Görüşleri Üzerine Bir Anket Çalışması. *Sayıştay Dergisi*, *Ocak-Mart 2014*(92), 30.

Pehlivanlı, D. (2008). *Kurumsal Risk Yönetimi Temelli İç Denetim ve Türkiye Uygulamaları* [Doktora Tezi, Kocaeli Üniversitesi]. Kocaeli.

Pehlivanlı, D. (2014). *Modern İç Denetim : Güncel İç Denetim Uygulamaları*. Beta.

Pitt, S.-A. (2014). *Internal Audit Quality: Developing a Quality Assurance and Improvement Program*. Wiley.

Ramamoorti, S., & Weidenmier, M. L. (2004). The Pervasive Impact of Information Technology on Internal Auditing. In (pp. 301-377).

Şahin, Ü. (2008). 5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanununda İç Denetim Sistemi. *KMU İİBF Dergisi*, *10*(15), 14.

Salehi, M. H., R. (2011). A Study of the Effect of Information Technology on Internal Auditing: Some Iranian Evidence. *African Journal of Business Management*, *5*(15), 11.

Sayılgan, G. (2011). *İşletme Finansmanı*. Turhan.

Sayıştay. (2013). *Uluslararası Yüksek Denetim Kurumları Standartları (ISSAI) -1-*. S. Başkanlığı.

Serbestoğlu, İ. (2014). Ali Rıza Efendi'nin teftişi esnasında canik ve amasya sancaklarında dini yapiların inşa ve tamir faaliyetleri. *Amasya Üniversitesi İlahiyat Fakültesi Dergisi*, *2014/2*.

Soylu, H. (2010). *İç Denetimin Yeni Bir Yaklaşım Olarak Kamu Sektöründe Uygulanması ve Mevcut Uygulamaların Verimlilik ve Başarısı: Türkiye Örneği* [Yüksek Lisans Tezi, Karamanoğlu Mehmetbey Üniversitesi]. Karaman.

Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, *16*(4), 640-661. https://doi.org/10.1108/09513570310492335

Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. N. (2015). The influence of internal audit on information security effectiveness: Perceptions of internal auditors. In.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation [Article]. *International Journal of Accounting Information Systems*, *13*(3), 228-243. https://doi.org/10.1016/j.accinf.2012.06.007

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2013). Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal of Information Systems*, *27*(2), 65-86.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15-29. https://doi.org/https://doi.org/10.1016/j.aos.2018.04.005

Stoel, D., Havelka, D., & Merhout, J. W. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. *International Journal of Accounting Information Systems*(1), 60.

Tabakoğlu, A. (2015). Osmanlida Mali Denetimin Kurumsal Gelişim - Maliye Teftiş Heyetinin Kuruluşu. *Journal of Management and Economics Research*, *13*(2). https://doi.org/10.11611/jmer621

Tanç, A. (2009). *Risk Odaklı İç Denetim Yaklaşımı ve Tekstil Sektöründe Bilgisayar Destekli Bir Uygulama* [Doktora Tezi, Erciyes Üniversitesi]. Kayseri.

TDK. *Güncel Türkçe Sözlük*. Erişim tarihi: 12.01.2018 Erişim adresi: www.tdk.gov.tr

TDK. (2017). Erişim tarihi: 14.09.2017 Erişim adresi: www.tdk.gov.tr

TİDE. (2010). Akademik Forum 2010. In (Vol. Yayın No: 2, pp. 143). Istanbul: Türkiye İç Denetim Enstitüsü Yayınları.

TİDE. (2011). İç Denetim Terimler Sözlüğü. In (pp. 5): Türkiye İç Denetim Enstitüsü Yayınları.

TİDE. (2012a). Akademik Forum 2012: Denetim Mesleğinin Gelişimi ve Beklentiler. In (Vol. Yayın No: 5, pp. 244). İstanbul: Türkiye İç Denetim Enstitüsü Yayınları.

TİDE. (2012b). IIA Uluslararası İç Denetim Standartları. In (pp. 25): Türkiye İç Denetim Enstitüsü.

TİDE. (2015). Yeni UMUÇ. In: Türkiye İç Denetim Enstitüsü, TİDE.

Tok, P. (2010). *Türkiye'de İç Denetim ve İç Denetçilik* Muğla Üniversitesi]. Muğla.

TSE. (2006). TS ISO/IEC 27001:2005. In (pp. 39). Ankara: Türk Standartları Enstitüsü.

TSE. (2013). TS ISO/IEC 27001:2013. In (pp. 31). Ankara: Türk Standartları Enstitüsü.

TSE. (2015a). TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Temel Eğitimi. In (pp. 122): Türk Standartları Enstitüsü, .

TSE. (2015b). TS ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi İç Tetkik Eğitimi. In (pp. 88): Türk Standartları Enstitüsü,.

Tufan, M. (2012). *Uluslararası İç Denetim Standartları Çerçevesinde Kamuda İç Denetim: Türkiye'deki İç Denetim Sisteminin Değerledirilmesi Üzerine Bir Araştırma* Çanakkale Onsekiz Mart Üniversitesi]. Çanakkale.

Türedi, H. e. a. (2014). Coso modeli: İç kontrol yapısı. *Marmara Üniversites Öneri Dergisi*, *11*(42), 15.

Tuttle, B., & Vandervelde, S. D. (2007). An empirical examination of CobiT as an internal control framework for information technology. *International Journal of Accounting Information Systems*, *8*(4), 240-263. https://doi.org/10.1016/j.accinf.2007.09.001

Uluslararası İç Denetçiler Enstitüsü. (2012). *Ek Rehber: IIA Standartları - GAGAS Karşılaştırma*. The Institute of Internal Auditors.

Ünlü, A. M., & Çakmak, T. (2023). Kamu Sektöründe Kurumlar Arasında Bilgi Paylaşımı: Türkiye'deki Politika ve Yasal Düzenlemelere Yönelik Bir Değerlendirme. *Bilgi Yönetimi*, *6*(1), 1-20.

Walker, D. M. (2005). Amerika Birleşik Devletleri Sayıştayı. *Çev. Müslüm Parlak) Sayıştay Dergisi*(58).

Weidenmier, L. M., & Ramamoorti, S. (2006). Research Opportunities in Information Technology and Internal Auditing. *Journal of Information Systems*, *20*(1), 205-205.

Yalçıner, K. (2008). *Uluslararası Finansman*. Gazi Kitabevi.

Yanık, R. (2010). *Basel II Kriterlerine Hazırlık Durumlarının Muhasebe ve Denetim Standartları Açısından Değerlendirilmesi* [Doktora Tezi, Atatürk Üniversitesi]. Erzurum.

Yereli, A. N. K., Suat. (2013). Risk Odaklı İç Denetim Uygulamalrında Yabancı Ortaklığın Etkisi: İMKB Uygulaması. *Muhasebe ve Denetime Bakış*, *12*(39), 41-64.

Yılancı, M. (2015). *İç Denetim ve İç Kontrol Değerleme Rehberi*. Detay.

Yıldız, H. (2014). Tanzimat'tan Günümüze Maarif Müfettişliği İle İlgili Düzenlemeler Bağlamında Etik İlkeler. *Türkiyat Mecmuası*, *Güz 2014*(24), 24.

Yurtsever, G. (2009). Teftişten iç denetime banka müfettişliği. In *Türkiye Bankalar Birliği yayın no: 265*. İstanbul : Türkiye Bankalar Birliği, 2009.

Zaman, M., & Sarens, G. (2013). Informal interactions between audit committees and internal audit functions. *Managerial Auditing Journal*, *28*(6), 495-515. https://doi.org/10.1108/02686901311329892

EK 1. GÖNÜLLÜ KATILIM FORMU

GÖNÜLLÜ KATILIM FORMU

Değerli Katılımcı, uygulanacak anket formuna yönelik gönüllü katılımcı olmaya ilişkin hususlar aşağıdaki maddelerde açıklanmıştır.

- Bu anket, Prof. Dr. Mustafa KILIÇ'ın danışmanlığında Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü İşletme Ana Bilim Dalı Doktora programında yürütülen "İç Denetimin Bilgi Güvenliğine Katkısı: Bir Alan Araştırması" konulu tez çalışmasında kullanılmak üzere hazırlanmıştır.

- Söz konusu anketin uygulanabilmesi için Hacettepe Üniversitesi Etik Komisyonundan izin alınmıştır.

- Bu çalışmaya katılım gönüllülük esasındadır ve katılıp katılmama konusunda seçme hakkınız bulunmaktadır. Yapılacak anket süre itibariyle 5 (beş) dakikadan fazla bir zaman almayacaktır. Ayrıca katıldıktan sonra istendiği anda vazgeçilebilecektir ve bu durum size hiçbir sorumluluk getirmeyecektir.

- Anket formuna verdiğiniz tüm cevaplar gizli tutulacak ve kimlik bilgileriniz talep edilmeyecektir.

- Anket formuna adınızı ve soyadınızı yazmayınız.

- Yanıtlarınızı, ifadelerin altında veya yanında yer alan seçenekler arasından uygun olanı işaretleyerek; açık uçlu sorularda sorunun altında bırakılan boşluğa yazarak belirtiniz. Anketin kullanılabilmesi için tüm soruların eksiksiz cevaplanması gerekmektedir

- Katılım sağladığınız ve vakit ayırdığınız için teşekkür ederiz.

- Çalışma ile ilgili herhangi bir sorunuz olduğunda ya da çalışmanın sonuçları hakkında bilgi talepleriniz için aşağıdaki kişi ile iletişim kurabilirsiniz:

Araştırmacı:
Adı, Soyadı: Borga Küçükkayalar
Adres: Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü İşletme Bölümü Beytepe- Çankaya / ANKARA

Tarih:
Ad, Soyadı:
Adres:
Tel:
İmza:
Çalışmaya katılmayı kabul ediyorsanız aşağıdaki kutucuğu X ile işaretleyiniz ve devam ediniz.

EK 2. ANKET

ANKET ÇALIŞMASI

Sayın Katılımcı,

Bu anket Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü İşletme Ana Bilim Dalı Doktora programında yürütülen "İç Denetimin Bilgi Güvenliğine Katkısı: Bir Alan Araştırması" konulu tez çalışmasında kullanılmak üzere hazırlanmıştır. Cevaplar gizli tutulacak olup, kişisel bilgiler ya da organizasyon bilgileri talep edilmemektedir. Soruların doğru ya da yanlış cevabı yoktur. Yalnızca görüş elde edilmeye çalışılmaktadır. Anketin kullanılabilmesi için tüm soruların eksiksiz cevaplanması gerekmektedir. Bu çalışmaya katılım gönüllülük esasındadır ve katılıp katılmama hakkınız bulunmaktadır. Çalışmamıza katkılarınız ve değerli zamanınızı ayırdığınız için teşekkür ederiz.

Borga KÜÇÜKKAYALAR Prof. Dr. Mustafa KILIÇ

1.	Aşağıdaki soruları, çalışmakta olduğunuz organizasyondaki **iç denetim ortamını** dikkate alarak cevaplayınız.	Hiç Katılmıyorum	Katılmıyorum	Kısmen Katılıyorum	Katılıyorum	Kesinlikle Katılıyorum
İç denetimin rolü eksiklikleri tespit etmek ve raporlamaktır.		1	2	3	4	5
İç denetimin rolü kurumsal politikaları uygulamaktır.		1	2	3	4	5
İç denetimin rolü farklı departmanlara verimlilik ve etkililik konusunda danışmanlık yapmaktır.		1	2	3	4	5
2.	Aşağıdaki soruları, çalışmakta olduğunuz organizasyondaki **iç denetim biriminin bilgi güvenliği yetkinliğini** dikkate alarak cevaplayınız.	Hiç Katılmıyorum	Katılmıyorum	Kısmen Katılıyorum	Katılıyorum	Kesinlikle Katılıyorum
İç Denetim Birimi bilgi güvenliği konusunda yetkindir.		1	2	3	4	5
İç Denetim Birimi, bilgi güvenliği konularında bilgisini güncel tutmaktadır.		1	2	3	4	5

3.	Aşağıdaki soruları, çalışmakta olduğunuz organizasyondaki **yönetişim ortamını** dikkate alarak cevaplayınız.	Hiç Katılmıyorum	Katılmıyorum	Kısmen Katılıyorum	Katılıyorum	Kesinlikle Katılıyorum
Üst yönetim, bilgi güvenliği için yeterli kaynak sağlamaktadır.		1	2	3	4	5
Üst yönetim, çalışanlar ile düzenli olarak bilgi güvenliğinin önemi hakkında iletişim kurmaktadır.		1	2	3	4	5
Üst yönetim, bilgi güvenliğinin önemli bir konu olduğunu düşünmektedir.		1	2	3	4	5
Üst yönetim, bilgi güvenliği sorunlarına ilişkin pasif değildir ve önceden önlem alır (proaktiftir).		1	2	3	4	5
Son 3 yılda bilgi güvenliğine ayrılan kaynak artmıştır.		1	2	3	4	5
Son 3 yılda üst yönetimin bilgi güvenliğine olan desteği artmıştır.		1	2	3	4	5
4.	Aşağıdaki soruları, çalışmakta olduğunuz organizasyondaki **fonksiyonel yapıyı** dikkate alarak cevaplayınız.	Hiç Katılmıyorum	Katılmıyorum	Kısmen Katılıyorum	Katılıyorum	Kesinlikle Katılıyorum
İç denetim ve bilgi güvenliği fonksiyonları arasında görev çatışması vardır.		1	2	3	4	5
İç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişki yakın ve kişisel boyuttadır.		1	2	3	4	5
İç denetim ve bilgi güvenliği fonksiyonları arasında iyi bir çalışma ilişkisi vardır.		1	2	3	4	5
5.	Aşağıdaki soruları, çalışmakta olduğunuz organizasyondaki **iç denetim birimi faaliyetlerini ve çıktılarını** dikkate alarak cevaplayınız.	Hiç Katılmıyorum	Katılmıyorum	Kısmen Katılıyorum	Katılıyorum	Kesinlikle Katılıyorum
İç denetim bulguları ve raporları, bilgi güvenliği fonksiyonuna faydalı bilgiler sağlamaktadır.		1	2	3	4	5
İç denetim bulgu ve raporları, üst yönetime bilgi güvenliğinin etkinliği hakkında faydalı bilgiler sağlamaktadır.		1	2	3	4	5
İç denetimin bilgi güvenliğini inceleme becerisinden tam olarak yararlanılmaktadır.		1	2	3	4	5
İç denetim, bilgi güvenliği incelemesine daha fazla katılım *gösterebilir.*		1	2	3	4	5

İç denetim, bilgi güvenliği incelemesine daha fazla katılım *göstermelidir.*		1	2	3	4	5
6.	Aşağıdaki soruları, çalıştığınız organizasyondaki **bilgi güvenliği ortamını** dikkate alarak cevaplayınız.	Hiç Katılmıyorum	Katılmıyorum	Kısmen Katılıyorum	Katılıyorum	Kesinlikle Katılıyorum
Son 3 yılda, operasyonları yarıda kesen ya da maddi zararla sonuçlanacak bilgi güvenliği olaylarının sayısı azaldı.		1	2	3	4	5
Son 3 yılda, bilgi güvenliğinin genel etkililiği (amaca ulaşma derecesi) arttı.		1	2	3	4	5
Son 3 yılda, iç denetimin bilgi güvenliğiyle ilgili bulgularının sayısı azaldı.		1	2	3	4	5
7.	Aşağıdaki soruları, çalışmakta olduğunuz organizasyonda **iç denetim birimince yapılan bilgi güvenliği denetimlerini** dikkate alarak cevaplayınız.	Hiç Yok / Nadiren	Seyrek	Orta Seviyede	Sıklıkla	Çok Sık
İş sürekliliği ve felaket kurtarma planları denetiminin gerçekleştirilme sıklığı		1	2	3	4	5
Kimlik ve erişim yönetimi kontrolleri denetiminin gerçekleştirilme sıklığı		1	2	3	4	5
Log-kayıtları ve sistem izleme denetiminin gerçekleştirilme sıklığı		1	2	3	4	5
Güvenlik duvarları ve diğer ağ erişim cihazları denetiminin gerçekleştirilme sıklığı		1	2	3	4	5
Şifreleme politikaları denetiminin gerçekleştirilme sıklığı		1	2	3	4	5
Yedekleme prosedürleri denetiminin gerçekleştirilme sıklığı		1	2	3	4	5
Değişim yönetimi kontrolleri denetiminin gerçekleştirilme sıklığı		1	2	3	4	5
Güvenlik politikaları denetiminin gerçekleştirilme sıklığı		1	2	3	4	5

8. Yaşınız: □<30 □30-39 □40-49 □>49

9. Cinsiyetiniz: □Kadın □Erkek

10. Eğitim Durumunuz: □Lisans □Yüksek Lisans □Doktora

11. Şu anki işyerinde iç denetim alanında çalıştığınız toplam süre:

□2 yıl veya daha az □3-6 yıl □7-10 yıl □11 yıl veya daha fazla

12. İş yaşamınızda iç denetim alanında çalıştığınız toplam süre:

□2 yıl veya daha az □3-6 yıl □7-10 yıl □11 yıl veya daha fazla

13. Kamu İç Denetim Sertifikasına sahip misiniz? □Hayır □Evet

14. İç Denetçiler Enstitüsü (IIA) ya da diğer Uluslararası Organizasyonlarca verilen sertifika(ları)nız var ise lütfen belirtiniz (birden fazla seçenek işaretleyebilirsiniz)?

- Bu kapsamda bir sertifikam yok
- Certified Internal Auditor (CIA)
- Certified Government Auditing Professional (CGAP)
- Certified Information Systems Auditor (CISA)
- Diğer (lütfen belirtiniz)
  :……..……

15. Çalıştığınız organizasyonun içinde bulunduğu sektör:

- Özel Sektör Kamu Sektörü Vakıf/Dernek Diğer (lütfen belirtiniz):……..

16. Çalışmakta olduğunuz organizasyonda bilgi güvenliği politikası uygulanıyor mu?

- Hayır → Lütfen 18.soruya geçiniz.
- Konuya ilişkin bilgim yoktur → Lütfen 18. Soruya geçiniz
- Evet →Lütfen 17. Soruya geçiniz

17. Cevabınız evet ise uygulanan bilgi güvenliği politikası türünü belirtiniz (birden fazla cevap işaretleyebilirsiniz):

- TS ISO/IEC 27001 – Bilgi Güvenliği Yönetim Sistemi uygulanmaktadır.
- Kurum içinde oluşturulmuş politika ve prosedürler uygulanmaktadır.
- Diğer (lütfen belirtiniz):…….

18. Bilgi güvenliğine ilişkin olarak organizasyon içi ya da dışı herhangi bir eğitim/seminer ya da konferansa katıldınız mı?

- Hayır Evet

19. Çalıştığınız organizasyonda herhangi bir bilgi güvenliği tehdidi ile karşılaştınız mı?

- Hayır Evet

Değerli vaktiniz için teşekkür ederiz.

Tarih: 29/01/2020 15:27
Sayı: E-35853172-300-00000976679

00000976679

T.C.
HACETTEPE ÜNİVERSİTESİ
Rektörlük

Sayı : 35853172-300
Konu : Borga KÜÇÜKKAYALAR (Etik Komisyon İzni)

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 02.01.2020 tarihli ve 12908312-300/00000934784 sayılı yazınız.

Enstitünüz İşletme Anabilim Dalı Doktora programı öğrencilerinden **Borga KÜÇÜKKAYALAR**'ın **Prof. Dr. Mustafa KILIÇ** danışmanlığında yürüttüğü **"İç Denetimin Bilgi Güvenliğine Katkısı: Bir Alan Araştırması"** başlıklı tez çalışması Üniversitemiz Senatosu Etik Komisyonunun **21 Ocak 2020** tarihinde yapmış olduğu toplantıda incelenmiş olup, etik açıdan uygun bulunmuştur.

Bilgilerinizi ve gereğini saygılarımla rica ederim.

e-imzalıdır
Prof. Dr. Rahime Meral NOHUTCU
Rektör Yardımcısı

Hacettepe Üniversitesi Rektörlük 06100 Sıhhiye-Ankara
Telefon:0 (312) 305 3001-3002 Faks:0 (312) 311 9992 E-posta:yazimd@hacettepe.edu.tr İnternet Adresi: www.hacettepe.edu.tr

Sevda TOPAL

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI BAŞKANLIĞINA

Tarih: 05/08/2024

Tez Başlığı "İÇ DENETİMİN BİLGİ GÜVENLİĞİNE KATKISI: BİR ALAN ARAŞTIRMASI"
Tez Başlığı (Almanca/Fransızca)*::……

Yukarıda başlığı verilen tezimin a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam …230… sayfalık kısmına ilişkin, 05/08/2024 tarihinde şahsım/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda işaretlenmiş filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 11 'dır.

Uygulanan filtrelemeler**:

1. ☐ Kabul/Onay ve Bildirim sayfaları hariç
2. ☒ Kaynakça hariç
3. ☐ Alıntılar hariç
4. ☒ Alıntılar dâhil
5. ☒ 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tezimin herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumlarda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Borga KÜÇÜKKAYALAR

Öğrenci Bilgileri			
	Ad-Soyad	Borga KÜÇÜKKAYALAR	
	Öğrenci No	N10143013	
	Enstitü Anabilim Dalı	Sosyal Bilimler Enstitüsü – İşletme Anabilim Dalı	
	Programı	İşletme	
	Statüsü	**Doktora** ☒	**Lisans Derecesi ile (Bütünleşik) Dr** ☐

DANIŞMAN ONAYI

UYGUNDUR.
Prof. Dr. Mustafa KILIÇ

*Tez **Almanca** veya **Fransızca** yazılıyor ise bu kısımda tez başlığı **Tez Yazım Dilinde** yazılmalıdır.
**Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Orjinallik Raporu Alınması ve Kullanılması Uygulama Esasları İkinci bölüm madde (4)/3'te de belirtildiği üzere: Kaynakça hariç, Alıntılar hariç/dahil, 5 kelimeden daha az örtüşme içeren metin kısımları hariç (Limit match size to 5 words) filtreleme yapılmalıdır.

TO HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF BUSINESS ADMINISTRATION

Date: 05/08/2024

Thesis Title (In English):"CONTRIBUTION OF INTERNAL AUDITING TO INFORMATION SECURITY: A FIELD STUDY"

According to the originality report obtained by myself/my thesis advisor by using the Turnitin plagiarism detection software and by applying the filtering options checked below on 05/08/2024 for the total of …230... pages including the a) Title Page, b) Introduction, c) Main Chapters, and d) Conclusion sections of my thesis entitled above, the similarity index of my thesis is 11 %.

Filtering options applied**:

1. ☐ Approval and Decleration sections excluded
2. ☒ References cited excluded
3. ☐ Quotes excluded
4. ☒ Quotes included
5. ☒ Match size up to 5 words excluded

I hereby declare that I have carefully read Hacettepe University Graduate School of Social Sciences Guidelines for Obtaining and Using Thesis Originality Reports that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.

I respectfully submit this for approval.

Borga KÜÇÜKKAYALAR

Student Information					
	Name-Surname	Borga KÜÇÜKKAYALAR			
	Student Number	N10143013			
	Department	Institute of Social Sciences – Department of Business Administration			
	Programme	Business Administration			
	Status	**PhD**	☒	**Combined MA/MSc-PhD**	☐

SUPERVISOR'S APPROVAL

APPROVED
Prof. Dr. Mustafa KILIÇ

**As mentioned in the second part [article (4)/3]of the Thesis Dissertation Originality Report's Codes of Practice of Hacettepe University Graduate School of Social Sciences, filtering should be done as following: excluding refence, quotation excluded/included, Match size up to 5 words excluded.