
GAZİ ÜNİVERSİTESİ
Gazi
1926

ISO 27001 BİLGİ GÜVENLİĞİ STANDARDI DENETİMLERİNİN SİBER GÜVENLİĞE ETKİLERİ ÜZERİNE BİR İNCELEME

Emrah BALCILAR

YÜKSEK LİSANS TEZİ
ADLİ BİLİŞİM ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

EYLÜL 2024

Emrah Balcılar tarafından hazırlanan "ISO 27001 BİLGİ GÜVENLİĞİ STANDARDI DENETİMLERİNİN SİBER GÜVENLİĞE ETKİLERİ ÜZERİNE BİR İNCELEME" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Adli Bilişim Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Prof. Dr. Çelebi ULUYOL

Gazi Üniversitesi / Bilgisayar ve Öğretim Teknolojileri Eğitimi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ...……

Başkan: Doç. Dr. Recep BENZER

Ankara Medipol Üniversitesi / Yönetim Bilişim Sistemleri Bölümü

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ……...

Üye: Doç. Dr. Murat DÖRTERLER

Gazi Üniversitesi / Bilgisayar Mühendisliği

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ……...

Tez Savunma Tarihi: 02/09/2024

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……..…….

Prof. Dr. Aslıhan TÜFEKCİ

Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

İmza

Emrah BALCILAR

…/…./2024

ISO 27001 BİLGİ GÜVENLİĞİ STANDARDI DENETİMLERİNİN SİBER GÜVENLİĞE ETKİLERİ ÜZERİNE BİR İNCELEME

(Yüksek Lisans Tezi)

Emrah BALCILAR

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Eylül 2024

ÖZET

Teknolojinin gelişmesi ve hayatın her alanında kullanılmaya başlanılması ile bilgi güvenliği kavramı önem kazanmıştır. Bilgi güvenliği bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak olarak tanımlanmaktadır. ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardı, siber güvenliğin sağlanarak siber olayların engellenmesi amacıyla, bilgi güvenliği ile ilgili risklerin tanımlanması, yönetilmesi ve faaliyetlerin etkinliğinin sürekli olarak değerlendirilmesi ile ilgili kontrolleri içeren bir standarttır. Bilgi güvenliği yönetiminde çerçeve oluşturan ISO 27001 Bilgi Güvenliği Yönetim Sistemi'ne ilgi artmakta olup; belgelendirilmiş kuruluşların standartta yer alan süreçleri doğru şekilde işletmesi önem arz etmektedir. Doğru işletilen bir ISO 27001 yönetim sistemi siber güvenliğin sağlanmasında ve siber olayların engellenmesinde fayda sağlayacaktır. Standarda göre sistemin etkin ve standarda uygun işleyişi periyodik olarak iç tetkiklere tabi tutulmalıdır. Bu bağlamda çalışmanın amacı ISO 27001 Bilgi Güvenliği Yönetim Sistemi kapsamında gerçekleştirilen iç tetkiklerin etkinliğinin tetkikçilerin görüşlerine göre incelenmesidir. Çalışma kapsamında araştırmacılar tarafından hazırlanan ankete 103 kişi katılmıştır. Çalışmada denetim süreçleri ile ilgili görüşler incelenerek, elde edilen veriler üzerinden yaşanan sorunların analizleri gerçekleştirilmiş ve ülkemizde BGYS belgesine sahip olan kurum/kuruluşlarda denetim etkinliğini ve bunun sonucu siber güvenliği etkileyebilecek riskler görülmüştür. ISO 27001 standardının iç tetkiklerde uyulmasını beklediği esaslara göre, tetkikçilerin sürekli gelişimi ve yetkinliği, denetimlerin objektiflik ve bağımsızlığı, denetim planlaması ve kriterleri, denetim bulgularının yönetimi konuları çalışmanın değerlendirme konu kategorileri olarak belirlenmiştir. Bu konu kategorilerindeki eksiklikler gerçekleştirilen denetimlerde siber güvenlik ve/veya bilgi güvenliği zafiyetlerinin tespit edilememesine, tespit edilse dahi raporlanamamasına ve raporlansa da etkin ve tekrar oluşmayacak şekilde kapatılmamasına sebep olabileceği değerlendirilmiştir.

Bilim Kodu	:	92401
Anahtar Kelimeler	:	ISO 27001, Bilgi Güvenliği Yönetim Sistemi, İç Tetkik, Bilgi Güvenliği Denetimi
Sayfa Adedi	:	103
Danışman	:	Prof. Dr. Çelebi ULUYOL

A REVIEW ON THE EFFECTS OF ISO 27001 INFORMATION SECURITY STANDARD AUDIT ON CYBER SECURITY

(M. Sc. Thesis)

Emrah BALCILAR

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

September 2024

ABSTRACT

With the evolution of technology and use of it in a lot of areas of life, the concept of information security has came into prominence. Information security is defined as protecting the confidentiality, integrity and accessibility of information. ISO 27001 Information Security Management System standard is a standard that includes the principles and controls regarding the identification and management of risks relative to information security and the continuous evaluation of the effectiveness of activities to provide cyber security and prevent cyber incidents. Interest in the ISO 27001 Information Security Management System, which creates a framework for information security management, is increasing; It is important for certified organizations to operate the processes included in the standard correctly. A properly operated ISO 27001 management system will be beneficial in ensuring cyber security and preventing cyber incidents. According to the standard, the effective and standard operation of the system should be subject to periodic internal audits. In this context, the purpose of the study is to examine the effectiveness of the audits carried out within the scope of the ISO 27001 Information Security Management System, according to the opinions of the auditors. Within the study, 103 people participated in the survey prepared by the researchers. In the study, opinions about the audit processes were examined, the problems experienced were examinated based on the data obtained, and risks that could affect the audit effectiveness and, as a result, cyber security in institutions/organizations with ISMS certificates in our country were observed. According to the issues that the ISO 27001 standard expects to be complied with in internal audits, continuous development and competence of auditors, objectivity and independence of audits, audit planning and criteria, management of audit findings have been determined as evaluation subject categories. It has been evaluated that deficiencies in these subject categories may cause cyber security and/or information security vulnerabilities not to be detected during the audits, not to be reported even if detected, and not to be closed effectively and in a way that will not occur again after being reported.

Science Code	:	92401
Key Words	:	ISO 27001, Information Security Management System, Information Security Audit
Page Number	:	103
Supervisor	:	Prof. Dr. Çelebi ULUYOL

TEŞEKKÜR

Bu çalışmada veri toplama aracılığı sorularıma değerli zamanlarını harcayarak katılım gösteren ISO 27001 Bilgi Güvenliği Yönetim Sistemi iç tetkiklerinde görev alan tetkikçilere, tez yazım çalışma sürecimde bilgileri ve deneyimlerini sunan değerli danışman hocam sayın Prof. Dr. Çelebi ULUYOL'a teşekkürlerimi sunarım.

İÇİNDEKİLER

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
BGYS	Bilgi Güvenliği Yönetim Sistemi
TSE	Türk Standartları Enstitüsü
ISO	International Standard Organization
IIA	Institute of Internal Auditors
ISACA	Information Systems Audit and Control Association
CBDDO	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
PUKÖ	Planla, Uygula, Kontrol Et, Önlem Al
ort	Ortalama
ss	Standart Sapma
bö	Bağıl Önem

1. GİRİŞ

Günümüzde teknoloji ve bilişim sistemleri sürekli gelişmekte; kullanım alanları da gün geçtikçe artmaktadır. Datareportal'ın 2024 yılı için yayınladığı "Dijital 2024" raporuna göre, dünya üzerinde 5,35 milyar insan interneti ve bunun aracılığıyla bilişim sistemlerini kullanmaktadır. 2000 yılı için aynı sayının 396 milyon kişi olduğu görülmektedir. Rapora göre, bilişim sistemleri kullanıcıları günlerinin ortalama 6 saat 40 dakikasını internet üzerinden bilişim sistemleri kullanarak geçirmektedir [1]. Bu yoğun talep sebebiyle özel veya kamu kuruluşları iş süreçlerinde ve sundukları hizmetlerde bilişim sistemlerini aktif olarak kullanmaktadırlar. Bilişim sistemlerinin söz konusu yoğun kullanımı, bu sistemleri kötü niyetli kişiler tarafından hedef haline getirmektedir. Uluslararası İç Denetim Enstitüsü (IIA) tarafından 2022, 2023 ve 2024 yıllarında yayınlanan Avrupa için risk odağı raporlarında siber güvenlik/bilgi güvenliği konuları en yüksek riskli alanlar olarak değerlendirilmiştir [2-4]. Bu kapsamda bilgi güvenliğinin temel unsurları olan bilginin gizliliğinin (bilginin sadece erişmeye yetkili olan kişi/kişiler tarafından erişilmesi), bütünlüğünün (bilginin değiştirme yetkisi olan kişiler tarafından değiştirilmesi) ve sürekliliğinin (erişim yetkisi olan kişilerin istediği zaman bilgiye erişebilmesi) sağlanması önem arz etmektedir. Yalnızca teknik tedbirlerle (anti virüs uygulamaları, veri sızıntı önleme uygulamaları, açıklık tarama sistemleri, saldırı önleme/tespit sistemleri, güvenlik duvarları, kriptografi, vb.) kuruluşlarda bilgi güvenliğini yüzde yüz sağlamak mümkün değildir. Bu sebepten ötürü teknik tedbirlerin yanında, insanları ve süreçleri içeren yönetim sistemleri ihtiyacı doğmuştur. Bu çerçevede ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS), işletmeler için bilgi güvenliğini sağlamak ve yönetmek amacıyla bir sistemin kurulması, işletilmesi, sürekli izlenmesi, gözden geçirilmesi ve iyileştirmesini içeren risk odaklı uluslararası bir yönetim sistemi standardıdır. Bilgi güvenliği konusunda en iyi uygulamalardan yararlanmak ve müşterilere güven vermek için ISO 27001 standardı tercih edilmekte ve dünya çapında yaygın olarak kullanılmaktadır. ISO tarafından 2022 yılında yayınlanan verilere göre, 151 farklı ülkede tarım, imalat ve sosyal hizmetler sektörlerine kadar farklı sektörlerde 70.000'in üzerinde ISO 27001 sertifikası alan kuruluş bulunmaktadır [5]. 2022 yılında güncellenen ISO 27001 BGYS standardı; içerisinde fiziksel güvenlik, erişim güvenliği, işletim güvenliği, kriptografi, iş sürekliliği yönetimi, haberleşme güvenliği, ihlal olayı yönetimi gibi konularda 93 kontrol maddesini içermektedir.

Teknolojinin yoğun kullanımı ve bilgi güvenliği konusun riski yüksek alan olarak değerlendirilmesi sebebiyle, bilgi güvenliği yönetiminde çerçeve oluşturan ISO 27001 BGYS'ye kuruluşların ilgisi bulunmaktadır. Ancak belgelendirilen kuruluşların bilgi güvenliği seviyelerini gerçekten arttırması için standartta yer alan süreçlerin doğru şekilde işletilmesi önem arz etmektedir. Doğru işletilen bir ISO 27001 BGYS siber güvenliğin sağlanmasında ve siber olayların engellenmesinde fayda sağlayacaktır. ISO 27001 standardına göre, yönetim sisteminin etkin ve standarda uygun işleyişini sağlamak için periyodik olarak denetimlere tabi tutulması gerekmektedir. Gerçekleştirilen bilgi güvenliği ile ilgili faaliyetler ve uygulanan kontroller, kuruluşların siber güvenlik seviyelerini artırmakta ve siber güvenliğe dair riskleri azaltmaktadır. Uygulanmayan veya yanlış uygulanan kontroller ise güvenlik zayıflıklarına ve bilgi güvenliği risklerine sebep olabilmektedir. BGYS işleten kurum ve kuruluşlarda standart kapsamında yapılan çalışmalar ve uygulanan kontrollerin ISO 27001 standardına göre denetimlere tabi tutulması zorunlu bir şart olarak bulunmaktadır. Bu denetimlerin etkinliği ve başarısı sertifika sahibi kuruluşun siber güvenliğini doğrudan etkilemektedir. Doğru bir şekilde gerçekleştirilmeyen denetimler siber güvenlik açıklıkları ve/veya bilgi güvenliği zafiyetlerinin tespit edilememesine, tespit edilse dahi raporlanamamasına veya raporlansa dahi bulguların tekrar oluşmayacak şekilde kapatılmamasına sebep olabilecektir. Ülkemizde, ISO 27001 sertifikası sahibi kuruluşlarda gerçekleştirilen iç tetkiklerin etkinliği ve uluslararası standartlara göre uygunluğu konusunda henüz bir çalışma bulunmadığı için mevcut durum tam olarak bilinmemekte ve çözüm önerileri sunulamamaktadır.

Araştırmanın amacı

Kurumlar ve şirketlerin siber güvenliğini doğrudan etkileyen BGYS kapsamında gerçekleştirilen iç tetkiklerin; ISO 27001 standardının kendi gereksinimlerine uygun şekilde; objektif/bağımsız olarak gerçekleştirilmesi, denetim sonuçlarının raporlanması, tetkikçilerin sürekli gelişimi ve yetkinliğinin sağlanması, denetimlerin planlanması, denetim kriterleri ve denetim sonrası tespit edilen uygunsuzluklar ile ilgili yürütülen iyileştirme faaliyetleri gibi konu kategorilerine göre değerlendirilmesini sağlamak ve yaşanan sorunlar ile ilgili mevcut durumu ortaya çıkarmaktır. Literatür taramasında bu konu özelinde ülkemizde henüz herhangi bir araştırma yapılmadığı görülmüştür. Araştırma sonucunda mevcut durum ortaya çıkarılarak, eğer varsa BGYS işleten kurumlarda iç tetkiklerde yaşanan eksikliklerin ortaya konulması, bu konuda iyileştirme önerileri sunulması ve bu kapsamda yapılacak

iyileştirmeler ile bilgi güvenliği/siber güvenlik konusunda kurum/kuruluşlarda risklerin azaltılmasına yardımcı olunması amaçlanmaktadır. İç tetkiklerde görev almış tetkikçilerin görüşleri çerçevesinde iç tetkik süreçleri ile ilgili aşağıdaki araştırma sorularına cevap aranmaktadır.

1. Denetim süreçlerinde kamuda ve özel sektörde görev alan ISO 27001 BGYS iç tetkikçileri özelinde farklılıklar nelerdir?
2. İç tetkikçilerin gerçekleştirdikleri denetimlerin objektifliği ve bağımsızlığı hakkında görüşleri nelerdir?
3. İç tetkikçilerin, denetim sonrası bulunan uygunsuzlukların raporlanması ve etkin şekilde çözümü için gerçekleştirilen faaliyetler ile ilgili görüşleri nelerdir?
4. İç tetkikçilerin, sürekli gelişimleri için yapılan faaliyetler ile ilgili görüşleri nelerdir?
5. Denetim yapan tetkikçilerin, özel uzmanlık gereken tetkiklerde gerekli yetkinliğe sahip olduklarına dair görüşleri nelerdir?
6. İç tetkikçilerin, denetim planlamalarının riskli konuların tespiti için yeterli olduğuna dair görüşleri nelerdir?

Kapsam

Bu araştırmada ulusal ve uluslararası alanda literatür araştırması gerçekleştirildikten sonra; sadece Türkiye'de gerçekleştirilen ISO 27001 BGYS standardı iç denetimlerinin etkinliği kapsamında veri toplanmıştır. Veri toplama aracında bulunan sorular, ISO 27001 sertifikasına sahip kamu kurum/kuruluşları ve özel şirketler ile örneklem usulü paylaşılmış, BGYS kapsamında denetim gerçekleştiren iç tetkikçilerden bilgi toplanmıştır.

Sınırlılıklar

Dış denetimler, akredite edilmiş kurum/kuruluşlar tarafından sınırlı sürede gerçekleştirilmesi sebebiyle çalışma kapsamına dahil edilmemiştir. Tüm çabalarla 103 katılımcıdan anket verisi toplanmıştır. İç tetkikçilerin gizlilik endişeleri ve standartlara uyum gösterme zorunluluğu sebebiyle kısıtlı ve taraflı bilgi sunabilecek olmaları çalışmanın sınırlılıklarındandır. Bu sınırlılığın engellenebilmesi için anket çalışmasında katılımcıların personel ve çalıştıkları kuruluşların ismi talep edilmemiş ve bu bilgi anket öncesi katılımcılara bildirilmiştir. Denetimlerde görev alan tetkikçiler özelinde gerçekleştirilen bu

çalışma için sertifikalandırılmış her bir kurumda kaç adet tetkikçinin görevli olduğu verisi bilinememektedir. Çok sayıda sertifikalandırılmış kuruluş bulunması sebebiyle örneklem yöntemiyle araştırma gerçekleştirilmiştir. Bu nedenle soruların paylaşıldığı kurumların hangilerinden yanıt alındığı tespit edilmemesi çalışmanın diğer bir sınırlılığı olarak bulunmaktadır.

Tanımlar

Bu çalışmada kullanılan ve açıklanması fayda sağlayacağı düşünülen kavramların tanımları, anlaşılabilir olması amacıyla İçişleri Bakanlığı ve Emniyet Genel Müdürlüğü tarafından geliştirilen ve siber güvenlik ile ilgili farkındalığı artırmayı amaçlayan Siberay projesi kapsamında oluşturulan basit tanımlamaları içeren Siberay Sözlük'teki tanımlamalardan faydalanılarak oluşturulmuştur.

Ağ (Network): Birbirinden farklı bilgisayarlar arasında, kablolu veya kablosuz iletişim araçları ve yazılım-donanım bileşenlerinin kullanılarak kurulan bağlantı sistemi [6].

Bilişim Sistemleri (Information System): Ağ teknolojileri aracılığıyla sunulan tüm hizmetlerin sunumunda rol oynayan sistemler [6].

Kriptografi (Cryptography): İstenmeyen kişilerin bilgilere erişimini engellemek ve gizliliği korumak için kullanılan şifreleme tekniklerinin tümü [6].

Güvenlik Açığı (Security Bug): Sistemdeki yazılım ve donanım kusurlarından kaynaklanan güvenlik açıkları [6].

Siber Güvenlik (Cyber Security): Kurumlar, kuruluşlar ve kullanıcıların varlıklarını siber saldırılara, tehditlere, sabotajlara ve terör faaliyetlerine karşı korumak için oluşturulan politika, dokümantasyon, güvenlik politikaları ve risk kontrol süreci [6].

Siber Olay (Cyber Event): Siber uzay kökenli saldırılar, tehditler ve sabotajlar [6].

Zafiyet (Vulnerability): Bilgisayar uygulamalarının veya işletim sistemlerinin kodlanması sırasında bilerek veya bilmeden yapılan kodlama hataları [6].

Bu bağlamda, yapılan araştırma 6 bölümden oluşturulmuştur. Birinci bölümde çalışmanın gerekçesi hakkında ön bilgiler, ikinci bölümde konu ile ilgili yapılan literatür çalışmasının sonuçları sunulmuştur. Üçüncü bölümde bilgi, bilgi güvenliği, BGYS ve bilgi güvenliği denetimine ait kavramsal bilgiler, standartlar ve rehberler hakkında bilgi verilmiştir. Dördüncü bölümde araştırma modeli, istatiksel analiz ve veri toplama aracını içerecek şekilde araştırma yöntemi; beşinci bölümde konu kategorilerini içerecek şekilde araştırma bulguları ve altıncı bölümde konu ile ilgili sonuç, tartışma ve öneriler sunulmuştur.

2. LİTERATÜR ARAŞTIRMASI

Bu çalışma ile ISO 27001 BGYS denetimlerinin siber güvenliğe etkileri araştırılmıştır. Bu kapsamda 2010 yılından itibaren günümüze gerçekleştirilen yayınlar incelenmiş, yakın tarihli çalışmalara odaklanılmıştır. Çalışma konusu ile ilgili katkı sağlayacak "ISO 27001", "ISO 27001 iç denetim", "İç denetim/İç tetkik", "Bilgi güvenliği yönetim sistemi", "ISO 27001 - siber güvenlik" anahtar sözlükleri üzerinden araştırma yapılmıştır. Yüksek Öğretim Kurulu Başkanlığı'nın "tez.yok.gov.tr" veri tabanından konu ile ilgili ulusal tez çalışmaları, ScienceDirect ve Scholar.Google veri tabanlarından uluslararası yayınlar araştırılmıştır. Information Systems Audit and Control Association (ISACA) ve Institute of Internal Auditors (IIA) tarafından konu ile ilgili yayınlanan raporlar incelenmiştir. İncelenen yayınlar ve raporlar içerisinde katkı sağlayacağı düşünülen; ISO 27001 standardının işletimi, ISO 27001 standardı ve bilgi güvenliği denetimleri, denetimlerin siber güvenliğe etkileri konularında içeriğe sahip yayınlardan değerlendirmeler bu çalışmaya eklenmiştir.

Bilgi Güvenliği Yönetim Sistemi

ISO 27001 BGYS'nin kurulum süreçleri ve faydaları hakkında literatürde çok sayıda çalışma bulunmaktadır. Podrecca, Culot, Nassimbeni ve Sartor tarafından ISO 27001'in kattığı değerler ve performans etkileri konusunda 2022 yılında yayınlanan çalışmada; ISO/IEC 27001 sertifikasyonunun karlılık, işgücü verimliliği ve satış performansındaki iyileşmelerle ilişkili olduğu belirtilmiştir. Çalışma, ISO/IEC 27001'in finansal etkilerine ilişkin ikincil verilere dayanan ilk büyük ölçekli ampirik araştırmayı geliştirerek bilgi güvenliği ve sertifikasyonlara ilişkin bilimsel tartışmalara katkıda bulunmuştur [7]. Shareef ve Alkhazaali tarafından bilgi güvenliği yönetim sistemlerinin analizinde güvenlik sorunları konusunda 2023 yılında yapılan çalışmada; ISO 27001 standardının günümüzün teknoloji odaklı dünyasında çok önemli olduğu vurgulanarak; kuruluşlar için ciddi sonuçlara yol açabilecek yetkisiz erişimin ve olası veri ihlallerinin önlenmesine yardımcı olduğu sonucuna varılmıştır [8]. Bolek, Romanová ve Korček tarafından elektronik işletmelerde bilgi güvenliği yönetim sistemleri konusunda 2023 yılında yayınlanan çalışmada; etkili bir BGYS'nin iş sürekliliği, artan rekabet gücü, artan karlılık, artan prestij ve gerçekleşen risklerden kaynaklanan tehditlerin ve kayıpların ortadan kaldırılması dahil olmak üzere çeşitli faydalar sağladığı sonucuna varılmıştır [9]. Podrecca ve Sartor tarafından 2023 yılında

gri model yaklaşımı ile ISO/IEC 27001'in yayılmasını tahmin etmek konusunda yapılan araştırmada; ISO 27001'in benimsenmesinin önümüzdeki yıllarda artmaya devam etmesinin beklendiği; bu da dünya çapında bilgi güvenliği standartlarının öneminin giderek daha fazla kabul edildiğini gösterdiği sonucuna varılmıştır [10]. Kitsios, Chatzidimitriou ve Kamariotou tarafından 2023 yılında ISO 27001 Bilgi Güvenliği Yönetim Standardı çerçevesinde bilişim teknolojileri sektöründe verilerden değer çıkartılması konusunda yapılan çalışmada; verileri korumak ve iş gereksinimlerini karşılamak için potansiyel risklerin belirlenmesinin önemli olduğu, risk değerlendirmesinin yapılması, bilgi güvenliği stratejisi geliştirmede en çok zaman alan ve en önemli adımlardan biri olduğu vurgulanmaktadır [11]. Gazdağı ve Çetinyokuş tarafından 2020 yılında yapılan araştırmada, bankalarda iş sürekliğinin ve bilgi güvenliğinin sağlanması için ISO 22301 İş Sürekliliği ve ISO 27001 BGYS standartlarının uygulanması çerçevesinde kavramsal çalışma gerçekleştirilmiştir. Araştırmacılar, ISO 27001 BGYS standardının, bankalarda tehdit ve zafiyetlerin belirli bir metodoloji ile ölçülmesinin sağlayarak bilgi güvenliği kontrollerinin etkin uygulanmasına neden olduğu, düzgün şekilde standardı işleten bankalar için rekabet avantajına sebep olarak banka varlıklarını koruduğu sonucuna varmışlardır [12].

ISO 27001 BGYS ile ilgili çalışmalar, bu standardın işletmelere birçok fayda sağladığını göstermektedir. Sertifikasyonun karlılık, işgücü verimliliği ve satış performansını artırdığı, yetkisiz erişim ve veri ihlallerini önleyerek bilgi güvenliğini sağladığı, iş sürekliliği ve rekabet gücünü artırdığı, prestij kazandırdığı ve risklerden kaynaklanan tehditleri ortadan kaldırdığı belirtilmiştir. Ayrıca, ISO 27001'in yaygınlaşmasının artmaya devam edeceği ve bilişim sektöründe potansiyel risklerin yönetilmesinde ve bilgi güvenliği stratejilerinin geliştirilmesinde önem taşıdığı vurgulanmıştır.

Üretilen, işlenen ve kullanılan bilgi günümüzde giderek artmakta bunun sonucu olarak bilgi güvenliği kavramı önem kazanmaktadır. Yılmaz tarafından 2014 yılında yayınlanan çalışmada, ISO 27001 BGYS'nin kurulması ve bilgi güvenliği tehdit ve zafiyetleri üzerinde durulmuştur. Bilgi güvenliği risklerini belirleyerek, bilgi güvenliğini sağlamak için bilgi teknolojileri alanına yatırım yapmak ve çeşitli teknolojilerin ve yöntemlerin kullanılmasıyla birlikte ISO 27001 gibi standartlar ile BGYS'nin kurulmasının önemi vurgulanmıştır [13]. Martin ve Pehlivan tarafından 2010 yılında yayınlanan çalışmada, BGYS'nin Türkiye'deki şirket ve kamu kurumlarındaki uygulamaları incelenmiştir. Söz konusu çalışmada, ISO 27001 BGYS standardı süreçlerinin zaman ve kaynak gerektirse de uzun vadede fayda

sağladığı; sistemin düzgün işlemesi ve yaygınlaşması için paydaşların özverili davranması gerektiği sonucuna varılmıştır [14]. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) 2020 yılında yayınlanan Bilgi ve İletişim Güvenliği Rehberi ile kuruluşlar ve kritik altyapı hizmeti sunan işletmeler için bilgi ve iletişim güvenliği alanında uygulanması gereken önlemleri belirlemiştir. Tarakçı ve Gönül tarafından 2023 yılında gerçekleştirilen Bilgi ve İletişim Güvenliği Rehberi ve ISO 27001 için siber güvenlik alanında uygulanabilir bir risk analizi ve değerlendirme çerçevesi sunulan çalışmada; risk analizi değerlendirmesinin dijital çağda gelişmeyi hedefleyen kuruluşlar için stratejik bir zorunluluk olduğu belirtilmiştir. Bilgi ve İletişim Güvenliği Rehberi'nin, büyük bir boşluğu doldurduğu ve bu alanda rehberlik sağladığı sonucuna varılmıştır [15].

Yapılan çalışmalar, ISO 27001 BGYS standardı kapsamında yönetim sisteminin kurulması ve risk analizinin önemine vurgu yapmaktadır. Bilgi güvenliği risklerini belirlemek, bilgi teknolojileri yatırımları yapmak ve çeşitli teknolojilerle yönetim sistemini desteklemenin gerekli olduğu belirtilmiştir. Kuruluşlarda BGYS uygulamalarının uzun vadede fayda sağladığı, ancak paydaşların özverili davranması gerektiği vurgulanmıştır. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin yayımladığı rehber ile bilgi ve iletişim güvenliği için uygulanması gereken önlemler belirlenmiş olduğu; siber güvenlik alanında çerçeve sunarak dijital çağda güvenliğini geliştirmeye çalışan kuruluşlar için stratejik bir zorunluluk olarak öne çıktığı belirtilmiştir.

Bilgi Güvenliği Yönetim Sistemi denetimleri ve denetimlerde yaşanan problemler

BGYS süreç tabanlı bir standart olup tek seferlik yapılan çalışmalar ile ISO 27001 standardına uyum sağlanamayacaktır. Uygulanan kontrollerin ve gerçekleştirilen çalışmaların sürekli olması, düzenli kontrol edilmesi gerekmektedir. Durdu ve Eren tarafından 2021 yılında yapılan araştırmada, ISO 27001 BGYS yazılımı tasarımı çalışmaları gerçekleştirilmiştir. ISO 27001 Bilgi Güvenliği Yönetim Sistemi'nin kurumların bilgi varlıklarını korumaları için yapılması gerekli süreçleri barındırdığı ve ISO 27001 BGYS'nin sürekli yaşayan ve sürdürülmesi gereken süreçler içerdiği belirtilmiştir [16]. Siber güvenliği sağlamak için gerçekleştirilen faaliyetlerde, uygulama ve sistemler kullanılsa da söz konusu süreçleri kurgulayan, sistem ve uygulamaları yöneten ve kullanan insan faktörü önem arz etmektedir. Çam, Aslay ve Özen tarafından 2019 yılında yapılan çalışmada, yüksek öğretim kurumlarında bilgi güvenliği farkındalığı seviyelerinin ölçümlenmesi üzerinde durulmuştur.

Bilgi güvenliği açısından, insan faktörünün en zayıf halka olduğu düşünülerek, fiziksel ve maliyetli teknik güvenlik önlemlerine geçmeden önce çalışanların farkındalığının artırılması ve bilgi güvenliği ile ilgili eğitimlerin verilmesiyle çalışanların güvenlik bilincinin oluşturulmasının işletmelere fayda sağlayacağı sonucuna varılmıştır [17].

Sürekli iyileştirmeyi sağlamak için siber güvenlik alanında yönetim sistemi çerçevesinde yapılan çalışmaların kontrolü gerekmektedir. Bu kontroller ise denetim faaliyetleri ile gerçekleştirilmektedir. Antunes, Maximiano ve Gomes tarafından 2022 yılında yayınlanan bilgi güvenliği ve siber güvenlik denetiminin standartlara uygunluğunu yönetmek için özelleştirilebilir bir web platformu konusunda yapılan çalışmada; bilgi güvenliğine yönelik uluslararası standartlara uygunluğun değerlendirilmesi ve sağlanması için ISO 27001 denetimlerinin yapılmasının büyük önem taşıdığı, ISO 27001 denetimlerinin, kuruluşların güvenlik risklerini etkili bir şekilde tanımlamasına ve ele almasına yardımcı olarak siber güvenlik üzerinde olumlu bir etkiye sahip olduğu belirtilmiştir. ISO 27001 denetim süreci ile ilişkin standardın katı olması ve denetim sürecinde fazla esnekliğe izin vermemesi sebebiyle farklı kurumsal ihtiyaçlara dayalı özelleştirmeyi sınırlandırdığı vurgulanmıştır [18]. Al-Karaki, Gawenmeh ve El-Yassami tarafından 2022 yılında yayınlanan akıllı denetim kullanarak bir kuruluş bilgi sisteminin genel güvenlik duruşunun pratik durumu üzerine yapılan çalışmada; denetimlerin, uluslararası standartlara uygunluğu sağlayarak gelişmiş siber güvenlik duruşuna yol açtığından kuruluşlar için çok önemli olduğu, bu denetimlerin kuruluşların Bilgi Güvenliği Yönetim Sistemi'nde güvenlik açıklarını, zayıflıkları ve potansiyel riskleri belirlemelerine yardımcı olduğu belirtilmiştir. Kuruluşların, denetimleri etkin bir şekilde yürütecek vasıflı personel eksikliği nedeniyle zorluklarla karşılaşabileceği vurgulanmıştır [19]. Slapničar, Vuko, Čular ve Drašček tarafından 2022 yılında yapılan siber güvenlik denetiminin etkinliği konulu çalışmada; ISO 27001 denetiminin gerçekleştirilmesinin, kuruluşların standart gerekliliklerini karşılamadaki etkinliğini değerlendirmelerine ve sağlamalarına olanak tanıdığından hayati önem taşıdığı, denetimlerden geçen kuruluşların, siber güvenlik uygulamalarını endüstri standartları ve en iyi uygulamalarla karşılaştırarak güvenlik önlemleri ile stratejilerini iyileştirilmesini sağlayabileceği belirtilmiştir. Siber güvenlik denetim süreçlerinde çeşitli yöntemlerin kullanılması nedeniyle kanıt toplama kapsamının zorlayıcı olabileceği vurgulanmıştır [20]. Mcintosh, Susnjak, Liu, Watters, Xu, Liu, Nowrozy ve Halgamuge tarafından 2024 yılında siber güvenlik çerçevelerinin değerlendirilmesinde fırsatlar, riskler ve mevzuata uygunluk konusunda yapılan araştırmada; ISO 27001 denetimlerinin, veri güvenliği, sürekli izleme ve

politika uyumluluğu gibi alanlara odaklanarak Avrupa Birliği yapay zeka yasasına hazırlık kapsamında değerlendirildiği için önem taşıdığı, denetim süreçlerinin, uluslararası standartlara ve en iyi uygulamalara uygunluğu sağlamak için Bilgi Güvenliği Yönetim Sistemi'nin değerlendirilmesine yardımcı olduğu belirtilmiştir. Gelişen siber tehditlere ve teknolojik gelişmelere ayak uydurmak, BGYS'nin sürekli güncellenmesini gerektirdiği ve bu durumun sınırlı kaynaklara sahip kuruluşlar için zorlayıcı olabileceği vurgulanmıştır [21]. Razikin ve Soewito tarafından 2022 yılında yapılan risk analizi ve siber güvenlik çerçevesine dayalı karar destek modeli konulu çalışmada; ISO 27001 denetimlerinin, siber güvenlik çerçevesine uygunluğun sağlanması ve bilgi teknolojileri güvenlik sistemindeki açıkların tespit edilmesi açısından büyük önem taşıdığı; güvenlik önlemlerinin ve mevcut kontrollerin etkinliğinin değerlendirilmesine katkı sağladığı; kontrollerin etkinliğinin değerlendirilmesine yardımcı olarak kuruluşların güvenlik duruşlarını güçlendirmelerine; hassas verileri siber tehditlerden korumalarına yardımcı olduğu belirtilmiştir. Kuruluşların, ekipleri içinde siber güvenlik ve denetim süreçleriyle ilgili beceri boşluklarıyla karşılaşabilecekleri, denetimlerini gerçekleştirmek için zaman ve personel gibi yeterli kaynakların tahsis edilmesinde zorluklar yaşayabilecekleri vurgulanmıştır [22]. Idayani, Nadlifatin, Subriadi, Janice ve Gumasing tarafından 2024 yılında yayınlanan fintech kullanımının etkileri üzerine siber risklerin incelenmesi konulu araştırmada; denetim sürecinin, kuruluşun bilgi güvenliği ihlalleriyle ilişkili riskleri ele alma becerisini değerlendirerek siber tehditlere ve saldırılara karşı dayanıklılığını artırdığını, ISO 27001'in gerektirdiği şekilde düzenli denetimler gerçekleştirilerek güvenlik açıklarının proaktif bir şekilde tespit edip giderebileceği belirtilmiştir. Denetim süreçlerinin karmaşıklığı ve kaynak yoğunluğunun, kuruluşlar için zorluklar oluşturabileceği ve önemli ölçüde zaman, çaba ve uzmanlık gerektirdiği vurgulanmıştır [23].

Yapılan araştırmalar, ISO 27001 BGYS'nin kurumların bilgi varlıklarını korumak için gerekli süreçleri içerdiğini ve bu süreçlerin sürekli iyileştirilmesi gerekli olduğunu göstermektedir. Siber güvenliği sağlamak için insan faktörünün kritik olduğu belirtilmiştir. Yönetim sistemi çerçevesinde yapılan çalışmaların denetim faaliyetleri ile kontrol edilmesi gerektiği vurgulanmaktadır. ISO 27001 denetimlerinin uluslararası standartlara uygunluğu sağlamada ve güvenlik risklerini tanımlamada önemli olduğu, ancak denetim sürecinin karmaşıklığı ve kaynak yoğunluğunun kuruluşlar için zorluklar oluşturabileceği belirtilmiştir. Denetimlerin, BGYS'nin etkinliğini değerlendirmeye ve güvenlik stratejilerinin iyileştirilmesini sağlamaya katkı sağladığı, siber tehditlere ve teknolojik

gelişmelere uyum sağlamak için BGYS'nin sürekli gözden geçirilmesi gerektiği vurgulanmıştır.

Denetimlerin siber güvenliğe etkileri

Denetim süreçleri ve bu süreçlerin siber güvenliğe etkileri ile ilgili, Michalec, Shreeve ve Rashid tarafından 2023 yılında geleceğin enerji sistemlerinde siber güvenlik vizyonu konulu araştırmada; düzenli denetimlerin, kuruluşların riskleri proaktif bir şekilde yönetmesine, olaylara müdahale yeteneklerini geliştirmesine ve kritik bilgi varlıklarını çeşitli siber tehditlerden korumasına yardımcı olacağı; denetim sürecinin, sağlam bir yönetim sisteminin uygulanmasını sağlayarak kuruluşlarda siber güvenliğin arttırılmasında önemli bir rol oynayacağı belirtilmiştir. Hem personel hem de teknoloji açısından kaynak eksikliğinin, kuruluşların kapsamlı denetimler yapmasını zorlaştırabileceği vurgulanmıştır [24]. Durst, Hinteregger ve Zieba tarafından 2024 yılında çevresel durumun siber güvenlik risk yönetimi ve organizasyonel dayanıklılık üzerindeki etkisi konulu çalışmada; denetim sürecinin, kuruluşların uluslararası standartlara uygunluğu göstererek paydaşlara, müşterilere ve düzenleyici kurumlara bilgi güvenliği konusundaki taahhütlerini göstermelerine yardımcı olacağını, kuruluşların denetimler sırasında uygunsuzlukları belirleyerek siber güvenlik savunmalarını güçlendirecek düzeltici eylemler gerçekleştirebileceğini ve potansiyel siber saldırılara karşı dayanıklılığı artırabileceğini belirtmişlerdir. Kuruluşlardaki sınırlı kaynaklar ve uzmanlığın, denetimlerin başarılı bir şekilde yürütülmesini engelleyebileceği ve siber güvenlik önlemlerine ilişkin değerlendirmelerin derinliğini ve doğruluğunu etkileyebileceği vurgulanmıştır [25]. Patterson, Nurse ve Franqueira tarafından 2024 yılında siber güvenlik olaylarından kurumsal öğrenmenin uygulamaları ve zorlukları konulu araştırmada; denetimler aracılığıyla kuruluşların bilgi güvenliğine olan bağlılıklarını göstererek ve küresel güvenlik standartlarına uygunluklarını sergileyerek paydaşların, müşterilerin ve iş ortaklarının güvenini kazanabileceği, denetim süreci aracılığıyla kuruluşların, güvenlik önlemlerindeki boşlukları ve zayıflıkları tespit ederek genel siber dayanıklılıklarını artırabileceği belirtilmiştir [26].

Aktaş tarafından 2020 yılında yapılan çalışmada, ISO 27001 BGYS sertifikası olan veya olmayan kuruluşların erişim güvenliği düzeylerinin incelenmesi üzerinde durulmuştur. Araştırma sonucuna göre güvenliğin sağlanması için ISO 27001 BGYS belgesine sahip olmanın yeterli olmadığı, kurum ve kuruluşların belirli aralıklarla denetimler yapmaları

gerektiği sonucuna varılmıştır [27]. Eulerich, Masli, Pickerd ve Wood tarafından 2023 yılında denetim teknolojisinin denetim görevi sonuçları üzerindeki etkisi konusunda yapılan çalışmada; düzenli denetimlerin bir kuruluşun yasal cezalardan kaçınmak ve piyasada iyi bir itibarı korumak için hayati önem taşıdığı; ilgili yasa, yönetmelik ve standartlara uymasını sağladığı belirtilmiştir [28]. Dumont, Xu, Felan ve Farges tarafından şirketlerin bilgi güvenliği durumunun teşhisi ile ilgili 2018 yılında yapılan çalışmada, bilgi güvenliği süreçlerinin optimum performansı ve etkin kontrolü için şirketlerin bilgi güvenliği uygulamalarını düzenli olarak değerlendirmesi gerekmekte olduğu; bu durumun BGYS'nin etkinliğini ve sağlamlığını korumaya yönelik bir destek olacağını belirtmişlerdir [29]. Fidancı tarafından 2022 yılında kurumlar için Bilgi Güvenliği Yönetim Sistemi'nin oluşturulması konusunda yapılan çalışmada; etkili bir bilgi ve siber güvenlik yönetimi için, üst düzey yöneticilerin destek ve bilinçli davranışlarının yanı sıra, tüm personelin farkındalığını artırmak ve idari düzenlemeler yapılması gerektiği vurgulanmıştır. Ayrıca, kurum için öncelikli tehditlerin belirlenmesi ve bu tehditleri en aza indirecek uygun çözümlerin tespit edilmesi, bu çözümlerin kurumun özellikleri ve hedeflerine uygun bir şekilde uygulanması, süreçlerin periyodik olarak denetlenmesi ve bu denetimlerin sonuçlarına dayanarak gerekli iyileştirmelerin ve düzenlemelerin yapılması gerektiği belirtilmiştir [30]. Söz konusu denetimler yönetim sisteminin işletildiği kurum/kuruluşlara fayda sağlamak için uygun bir şekilde gerçekleştirilmelidir. Havelka ve Merhout tarafından 2013 yılında yayınlanan, bilgi teknolojileri denetim süreci hakkında yapılan çalışmada; bilgi teknolojisi denetim sürecini iyileştirmek için denetimlerin etkinlik, verimlilik ve kalite ile olan ilişkileri gelecekteki araştırma alanları olduğu sonucuna varılmıştır [31]. Flora ve Rai tarafından 2015 yılında yayınlanan çalışmada, iç denetçilerin siber güvenlik risklerinin uygun şekilde ele alınmasını sağlamak için organizasyonda tamamlayıcı bir rol oynamaları gerektiği; iç denetimin kuruluşun bilgi güvenliği programının etkili ve verimli olmasını sağlamada önemli bir rolü olduğu, iç denetimin kuruluşların bilgi teknoloji birimlerinin iyi performans gösterdiği ve kurumun risk toleransına dayalı olarak riski azaltmak için uygun kontrollere sahip olduğu konusunda güvence sağlayarak kuruma yardımcı olabileceğini belirtmişlerdir [32].

Yapılan araştırmalarda, ISO 27001 denetimlerinin, kuruluşların riskleri yönetmesine, siber olaylara müdahale yeteneklerini geliştirmesine ve kritik bilgi varlıklarını siber tehditlerden korumasına yardımcı olduğu belirtilmiştir. Ayrıca, denetim sürecinin kuruluşların siber güvenlik seviyelerini arttırmada önemli bir rol oynadığı, güvenlik risklerini tanımlamakta ve

güvenlik stratejilerinin iyileştirilmesine katkı sağladığı vurgulanmıştır. Denetimlerin, kuruluşların bilgi güvenliği açıklarını ve zayıflıklarını tespit ederek genel siber dayanıklılıklarını artırmalarına yardımcı olduğu; bununla birlikte, kaynak eksikliği ve uzmanlık konusunda yetersizlikler gibi faktörlerin, denetim süreçlerinin başarısını olumsuz etkileyebileceği vurgulanmaktadır. Denetimlerin, yasa ve standartlara uyum sağlamak, itibarı korumak ve bilgi güvenliği programlarının etkili ve verimli olmasını sağlamak açısından önemli olduğu ifade edilmiştir.

ISO 27001 BGYS'yi işleten kuruluşlarda denetimlerin uygun bir şekilde gerçekleştirilmesi ve denetim sonuçları kuruluşların siber güvenliklerini doğrudan etkilemektedir. Uluslararası İç Denetim Enstitüsü (IIA) tarafından 2024 yıllında yayınlanan "Global Risk Odağı" raporunda siber güvenlik/bilgi güvenliği konuları en yüksek riskli ve denetçilerin en fazla efor sarf ettiği alanlar olarak değerlendirilmiştir [33]. Uluslararası İç Denetim Enstitüsü'nün 2022 yılında yayınladığı "Kuzey Amerika İç Denetimin Nabzı" yayınına göre siber güvenlik, bilgi teknolojileri ve üçüncü taraf ilişkileri ile ilgili konuların en yüksek riskli alanlar olarak belirlendiği; siber güvenlik riskinin araştırma katılımcılarının %85'i tarafından en yüksek risk olarak tanımlandığı görülmektedir [34]. Cisco sponsorluğunda Cybersecurity Ventures tarafından yayınlanan 2022 yılı siber güvenlik yıllık raporuna göre, 2025 yılına kadar siber saldırı kaynaklı maliyet miktarının yıllık olarak %15 yükselerek 10,5 trilyon dolar olması beklenmektedir [35]. Bu bilgiler ışığında, siber güvenliğin kuruluşların en önemli risk konularına dönüştüğü görülmektedir. Bu sebeple denetimlerde siber güvenlik süreçlerinin de değerlendirilmesi gerekmektedir. Uluslararası İç Denetim Enstitüsü'nün 2022 yılında yayınladığı "Küresel Bakış Açıları ve Anlayışlar 2022 Yılında Siber Güvenlik" raporuna göre iç denetimin kuruluşun siber güvenlik stratejisinde dikkate alınması gereken varlıklarının envanterini çıkarması gerektiği; iç denetim ve bilgi güvenliği arasında kurulan doğru ilişkinin, kuruluşun siber güvenlik risk profilinin uyumlulaştırılması gibi siber/bilgi güvenlik riskleri ve fırsatlarının yönetimi ile kuruluşa fayda sağladığı belirtilmektedir [36]. Uluslararası İç Denetim Enstitüsü (IIA) tarafından 2023 yılında yayınlanan "Küresel Bakış Açıları ve Anlayışlar Siber Güvenlik" raporunda; siber güvenliğin kuruluşların büyüklüğünden bağımsız olarak önemli bir tehdit oluşturduğu belirtilmiştir. Raporda, riskler göz önünde bulundurulduğunda, iç denetimin bu riskleri ele alabilen bir ekibi nasıl oluşturacağına dair tavsiyeler bulunduğu görülmektedir. Bu tavsiyeler denetim ile ilgili becerilerin birleşiminin aranması, denetim ile ilgili becerilerin yeni teknolojilere entegre edilmesi, dış kaynak kullanımı, işbirliğinin göz önünde bulundurulması, kurum içi ilişkiler

kurulması, mevcut kaynaklardan faydalanılması konu başlıklarında tanımlanmıştır [37]. Kohnke, Shoemaker ve Sigler (2016) tarafından yapılan çalışmada 2019'da yayınlanan Amerika Birleşik Devletleri (ABD) Genel Muhasebe Ofisi (GAO) raporundan alıntı yapılarak, bilgisayar sistemleri ve ağların siber güvenliğinin tamamen teknik ve mühendislik yöntemleriyle sağlanamayacağına ışık tuttuğu, çünkü siber saldırıların yüzde yetmiş biri insan davranışına bağlı olduğu belirtilmiştir. Bu nedenle bilgi ve iletişim sistemlerinin korunması için, yönetişim temelli kontrol ve denetim süreçlerini dikkate alan her şey dahil bir çerçeve ile desteklenmesi gereken gerçekçi yaklaşımların gerekmekte olduğu sonucuna varılmıştır [38].

ISO 27001 BGYS'yi işleten kuruluşlarda denetim sonuçları ve bu denetimlerin uygun şekilde gerçekleştirilmesi, siber güvenliği doğrudan etkilediği değerlendirilmektedir. Uluslararası İç Denetim Enstitüsü'nün raporları, siber güvenliğin en yüksek riskli alanlardan biri olduğunu ve denetçilerin en çok bu alanda çalıştığını göstermektedir. Siber saldırıların maliyetlerinin artması ve siber güvenliğin önemli bir risk olarak öne çıkması nedeniyle, denetimlerde siber güvenlik süreçlerinin de değerlendirilmesi gerekmektedir. Ayrıca, iç denetim ile bilgi güvenliği/siber güvenlik organizasyonu arasında doğru bir ilişkinin kurulması, kuruluşların siber güvenlik risk durumunu iyileştirmekte olduğu belirtilmiştir. Siber güvenliğin sadece teknik yöntemlerle sağlanamayacağı için yönetişim temelli kontrol ve denetim süreçlerini içeren kapsamlı bir çerçeve gerekmekte olduğu vurgulanmıştır.

Denetimler özelinde denetçilerin bağımsızlığı, tarafsızlığı ve yetkinlikleri gerçekleştirilen denetim sonuçlarının doğrudan etkileyecektir. Vitali ve Giuliani tarafından 2024 yılında gelişen dijital teknolojiler ve denetim firmalarının fırsatlar ile zorlukları hakkında gerçekleştirilen çalışmada, gelecekteki denetçilerin etkili bir şekilde denetim analizi yapabilmek için bilgi teknolojileri ve veri analitiği becerileri kazanmaları beklendiği, bu durumun bilgi teknolojisi denetçisi adı verilen yeni bir denetçi türünün ortaya çıkmasına yol açabileceği belirtilmiştir [39]. Almaqtari, Farhan, Al-Hattami, Elsheikh ve Al-Dalaien tarafından 2024 yılında yapay zekanın bilgi teknolojileri denetimine etkisi hakkında yapılan çalışmada; bilgi denetçilerinin teknolojik gelişmelere ayak uydurabilmeleri ve böylece hızla gelişen denetim ortamında verimliliklerini ve adaptasyonlarını artırmaları için sürekli eğitim ve öğretimin yapılmasının gerektiği sonucuna ulaşılmıştır [40]. Yıldız tarafından 2021 yılında Uluslararası standartlara uyum ve iç denetimin etkinliği üzerine yapılan çalışmada, denetim sonuçlarının, denetçilerin çabaları ve kişisel değerlendirmeleri tarafından

şekillendirildiği ve bu nedenle yetkinliğin, iç denetimin etkinliği açısından kritik bir öneme sahip olduğu belirtilmiştir [41]. Deloitte Development tarafından 2017 yılında yayınlanan "Siber Güvenlik ve İç Denetimin Rolü - Acil Eylem Çağrısı" raporunda; güncel risk ortamına ilişkin uygun teknik becerilere ve bilgiye sahip denetim personelinin sürece dahil edilmesinin kritik düzeyde önemli olduğu vurgulanmıştır [42]. Denetim süreçlerinin etkinliği ve sürece katılan kişilerin yetkinliğinin önemi bir çok çalışmada vurgulanmaktadır. Héroux ve Fortin tarafından 2013 yılında yayınlanan çalışmada, iç denetim fonksiyonunun, bilgi güvenliği yönetişimi, teknoloji farkındalığı, denetçilerin bilişim teknolojileri yetkinliği ve bilgi güvenliği/siber güvenlik risk yönetimi çalışmalarında aktif bir rol oynaması ve etkinliğinin artırılması gerektiğini belirtmişlerdir [43]. Steinbart, Raschke, Gal ve Dilla tarafından 2012 yılında yayınlanan, iç denetimler ve bilgi güvenliği hakkında ilişkiyi inceleyen çalışmada; araştırmacılar denetçi bağımsızlığı, denetçi nitelikleri, bilgi ve becerileri gibi çeşitli iç denetim kalitesi ölçütleri hakkında bilgi toplayamadıklarını ve durumun iç denetim ile bilgi güvenliği organizasyonu arasındaki ilişkinin etkinliğini önemli ölçüde etkilemesi muhtemel olduğunu belirtmişlerdir [44].

Denetim süreçlerinde denetçilerin bağımsızlığı, tarafsızlığı ve yetkinlikleri, denetim sonuçlarını doğrudan etkileyecektir. Yapılan araştırmalar, denetçilerin teknik beceri ve bilgi düzeylerinin, denetim süreçlerinin etkinliği üzerinde kritik bir rol oynadığını göstermektedir. Bu bağlamda, denetçilerin güncel risklerle ilgili derin bir anlayışa sahip olmaları ve bu bilgiyi denetim süreçlerinde etkili bir şekilde kullanabilmeleri önem taşımaktadır. Ayrıca, iç denetim fonksiyonunun bilgi güvenliği yönetişimi ve teknoloji farkındalığında aktif olarak yer alması, kurumların bilgi güvenliği risklerini etkin bir şekilde yönetmelerine yardımcı olabilecektir.

Literatür araştırmasında ISO 27001 BGYS'nin kurum ve kuruluşlara fayda sağladığı ve bu yönetim sisteminin uygulanmasının varlıkların korunmasında ve rekabet avantajında etkili olduğu; ancak sistemin sürekli yaşayan bir sistem olduğu vurgulanmaktadır. Denetimlerin etkinlik, verimlilik ve kalite ile olan ilişkileri gelecekteki araştırma alanları olduğu değerlendirilmiştir. Çalışmalarda iç denetim fonksiyonlarının bilgi güvenliği denetimlerinde aktif rol alması gerektiği belirtilmiştir. Denetçi bağımsızlığı, denetçi nitelikleri, bilgi ve becerileri gibi çeşitli iç denetim kalitesi ölçütlerinin iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin kalitesini önemli ölçüde etkilemesi muhtemel olduğu ifade

edilmiştir. Siber güvenliğin tamamen teknik ve mühendislik yöntemleriyle sağlanamayacağı belirtilerek yönetim sistemi ve bilgi güvenliği denetimlerinin önemi vurgulanmıştır.

Araştırmada özet olarak ISO 27001 standardının karlılık, işgücü verimliliği, satış performansı ve rekabet avantajı gibi konularda fayda sağlaması ile ilgili bir çok çalışma olduğu görülmüştür. BGYS denetim süreçlerinin önemi vurgulanarak yönetim sisteminin sürekli etkin denetlenmesi gerektiği belirtilmiştir. Siber güvenlik üzerine yapılan çalışmalarda yayınlanmış uluslararası raporlara göre siber güvenliğin en riskli konulardan olduğu ve iç denetimin siber güvenliğin sağlanması konusunda fayda sağladığı değerlendirilmektedir. Denetimlerin etkinliği için denetim kaynağı, denetçilerin teknik becerileri, bağımsızlığı ve objektifliği gibi kriterler vurgulanarak gelecekteki araştırma konuları olarak belirtilmiştir.

Bu çerçevede konu ile ilgili literatür araştırmasında ISO/IEC 27001 BGYS'nin kurulumu, risk yönetiminin uygulanması ve genel iç denetim süreçleri ile ilgili birçok çalışma olduğu görülmüştür. Bu çalışmalar da denetim ve kontrol faaliyetlerinin önemi vurgulanmakla birlikte ISO/IEC 27001 denetim süreci, denetim sürecinde yaşanan zorluklar ve yapılabilecek iyileştirmeler ile ilgili ülkemizde bir çalışma olmadığı görülmüştür. Denetim süreçlerinde tespit edilen veya edilemeyen siber güvenlik eksikliklerinin kurum ve kuruluşların siber güvenliğini doğrudan etkileyeceği düşünülerek; bu kapsamda literatürde bulunan bu boşluk ile ilgili araştırma çalışması gerçekleştirilmiştir.

3. BİLGİ GÜVENLİĞİ ve DENETİMİ

3.1. Bilgi

Türk Dil Kurumu (TDK) sözlüğü tarafından bilgi “insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bilgi, malumat”, “öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek; haber, malumat, vukuf”, “insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf”, “duyu organları yoluyla algılama, hayal gücü ve bellek yardımıyla zihnin ilk olarak kavradığı temel düşünceler” veya “verinin anlam kazanmış biçimi” şeklinde tanımlanmıştır [45].

Şekil 3.1. Bilgi piramidi

Şekil 3.1’de bilgi piramidinde verinin hiyerarşik ilerleme yolu görülmektedir. Piramitte bulunan kavramlardan veri için “data”, anlamlandırılmış veri için “information”, öğrenilmiş bilgi için “knowledge” ve bilgelik için “wisdom” şeklinde İngilizce çevirileri olsa da farklı anlamları olan bu sözcüklerin çoğunlukla Türkçe’ye “bilgi” şeklinde çevrilerek kullanılmaktadır.

Gökçen (2011) ise çalışmasında bilgiyi, yöneticilerin yararına olacak şekilde şekillendirilmiş bir biçimde, belirlenmiş hedeflere ulaşmak veya bakış açısını geliştirmek için dönüştürme ve

analiz sürecinin sonucu olarak tanımlamaktadır [46]. Bu tanımlamaya göre anlamlandırılabilen veriye bilgi denilmektedir. Örnek olarak sadece rakam ve sayılar verileri oluştururken, bu sayılar satış yüzdeleri veya sınav notları gibi anlamlandırılabildiğinde bilgiye dönüşmektedir. Günümüzde teknolojinin çok hızlı bir şekilde gelişmesi sebebiyle, veri ve bilgi sayıları çok hızlı bir şekilde artmaktadır. 2020 yılı itibari ile 7,75 milyar dünya nüfusu için 5,19 milyar mobil telefon kullanıcısı; 4,54 milyar internet kullanıcısı ve 3,8 milyar sosyal medya kullanıcısı bulunmaktadır [47]. Buzdolapları, klimalar, fırınlar internete bağlanabilmekte, şehirler akıllanmaktadır. Bu nesnelerin hepsi ayrı ayrı veri üretmekte ve bu veriler bilgiye dönüşebilmektedir. Geçmişte sadece fiziksel ortamda depolanan veriler ise dijital ortama taşınıp farklı bilgi sistemlerinde ve/veya bulut ortamlarında saklanmaktadır. Dijital ortama geçişten sonra bilginin paylaşımı; taşınabilir disk, e-posta, bulut paylaşımı gibi birçok farklı yöntem ile gerçekleştirilmektedir. Bilginin miktarı, saklanma ve iletim yöntemlerinin arttığı ve çeşitlendiği günümüzde bilgi güvenliği kavramı önemini artırmaya devam etmektedir.

3.2. Bilgi Güvenliği

Bilginin ve dolayısıyla güvenliğinin önem kazandığı günümüzde bilgi güvenliği kavramı ile ilgili literatürde farklı tanımlamalar yapılmıştır. Nazarov ve Kovtun (2021) bilgi güvenliğini; bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için bilginin yetkisiz erişimden, açığa çıkarılmasından, yetkisiz değiştirilmesinden ve yok edilmesinden korunması olarak tanımlamışlardır [48]. Somepalli, Tangella, Yalamanchili (2020) bilgi güvenliği kavramı hakkında, verilere yetkisiz erişimi, kullanımı, ifşa edilmesini, kesintiye uğramasını, değiştirilmesini veya imha edilmesini önlemeyi içeren bilgi risklerini azaltarak bilgileri koruma uygulaması şeklinde bahsetmiş; hassas bilgilerin korunmasına ve güvenin korunmasına yardımcı olduğundan, teknoloji alanında çalışan herkes veya güvenlik ihlali riskiyle karşı karşıya olan herhangi bir kuruluş için çok önemli olduğunu belirtmişlerdir [49]. Canbek ve Sağıroğlu (2006) bilgi güvenliğini; bilgiye gelebilecek zararların engellenmesi için uygun teknolojilerin uygun yollarla kullanılması ve yetkisiz erişimi önlemek için bilgiye yetkisiz kişilerin ulaşmasının engellenmesi olarak tanımlamıştır [50]. Solms (2006) ise bilgi güvenliğini; kurumsal bilgi teknolojisi varlıklarının erişilebilirliği, bütünlüğü ve gizliliği üzerindeki risklerini yönetmeyi amaçlayan bir alan şeklinde tanımlamıştır [51]. Baykara, Daş ve Karadoğan (2013) tarafından yapılan çalışmada ise bilgi güvenliği kavramı; bilgiye sürekli erişilebilirlik ihtiyacı duyulduğunda, bilginin başlangıç noktasından varış noktasına kadar

gizlilik içinde, değişmeden veya bozulmadan, yetkisiz erişim olmaksızın iletilmesi olarak tanımlanmıştır [52]. Galinkin (2021) tarafından yapılan çalışmada bilgi güvenliği ile ilgili saldırganların, ekonomik kazanç, siyasi motivasyonlar, fikri mülkiyet hırsızlığı ve bunun gibi çeşitli nedenlerle saldırı gerçekleştirdiklerini, bilgi güvenliğini savunanların ise, mümkün olduğu kadar saldırganların ilk erişimini engellemeye çalıştığını; başarısız olmaları durumunda saldırıyı mümkün olduğu kadar çabuk tespit etmeye çalıştıklarını belirtmişlerdir [53].

Bilgi güvenliğinin tanımlarında bulunan üç temel unsur Şekil 3.2'de bulunmaktadır.

Şekil 3.2. Bilgi güvenliği unsurları

Şekil 3.2'de bulunun bilgi güvenliği temel unsurları; "gizlilik" bilgiye sadece erişmeye yetkili kişilerce erişilmesi, "bütünlük" bilginin değiştirme yetkisi olan kişiler tarafından değiştirilmesi ve "süreklilik" erişim yetkisi olan kişilerin istediği zaman bilgiye erişebilmesi olarak tanımlanmaktadır.

2006 yılında Türkçe çevirisi yayınlanan ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardında ise “gizlilik, bilginin yetkisiz kişiler, varlıklar ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliği; bütünlük, varlıkların doğruluğunu ve tamlığını koruma özelliği; kullanılabilirlik, etkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği” olarak tanımlanmaktadır [54]. Örnek vermek gerekirse; bilgisayarda oluşturulan bir belge için, yetkisiz kişiler tarafından dosyaya ulaşılması gizliliğin ihlaline, yetkisiz yollarla erişilen belge içerisindeki verilerin değiştirilmesi bütünlüğün ihlaline, belgenin silinerek tekrar ulaşılamaz hale getirilmesi ise erişilebilirliğin ihlaline örnek olarak verilebilir.

Bilgi güvenliğinin gizlilik, bütünlük ve erişilebilirlik temel unsurlarının yanında güvenliğin sağlanması amacıyla ek unsurları da bulunmaktadır. Bunlar izlenebilirlik/kayıt tutma (Accountability), yetkilendirme (Authorization), kimlik doğrulama (Authentication), inkar edememe (Non-repudiation) ve güvenilirlik (Reliability-Consistency) olarak literatürde tanımlanmıştır.

Kimlik doğrulama, bir kişinin veya kuruluşun belirli bilgi veya kaynaklara erişmesine izin vermeden önce kimliğinin doğrulanması işlemi; yetkilendirme, kimliği doğrulanmış bir kullanıcının bir sistem içinde veya belirli kaynaklarla ne yapmasına izin verildiğini belirleme süreci olarak tanımlanmaktadır [55]. İzlenebilirlik/kayıt tutma, eylem veya olayların, bunu gerçekleştiren kişiye veya sisteme kadar izlenebilmesini sağlamak, sorumlu tarafların belirlenmesini ve eylemlerinden sorumlu tutulmasını mümkün kılmak kavramını ifade etmektedir [56].

İnkar edememe bir kişi veya kuruluşun dijital işlemlerde mesaj göndermek veya işlem yapmak gibi eylemlerini inkar edememesi olarak tanımlanmaktadır [57]. Öte yandan bilgi güvenliğinde güvenilirlik; bir bilgisayar, bilgi veya iletişim sisteminin yüksek düzeyde güvenlik sağlarken, belirlenen özelliklere ve tasarım ön koşullarına göre titiz, kesin bir şekilde çalışabilme kapasitesini ifade etmektedir [50].

Bilgi güvenliğine dair saldırılar virüsler, solucanlar, sosyal mühendislik, dağıtık servis dışı bırakma saldırıları (DDOS), botnet saldırıları ve fidye yazılımları gibi bir çok farklı yöntem ile gerçekleştirilmektedir. Siber saldırılarda, bilinen zafiyetler veya 0 gün açıklıkları olarak henüz güvenlik önlemi/yaması yayınlanmamış zafiyetler/açıklıklar saldırganlar tarafından

istismar edilmektedir. Yazılım ve bilişim sistemleri geliştiricileri ise tespit edilen zafiyet/açıklıklar için güvenlik yamaları üretmektedir. Örneğin 2014 yılında bildirilen ve tüm dünyada büyük etki yaratan Linux tabanlı işletim sistemlerinde kritik seviyeli uzak saldırganların hazırlanmış bir ortam aracılığıyla rastgele kod yürütmesine olanak tanıyan Shellshock [58] ve Windows tabanlı işletim sistemlerinde uzaktaki saldırganların hazırlanmış paketler aracılığıyla rastgele kod yürütmesine olanak tanıyan Winshock [59] açıkları için çok kısa sürede güvenlik yamaları geliştiriciler/üreticiler tarafından yayınlanmıştır. Ancak bu açıklıkların yaklaşık 20 yıldır kullanılan söz konusu işletim sistemlerinde; güvenlik yamaları yayınlanmadan önce hangi saldırganlar tarafından istismar edildiği bilinememektedir.

3.3. Siber Güvenlik

Siber güvenlik, son zamanlarda teknolojiye ve internete bağımlılığın katlanarak artması göz önüne alındığında, çağdaş dijital ortamlarda hayati bir unsur haline gelmiştir. Günümüzde sanal alandaki verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumakla ilgili temel yükümlülükler zorlaşmıştır. Tüm paydaşlar, çeşitli iş ve işlemler için büyük ölçüde siber sistemleri kullanmakta ve bu durum her bireyi potansiyel siber tehditlere karşı hedef haline getirmektedir. Bu, riskleri azaltmak ve dijital alanda faaliyet gösteren kötü niyetli aktörlere karşı savunmaları güçlendirmek için sağlam siber güvenlik önlemlerine zorunlu ihtiyaç duyulmaktadır.

Siber güvenlik bilgi güvenliğinin bir alt bileşeni olarak tanımlanabilmektedir. Bilgi güvenliği öncelikle her türlü verinin korunmasına odaklanırken, siber güvenlik özellikle ağlar, bilgisayarlar ve uygulamalar dahil olmak üzere dijital alandaki bilgilerin korunmasıyla ilgilenir. Siber güvenlik, bilgisayar korsanları ve siber saldırılar gibi çevrimiçi tehditlere karşı korumayı vurgulayan, bilgi güvenliğinin bir alt kümesidir. Bilgi güvenliğinin daha geniş bir veri koruma yelpazesini kapsadığı, siber güvenliğin ise dijital tehditler ve savunmalara odaklandığı günümüzün teknoloji odaklı dünyasında her ikisi de hayati öneme sahiptir [60]. Taherdoost (2022) çalışmasında siber güvenlik ve bilgi güvenliğinin birbiriyle yakından ilişkili olmasına ve bazı yönlerden örtüşmesine rağmen temel farkın bilgiyle ilgili olduğunu belirtmiş, bilgi güvenliğinin her yerde bilgiyi korumaya odaklanırken siber güvenliğin özellikle siber uzaydaki bilgilere odaklandığını vurgulamıştır [61]. Siber güvenliğin gün geçtikçe popülerlik kazandığı günümüzde siber güvenlik kavramı ile ilgili literatürde farklı tanımlamalar yapılmıştır. Bagó (2023) tarafından siber güvenlik, bilgisayar sistemlerinin,

ağlarının ve verilerinin siber saldırılara karşı korunması olarak tanımlanmıştır [62]. Pour, Nader, Friday ve Bou-Harb (2023) tarafından siber güvenlik; bilgisayar ve elektronik sistemleri, mobil cihazları, ağ sistemleri ve verileri kötü niyetli saldırılara karşı koruma uygulaması olarak tanımlanmıştır. İnternetin kritik bir altyapı haline gelerek toplumu siber saldırılara karşı daha savunmasız hale getirdiği vurgulanmıştır [63]. Hasan, Habib, Islam, Safie, Abdullah ve Pandey (2023) tarafından siber güvenlik, dijital sistemleri, ağları ve cihazları siber saldırılardan, yetkisiz erişimden ve veri ihlallerinden korumak için alınan önlemler olarak tanımlanmıştır [64].

Türkiye'deki Mevzuat

Siber güvenlik, bilgisayar ekipmanı, personel, uygulamalar ve bilgi dahil olmak üzere dijital alandaki kurumların, kuruluşların ve bireylerin varlıklarını korumak için tasarlanmış çeşitli araçları, politikaları, kavramları, yönergeleri ve teknolojileri kapsamaktadır. Türkiye'de siber güvenlik ile ilgili süreç ve sorumlulukların tanımlanması için çalışmalara başlanıldıktan sonra; Bakanlar Kurulu tarafından 11 Haziran 2012 tarihli "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetimi ve Koordinasyonu Kararı" ile Siber Güvenlik Kurulu oluşturularak; o zamanki ismi ile Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na siber güvenliğin yönetimi ve koordinasyonu konusunda görevler verilmiştir. Dana sonra, 6 Şubat 2014 tarihinde yayınlanan 6518 sayılı Ulusal Siber Güvenlik Çalışmaları Kanunu'nda 5809 sayılı Elektronik Haberleşme Kanunu'nda değişiklikler yapılmış ve Bakanlar Kurulu kararı güncelleştirilerek siber güvenlik görevleri Bilgi Teknolojileri ve İletişim Kurumu'na atanmıştır [65]. Son olarak kurulan Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) ise, proje geliştirme yoluyla siber güvenlik ve bilgi güvenliğini geliştirmek için 10 Temmuz 2018 tarihli 1 sayılı Cumhurbaşkanlığı Kararnamesi ile görevlendirilmiştir [66].

İlk olarak Siber Güvenlik Kurulu'nun kurulması ile Türkiye'de Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarının geliştirilmesine başlanmıştır. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı olarak bilinen ilk plan 25 Mart 2013 tarihinde onaylanmıştır. Eylem planı kapsamında, Ulusal Siber Olay Müdahale Merkezi (USOM) ve Bilgi Teknolojileri ve İletişim Kurumu bünyesinde Sektörel Siber Olay Müdahale Ekibinin kurulması ile Türkiye'deki siber olaylara müdahale için koordinasyon amaçlanmıştır. USOM, özellikle kritik altyapı alanlarında elektronik ve iletişim sektörünü denetlemekle görevlendirilmiştir [67]. Son olarak 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem

Planı, ulusal siber güvenliğin hedefler doğrultusunda yönetilmesi amacıyla 29 Aralık 2020'de yayınlanmıştır.

Kilitli Kalkan (Locked Shields) tatbikatları

Siber güvenlik ile ilgili sorumluluklar ve mevzuatın tanımlanması sürecinde Türkiye aynı zamanda NATO kilitli kalkan tatbikatlarına aktif olarak katılım sağlayarak konu ile ilgili yetkinliklerini test etmiş ve kendini geliştirme fırsatı bulmuştur. NATO Siber Savunma Mükemmeliyet Merkezi tarafından 2010 yılından bu yana düzenlenen yıllık tatbikatlar ile siber güvenlik uzmanlarına, ulusal BT sistemlerini ve kritik altyapıyı gerçek zamanlı saldırılar altında savunma becerilerini geliştirme imkanı tanınmaktadır. Tatbikatların odak noktası, gerçekçi senaryolar, en son teknolojiler ve stratejik karar alma, hukuki ve iletişim hususları da dahil olmak üzere siber olayların tüm karmaşıklığının simülasyonudur [68].

Türkiye 2014 yılından bu yana bu tatbikatlara katılmaktadır. Tatbikat sırasında siber varlıkları ve kritik altyapıları hedef alan çeşitli siber saldırı senaryoları değerlendirilerek ve Türk Silahlı Kuvvetleri, kamu kurumları/kuruluşları ve siber güvenlik konusunda uzmanlaşmış şirketlerin aktif katılımıyla siber alandaki yeterlilik test edilmektedir. Tatbikat ile kurumlar arası bilgi paylaşımını ve koordinasyonunu geliştirmek amaçlanmaktadır [69]. Kilitli Kalkan siber savunma tatbikatları, siber savunma ekiplerinin yetkinliklerini ve karar verme yeteneklerini incelemek ve değerlendirmek için hazırlanmış karmaşık bir siber olayın karmaşık ve kapsamlı bir simülasyonunu temsil etmektedir. Kilitli Kalkan gibi siber savunma tatbikatları, ilerleyen siber riskler ışığında hayati altyapıların ve kuruluşların sağlamlığını geliştirmede ve değerlendirmede çok önemli bir rol oynamaktadır. Bu alıştırmalar, katılımcılara teknik yeteneklerini geliştirme, olay müdahale protokollerini test etme ve zorlu koşullar altında uyumlu bir birim olarak verimli bir şekilde işbirliği yapma kapasitelerini geliştirme fırsatı sunmaktadır [70].

Türkiye, siber güvenlik sorumluluklarını ve mevzuatını geliştirirken NATO'nun Kilitli Kalkan tatbikatlarına katılarak yetkinliklerini test etmiştir. 2014'ten beri katıldığı bu tatbikatlar, siber güvenlik uzmanlarına bilgi sistemlerine siber saldırılar sırasında savunma becerilerini artırmalarına yardımcı olmaktadır. Tatbikatlar, kurumlar arası bilgi paylaşımını ve koordinasyonunu geliştirmeyi amaçlamaktadır. Bu sayede, hayati altyapıların sağlamlığı artırılmakta ve katılımcılar teknik yeteneklerini geliştirme fırsatı bulmaktadır.

3.4. ISO 27001 Bilgi Güvenliği Yönetim Sistemi

BGYS uluslararası kabul görmüş şekilde süreç ve kontroller aracılığıyla bilgi güvenliği süreçlerinin yönetişimini sağlayan bir standarttır. Azinheira, Antunes, Maximiano ve Gomes (2023) çalışmalarında standardın karmaşık olmasına rağmen telekomünikasyon, fiziksel, çevresel, insan kaynakları, uygulama güvenliği ve lisanslama gibi birden fazla güvenlik hususunu ele aldığından kapsamlı bir standart olarak ortaya çıktığını belirtmişlerdir. Süreç ve prosedür içeriğiyle standardın gereklilikleri genel olduğundan işin türü, büyüklüğü veya niteliği ne olursa olsun tüm kuruluşlar için geçerli olduğunu vurgulamışlardır [71]. Stoica ve Candoi-Savu (2020) çalışmalarında ISO 27001 standardının BGYS'nin kurulması, uygulanması, sürdürülmesi ve sürekli olarak iyileştirilmesi için bir çerçeve sağlayan, bilgi güvenliğini yönetmek için uluslararası bir standart olduğunu belirtmişlerdir [72]. Singgrit ve Pamuji (2020) çalışmalarında ISO 27001 için bilgi güvenliğini yönetmek için bir çerçeve sağlayan, kuruluşların Bilgi Güvenliği Yönetim Sistemi'nin benimsenmesi yoluyla bilgilerini sistematik ve uygun maliyetli bir şekilde korumalarına yardımcı olan uluslararası bir standart olarak bahsetmişlerdir. ISO 27001'in uygulanmasının riskleri tanımlayarak, etkilerini değerlendirerek ve herhangi bir zararı sınırlamak için sistemli kontroller uygulayarak kuruluşların bilgilerini korumalarına yardımcı olduğunu ve böylece genel güvenlik duruşlarını geliştirdiğini belirtmişlerdir [73]. Ersoy (2012) tarafından; BGYS olarak kısaltılan Bilgi Güvenliği Yönetim Sistemi'nin, bilgilerin yönetimi için benimsenen planlı bir standart olarak ana hedefinin önemli bilgilerin korunması olduğu; bilgi gizliliği, bütünlüğü ve erişilebilirliği için sistemli, devamlılığı sağlayan, belgelenmiş, üst yönetim tarafından kabul edilen ve desteklenen, uluslararası standartlara dayanan bir bütün olduğu belirtilmektedir [74]. Calder ve Watkins (2008) kitaplarında BGYS'nin faydaları ile ilgili; sertifikalandırılmanın mevcut veya BGYS'yi kurmayı hedefleyen kuruluşlar için etkin bilgi güvenliği proseslerinin tanımlanması ve uygulanması ile güvence oluşturduğunu, sertifikasyonun sürekli iyileştirme sağladığını belirtmişlerdir [75]. Vural ve Sağıroğlu (2008) çalışmalarında BGYS'nin insanı, iş süreçlerini ve bilgi sistemlerini içeren ve yönetimce desteklenen bir yönetim sistemi olduğu; kuruluşlar için kritik bilgilerin ve bilgi sistemlerinin korunması, risklerin azaltılması ve erişilebilirliğin yükseltilmesini sağladığını belirtmişlerdir [76].

Günümüzde bilgi güvenliğinin sağlanması amacıyla birçok bilişim sistemleri ve yazılım geliştirilmesine/üretilmesine rağmen, bu bilişim sistemleri ve yazılımlarının bilgi güvenliğinin tam olarak sağlanması mümkün olmamaktadır. Bilgi güvenliği yatırımlarının büyük bir kısmı teknik önlemlere harcanıyor olsa bile, insan faktörü bilgi güvenliği zincirinin en önemli halkalarındandır. İletişim ortamlarının kullanımının artmasıyla birlikte, bilgi güvenliğinin sağlanma gerekliliği her geçen gün daha da artmıştır. Yalnızca teknik tedbirlerle (anti virüs uygulamaları, veri sızıntı önleme uygulamaları, açıklık tarama sistemleri, saldırı önleme/tespit sistemleri, güvenlik duvarları, kriptografi, vb.) kuruluşlarda bilgi güvenliğini %100 sağlamak mümkün değildir. Bu sebepten ötürü teknik tedbirlerin yanında, insanları ve süreçleri içeren yönetim sistemleri ihtiyacı doğmuştur. Kurum ve şirketlerde, bilgi güvenliğinin sağlanması, risklerin yönetilmesi amacıyla yönetim sistemleri kurulmaya ve işletilmeye başlanmıştır.

Ersoy (2012) çalışmasında ISO 27001 standardını; kuruluşların güvenlik ihtiyaçlarını tanımlayan, ancak gerçekleştirme yöntemini kuruluşların belirlemesini isteyen; içeriden veya dışarıdan kötü niyetli kullanımı önlemek için gereksinimleri barındıran bir standart olarak tanımlamıştır. ISO/IEC 27001 içerisinde, standardın amacının BGYS'yi kurmak, uygulamak, işletmek, izlemek, gözden geçirmek, devam ettirmek ve geliştirmek için bir çerçeve oluşturması şeklinde tanımlandığı belirtilmiştir [77]. Vural ve Sağıroğlu (2008) çalışmalarında; işletmelerin bilgi güvenliği ile iş sürekliliklerini sağlamaları için, teknik tedbirlerin yanı sıra insan, dokümantasyon ve süreçsel diğer tedbirleri almaları gerektiği; süreçlerin sürdürülebilirliğini sağlayarak standart şartlarına uygun olarak yönetilebilmesi için insan, süreç ve bilişim teknolojilerini kapsayan BGYS'nin kurulmasının fayda sağlayacağını belirtmişlerdir [76].

3.4.1. ISO 27001 BGYS standardı içeriği

ISO/IEC 27001 BGYS standardı ISO 27000 standart ailesinin şirketler/kurumlar tarafından belgelendirilen ana standardıdır. Standart Çizelge 3.1'te 10 ana madde ve Çizelge 3.2'de 4 başlıkta bulunan 93 ek kontrol maddesini içermektedir [78].

Çizelge 3.1. ISO 27001 standardı ana maddeleri

No	Başlık
0	Giriş
1	Kapsam
2	Atıf yapılan standartlar ve/veya dokümanlar
3	Terimler ve tarifler
4	Kuruluşun bağlamı
5	Liderlik
6	Planlama
7	Destek
8	İşletim
9	Performans değerlendirmesi
10	İyileştirme

Çizelge 3.1'de ISO 27001 standardı ana maddeleri bulunmaktadır. Giriş bölümü sonrası, birinci bölümde standardın kapsamı, ikinci bölümde atıf yapılan standart ve dokümanlar, üçüncü bölümde ise tanımlar ile ilgili bilgiler bulunmaktadır. Dördüncü bölümde yönetim sisteminin kurulacağı kuruluşun bağlamı ve ilgili tarafların beklentileri ile ilgili esaslar, beşinci bölümde yönetimin liderliği ve bilgi güvenliği politikası esasları, altıncı bölümde riskler ve hedefler kapsamında planlama ve sekizinci bölümde riskler ve hedefler kapsamında işletim esasları bulunmaktadır. ISO 27001 standardı; yedinci bölümünde farkındalık, iletişim, dokümantasyon, dokuzuncu bölümünde yönetim sistemi performansı değerlendirme, iç tetkikler ve onuncu bölümünde sürekli iyileştirme ile ilgili hususları içermektedir.

Çizelge 3.2. ISO 27001 standardı ek kontrol maddesi ana başlıkları

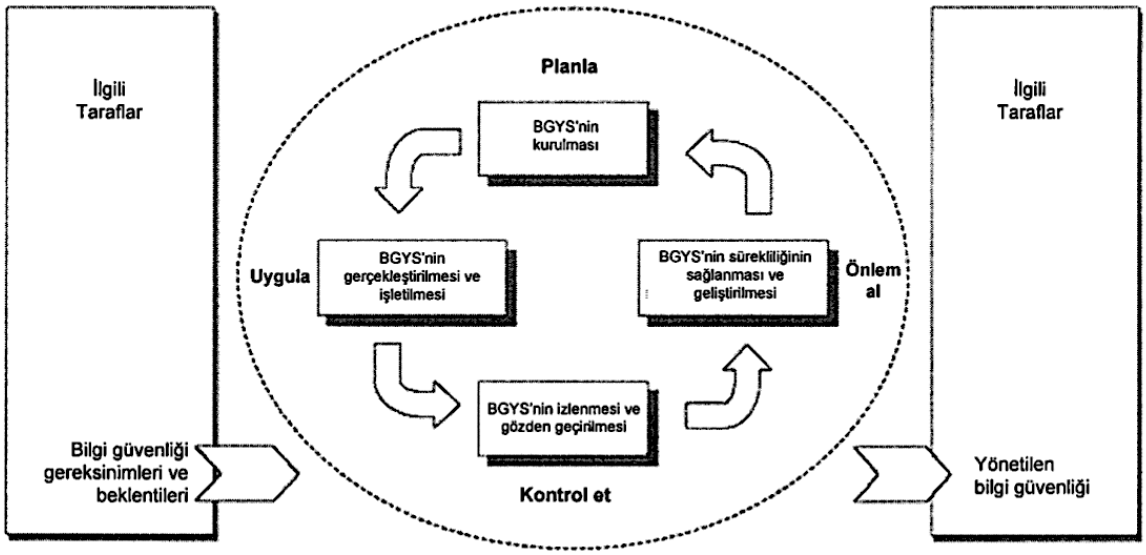
Kontrol Maddesi No	Kontrol Başlığı
A.5	Kurumsal Kontroller
A.6	Kişi Kontrolleri
A.7	Fiziksel Kontroller
A.8	Teknolojik Kontroller

Çizelge 3.2'de ISO 27001 standardı ek kontrol başlıkları bulunmaktadır. Standartta bulunan kurumsal kontroller başlığı içerisinde genel olarak süreç ve dokümantasyon ile ilgili kontroller, örneğin "5.1 Bilgi güvenliği politikaları"; kişi kontrolleri başlığı içerisinde insan kaynağı ile ilgili kontroller, örneğin "6.3 Bilgi güvenliği farkındalığı, eğitim ve öğretim"; fiziksel kontroller başlığı içerisinde genel olarak fiziksel mekanlar ile ilgili kontroller, örneğin "7.3 Ofislerin, odaların ve tesislerin güvenliğini sağlama" ve teknolojik kontroller başlığı içerisinde teknik konularda kontroller, örneğin "8.4 Kaynak koduna erişim" gibi kontroller bulunmaktadır.

3.4.2. ISO 27001 BGYS'nin kurulumu

ISO 27001 standardı, BGYS'nin kuruluşu, uygulanışı, sürdürülüşü ve sürekli iyileştirilmesi için gereksinimleri içermektedir. BGYS; bilgi güvenliği unsurları olan bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini; risk yönetimi süreci aracılığıyla sağlayarak, risklerin doğru şekilde yönetildiğine dair güvence sunar. ISO 27001 standardında belirtilen gereksinimler geneldir ve tüm kurum ile şirketler için uygulanabilir olması amaçlanmıştır. Standarda uyumlu olduğunu iddia edenler, 4. Madde ile 10. Madde arasında bulunan esaslara uygunluk sağlaması gerekmektedir [78].

ISO 27001 BGYS'yi kuran ve sertifikalandırılmak isteyen bir kuruluşun standarda göre BGYS kapsamını, ilgili tarafları ve bu tarafların beklentilerinin belirlemesi gerekmektedir. Bu kapsamda bilgi güvenliği politikası oluşturulur, roller/sorumluluklar/yetkiler tanımlanır ve standardın istediği gerekli dokümantasyon oluşturulur. Bilgi güvenliği riskleri belirlenip, değerlendirildikten sonra gerekli kontroller uygulanır. Bu aşamadan sonra yapılan çalışmalar izlenmekte, ölçülmekte, iç tetkik ile kontrol edilmekte ve yönetim tarafından gözden geçirilmektedir. İyileştirilebilir ve/veya uygunsuz alanlar için düzeltici faaliyetler gerçekleştirilmelidir. Son olarak belgelendirilme şirketine başvurularak, belgelendirme denetim ve süreçlerinden geçilmesi gerekmektedir.



Şekil 3.3. PUKO modeli [54]

Şekil 3.3'de Planla, uygula, kontrol et, ve önlem al (PUKÖ) modeli bulunmaktadır. Bu modele göre ISO 27001 BGYS kurmak ve sertifikalandırılmak isteyen kuruluş öncelikle planlama faaliyetleri yürütmeli, bu planlarını uygulamalı daha sonra yapılan çalışmaları kontrol etmeli ve gerekli önlemleri alarak döngünün başına dönmelidir [54]. Bu tez çalışmasının konusu olan iç denetim/tetkikler kontrol et aşamasının başlıca faaliyetleridir. Bilgi güvenliği kapsamında yapılan çalışmaların, periyodik denetimler ile uygun kontrolü kuruluşun bilgi güvenliği ve siber güvenliği için önem arz etmektedir.

3.4.3. ISO 27001 BGYS standardı tarihçesi

ISO 27001 Standardı, bilgi güvenliği veya siber güvenliğe yönelik ISO 27000 standartlar serisinin birinci standardı olarak yayımlanmıştır. İlk olarak 2005 yılında yayınlanan standart; değişen bilgi güvenliği süreçlerine daha iyi uyum sağlamak için 2013 yılında ve ardından 2022 yılında revize edilmiştir. Güncel versiyona "ISO 27001:2022 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Gereksinimler" adı verilmiştir. ISO 27001, 2005 yılı öncesinde bir İngiliz standardı olan BS 7799'i temel almakta olup ISO 17799 olarak isimlendirilmiştir.

ISO 27001 standardının 2022'de yayınlanan versiyonunda ISO 27001:2013 standardındaki ana maddelerde değişiklik yapılmamıştır. Standardın 6. Planlama maddesine "6.3 değişikliklerin planlanması" maddesi değişiklik yönetim süreci ile ilgili esasları içerecek

şekilde eklenmiştir. Toplam kontrol sayısı 114'ten 93'e indirilmiştir. Bazı kontrol maddeleri birleştirilmiş ve 11 yeni kontrol maddesi eklenmiştir [78]. Standarda yeni eklenen kontrol maddeleri Çizelge 3.3'de görüldüğü şekildedir.

Çizelge 3.3. ISO 27001:2022 yeni eklenen kontrol maddeleri

No	İsim
1	A.5.7 Tehdit İstihbaratı
2	A.5.23 Bulut Hizmetlerinin Kullanımı için Bilgi Güvenliği
3	A.5.30 Bilgi ve İletişim Teknolojisi (ICT) 'nin İş Sürekliliğine Hazır Olması
4	A.7.4 Fiziksel Güvenlik İzleme
5	A.8.9 Yapılandırma Yönetimi
6	A.8.10 Bilgilerin Silinmesi
7	A.8.11 Veri Maskeleme
8	A.8.12 Veri Sızıntısını Önleme
9	A.8.16 İzleme Faaliyetleri
10	A.8.23 Web Filtreleme
11	A.8.28 Güvenli Kodlama

Çizelge 3.3'de ISO 27001 standardına 2022 yılında eklenen kontrol maddeleri görülmektedir. Günümüzde kullanım alanı artan ve teknolojinin gelişmesi ile ortaya çıkan; tehdit istihbaratı, bulut hizmetleri gibi güncel konularda kontrol maddelerinin eklendiği görülmektedir.

3.4.4. ISO 27000 standart ailesi

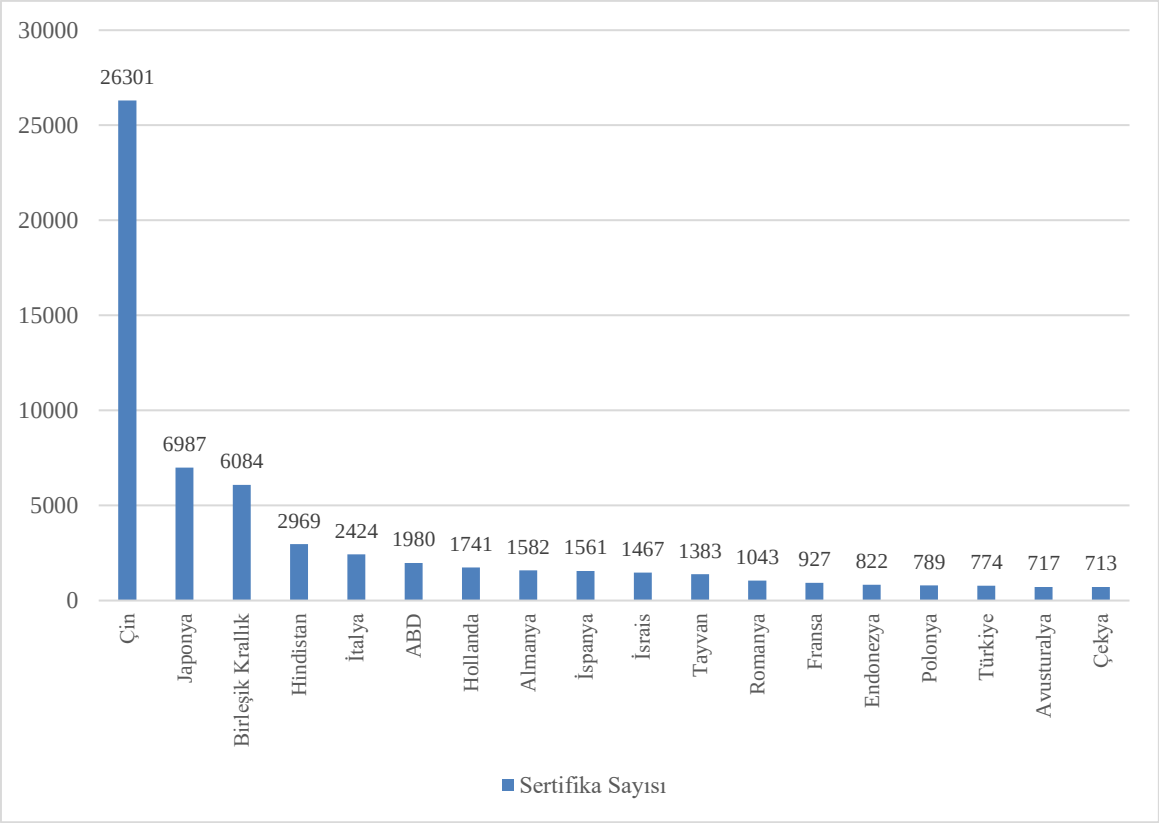
ISO 27000 standart ailesi bilgi güvenliği konusunda uluslararası standartlardan oluşmaktadır. ISO 27001 BGYS standardı sertifikalandırılan temel yönetim sistemi standardıdır. Bunun dışında standart ailesi içerisinde bulunan belirli başlı standartlar Çizelge 3.4'te açıklanmıştır.

Çizelge 3.4. ISO 27001 standart ailesinde bulunan belirli standartların açıklamaları

Standart No	Açıklama
ISO 27002	ISO 27002, siber güvenliğe odaklanan bir Bilgi Güvenliği Yönetim Sistemi kurmayı, uygulamayı ve geliştirmeyi hedefleyen kuruluşlara rehberlik sağlayan uluslararası bir standarttır. ISO/IEC 27001, bir BGYS için gereksinimleri belirlerken, ISO/IEC 27002, erişim kontrolü, kriptografi, insan kaynakları güvenliği ve olay müdahalesi gibi temel siber güvenlik yönleriyle ilgili en iyi uygulamaları ve kontrol hedeflerini içerir [79].
ISO 27004	ISO 27004 standardı, kuruluşlara bilgi güvenliği performansı ile BGYS'nin etkinliğinin değerlendirmesinde yardım sağlamak amacıyla ISO 27001'in 9.1 maddesi gerekliliklerine uygun rehberlik sunar [80].
ISO 27006	ISO 27006 bilgi yönetim sisteminin denetimini ve sertifikasyonunu gerçekleştiren kurum/kuruluşlar için gereksinimler ve rehberlik esaslarını içerir [81].
ISO 27011	ISO 27011 telekomünikasyon kuruluşlarında bilgi güvenliği kontrollerinin uygulanmasını destekleyen kılavuzları tanımlamaktadır [82].
ISO 27013	ISO/IEC 27001 ve ISO/IEC 20000-1'in entegre uygulanması konusunda rehber esaslarını içerir [83].

3.4.5. Küresel olarak ISO 27001 BGYS sertifikasyonu sayıları

International Standart Organization (ISO), yayınladığı standartlara göre sertifikalandırılan kuruluşların istatistiki bilgilerini internet sitesi aracılığı ile sunmaktadır. 2022 yılı için yayınlanan verilere göre, farklı ülkelerde ISO 27001 sertifika sayıları Şekil 3.4'de bulunmaktadır [5].



Şekil 3.4. Dünyadaki ISO 27001 sertifikası alan kuruluş sayıları [5]

Şekil 3.4'te görüldüğü gibi sertifikalandırılmış kuruluş sayısında ilk üç sırada Çin, Japonya ve Birleşik Krallık bulunmakta olup, Türkiye 774 sertifikalandırılmış kuruluş ile tüm dünyada sertifikası bulunan 151 ülke içerisinde 16. Sırada bulunmaktadır. Türkiye'de sertifikalandırılan kuruluşların büyük bir kısmının Türkiye'de yayınlı regülasyonlardan ötürü olduğu değerlendirilmektedir.

3.4.6. ISO 27001 BGYS standardı ile ilgili Türkiye'deki regülasyonlar

Türkiye'de kuruluşların ISO 27001 standardına göre sertifikalandırılmasını zorunlu tutan birçok regülasyon yayınlanmıştır. Konu ile ilgili örnek olarak aşağıdaki regülatif düzenlemeler bulunmaktadır.

Bilgi Teknolojileri Kurumu

Bilgi Teknolojileri Kurumu tarafından hazırlanan Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği'nde, "MADDE 36 – (1) İşletmeci, yetkilendirmesine ilişkin tüm hizmetleri ve kritik sistemleri kapsayacak şekilde kurduğu BGYS için belgelendirme

kuruluşlarından uygunluk belgesi alır ve Kuruma gönderir" hükmü bulunmaktadır [84]. Bu regülasyon çerçevesinde elektronik haberleşme sektöründe çalışan kuruluşların BGYS'yi kurması ve belgelendirilmesi beklenmektedir.

Enerji Piyasası Denetleme Kurulu

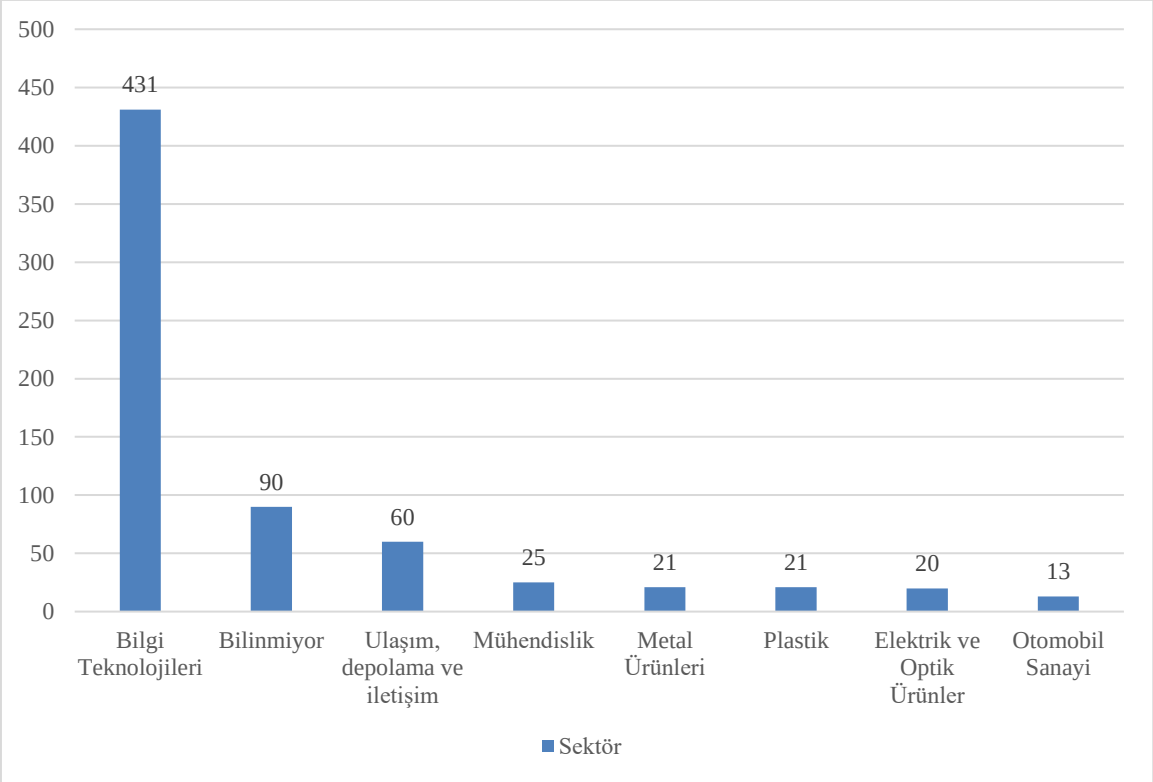
Enerji Piyasası Denetleme Kurulu tarafından hazırlanan Elektrik Piyasası Lisans Yönetmeliği'nde, "MADDE 30 – (2)– f) Geçici kabul tarihinden itibaren yirmi dört ay içerisinde OSB üretim lisansı sahipleri hariç olmak üzere, işletmeye geçmiş kurulu gücü 100 MWe ve üzerinde olan bütün üretim tesisleri için kurumsal bilişim sistemi ile endüstriyel kontrol sistemlerini TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardına uygun bir şekilde işletmek, TS ISO/IEC 27001 standardına uygun faaliyet gösterdiğini Türk Akreditasyon Kurumuna akredite olmuş bir belgelendirme kurumuna ispat ederek sistemlerini belgelendirmek ve söz konusu belgelerin geçerliliğini sağlamak, TS ISO/IEC 27001'e göre kuracakları Bilgi Güvenliği Yönetim Sistemi'nde TS ISO/IEC 27002 Uygulama Rehberine ek olarak ISO/IEC TR 27019 rehber dokümanını da referans almak" esası bulunmaktadır [85]. Bu regülasyon çerçevesinde belirli büyüklüğün üzerinden tüm enerji üretim tesislerinin BGYS kurması ve belgelendirilmesi istenmektedir.

Ulaştırma ve Altyapı Bakanlığı

Ulaştırma ve Altyapı Bakanlığı tarafından hazırlanan Kamunet Ağına Bağlanma ve Kamunet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliği'nde, "MADDE 4 – (1)– b) Kurmuş olduğu BGYS için, TS ISO/IEC 27001 veya ISO/IEC 27001 standardına göre belgesini alır ve güncelliğini sağlar. Bu belgeleri, TS ISO/IEC 27001 veya ISO/IEC 27001 standardı kapsamında Türk Akreditasyon Kurumu tarafından akredite edilen belgelendirme kuruluşları veya Uluslararası Akreditasyon Forumu Karşılıklı Tanınma Antlaşmasında yer alan ulusal akreditasyon kurumlarınca akredite edilmiş belgelendirme kuruluşlarından temin eder " [86] hükmü bulunmaktadır. Bu regülasyon çerçevesinde Kamunet ağına bağlanacak tüm kuruluşların BGYS kurması ve belgelendirilmesi istenmektedir.

3.4.7. Türkiye'deki ISO 27001 BGYS sertifikası sayıları

2022 yılı için yayınlanan verilere göre Türkiye'de ISO 27001 sertifika almış kuruluşların sektör dağılımı Şekil 3.5'de bulunmaktadır [5].



Şekil 3.5. Türkiye'deki ISO 27001 sertifikası bulunan kuruluşların sektör dağılımı [5]

Şekil 3.5'de görüldüğü üzere Türkiye'de sertifikalandırılmış kuruluşların sektör dağılımında bilinen sektörler içerisinde bilgi teknolojileri, ulaşım, depolama ve iletişim sektörlerinin en fazla sertifikaya sahip olduğu görülmektedir. Türkiye'deki ISO 27001 sertifika sayısı ve sektör dağılımının bu çalışmada da bahsedilen regülatif zorunluluklar nedeni ile olduğu değerlendirilmektedir.

3.5. Bilgi Güvenliği Denetimine Dair Rehber ve Standartlar

Bilgi güvenliği denetimi için genel denetim süreçlerinde kullanılan veya özel olarak hazırlanmış farklı standart, esas, kılavuz veya rehberler bulunmaktadır. Bu bölümde söz konusu dokümanlardan başlıca kullanılanlar hakkında bilgi sunulmaktadır. ISO 27001 BGYS standardının kendi içinde bulunan, iç tetkik ve uygunsuzluk ile düzeltici faaliyet bölümlerinde

BGYS tetkikine dair uyulması zorunlu olan esaslar tanımlanmıştır. ISO 19011 Yönetim Sistemleri Tetkik Kılavuzu standardında ise tüm yönetim sistemleri tetkiklerinde kullanılabilecek uyulması fayda sağlayan hususlar bulunmaktadır. Uluslararası İç Denetim Enstitüsü tarafından yayınlanan iç denetim standartları ise tüm denetimlerde iç denetçiler tarafından uyulması zorunlu olan esasları içermekte olup; bilgi güvenliği iç tetkikçileri için kılavuz esasları barındırmaktadır. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayınlan Bilgi ve İletişim Güvenliği Denetim Rehberi ise 2020 yılında aynı kurum tarafından ülkemizdeki bilgi güvenliğinin artırılması amacıyla yayınlanmış bulunan Bilgi ve İletişim Güvenliği Rehberi çerçevesinde gerçekleştirilen çalışmaların denetim sürecinde uyulması gereken esasları içermektedir.

3.5.1. ISO 27001 BGYS standardı denetim bölümleri

ISO 27001 BGYS standardı içerisinde iç tetkik sürecinde uyulması gerekenler ile ilgili "9.2 İç Tetkik" bölümü bulunmaktadır. Bu çalışmanın amacına uygun olarak belirlenen konu kategorileri standardın içeriğinde yer almaktadır.

ISO 27001 standardının "9.2 İç Tetkik" maddesine göre; yönetim sistemine uyum sağlamak isteyen kuruluşların planlanan aralıklarda iç tetkik gerçekleştirmesi gerekmektedir. Bu iç tetkiklerde kuruluşun ve standardın BGYS ile ilgili şartlarına uyumun, etkin bir şekilde uygulanmakta olduğunun denetlenmesi beklenmektedir. Denetim sıklığı, yöntemler, sorumluluklar ve raporlama gibi konuları içeren bir denetim programının hazırlanması ve uygulanması istenmektedir. Bu programın, kuruluşun ilgili süreçlerinin önemi ve daha önce yapılan denetimlerin sonuçlarını göz önünde bulundurarak hazırlanması gerekmektedir. Tüm denetimler için kriterlerin ve kapsamın tanımlanması, denetimlerin tarafsızlık ve objektiflik sağlanacak şekilde yürütülmesi, denetim sonuçlarının uygun yönetim kademesine raporlanması, denetim programı ve sonuçlarının muhafaza edilmesi beklenmektedir [78].

Tespit edilen uygunsuzluklar ile ilgili ilgili süreç ve uyulması gereken esaslar, ISO 27001 BGYS standardının "10.2 Uygunsuzluk ve Düzeltici Faaliyet" maddesinde tanımlıdır.

Standardın "10.2 Uygunsuzluk ve Düzeltici Faaliyet" maddesine göre yönetim sistemine uyum sağlamak isteyen kuruluşların; bir uygunsuzluk oluştuğunda, uygunsuzluğu tespit etmesi, düzeltilmesi için harekete geçmesi ve uygunsuzluğun sonuçlarıyla ilgilenmesi

beklenmektedir. Uygunsuzluğun tekrarlaması veya başka bir yerde meydana gelmemesi için gözden geçirme, nedenlerini belirleme ve benzer uygunsuzlukların var veya olası olmasının değerlendirmesi istenmektedir. Uygunsuzluklarla ilgili tüm gereken faaliyetlerin gerçekleştirilmesi, düzeltici faaliyetlerin etkinliğinin değerlendirilmesi ve gerektiğinde Bilgi Güvenliği Yönetim Sistemi'nde değişiklikler yapılması gerekmektedir. Ayrıca, uygunsuzluk ve düzeltici faaliyet ile ilgili bilgilerin muhafaza edilmesi beklenmektedir [78].

BGYS ile ilgili çalışan kişilerin yetkinliklerinin belirlenmesi ve yönetilmesi ilgili süreç ve uyulması gereken esaslar, BGYS standardının "7.2 Yetkinlik" maddesinde tanımlıdır.

Standardın "7.2 Yetkinlik" maddesine göre bilgi güvenliği performansını etkileyen kişi/kişilerin gerekli yetkinliklerinin belirlenmesi beklenmektedir. Bu kişilerin uygun öğretim, eğitim ve deneyim temelinde yetkin olmalarının sağlanması istenmektedir. Gerekli yeterliliğin sağlanması için tedbirler alınmalı ve bu tedbirlerin etkinliği değerlendirilmesi beklenmektedir. Ayrıca, yeterliliğin kanıtı olan bilgilerin muhafaza edilmesi istenmektedir [78].

Yukarıda alıntı yapılan ISO 27001 standardı maddelerinin açıklamaları ve bu çalışmada değerlendirme başlıkları olarak belirlenen konu kategorileri Çizelge 3.5'de bulunmaktadır.

Çizelge 3.5. ISO 27001 standardı denetim maddeleri açıklaması

ISO 27001 Standardı Madde No:	Açıklama	Konu Kategorisi
9.2.1. a)	Denetlenmesi istenen şartlar listelenmiştir. Standartta bulunan tüm maddelerin ve kuruluş şartlarının denetlenmesi beklenmektedir.	Denetim Planlaması ve kriterler
9.2.1. b)	Denetimlerin etkin bir şekilde uygulanması ve sürdürülmesi beklenmektedir.	Genel
9.2.2	Süreçlerin önemi değerlendirilerek denetim programlarının planlanması beklenmektedir. Tetkik ile ilgili kayıtların muhafaza edilmesi beklenmektedir.	Denetim Planlaması ve kriterler
9.2.2. a)	Denetim kriterlerinin (denetim sorularının/kontrollerinin) ve denetim kapsamının belirlenmesi beklenmektedir.	Denetim Planlaması ve kriterler
9.2.2 b)	Tetkik sürecinin tarafsızlığı ve objektifliğini sağlayacak şekilde tetkiklerin yürütülmesi beklenmektedir.	Objektiflik ve Bağımsızlık
9.2.2. c)	Tetkik sonuçlarının uygun yönetim kademelerine raporlanması beklenmektedir.	Denetim Raporlama
10.2.a	Uygunsuzluğun öncelikli olarak düzeltmesi için faaliyetler beklenmektedir.	İyileştirme ve Bulgular
10.2.b	Uygunsuzluğun kök sebebinin tespit edilerek benzerlerinin tekrar yaşanmaması için faaliyetler beklenmektedir.	İyileştirme ve Bulgular
10.2.c	Uygunsuzluk ile ilgili gerekli tüm çalışmaların gerçekleştirilmesi beklenmektedir.	İyileştirme ve Bulgular
10.2.d	Uygunsuzluk kapsamında gerçekleştirilen faaliyetlerin etkinliğinin gözden geçirilmesi beklenmektedir.	İyileştirme ve Bulgular
10.2.e	BGYS'de uygunsuzluk ile ilgili gerekli tüm değişikliklerin gerçekleştirilmesi beklenmektedir.	İyileştirme ve Bulgular
7.2.a	Bilgi güvenliği performansını etkileyen kişi/kişilerin gerekli yetkinliklerinin belirlenmesi beklenmektedir.	Sürekli Gelişim ve Yetkinlik
7.2.b	Bilgi güvenliği performansını etkileyen kişi/kişilerin belirlenen yetkinliklerde olmasının sağlanması beklenmektedir.	Sürekli Gelişim ve Yetkinlik

Çizelge 3.5'de görüldüğü üzere gerçekleştirilen denetimlerde; standart maddelerine uyumun kontrol edilmesi, riskli alanlara göre denetimlerin planlanması, denetim kapsamının belirlenerek tarafsızlığı/objektifliği sağlayacak şekilde denetimlerin yürütülmesi ve kayıt altına alınması, sonuçların yönetim kademelerine raporlanması, uygunsuzluklarla ilgili kök sebebi giderecek faaliyetler gerçekleştirilerek etkinliklerinin ölçülmesi ve tetkikçiler dahil BGYS'de görev alan personelin yetkinliğinin belirlenerek, sağlanması beklenmektedir.

3.5.2. ISO 19011 yönetim sistemleri tetkik klavuzu standardı

ISO 19011 Yönetim Sistemleri Tetkik Klavuzu Standardı tetkik süreci ile ilgili uyulması önerilen hususları içermektedir. Söz konusu standardın içerisinde, bu çalışmada değerlendirilen konu kategorileri ile ilgili aşağıdaki hususlar bulunmaktadır.

Objektiflik ve bağımsızlık

ISO 19011 Yönetim Sistemleri Tetkik Klavuzu Standardına göre; tetkikçilerin uygulanabilir olduğu yerlerde incelenen faaliyetten bağımsız olmaları ve her zaman tarafsız ve çıkar çatışmasından uzak bir şekilde hareket etmeleri gerekmektedir. İç tetkiklerde, tetkikçilerin, incelenen fonksiyonu yöneten kişilerden bağımsız olmaları gerekmektedir. Tetkikçilerden, tetkik bulgularının ve sonuçlarının sadece tetkik delillerine dayandığından emin olmaları ve süreç boyunca tarafsızlıklarını korumaları istenmektedir. Küçük işletmelerde, iç tetkikçilerin incelenen faaliyetten tamamen bağımsız olmaları zor olabileceği belirtilerek; her türlü çaba gösterilerek yanlılığın önlenmesi ve objektifliğin sağlanması beklenmektedir [87].

Denetim raporlama

Standardın 6.5.1 maddesine göre tetkik ekibi liderinden, tetkik sonuçlarını tetkik programı prosedürlerine uygun olarak rapor etmesi beklenmektedir. Tetkik raporu; tetkikin tam, doğru, öz ve açık bir kaydını sunması istenmektedir. Tetkik raporunda, tetkik hedefleri, kapsamı, incelenen süreçler veya fonksiyonel birimlerin detaylı tanımı, ekibin ve incelenen katılımcıların tanımlanması, tetkik faaliyetlerinin gerçekleştirildiği tarihler ve yerler, tetkik kriterleri, bulgular ve ilgili kanıtlar, sonuçlar ve tetkik kriterlerinin ne ölçüde yerine getirildiğinin bulunulması gerekmektedir. Standardın 6.5.2 maddesine göre tetkik raporunun üzerinde anlaşılan bir zaman dilimi içinde yayımlanması gerekmektedir [87].

Tetkikçi yetkinliği ve sürekli gelişimi

Standardın 7.6 maddesine göre tetkikçiler ve tetkik ekip liderleri sürekli olarak yeterliliklerini geliştirmesi beklenmektedir. Tetkikçiler yönetim sistemi tetkiklerine düzenli katılım sağlayarak ve sürekli mesleki gelişim ile tetkik yeterliliklerinin sürekliliğini sağlaması istenmektedir. Sürekli mesleki gelişimin; yeterliliğin geliştirilmesini ve bunun devamlı olmasını içerdiği; ilave iş deneyimi, eğitim, özel çalışmalar, eğitmenlik, toplantılara, seminerlere ve konferanslara veya diğer ilgili faaliyetlere katılım gibi yollar ile elde edilebileceği belirtilmektedir [87].

Standardın 7.1 maddesine göre; tetkik sürecine olan güven ve hedeflere ulaşma yeteneği; tetkikçiler ve tetkik ekibi liderleri dahil tetkiklerde görev alan kişilerin yeterliliğine bağlı olduğu belirtilmektedir. Yeterlilik, kişisel davranışlar, tecrübe, eğitim ve deneyim gibi faktörleri dikkate alan bir süreçle değerlendirilmesi istenmektedir. Bu sürecin, tetkik programının ve hedeflerinin gereksinimlerini karşılaması gerektiği vurgulanmaktadır. Standardın 7.2.3 maddesine göre; her bir tetkikçinin aynı düzeyde yeterliliğe sahip olmasının zorunlu olmadığı, ancak tetkik ekibinin toplam yeterliliğinin tetkik hedeflerini başarmak için yeterli olması gerektiği belirtilmektedir. Tetkikçilerden, belirli yönetim sistemi ve sektör tipine uygun mesleki ve sektöre özel bilgi ve becerilere sahip olması beklenmektedir [87].

Denetim planlama

Standardın 5.1 maddesine göre; tetkik edilen kuruluşun yönetim sisteminin etkinliğini belirlemeye katkı sağlayacak bir tetkik planı/programı oluşturması gerekmektedir. Bu programın/planın, ayrı veya birleşik olarak yönetilen birden fazla yönetim sistemi standardını içerebileceği belirtilmektedir. Üst yönetimin, tetkik programı hedeflerini belirlemesi ve bir veya daha fazla yeterlilik sahibi kişiyi tetkik programını yönetmek üzere ataması istenmektedir. Tetkik programının kapsamının, kuruluşun büyüklüğü, niteliği, karmaşıklığı ve yönetim sisteminin olgunluk seviyesine göre belirlenmesi gerekmektedir. Kaynakların dağıtımında öncelik, yönetim sistemi içindeki önemli konulara verilmesi; bu konuların, ürün/hizmet kalitesindeki önemli özellikler, sağlık ve güvenlikle ilgili tehditleri veya çevresel konuları ve bunların kontrolünü içerebileceği belirtilmektedir [87].

Denetim kriterleri

Standardın 5.4.2 maddesine göre her tetkik; belgelenmiş, tetkik hedeflerine, kapsama ve kriterlere dayandırılması gerekmektedir. Bu kriter ve hedeflerin tetkik programını yöneten kişi tarafından tanımlanması ve genel tetkik programı hedeflerine uygun olması istenmektedir [87].

Denetim sonrası uygunsuzluklarla ilgili faaliyetler

Standardın 6.7 maddesine göre tetkik hedeflerine bağlı olarak tetkikin sonuçları; düzeltmeler için, düzeltici faaliyetler için veya iyileştirme faaliyetleri için ihtiyaçları göstermesi beklenmektedir. Bu faaliyetlerin tamamlanması ve etkinliğinin doğrulanması gerekmektedir. Bu doğrulama işlemi, bir sonraki tetkikin bir kısmını teşkil edebileceği belirtilmektedir [87].

Yukardaki standart maddelerinden anlaşılacağı üzere ISO 19011 standart maddelerine göre denetimlerde objektiflik ve bağımsızlığın sağlanması, belirlenen içerikleri barındıran raporların üretilmesi, tetkikçi yeterliliğinin sağlanması, önemli konuların denetim planlamasına dahil edilmesi, denetim sonrası bulgular ile ilgili faaliyetlerin etkinliğinin doğrulanması beklenmektedir.

3.5.3. Uluslararası iç denetim standartları

Uluslararası İç Denetim Enstitüsü tarafından "Mesleki Uygulama Çerçevesi Kapsamında Uluslararası İç Denetim Standartları" yayınlanmıştır. İç denetim birimlerinin bu standartlara uyması zorunludur. Ancak; bu standartların BGYS iç tetkiklerinde uygulanması zorunlu olmasa da tetkikler için iyi uygulama açısından kılavuzluk etmektedir. Bu standartların amaçları iç denetim birimleri için aşağıdaki şekilde tanımlanmıştır.

1. Uluslararası Mesleki Uygulama Çerçevesi'nin zorunlu unsurları ile uyuma kılavuzluk etmek.
2. Geniş bir yelpazedeki katma değerli iç denetim hizmetlerini teşvik etmeye ve hayata geçirmeye yönelik bir çerçeve sağlamak.
3. İç denetim performansının değerlendirilmesine uygun bir zemin oluşturmak.
4. Gelişmiş kurumsal süreç ve faaliyetleri teşvik etmek [88].

ISO 27001 BGYS içerisinde bulunan denetim esasları ile uyumlu iç denetim standartlarında bu çalışmada değerlendirilen konu kategorileri ile ilgili aşağıdaki hususlar bulunmaktadır.

Objektiflik ve bağımsızlık

“1100 - Bağımsızlık ve Objektiflik: İç denetim faaliyeti bağımsız olmak zorundadır ve iç denetçiler görevlerini yaparken objektif davranmak zorundadır” [88]. İç denetim gerçekleştiren personelin görevi, görev yaptığı birimi ve yöneticileri açısından değerlendirildiğinde bağımsız ve objektif olması beklenmektedir.

Tetkikçi sürekli gelişimi ve yetkinliği

“1200 - Yeterlilik ve Azami Mesleki Özen ve Dikkat: Görevler, yeterlilik ve azami mesleki özen ve dikkat ile yerine getirilmek zorundadır” [88]. İç denetim gerçekleştiren personelin gerekli olan özelliklere sahip olması beklenmektedir. Denetim sürecindeki çalışmalarında azami özen ve dikkatle çalışmalarını gerçekleştirmesi istenmektedir. “1230 - Sürekli Mesleki Gelişim: İç denetçiler, mevcut bilgi, beceri ve diğer vasıflarını sürekli mesleki gelişimle artırmak ve güçlendirmek zorundadır” [88]. İç denetim gerçekleştiren personelin sürekli mesleki gelişim kapsamında periyodik eğitimler gibi yollar ile yetkinliğini artırması beklenmektedir.

Denetim planlaması

“2010 - Planlama: İç Denetim Yöneticisi, kurumun hedeflerine uygun olarak, iç denetim faaliyetinin önceliklerini belirleyen bir risk esaslı plan yapmak zorundadır” [88]. İç denetim plan ve programlarının risk esaslı olarak oluşturulması, riski yüksek alan/süreçlerin denetim kapsamına alınması beklenmektedir.

Denetim raporlaması

“2400 - Sonuçların Raporlanması: İç denetçiler, görev sonuçlarını raporlamak zorundadır. 2440 - Sonuçların Dağıtımı: İç Denetim Yöneticisi, görev sonuçlarını uygun taraflara dağıtmak zorundadır” [88]. Denetim sonuçlarının raporlanması ve uygun taraflara bildirilmesi beklenmektedir.

Anlaşılacağı üzere Uluslararası İç Denetim Standartları maddelerine göre denetimlerde objektiflik ve bağımsızlığın sağlanması, denetim sonuçlarının raporlanması, denetçilerin gerekli bilgi/becerilere sahip olması ve sürekli gelişimlerinin sağlanması, risk esaslı denetim planlarının oluşturulması beklenmektedir.

3.5.4. Bilgi ve iletişim güvenliği rehberi

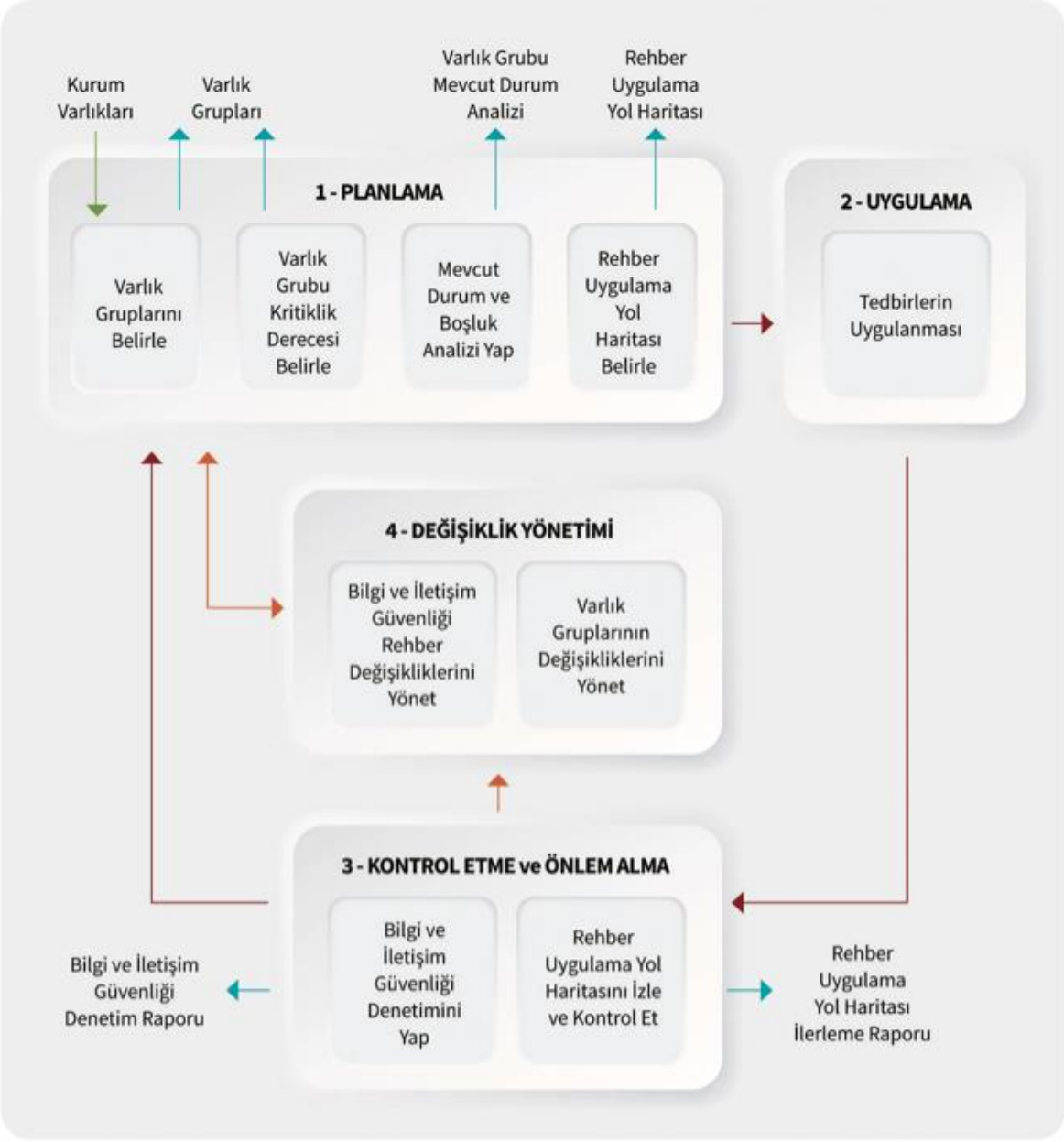
Cumhurbaşkanlığı tarafından 5 Temmuz 2019 tarihinde yayımlanan "Bilgi ve İletişim Güvenliği Tedbirleri" konulu genelge doğrultusunda Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) koordinasyonunda kritik altyapı hizmetleri sunan tüm kamu kurum ve işletmelerinde uygulanacak Bilgi ve İletişim Güvenliği Rehberi'nin yayınlanacağı belirtilmiştir. Genelgede, bilgi ve iletişim güvenliği önlemleri ile ilgili 21 genel önlemin ana hatları çizilerek; yayınlanacak rehbere bilgi teknolojisi altyapılarının, güvenlik düzeylerine göre, belirtilen planın bir parçası olarak aşamalı şekilde uyum sağlayacağı vurgulanmaktadır. Kuruluşların rehbere uyumu sağlamak için izleme mekanizmaları kuracakları ve yıllık bazda denetleyecekleri belirtilmektedir [89].

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı (CBDDO) koordinasyonunda Bilgi ve İletişim Güvenliği Rehberi hazırlanmış; 24 Temmuz 2020 tarihinde yayınlanmıştır. Bu rehber ile kamu kuruluşlarının ve kritik altyapı hizmeti sunan şirketlerin bilgi ve iletişim güvenliği konularında uygulaması gereken tedbirlerin belirlenmesi amaçlanmaktadır. Bilgi ve İletişim Güvenliği Rehberi'nin yayım tarihinden itibaren 24 aylık süre içerisinde ilgili kurum ve kuruluşlardan uyum beklenmiş olup, 27 Temmuz 2022 tarihi itibari ile uyum çalışmaları için belirlenen süre tamamlanmıştır.

Ağdeniz (2021) çalışmasında bilgi teknolojileri yönetiminde ISO 27000, COBIT gibi birçok farklı çerçevenin bulunduğu ve uygulanmakta olduğu, BT denetiminin risklerin yönetiminde kuruluş yönetimlerine güvence sağlayarak önem arz ettiğini belirtmiştir. Dijital Türkiye için önemli konulardan biri olarak Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin kurulduğunu ve bu ofis tarafından 2020 yılında Bilgi ve İletişim Güvenliği Rehberi'nin yayınlanmasıyla bilgi teknolojileri risklerini yönetmek ve denetlemek için yeni bir dönemin başladığını vurgulamıştır [90]. Tulgar, Zaim ve Aydın (2022) çalışmalarında; Bilgi ve İletişim Güvenliği Rehberi'nin farklı ve teknik konularda çok sayıda tedbiri içerdiği, bilgi

teknolojilerindeki farklı alanlara dokunduğu, tedbirlerinin teknoloji ve ürünlerden bağımsız olduğu, kolektif çalışmalar ile hazırlanması, mevzuat ve standartlarla uyum içinde olması gibi özellikleri ile güçlü bir içeriğe sahip olduğunu belirtmişlerdir [91].

Bilgi ve İletişim Güvenliği Rehberi uygulama süreci Şekil 3.6'da görülmektedir.



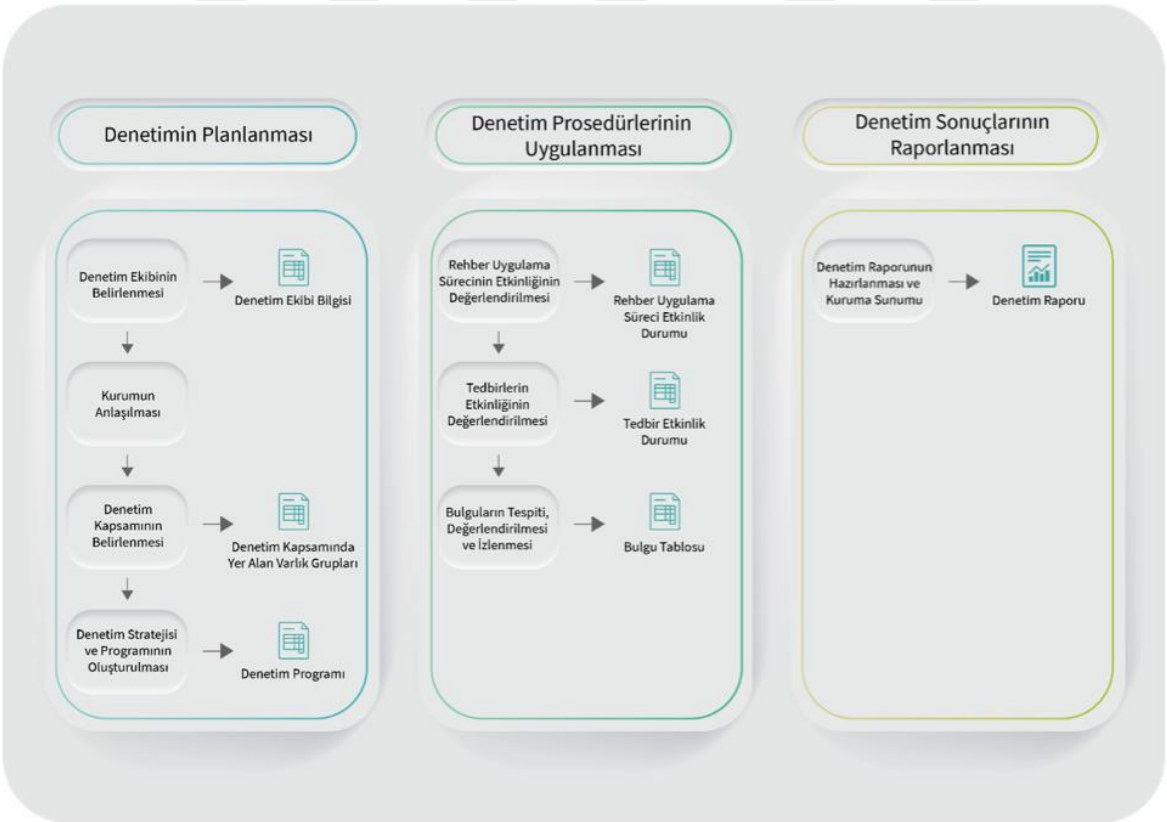
Şekil 3.6. Bilgi ve İletişim Güvenliği Rehberi uygulama süreci [92]

Şekil 3.6'da görüldüğü üzere Bilgi ve İletişim Güvenliği Rehberi uygulanması sürecinde varlık grupları belirlenmeli, varlık envanterindeki varlıklar bu varlık grubu altında tanımlanmalıdır. Daha sonra belirlenen varlık gruplarının kritiklik derecesi belirlenmeli,

kritik derecesi özelinde rehberde yer alan tedbirlere göre mevcut durum ve boşluk analizi çalışması yapılmalıdır. Bu aşamadan sonra, mevcut durum ve boşluk analizinde belirlenen uygulanmayan tedbirler için yol haritası belirlenmesi ve ilgili tedbirlerin uygulanması beklenmektedir. Kontrol et ve önlem al aşamasında; hazırlanan bu yol haritasının kontrol edilmesi ve rehber denetimlerinin gerçekleştirilmesi gerekmektedir.

3.5.5. Bilgi ve iletişim güvenliği denetim rehberi

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı (CBDDO) koordinasyonunda Bilgi ve İletişim Güvenliği Rehberinin denetiminin belirli bir metodolojide gerçekleştirilmesi amacıyla Bilgi ve İletişim Güvenliği Denetimi Rehberi hazırlanmış ve 10 Ekim 2021 tarihinde yayınlanmıştır. Denetim rehberine göre; denetimlerin her yıl için kuruluşların iç denetim birimlerinde görevli bilgi teknolojileri alanında denetimlerde görevlendirilebilecek nitelikte iç denetçiler tarafından gerçekleştirilmesi beklenmektedir. Bilgi ve İletişim Güvenliği Denetim Rehberi'ne göre denetim süreci Şekil 3.7'de görülmektedir.



Şekil 3.7. Bilgi ve İletişim Güvenliği Denetim Rehberi denetim ana ve alt süreçleri [93]

Şekil 3.7'da görüldüğü üzere Bilgi ve İletişim Güvenliği Rehberi denetimlerinin üç bölüme ayrıldığı görülmektedir. Denetim planlaması bölümü; denetim ekibinin belirlenmesi, denetim kapsamının belirlenmesi ve denetim programının oluşturulmasını içermektedir. Denetim prosedürlerinin uygulanması bölümünde; rehber uygulama ve tedbir uygulama süreçlerinin etkinliğinin değerlendirilmesi ve bulgu süreci bulunmaktadır. Denetim sonuçlarının raporlanması bölümünde ise; denetim raporunun hazırlanması ve Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'ne sunulması ile ilgili esaslar bulunmaktadır.

Bu çalışmada değerlendirilen konu kategorileri ile ilgili Bilgi ve İletişim Güvenliği Denetim Rehberi ve Bilgi ve İletişim Güvenliği Rehberi içerisinde aşağıdaki esaslar bulunmaktadır.

Objektiflik ve bağımsızlık

EK – J: Tarafsızlık Taahhütnamesi örneği içerisinde aşağıdaki şekilde denetçilerin imzalaması gereken taahhüt maddeleri bulunmaktadır.

> a) Bilgi ve İletişim Güvenliği Rehberi uyum çalışmalarını yürüten bilgi işlem biriminde görev almadığımı,
> b) Denetim kapsamında yer alan birimlerde birinci, ikinci ve üçüncü derece kan ve sıhri hısımım olan veya maddi/manevi menfaat ilişkimin bulunduğu herhangi bir kişinin bulunmadığını,
> c) Denetim başlangıç / denetim işi hizmet alım sözleşmesi tarihinden önceki iki yıl içerisinde kuruma Bilgi ve İletişim Güvenliği Rehberi uyum faaliyetleri konusunda danışmanlık hizmeti vermediğimi [93].

Denetimlerin raporlaması

> Denetim ekibi, denetim görüşünü oluşturmaya yönelik herhangi bir kısıt veya engel ile karşılaşmadığı durumda denetim raporunu aşağıda başlıkları içerecek şekilde hazırlamalıdır.
> a) Rapor Kapağı, b) Yönetici Özeti, c) İçindekiler, ç)Tanımlar ve Kısaltmalar, d) Giriş, e) Denetim Kapsamına İlişkin Bilgi, f) Denetim Görüşü, g) Ekler
>
> Bahse konu hüküm uyarınca denetim raporunun aşağıda yer verilen bölümleri denetim raporunun oluşturulma tarihinden itibaren en geç iki aylık süre içinde DDO'nun tesis edeceği sisteme, 5070 sayılı Elektronik İmza Kanunu hükümlerine göre oluşturulan güvenli elektronik imza ile Üst Yönetici veya Üst Yöneticinin yetkilendirdiği personel tarafından imzalanarak DDO'ya iletilir [93].

Tetkikçi sürekli gelişimi ve yetkinliği

3.1.1. b)Denetim ekibi kurum iç denetçisi, kurum içi personel veya diğer kamu kurum ve kuruluşlarından görevlendirilecek personelden oluşuyor ise; Personel aşağıda yer verilen yetkinliklerin en az birini sağlamalıdır.
-ISO/IEC 27001 Başdenetçi sertifikasına sahip olmak,
-CISA sertifikasına sahip olmak,
-Belgelendirme Programı kapsamında yetkilendirilmiş denetçi veya başdenetçi olmak.
d) Denetim çalışmalarında, denetim ekibindeki denetçilere ilave olarak özel uzmanlık veya ihtisas gerektiren alanlarda tecrübesinden faydalanılmak üzere uzman personel görevlendirilebilir. Denetim ekibinde uzman yer alması durumunda, uzmanın yapacağı çalışmalar denetçi refakatinde gerçekleştirilmelidir. Uzmanın; hangi varlık grupları, tedbirler ya da süreçler üzerinde çalışma yapacağı, çalışmaların denetçiye nasıl raporlanacağı denetçiler tarafından belirlenmelidir [93].

Denetim planlaması

3.1.3 Denetim ekibi, yapacağı risk değerlendirmesi çerçevesinde kapsamı belirlerken Rehber uyum çalışmalarıyla tanımlanan varlık grubu ana başlıkları ile ilişkili en az bir varlık grubunu kapsama dâhil etmelidir. Risk değerlendirme surecinde varlık grubunun gizliliği, bütünlüğü, erişilebilirliği ile etki alanları (bağımlı varlıklar, etkilenen kişi sayısı, kurumsal ve toplumsal sonuçlar, sektörel etki) dikkate alınmalıdır. Risk değerlendirmesinde; önceki yıl denetiminden bu yana bilgi sistemleri üzerindeki önemli değişiklikler, önceki yıl denetiminde kapsama dâhil edilen varlık grupları, elde edilen bulgular ve bulgulara yönelik gerçekleştirilen düzeltici ve önleyici faaliyetler de göz önünde bulundurulmalıdır [93].

Denetim sonrası uygunsuzluklarla ilgili faaliyetler

3.2.4 Denetim faaliyetini yürüten denetim ekibinin kurum içi personelden oluştuğu durumlarda denetim ekibi aracılığıyla; diğer kamu kurum ve kuruluşlarından geçici görevlendirme veya hizmet alım yolu ile oluştuğu durumlarda ise Kurum tarafından görevlendirilecek birim/personel aracılığıyla bulguların takibine yönelik izleme sistemi tanımlanmalı ve işletilmelidir. İzleme sistemi; elde edilen bulguların kök neden analizinin yapılması, kritiklik derecesi yüksek olan bulgular öncelikli olmak üzere bunları ortadan kaldırmaya veya kritiklik derecesini düşürmeye yönelik düzeltici veya önleyici faaliyetlerin belirlenmesi, aksiyon planlarının hazırlanması ve bunları gerçekleştirecek sorumlu birim/personelin belirlenmesine yönelik temel süreç ve faaliyetleri içermelidir [93].

Denetim kriterleri

Bilgi ve İletişim Güvenliği Denetim Rehberi'nde "bu süreçte denetim ekibi, Rehberde yer alan her varlık grubu ve tedbir maddesi için tanımlı denetim yöntemi ve denetim soru

önerilerinden faydalanabilir" esası bulunmaktadır [93].

Bilgi ve İletişim Güvenliği Rehberinde varlık gruplarına, sıkılaştırma faaliyetlerine, uygulama ve teknoloji alanlarına yönelik güvenlik tedbirleri başlıkları altında 661 tedbir maddesi bulunmaktadır. Bu tedbir maddelerinin denetimlerine dair denetim yöntem önerileri ve denetim soru önerileri rehber içerisinde belirtilmiştir. Bu denetim yöntem ve soru içerikleri denetim kriterleri açısından önemli bir girdi teşkil etmektedir. Örnek sunmak amacıyla Çizelge 3.6'da 661 tedbir maddesinden bir kaçı için örnek denetim soruları ve denetim yöntem önerileri bulunmaktadır.

Çizelge 3.6. Bilgi ve İletişim Güvenliği Rehberi örnek tedbir maddesi soruları ve denetim yöntemleri [92]

Tedbir No	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.1.7	Kurum Ağı Bağlantı Noktalarında Kimlik Denetimi Yapılması	Mülakat, Sızma Testi	Port seviyesinde erişim kontrolü yapılmakta mıdır? Kurum ağına bağlanan cihazlar için 802.1x veya NAC çözümleri kullanılarak kimlik denetimi yapılmakta mıdır?
3.1.1.9	Sabit Disk Güvenliği	Mülakat, Gözden Geçirme	Kurum tarafından temin edilen ve kullanıcı bilgisayarlarında kullanılması planlanan sabit diskleri sisteme dâhil etmek amacıyla bir süreç tanımlanmış ve uygulanmakta mıdır? Temin edilen sabit diskler, sisteme dâhil edilmeden önce hangi güvenli silme işlemlerine tabi tutulmaktadır?

Yukarıdaki rehber maddelerinden anlaşılacağı üzere Bilgi ve İletişim Güvenliği Rehberi ve Bilgi ve İletişim Güvenliği Denetim Rehberi içeriğinde bu çalışmada incelenen konu kategorileri ile ilgili detay esaslar bulunmaktadır.

4. ARAŞTIRMA YÖNTEMİ

4.1. Araştırma Modeli ve Süreci

Literatür araştırmasında, ISO 27001 standardının çeşitli alanlarda fayda sağladığını gösteren birçok çalışmanın mevcut olduğu görülmüştür. Bilgi Güvenliği Yönetim Sistemi (BGYS) denetim süreçlerinin önemi vurgulanmış ve yönetim sisteminin sürekli olarak etkin bir şekilde denetlenmesi gerektiği belirtilmiştir. Siber güvenlik üzerine yapılan araştırmalar ve uluslararası raporlar, siber güvenliğin en riskli konulardan biri olduğunu ve iç denetimlerin siber güvenliğin sağlanmasında önemli katkılar sunduğunu göstermektedir. Denetimlerin etkinliği için denetim kaynakları, denetçilerin teknik yetkinlikleri, bağımsızlıkları ve objektiflikleri gibi kriterler öne çıkarılarak gelecekteki araştırma konuları arasında yer alması gerektiği vurgulanmıştır.

Bu bağlamda, literatür araştırmasında ISO/IEC 27001 BGYS'nin kurulumu, risk yönetimi uygulamaları ve genel iç denetim süreçleri ile ilgili çok sayıda çalışmanın bulunduğu görülmüştür. Bu çalışmalar, denetim ve kontrol faaliyetlerinin önemine dikkat çekmekle birlikte, ISO/IEC 27001 denetim süreci, bu süreçte karşılaşılan zorluklar ve olası iyileştirmeler konusunda ülkemizde bir çalışma yapılmadığını ortaya koymaktadır.

Bu çalışma ISO 27001 BGYS iç denetimleri ile ilgili olması sebebiyle, ISO 27001 standardı içerisinde bulunan ve uyum gösterilmesi de zorunlu olan denetimlerle ilişkili içerik incelenmiştir. Standart içerisinden "9.2 İç tetkik (denetim)", "10.2 Uygunsuzluk ve düzeltici faaliyetler", "7.2 Yetkinlik" maddelerinden bu çalışma için değerlendirilmesi amaçlanan unsurlar konu kategorisi olarak belirlenmiştir. Bu konu kategorileri için soruları yanıtlayacak olan iç tetkikçilerin görüşlerinin alınmasını sağlayan ifadeler oluşturulmuştur. Hazırlanan bu soruların içeriği; öncelikle konusunda uzman ISO 27001 baş tetkikçi sertifikasına sahip uzman görüşü ile düzenlenmiş; anlaşılırlık, veri toplama için uygunluk gibi hususları kontrol etmek için deneme (pilot) çalışması yapılmıştır. Bunun için seçilen bir kurum/kuruluştan örnek kişiler ile görüşülmüştür. Pilot çalışma sonucunda alınan görüşler çerçevesinde bu çalışmada bulunan sorular son halini almıştır.

2022 yılı ISO verilerine göre ülkemizde 2022 yılında 774 adet sertifikalandırılmış

kurum/kuruluş bulunmaktadır [5]. Çok sayıda sertifikalandırılmış kuruluş bulunması sebebiyle örneklem yöntemiyle araştırma gerçekleştirilmiştir. Denetimlerde görev alan tetkikçiler özelinde gerçekleştirilen bu çalışma için sertifikalandırılmış her bir kurumda kaç adet tetkikçinin görevli olduğu verisi bilinememektedir. Örneklem seçimi ve örneklem boyutu seçimi ile incelenecek grup hakkında sonuçlara varmak için makul bir temel oluşturulmaya çalışılmış, istatistiki olmayan muhakemeye dayalı örneklem seçimi kullanılmıştır. Bu çalışma soruları ISO 27001 BGYS sertifikasına sahip kuruluşlar içerisinden rastgele seçilmiş 30 adet kamu ve 30 adet özel sektörden kuruluş ile bilişim sistemleri üzerinden "Google Forms" uygulaması aracılığıyla paylaşılmış ve BGYS kapsamında gerçekleştirilen iç tetkiklerle ilgili bilgi toplanmıştır. İç tetkikçilerin gizlilik endişeleri ve standartlara uyum gösterme zorunluluğu sebebiyle kısıtlı ve taraflı bilgi sunabilecek olmaları çalışmanın sınırlılıklarındandır. Bu sınırlılığın engellenebilmesi için anket çalışması yapılan personel ve kurum/şirketlerin ismi talep edilmemiş ve bu bilgi anket öncesi katılımcılara iletilmiştir. Bu nedenle soruların paylaşıldığı kurumlardan hangilerinden yanıt alındığı tespit edilememesi çalışmanın diğer bir sınırlılığı olarak bulunmaktadır.

Çalışma kapsamında ISO 27001 süreç ve kontrollerinin iç denetimini etkileyen faktörlerin tespit edilmesi için çalışmanın amacına uygun olarak belirlenen konu kategorilerini içeren 33 soruluk "ISO 27001 BGYS Denetimleri" isimli veri toplama anketi oluşturulmuştur. Anket soruları yanıtlarında 5 seçenekli ("Kesinlikle Katılmıyorum", "Katılmıyorum", "Kararsızım", "Katılıyorum", "Kesinlikle Katılıyorum") Likert Tipi ölçme aracı kullanılmıştır.

Anket ISO 27001 BGYS iç tetkiklerinde görev alan çalışanların katılımı ile gerçekleştirilmiştir. 5 genel bilgi sorusu 27 kapalı uçlu soruya yanıt alınmıştır. Anket içerisinde 1 adet eklemek istedikleriniz sorusu bulunmaktadır. Gazi Üniversitesi Etik Komisyonunun 30.10.2022 tarihli onayı sonrası, çevrimiçi olarak ilgili veriler toplanmıştır.

Anket soruları ISO 27001 standardı içerisinde bulunan denetimlerle ilişkili içerik içerisinden bu çalışmanın amacına uygun olarak belirlenmiş konu kategorileri çerçevesinde oluşturulmuştur. Bu çalışmanın 4.3. Araştırma Verisi Toplama Aracı bölümünde sorular, soruların ilgili olduğu konu kategorisi ve ilgili uluslararası standart maddeleri belirtilmiştir. Soruların açık, net, kısa ve anlaşılabilir olmasına dikkat edilmiştir.

4.2. İstatiksel Analiz

Ankete 103 kişi katılım göstermiştir. Veri toplama aracı olarak kullanılan ankete katılan 103 katılımcıdan 75 kişi kamu kurum/kuruluşlarında, 28 kişi ise özel sektörde çalışmaktadır. Katılımcılardan 13 kişi yönetici, 15 kişi iç denetçi/müfettiş ve 77 kişi çalışan pozisyonunda çalıştıklarını belirtmişlerdir. Anket katılımcıları bu pozisyonlarda çalışarak ISO 27001 iç tetkiklerinde görev aldıklarını beyan etmişlerdir. 79 katılımcı 251 ve üzeri çalışan sayısı bulunan kurum ve kuruluşlarda, 10 katılımcı 11-50 çalışan sayısı bulunan kurum ve kuruluşlarda, 9 katılımcı 51-250 çalışan sayısı bulunan kurum ve kuruluşlarda, 5 kişi ise 1-10 çalışan sayısı bulunan kurum ve kuruluşlarda çalışmaktadır.

Katılımcıların verdiği cevaplar analiz edilmiş ve analiz için IBM SPSS programının 29.0 versiyonu kullanılmıştır. Anket soruları gruplanmış ve konu kategorilerine göre genel (tüm katılımcılar), kamu kurumlarında görev alan iç tetkikçiler ve özel sektörde görev alan iç tetkikçiler için yanıtların ortalaması ve standart sapma değerleri özelinde istatiksel olarak analiz edilmiştir. ISO 27001 tetkik süreci ile ilgili sorularda 5'li Likert ölçeği kullanılmıştır. Bu sorular için anket analizinde puanlama "Kesinlikle Katılmıyorum" (1), "Katılmıyorum" (2), "Kararsızım" (3), "Katılıyorum" (4) ve "Kesinlikle Katılıyorum" (5) şeklinde hesaplanmıştır. Anket sonuçlarının önemliliğinin değerlendirilmesi için standart sapma ve ortalamalar sonrası bağıl önem değerleri Eş.4.1'e göre hesaplanmıştır [94].

Ortalama (ort) her bir soru için yanıtların hepsinin toplanarak toplam veri sayısına bölünmesi ile bulunmakta ve yanıtların merkezsel değerini tek bir sayı ile göstermektedir. Standart sapma (ss) her bir soru için yanıt değerlerinin aritmetik ortalamasının farkının karesinin toplamının veri sayısının bir eksiğine bölümünün karekökü ile hesaplanmakta ve verilerin ortalama etrafında ne ölçüde değiştiğini ifade etmektedir. Standart sapma yanıt değerlerinin yayılımı konusunda özet vermektedir. Ayrıca, çalışma sonucunda elde edilen verilerin anlamlandırılması amacıyla bağıl önem (bö) hesaplaması kullanılmıştır.

$$\text{Bağıl Önem Değeri} = (\text{Ortalama} / \text{Anket Üst Değeri}(5))*100 \quad \text{(Eşitlik 4.1)}$$

Bağıl önem hesaplamalarına göre bağıl önem seviyeleri Çizelge 4.1'de gösterilen değerlere göre belirlenmiştir [94].

Çizelge 4.1. Bağıl önem değer, ortalama ve seviye eşleştirme tablosu

Bağıl Önem Değeri	Bağıl Önem Seviyesi	Ortalama
0-60	Zayıf	0 – 3,00
61-70	Kritik	3,01 – 3,50
71-80	İyi	3,51 – 4,00
81-90	Çok İyi	4,01 – 4,50
91-100	Mükemmel	4,51 – 5,00

Çizelge 4.1'de görüldüğü üzere bağıl önem değerine göre "Mükemmel", "Çok iyi", "İyi", "Kritik" ve "Zayıf" seviyeleri bulunmaktadır. Verilen yanıtların önemini belirlemek için bağıl önem değeri kullanılmıştır. Bağıl önem seviyesi "Zayıf" olan soruların yanıtları bir riski işaret edebileceği değerlendirilerek sonuç bölümünde belirtilmiştir.

Araştırmanın güvenilirliği

Bu çalışmanın güvenilirliği, hazırlanmış metodoloji ve veri toplama süreçleriyle desteklenmektedir. Anket soruları, ISO 27001 standardının ilgili maddeleri göz önünde bulundurularak oluşturulmuş, uzman görüşü alınmış ve pilot çalışma ile anlaşılırlığı ve uygunluğu test edilmiştir. Katılımcıların gizlilik endişeleri ve objektif yanıtlar verebilmesi için anonimlik sağlanmıştır.

Denetim evreni için sertifikalandırılan kuruluş sayısı bilinmesine rağmen; bu kuruluşlarda görevli toplam iç tetkikçi sayısı verisi bilinememektedir. Bu sebeple örneklem boyutu seçiminde; muhakemeye dayalı örneklem seçimi kullanılmıştır. Veri analizi için IBM SPSS programı kullanılmış ve sonuçlar istatistiksel olarak değerlendirilmiştir. Veri toplama aracının güvenilirliği, araştırmanın doğruluk ve tekrarlanabilirlik seviyesini belirleyen kritik bir unsurdur. Güvenilirlik sağlamak için veri toplama aracı, kapsamlı inceleme sonucunda oluşturulmuş ve pilot çalışmalarda test edilmiştir. Pilot çalışmalar, soruların anlaşılırlığını ve veri toplama sürecinin etkinliğini değerlendirmek amacıyla gerçekleştirilmiş ve elde edilen geri bildirimler doğrultusunda gerekli düzeltmeler yapılmıştır. Ayrıca, kullanılan anketlerin iç tutarlılığı, Cronbach's Alpha gibi güvenilirlik analizleriyle test edilmiş ve yüksek güvenilirlik katsayısı elde edilmiştir.

Veri toplama araçlarında, toplanan verilerin güvenilirliğini tespit etmek için güvenilirlik

testleri yapılmaktadır. Sonuçların güvenilirliği, tutarlı, dengeli ve tekrarlanabilir sonuçlar elde etme durumlarına göre belirlenmektedir. Güvenilirliği değerlendirirken tasarlanmış anketten elde edilen yanıtların tutarlılığına odaklanılarak tipik olarak Likert ölçeği aracılığıyla toplanan verilerin güvenilirliği incelenmektedir. Güvenilirliği değerlendirmek için yaygın kullanılan yöntem Cronbach'ın Alfa'dır. Alfa katsayısı 0.7'yi aşarsa, verilerin yeterince güvenilir olduğu genel olarak kabul edilmektedir [95]. Daha ayrıntılı güvenilirlik analizi değerlendirme tablosu Çizelge 4.2'de bulunmaktadır.

Çizelge 4.2. Güvenilirlik analizi değerlendirme tablosu [96]

Cronbach's alpha değeri	Güvenilirlik
$\alpha \geq .8$	Yüksek seviye güvenilirlik
$.8 > \alpha \geq .6$	Güvenilir
$.6 > \alpha \geq .4$	Düşük güvenilirlik
$.4 > \alpha$	Güvenilir değil

Veri analizi neticesinde geliştirilen veri toplama aracının Cronbach Alpha güvenilirlik değeri 0,921 ölçülmüştür. Çizelge 4.2.'ye göre yüksek seviye güvenilirlik düzeyinde olduğu görülmektedir.

4.3. Araştırma Verisi Toplama Aracı

Araştırmaya ilişkin veri toplama aracı iki bölümden oluşmaktadır. Birinci bölümde katılımcıların çalıştıkları kuruluş ve çalıştıkları kuruluştaki ISO 27001 sertifikası çerçevesinde genel sorular bulunmaktadır. İkinci bölümde ise tetkikçilerin gerçekleştirdikleri ISO 27001 BGYS iç denetim süreçleri ile ilgili sorular yer almaktadır.

Anket soruları için bu çalışmanın amacına uygun olarak değerlendirilen konu kategorisi, ilişkilendirilen ISO 27001 BGYS standardı maddesi, ilgili ISO 19011 Yönetim Sistemleri Denetleme Kılavuzu standardı maddesi ve ilgili Uluslararası İç Denetim Standartları maddesi Çizelge 4.3'de bulunmaktadır.

Çizelge 4.3. Anket soruları ve standart ilişkilendirme tablosu

Soru Numarası	Konu Kategorisi	ISO 27001 Maddesi	ISO 19011 Maddesi	Uluslararası İç Denetim Standartları Maddesi
7,8,9,11	Objektiflik ve Bağımsızlık	9.2.2.b	4.e	1100 - Bağımsızlık ve Objektiflik
10,27	Raporlama	9.2.2.c	6.5.1 6.5.2	2400 - Sonuçların Raporlanması
12,13,14,15, 16,17,18	Sürekli Gelişim ve Yetkinlik	7.2.a 7.2.b	7.6 7.1 7.2.3.3	1230 - Sürekli Mesleki Gelişim 1200 - Yeterlilik ve Azami Mesleki Özen ve Dikkat
19,20,21,22, 23,24,25,26	Denetim Planlaması ve Kriterler	9.2.1.a 9.2.2.a 9.2.2	5.1 5.4.2	2010 - Planlama 2240 - Görev İş Programı
28,29,30,31,32	İyileştirme ve Bulgular	10.2	6.7	2500 - İlerlemenin Gözlenmesi

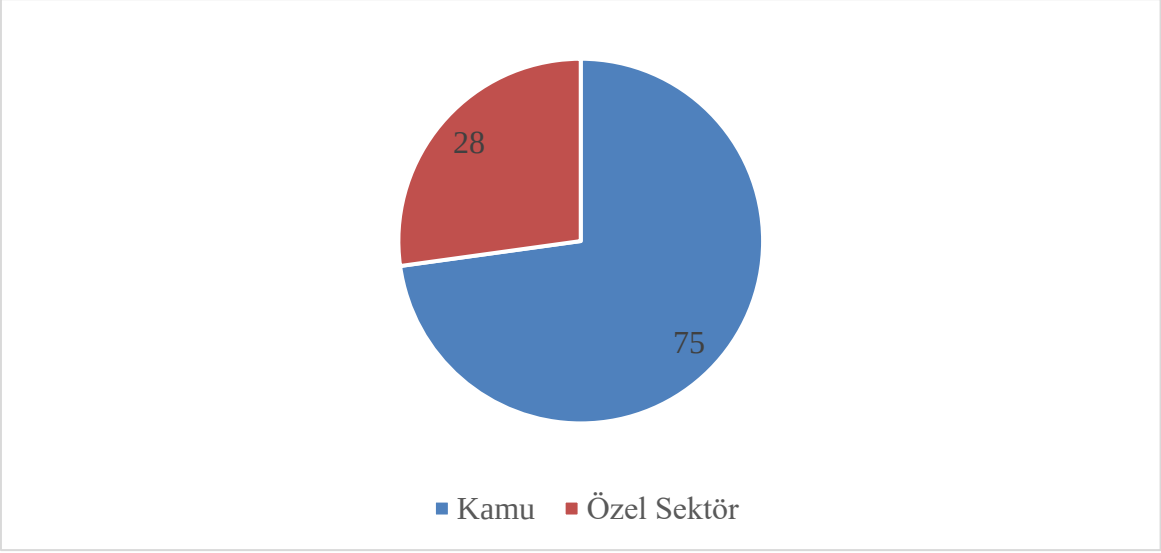
Çizelge 4.3'de bu çalışmada gerçekleştirilen anket içerisindeki soruların değerlendirme konu kategorileri olarak belirlenen objektiflik ve bağımsızlık, raporlama, sürekli gelişim ve yetkinlik, denetim planlaması ve kriterler, iyileştirme ve bulgular konuları ile ilişkilendirmesi görülmektedir. Ayrıca, anket sorularının bu çalışmanın 3. bölümünde bahsedilen ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardı, ISO 19011 Yönetim Sistemleri Denetleme Kılavuzu standardı ve ilgili Uluslararası İç Denetim Standartlarında bulunan esaslar ile ilişkilendirmesi de yer almaktadır.

5. BULGULAR

5.1. Genel Bilgiler

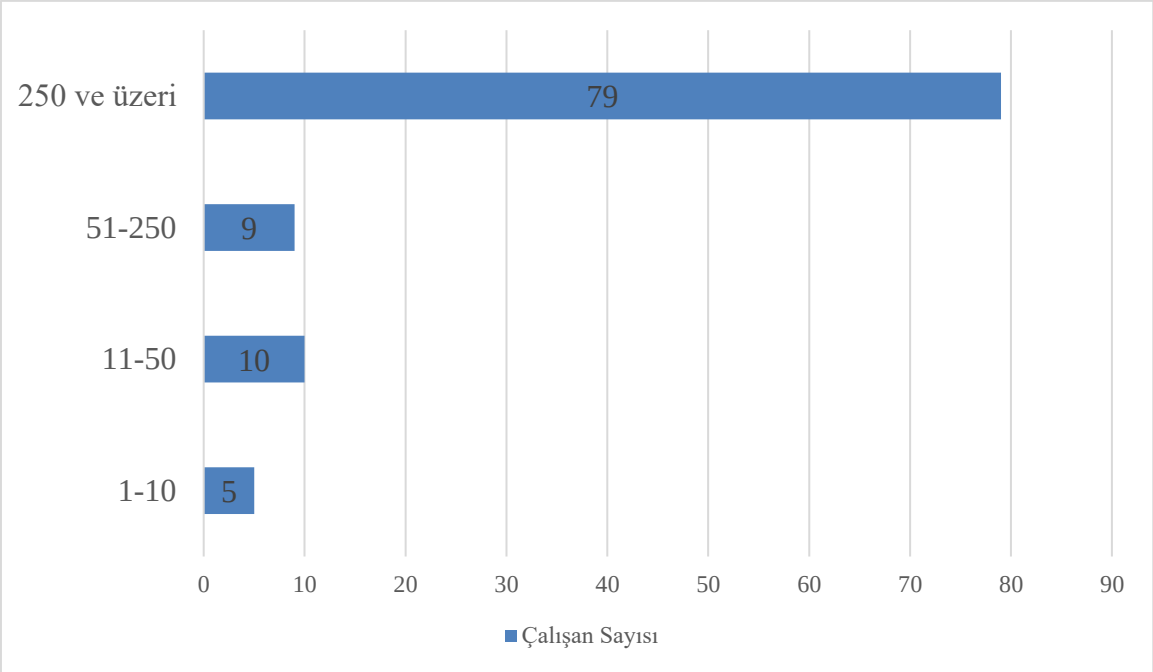
Veri toplama aracı olarak kullanılan ankete katılan 103 katılımcıdan 75 kişi kamu kurum/kuruluşlarında, 28 kişi ise özel sektörde çalışmaktadır. Kamu ve özel sektörde farklı kuruluşlardan çalışanların katılımı, araştırma sonuçlarının çeşitliliğini sağlamıştır. Konu ile ilgili grafik Şekil 5.1'de bulunmaktadır.

Katılımcılardan 13 kişi yönetici, 15 kişi iç denetçi/müfettiş ve 77 kişi çalışan pozisyonunda çalıştıklarını belirtmişlerdir. Anket katılımcıları bu pozisyonlarda çalışarak ISO 27001 iç tetkiklerinde görev aldıklarını beyan etmişlerdir. 79 katılımcı 251 ve üzeri çalışan sayısı bulunan kurum ve kuruluşlarda, 10 katılımcı 11-50 çalışan sayısı bulunan kurum ve kuruluşlarda, 9 katılımcı 51-250 çalışan sayısı bulunan kurum ve kuruluşlarda, 5 kişi ise 1-10 çalışan sayısı bulunan kurum ve kuruluşlarda çalışmaktadır. Bu durum farklı büyüklüklerdeki kuruluşlar için araştırma sonuçlarının çeşitliliğini sağlamıştır. Konu ile ilgili grafik Şekil 5.2'de bulunmaktadır.



Şekil 5.1. Ankete katılanların çalıştıkları kurum/şirket

Şekil 5.1'de görüldüğü üzere katılımcıların daha büyük bir kısmının kamuda ISO 27001 BGYS iç tetkiklerinde görev almış tetkikçilerden oluştuğu görülmektedir.

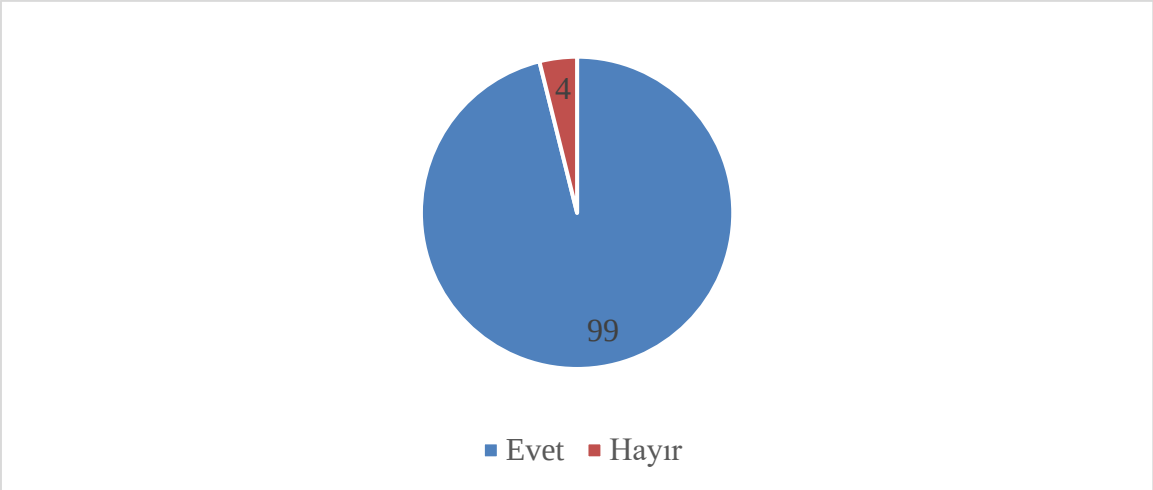


Şekil 5.2. Çalışılan kurumdaki/şirketteki çalışan sayısı

Şekil 5.2'de görüldüğü üzere katılımcıların daha büyük bir kısmının 250 ve üzeri çalışan bulunan kuruluşların ISO 27001 BGYS iç tetkiklerinde görev aldıkları, sadece 5 tetkikçinin 1-10 arası çalışanı bulunan küçük kuruluşların tetkiklerinde görev aldığı görülmektedir.

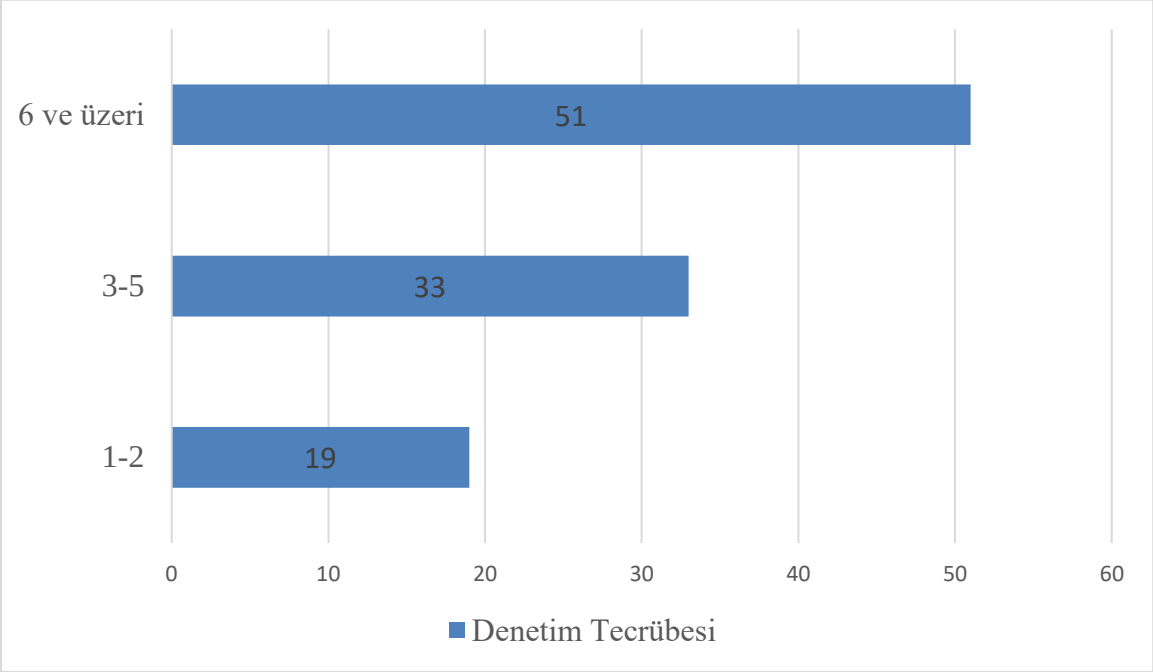
5.2. ISO 27001 Tetkikleri ile İlgili Genel Sorular

Anket katılımcılarından 99 kişi, ISO 27001 BGYS tetkiki/denetimi ile ilgili eğitim aldığını belirtmiştir. Sadece 4 kişi eğitim almadığı yönünde beyanda bulunmuştur. Konu ile ilgili grafik Şekil 5.3'de bulunmaktadır. Katılımcılar farklı sayılarda ISO 27001 BGYS denetimine katıldıklarını belirtmiştir. Bu durum farklı denetim tecrübesinde bulunan tetkikçilerden bilgi toplandığını göstermektedir. Konu ile ilgili grafik Şekil 5.4'te bulunmaktadır.



Şekil 5.3. Katılımcıların ISO 27001 BGYS tetkiki/denetimi ile ilgili eğitim alma durumu

Şekil 5.3'de görüldüğü üzere ISO 27001 BGYS iç tetkiklerinde görev alan katılımcıların büyük bir kısmının BGYS tetkiki/denetimi ile ilgili eğitim aldığı görülmektedir.



Şekil 5.4. Katılımcıların ISO 27001 BGYS tetkiki/denetimi katılım sayıları

Şekil 5.4'te görüldüğü gibi katılımcılardan 51 kişi 6 ve üzeri, 33 kişi 3-5 arası ve 19 kişi 1-2 arası ISO 27001 BGYS iç denetimine katıldığı görülmektedir.

5.3. ISO 27001 Tetkik Süreci ile İlgili Sorular

Veri toplama aracı anket içerisinde bulunan ISO 27001 tetkik süreci ile ilgili sorular Bkz. Çizelge 4.3.'de farklı konu kategorilerine göre gruplanmıştır. Çalışmanın amacına uygun olarak, bu konu kategorileri çerçevesinde değerlendirilme gerçekleştirilmiştir. ISO 27001 tetkik süreci ile ilgili sorularda 5'li Likert ölçeği kullanılmıştır. Bu ölçeğin analizinde puanlama "Kesinlikle Katılmıyorum" (1), "Katılmıyorum" (2), "Kararsızım" (3), "Katılıyorum" (4) ve Kesinlikle Katılıyorum" (5) şeklinde hesaplanmıştır. Tüm araştırma sorularının genel ortalaması 3,43 olarak hesaplanmıştır.

Bu çalışmanın birinci bölümündeki araştırmanın amacı kısmında "1. Denetim süreçlerinde kamuda ve özel sektörde görev alan ISO 27001 BGYS iç tetkikçileri özelinde farklılıklar nelerdir?" sorusuna cevap arandığı belirtilmiştir. Çizelge 5.1, Çizelge 5.2, Çizelge 5.3, Çizelge 5.4. ve Çizelge 5.5. içerisinde farklı konu başlıklarına göre kamuda ve özel sektörde görev alan denetçilerin görüşleri görülmektedir. Görüş farklılıkları konu başlıkları altında ve sonuç bölümünde değerlendirilmiştir.

5.3.1. Objektiflik ve bağımsızlık

Denetimlerin objektif ve bağımsız gerçekleştirilmesi elde edilen denetim sonuçlarının doğru ve yeterli olması için büyük önem arz etmektedir. IIA Uluslararası İç Denetim Standartlarına göre bağımsızlık "iç denetim faaliyetinin sorumluluklarını tarafsız olarak yerine getirme kabiliyetini tehdit eden şartlardan uzak olmak demektir" şeklinde, objektiflik ise "iç denetçilerin görevlerini, iş sonucunda çıkan ürüne gerçekten ve dürüst bir şekilde inanacakları ve bu ürünün kalitesinden önemli bir taviz vermeyecekleri şekilde yapmalarını sağlayan tarafsız bir zihinsel tutumdur" şeklinde tanımlanmıştır [88]. Objektif ve bağımsız olarak gerçekleştirilmeyen denetimlerde, tespit edilemeyen hususlar sonucu, siber güvenlik açıklıklarının raporlanamaması ve kapatılmaması ihtimal dahilindedir. Örnek olarak kişisel ilişkileri sebebiyle objektif davranamadığı için tespit ettiği bir uygulamadaki güvenlik açıklığı ile ilgili bir bulguyu raporlayamayan bir tetkikçi, bu açıklığın kapatılmamasına ve denetimi gerçekleştirdiği kurum/kuruluşun siber güvenlik zafiyetleri sonucu risk altında kalmasına sebep olabilecektir. Çizelge 5.1'de konu ile ilgili bu çalışmadaki sorular ve cevap analizi bulunmaktadır.

Çizelge 5.1. Objektiflik ve bağımsızlık ile ilgili sorular ve cevap analizi

Soru No	Soru	Genel			Kamu			Özel Sektör		
		ort	ss	bö	ort	ss	bö	ort	ss	bö
7	Gerçekleştirdiğim denetimlerde bağımsızlığı sağlamak amacıyla kendi birimim dışındaki birimlerin denetiminde görevlendiriliyorum.	3,40	1,57	Kritik	3,68	1,44	İyi	2,64	1,68	Zayıf
8	Denetimlerini gerçekleştirdiğim birim ve süreçlerin yöneticileri ve/veya bir üst yöneticileri benim yöneticim değil.	2,58	1,6	Zayıf	2,68	1,62	Zayıf	2,32	1,54	Zayıf
9	Şirketimde/Kurumumda ISO 27001 BGYS iç denetimleri objektif bir şekilde gerçekleştiriliyor.	3,96	1,07	İyi	4,04	1,03	Çok İyi	3,75	1,17	İyi
11	Gerçekleştirdiğim denetimlerde bulgularım ile ilgili herhangi bir baskıya maruz kalmıyorum.	4,37	1.00	Çok İyi	4,37	0,96	Çok İyi	4,36	1,09	Çok İyi

Çizelge 5.1'de görüldüğü üzere tetkikçilerin denetimlerde kendi çalıştıkları birimleri dışında tetkiklerde görev almaları durumunun ölçüldüğü 7. soru; genel sonuçlara göre 3,40 ortalama ile "Kritik" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 3,68 ortalama ile "İyi" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde en düşük 3. değer olarak 2,64 ortalama ile "Zayıf" bağıl önem seviyesinde yanıtlanmıştır.

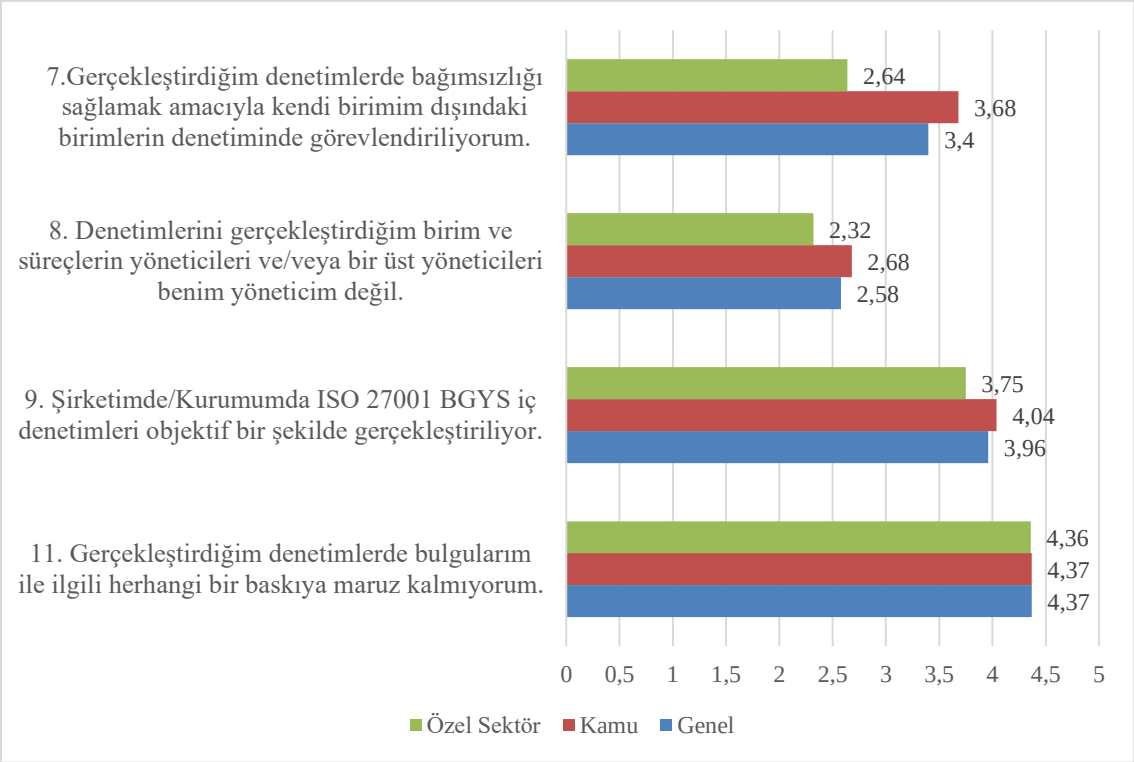
Tetkikçilerin denetim gerçekleştirdikleri birim yöneticileri ve/veya bir üst yöneticinin kendi yöneticileri olması durumunun ölçüldüğü 8. soru; genel sonuçlara göre en düşük değer olarak 2,58 ortalama ile "Zayıf" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde en düşük değer olarak 2,68 ortalama ile "Zayıf" bağıl önem

seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde en düşük değer olarak 2,32 ortalama ile “Zayıf” bağıl önem seviyesinde yanıtlanmıştır.

Tetkikçilerin denetimleri objektif olarak gerçekleştirdikleri hakkında görüşlerinin ölçüldüğü 9. soru; genel sonuçlara göre 3,96 ortalama ile “İyi” bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 4,04 ortalama ile “Çok iyi” bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 3,75 ortalama ile “İyi” bağıl önem seviyesinde yanıtlanmıştır.

Tetkikçilerin denetimlerde baskıya maruz kalmadıkları hakkında görüşlerinin ölçüldüğü 11. soru; genel sonuçlara göre 4,37 ortalama ile “Çok iyi” bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 4,37 ortalama ile “Çok iyi” bağıl önem seviyesinde, özel sektöre görev alan ISO 27001 BGYS tetkikçileri özelinde 4,36 ortalama ile “Çok iyi” bağıl önem seviyesinde yanıtlanmıştır.

ISO 27001 BGYS tetkikçilerinin denetim süreçlerindeki görüşleri çeşitli açılardan incelenmiştir. Tetkikçilerin kendi çalıştıkları birim denetimlerinde görev alması sorusu genel olarak "Kritik" bağıl önem seviyesinde değerlendirilmiştir, özellikle özel sektörde bu durum daha düşük ortalama ile yanıtlanmıştır. Tetkikçilerin, kendi yöneticilerini denetlemeleri konusu, hem kamu hem de özel sektörde bağıl önem seviyesi "Zayıf" olarak değerlendirilmiştir. Genel sonuçlar ve farklı sektörlerdeki ISO 27001 BGYS tetkikçileri arasında bu durumun önemli bir zayıflık olarak algılandığı görülmektedir. Bir başka örnekte ise, tetkikçilerin denetimleri objektif olarak gerçekleştirdikleri görüşü genel olarak "İyi" bağıl önem seviyesinde yanıtlanmıştır. Ayrıca, tetkikçilerin baskıya maruz kalmadıkları algısı da genel olarak "Çok iyi" bağıl önem seviyesinde değerlendirilmiştir. Bu bulgular, ISO 27001 denetim süreçlerindeki zayıf yönleri belirlemede önemli bir kılavuzluk sağlamaktadır, özellikle kamu ve özel sektördeki tetkikçiler arasındaki algı farklılıklarını vurgulamaktadır.



Şekil 5.5. Objektiflik ve bağımsızlık konu başlıklarındaki soruların yanıt ortalamaları

Bu çalışmanın birinci bölümündeki araştırmanın amacı kısmında "2. İç tetkikçilerin gerçekleştirdikleri denetimlerin objektifliği ve bağımsızlığı hakkında görüşleri nelerdir?" sorusuna cevap arandığı belirtilmiştir. Şekil 5.5'de denetçilerin yanıtları görülmekte olup sonuçların objektiflik ve bağımsızlığı tehdit edebileceği değerlendirilmektedir. Bir tetkikçinin kendi biriminde ve kendi yöneticisinin sorumluluğunda olan birimlerde gerçekleştirdiği denetimlerin objektiflik ve tarafsızlık açısından risk teşkil edebileceği düşünülmektedir. Ayrıca, bu yanıtlara rağmen farklı bir soruda tetkikçilerin daha yüksek oranda gerçekleştirdikleri denetimleri objektif olarak yürüttüklerini ve baskıya maruz kalmadıklarını düşündükleri görülmektedir.

Ercan (2017) tarafından yapılan çalışmada; denetimin güvenilirliği için denetçilerin bağımsızlığının kritik bir rolü bulunduğu; bağımsızlığın sağlanmasında ilk derecede sorumluluğun denetçilerde bulunsa da, denetim gerçekleştirilen kuruluş ve düzenleyicilere de önemli görevler düşmekte olduğu sonucuna ulaşılmıştır [97]. Bu çerçevede objektiflik ve tarafsızlık açısından risk teşkil edecek durumların çözümü için denetçiler ve denetlenen kuruluş tarafından önlem alınması gerektiği düşünülmektedir.

5.3.2. Denetim Raporlama

Tespit edilen uygunsuzlukların raporlanması ve denetim sonuçlarının yetkili kademelere bildirilmesi denetim sonucunda iyileştirmeler sağlanması için önemli bir husustur. Raporlanmayan veya doğru kademelere bildirilmeyen uygunsuzluklar düzeltilmeyebilir ve bu durum siber güvenlik açıklıklarının kapatılmamasına sebep olabileceği gibi; bu eksiklikler ve açıklıklar sebebiyle kurum kuruluşların siber olay ile karşılaşmaları olası olabilmektedir. Örnek olarak sistem odası iklimlendirme sistemleri ile ilgili maddi kaynak ayrılarak çözülmesi gereken bir uygunsuzluk raporlanmaması veya doğru yetkili kademelere bildirilmemesi sebebiyle riskli konu yönetilemeyebilir ve/veya kaynak ayrılamayabilir. Bu durum kuruluşların siber güvenlik zafiyetleri sonucu risk altında kalmasına sebep olabilecektir. Çizelge 5.2'de konu ile ilgili sorular ve cevap analizi bulunmaktadır.

Çizelge 5.2. Denetim raporlama ilgili sorular ve cevap analizi

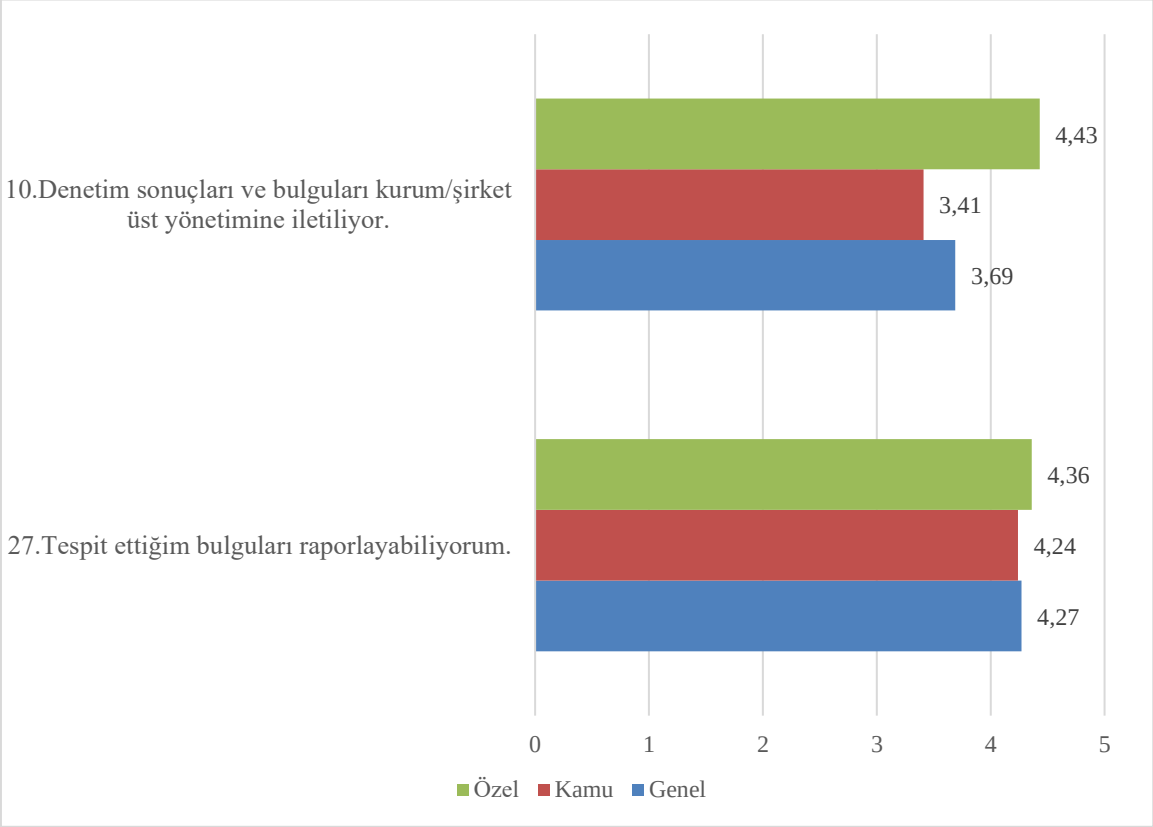
Soru No	Soru	Genel			Kamu			Özel Sektör		
		ort	ss	bö	ort	ss	bö	ort	ss	bö
10	Denetim sonuçları ve bulguları kurum/şirket üst yönetimine iletiliyor.	3,69	1,49	İyi	3,41	1,55	Kritik	4,43	1,00	Çok İyi
27	Tespit ettiğim bulguları raporlayabiliyorum.	4,27	0,98	Çok İyi	4,24	1,00	Çok İyi	4,36	0,95	Çok İyi

Çizelge 5.2'de görüldüğü üzere denetim sonuçlarının kurum/şirket üst yönetimine iletilme durumunun ölçüldüğü 10. soru; genel sonuçlara göre 3,69 ortalama ile "İyi" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 3,41 ortalama ile "Kritik" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 4,43 ortalama ile "Çok iyi" bağıl önem seviyesinde yanıtlanmıştır.

Tetkikçilerin tespit ettikleri bulguları raporlayabildiklerine dair görüşlerinin ölçüldüğü 27. soru; genel sonuçlara göre 4,27 ortalama ile "Çok iyi" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 4,24 ortalama ile "Çok iyi" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 4,36 ortalama ile "Çok iyi" bağıl önem seviyesinde yanıtlanmıştır.

ISO 27001 BGYS tetkikçilerinin denetim sonuçlarını kurum veya şirket üst yönetimine iletmesi sorusu genel olarak "İyi" bağıl önem seviyelerinde değerlendirilmiştir. Kamuda

görev alan tetkikçilerde bu durum "Kritik" seviyede değerlendirilirken, özel sektörde görev alan tetkikçilerde ise "Çok iyi" seviyesinde değerlendirme almıştır. Ayrıca, tetkikçilerin tespit ettikleri bulguları raporlayabilme yetenekleri genel olarak "Çok iyi" bağıl önem seviyesinde değerlendirilmiştir, hem kamuda hem de özel sektörde bu algı yüksek seviyede tutulmuştur. Bu bulgular, ISO 27001 denetim süreçlerinde bulguların etkin bir şekilde iletilmesi ve raporlanmasının önemini vurgulamaktadır, kamu ve özel sektördeki tetkikçilerin algıları arasındaki farklılıkları da ortaya koymaktadır.



Şekil 5.6. Raporlama konu başlığındaki soruların yanıt ortalamaları

Bu çalışmanın birinci bölümündeki araştırmanın amacı kısmında "3. İç tetkikçilerin denetim sonrası bulunan uygunsuzlukların raporlanması ve etkin şekilde çözümü için gerçekleştirilen faaliyetler ile ilgili görüşleri nelerdir?" sorusuna cevap arandığı belirtilmiştir. Şekil 5.6'da denetimlerde tespit edilen uygunsuzlukların raporlanması konusunda denetçilerin yanıtları görülmektedir. Bulguların üst yönetime bildirilmesi bir zorunluluk olmamakla birlikte üst yönetimin uygunsuzluk ve BGYS kapsamında çalışmalar hakkında bilgi sahibi olmasının; gerekli desteği sağlaması ve kaynak ayırabilmesi açısından önemli olduğu değerlendirilmektedir.

İç Denetim Enstitüsünün 2015 yılı "Global Perspektifler ve Anlayışlar" raporunda; kuruluşların çoğunun gerçekleştirmesi gereken pek çok faaliyet bulunduğu, iç denetimlere ait raporların amaca uygun olarak, güvenilir ve inandırıcı olmasını sağlamak için kuruluş içerisinde etkili konumlandırılması gerektiği sonucu belirtilmiştir [98]. Bu çerçevede denetçilerin ve kuruluşların, raporlama içeriği ve raporların ilgililere ulaşması konusunda risk teşkil edecek durumların çözümü için önlem alması gerektiği düşünülmektedir.

5.3.3. Sürekli gelişim ve yetkinlik

Denetim sonuçları açısından, denetimi gerçekleştiren kişilerin yetkinliği kritik önemdedir. Denetim süreçleri ve teknik konularda yetkinliğe sahip olmayan tetkikçiler uygunsuzlukların tespit edilmemesine ve bu sebeple siber güvenlik açıklıklarının kapatılmamasına sebep olabileceklerdir. ISO 27001 BGYS teknik kontrol maddeleri bulunan bir standarttır. Bu çalışmanın 3.4. bölümünde bahsedildiği gibi erişim yönetimi, işletim yönetimi, haberleşme ve kriptoloji gibi konularda teknik kontrol maddeleri içermektedir. Bu teknik kontrol maddelerinin etkin denetimi için teknik bilgi sahibi kişilerin tetkiklerde görev alması gerekmektedir. Bu konu ile ilgili anket sorularından 15, 16, 17, 18 numaralı sorular, tüm tetkikçiler teknik sistemlerin denetimini gerçekleştirmediği için yanıtlanması zorunlu tutulmamıştır. Teknik konularda uzmanlığı olmayan ve teknik uzman kullanmayan tetkikçiler bu konulardaki eksikleri tespit edemeyebilecektir. Tespit edilemeyen teknik eksiklikler ise siber güvenlik açıklıklarına sebep olacaktır. Örnek olarak yazılım geliştirme veya veri tabanı gibi teknik süreçlerde denetim gerçekleştiren tetkikçi, bu alanlarda teknik bilgiye sahip olmaması sebebiyle parola yönetimi, log yönetimi veya yazılım kaynak kod yönetimi gibi teknik hususlardaki yanlış yapılandırma veya güvenlik açıklıklarını tespit edemeyerek raporlayamayacaktır. Raporlanamayan bu hususular denetlenen kurum/kuruluş için siber güvenlik risklerine sebep olabilecektir. Çizelge 5.3'te bu çalışmadaki konu ile ilgili sorular ve cevap analizi bulunmaktadır.

Çizelge 5.3. Tetkikçi sürekli gelişimi ve yetkinliği ile ilgili sorular ve cevap analizi

Soru No	Soru	Genel			Kamu			Özel Sektör		
		ort	ss	bö	ort	ss	bö	ort	ss	bö
12	ISO 27001 BGYS Denetimi/Tetkiki ile ilgili düzenli eğitimler almaktayım.	2,77	1,42	Zayıf	2,83	1,41	Zayıf	2,61	1,45	Zayıf
13	Gerçekleştirdiğim denetimleri için gerekli bilgi, beceri ve vasıflara sahibim.	4,18	0,93	Çok İyi	4,13	0,93	Çok İyi	4,32	0,9	Çok İyi
14	Denetlediğim birimler ile ilgili denetimi gerçekleştirebilecek teknik bilgiye sahibim.	3,83	1,18	İyi	3,64	1,2	İyi	4,32	0,94	Çok İyi
15	Yazılım geliştirme konusunda denetim gerçekleştiriyorum ve bu konuda teknik bilgiye sahibim.(*)	3,0	1,53	Zayıf	2,78	1,45	Zayıf	3,54	1,61	İyi
16	Veritabanı konusunda denetim gerçekleştiriyorum ve bu konuda teknik bilgiye sahibim. (*)	2,99	1,54	Zayıf	2,71	1,44	Zayıf	3,85	1,53	İyi
17	Network konusunda denetim gerçekleştiriyorum ve bu konuda teknik bilgiye sahibim. (*)	3,13	1,44	Kritik	3,02	1,37	Kritik	3,43	1,59	Kritik
18	İşletim Sistemleri konusunda denetim gerçekleştiriyorum ve bu konuda teknik bilgiye sahibim. (*)	3,26	1,41	Kritik	3,13	1,37	Kritik	3,64	1,50	İyi
(* Cevap verilmesi zorunlu beklenmeyen soru)										

Çizelge 5.3'te görüldüğü üzere tetkikçilerin denetim süreçleri ile ilgili düzenli eğitim alma durumunun ölçüldüğü 12. soru; genel sonuçlara göre en düşük 2. değer olarak 2,77 ortalama ile "Zayıf" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 2,83 ortalama ile "Kritik" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde en düşük 2. değer olarak 2,61 ortalama ile "Zayıf" bağıl önem seviyesinde yanıtlanmıştır.

Tetkikçilerin gerçekleştirdikleri denetimlerle ilgili gerekli bilgi, beceri ve vasıflara sahip olduklarına dair görüşlerinin ölçüldüğü 13. soru; genel sonuçlara göre 4,18 ortalama ile "Çok

iyi" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 4,13 ortalama ile "Çok iyi" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 4,32 ortalama ile "Çok iyi" bağıl önem seviyesinde yanıtlanmıştır.

Tetkikçilerin görevlendirildikleri denetimlerle ilgili denetimi gerçekleştirebilecek teknik bilgiye sahip olmalarına dair görüşlerinin ölçüldüğü 14. soru; genel sonuçlara göre 3,83 ortalama ile "İyi" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 3,64 ortalama ile "İyi" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 4,32 ortalama ile "Çok iyi" bağıl önem seviyesinde yanıtlanmıştır.

Yazılım geliştirme konusunda denetim gerçekleştiren tetkikçilerin bu konuda teknik bilgiye sahip olmalarına dair görüşlerinin ölçüldüğü 15. soru; genel sonuçlara göre 3,00 ortalama ile "Zayıf" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde en düşük 3. değer olarak 2,78 ortalama ile "Zayıf" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 3,54 ortalama ile "İyi" bağıl önem seviyesinde yanıtlanmıştır.

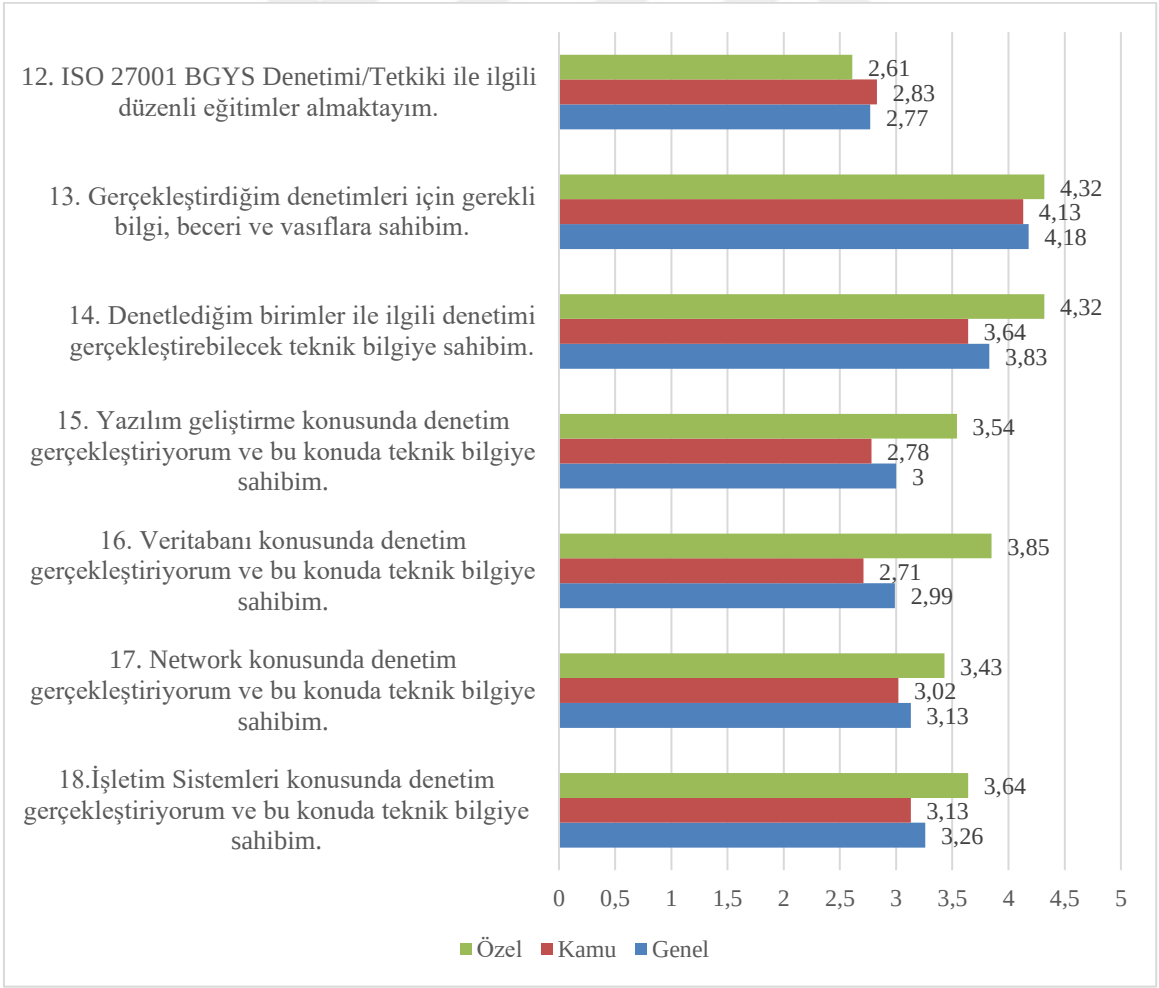
Veri tabanı konusunda denetim gerçekleştiren tetkikçilerin bu konuda teknik bilgiye sahip olmalarına dair görüşlerinin ölçüldüğü 16. soru; genel sonuçlara göre 2,99 ortalama ile "Zayıf" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde en düşük 2. değer olarak 2,71 ortalama ile "Zayıf" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 3,85 ortalama ile "İyi" bağıl önem seviyesinde yanıtlanmıştır.

Network konusunda denetim gerçekleştiren tetkikçilerin bu konuda teknik bilgiye sahip olmalarına dair görüşlerinin ölçüldüğü 17. soru; genel sonuçlara göre 3,13 ortalama ile "Kritik" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 3,02 ortalama ile "Kritik" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 3,43 ortalama ile "Kritik" bağıl önem seviyesinde yanıtlanmıştır.

İşletim sistemleri konusunda denetim gerçekleştiren tetkikçilerin bu konuda teknik bilgiye sahip olmalarına dair görüşlerinin ölçüldüğü 18. soru; genel sonuçlara göre 3,26 ortalama ile "Kritik" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri

özelinde 3,13 ortalama ile "Kritik" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 3,64 ortalama ile "İyi" bağıl önem seviyesinde yanıtlanmıştır.

ISO 27001 BGYS tetkikçileri düzenli eğitim alma durumlarını genel olarak bağıl önem seviyesi "Zayıf" olarak değerlendirmiştir. Ayrıca, tetkikçilerin denetimlerde gerekli bilgi, beceri ve vasıflara sahip olduklarına dair genel görüşler "Çok iyi" bağıl önem seviyesinde değerlendirilmiştir. Ancak; yazılım geliştirme, veri tabanı, network ve işletim sistemleri gibi özel konularda özel sektördeki tetkikçilerin daha iyi performans sergilediği görüşünde oldukları, kamudaki tetkikçilerin ise bu konularda soruları bağıl önem seviyesi "Zayıf" ve "Kritik" olarak yanıtladığı görülmüştür. Bu sonuçlar, ISO 27001 denetimlerinde teknik bilgi ve eğitimin önemini vurgulamakta ve kamu ile özel sektörde tetkikçiler arasındaki yetkinlik farklarını ortaya koymaktadır.



Şekil 5.7. Sürekli gelişim ve yetkinlik konu başlıklarındaki soruların yanıt ortalamaları

Bu çalışmanın birinci bölümündeki araştırmanın amacı kısmında “4. İç tetkikçilerin sürekli gelişimleri için yapılan faaliyetler ile ilgili görüşleri nelerdir? 5. Denetim yapan tetkikçilerin, özel uzmanlık gereken tetkiklerde gerekli yetkinliğe sahip olduklarına dair görüşleri nelerdir?” sorularına cevap arandığı belirtilmiştir. Şekil 5.7’de denetçilerin sürekli gelişimi ve yetkinliği konularında yanıtları görülmektedir. Yazılım geliştirme, veri tabanı, network ve işletim sistemleri konularında teknik bilginin, denetimlerin etkin bir şekilde gerçekleştirilmesi, uygunsuzluk ve iyileştirilebilir alanların tespit edilmesi için önem arz ettiği değerlendirilmektedir. Bu konunun siber güvenlik açıklıklarının tespiti ve sonrası kapatılması için risk teşkil edebileceği düşünülmektedir. Ayrıca yanıtlara göre tetkikçilerin yetkinliğinin sağlanması ve etkin denetimler gerçekleştirmesi için düzenli eğitimler almaları konusunda eksiklikler olduğunu düşündükleri değerlendirilmektedir.

Arslan ve Özbilger (2022) tarafından yayınlanan çalışmada; iç denetimlerde görev alanların bilişim denetimi alanındaki yetkinlik ve kabiliyetlerinin artırılmasının, kamu kurumlarının bilişim mevzuatına uyumu için öneme sahip olduğu belirtilmiştir [99]. Bu kapsamda teknik konuları içeren denetimlerde teknik uzman kullanımı ve denetçi teknik yetkinliklerinin artırılması konularında, risk teşkil edecek durumların çözümü için denetçiler ve denetlenen kuruluş tarafından önlem alınması gerektiği düşünülmektedir.

5.3.4. Denetim planlaması ve kriterler

Denetimin doğru planlanması ve denetim öncesi hazırlıklar başarılı bir denetim için önem arz etmektedir. ISO 27001 tetkiklerinin planlanmasında riskli alanların denetim kapsamına alınması, bu alanların tespiti için yeterli periyotlarda ve yeterli zaman ayrılarak denetimlerin gerçekleştirilmesi, denetim etkinliğini doğrudan etkilemektedir. Riskli alanların denetlenmediği, yeterli denetim zamanın ayrılmadığı ve/veya uzun süre denetlenmemiş alanlara sebep olan denetim planlaması, tespit edilemeyen iyileştirilebilir alanlara sebep olabilecektir. Ayrıca denetim öncesi yeterli ön hazırlığın yapılmaması denetim sonuçlarını doğrudan etkileyebilecektir. Örnek olarak denetlenen kurum/kuruluş için önemli olan web sayfası, kurumsal kaynak yönetim yazılımı gibi süreçlerin denetim kapsamına alınmaması veya yeterli denetim zamanının ayrılmaması sebebiyle denetlenememesi durumunda bu sistemlerde bulunan açıklıklar tespit edilemeyecek ve raporlanamayacaktır. Tespit edilemeyen söz konusu bulgular siber güvenlik risklerine sebep olabilecektir. Çizelge 5.4’te konu ile ilgili sorular ve cevap analizi bulunmaktadır.

Çizelge 5.4. Denetim planlaması ve denetimde kullanılan kriterlere dair sorular ve cevap analizi

Soru No	Soru	Genel			Kamu			Özel Sektör		
		ort	ss	bö	ort	ss	bö	ort	ss	bö
19	Şirketimde/Kurumumda riskli alanlar göz önünde bulundurularak iç denetim planlaması yapılmaktadır.	2,90	1,43	Zayıf	2,97	1,43	Zayıf	2,71	1,44	Zayıf
20	Şirketimde/Kurumumda riskli alanları tespit etmek için yeterli periyotlarda denetim gerçekleştiriliyor.	3,76	1,26	İyi	3,69	1,24	İyi	3,93	1,33	İyi
21	Şirketimde/Kurumumda riskli alanları tespit etmek için yeterli denetim zamanı denetçilere veriliyor.	3,12	1,40	Kritik	3,04	1,39	Kritik	3,32	1,44	Kritik
22	Üst üste aynı birim/süreçlerin denetimi aynı kişi tarafından gerçekleştirilmiyor.	3,06	1,47	Kritik	3,19	1,42	Kritik	2,71	1,58	Zayıf
23	Şirketimde/Kurumumda riskli alanları tespit etmek için denetimlerde yeterli sayıda örnek üzerinde kontrol sağlanabiliyor.	2,98	1,39	Zayıf	2,91	1,35	Zayıf	3,18	1,52	Kritik
24	Şirketimde/Kurumumda denetime ön hazırlık yapabilmek için yeterli zaman denetçilere sunuluyor.	3,19	1,39	Kritik	3,19	1,41	Kritik	3,21	1,37	Kritik
25	Denetlediğim birimler ile ilgili ön hazırlık gerçekleştiriyorum.	3,52	1,24	İyi	3,44	1,25	Kritik	3,75	1,21	İyi
26	Şirketimde/Kurumumda denetim için soru ve kontrol listeleri riskli alanları tespit etmek için yeterli.	3,23	1,37	Kritik	3,03	1,34	Kritik	3,79	1,32	İyi

Çizelge 5.4'te görüldüğü üzere tetkikçilerin denetim planlarının riskli alanlara göre yapılmasına dair görüşlerinin ölçüldüğü 19. soru; genel sonuçlara göre 2,90 ortalama ile "Zayıf" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 2,97 ortalama ile "Zayıf" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 2,71 ortalama ile "Zayıf" bağıl önem seviyesinde yanıtlanmıştır.

Tetkikçilerin yeterli periyotlarda denetim gerçekleştirilmesine dair görüşlerinin ölçüldüğü 20. soru; genel sonuçlara göre 3,76 ortalama ile "İyi" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 3,69 ortalama ile "İyi" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 3,93 ortalama ile "İyi" bağıl önem seviyesinde yanıtlanmıştır.

Tetkikçilerin yeterli denetim zamanının kendilerine verilmesine dair görüşlerinin ölçüldüğü 21. soru; genel sonuçlara göre 3,12 ortalama ile "Kritik" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 3,04 ortalama ile "Kritik" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 3,32 ortalama ile "Kritik" bağıl önem seviyesinde yanıtlanmıştır.

Üst üste aynı birim/süreçlerin denetiminin aynı kişi/kişiler tarafından gerçekleştirilme durumunun ölçüldüğü 22. soru; genel sonuçlara göre 3,06 ortalama ile "Kritik" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 3,19 ortalama ile "Kritik" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 2,71 ortalama ile "Zayıf" bağıl önem seviyesinde yanıtlanmıştır.

Tetkikçilerin denetimlerde yeterli sayıda örnek üzerinde kontrol gerçekleştirebildiklerine dair görüşlerinin ölçüldüğü 23. soru; genel sonuçlara göre 2,98 ortalama ile "Zayıf" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 2,91 ortalama ile "Zayıf" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 3,18 ortalama ile "Kritik" bağıl önem seviyesinde yanıtlanmıştır.

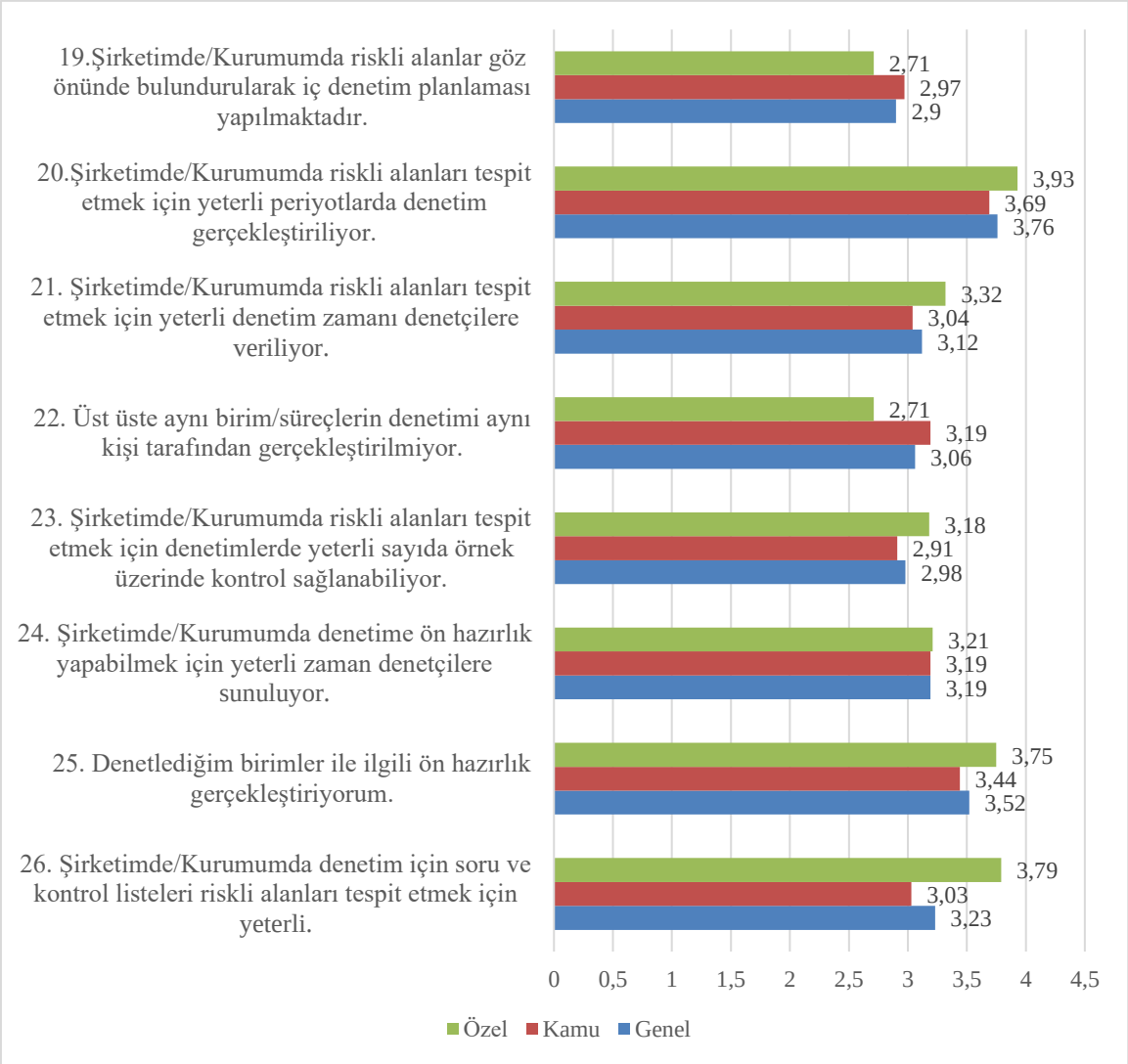
Tetkikçilerin denetimlerde ön hazırlık gerçekleştirmek için yeterli zamanlarının bulunması durumunun ölçüldüğü 24. soru; genel sonuçlara göre 3,19 ortalama ile "Kritik" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 3,19 ortalama ile

“Kritik” bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 3,21 ortalama ile “Kritik” bağıl önem seviyesinde yanıtlanmıştır.

Tetkikçilerin denetimler için ön hazırlık gerçekleştirme durumunun ölçüldüğü 25. soru; genel sonuçlara göre 3,52 ortalama ile “İyi” bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 3,44 ortalama ile “Kritik” bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 3,75 ortalama ile “İyi” bağıl önem seviyesinde yanıtlanmıştır.

Tetkikçilerin denetimde kullanılan kontrol listelerinin yeterliliğine dair görüşlerinin ölçüldüğü 26. soru; genel sonuçlara göre 3,23 ortalama ile “Kritik” bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 3,03 ortalama ile “Kritik” bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 3,79 ortalama ile “İyi” bağıl önem seviyesinde yanıtlanmıştır.

ISO 27001 BGYS tetkikçilerinin denetim planlarının riskli alanlara göre yapılması konusunda görüşünün genel olarak bağıl önem seviyesi “Zayıf” olarak yanıtlandığı gözlemlenmiştir. Özellikle kamuda görev alan tetkikçilerde bu konudaki algı bağıl önem seviyesi yine “Zayıf” düzeydedir. Diğer yandan, tetkikçilerin yeterli periyotlarda denetim gerçekleştirmesi konusunda görüşlerinde genel olarak bağıl önem seviyesinin “İyi” olduğu görülmüştür. Üst üste aynı birim veya süreçlerin aynı kişi veya kişiler tarafından denetlenmesi konusunda ise kamuda ve özel sektördeki tetkikçiler arasında farklı düzeylerde yanıtlar bulunmaktadır. Genel olarak, bu durumun “Kritik” bağıl önem seviyesinde olduğu belirtilmiştir. Tetkikçilerin denetimlerde yeterli sayıda örnek üzerinde kontrol gerçekleştirebilmeleri konusunda ise genel bağıl önem seviyesinin “Zayıf” olduğu görülmektedir. Ancak denetimde kullanılan kontrol listelerinin yeterliliği konusu genel olarak bağıl önem seviyesi ”Kritik” olarak yanıtlanmıştır. Bu sonuçlar, ISO 27001 BGYS denetimlerinde planlama, zaman yönetimi ve denetim süreçlerinin optimize edilmesi gerekliliğini göstermektedir.



Şekil 5.8. Denetim planlaması ve kriterler konu başlıklarındaki soruların yanıt ortalamaları

Bu çalışmanın birinci bölümündeki araştırmanın amacı kısmında "6. İç tetkikçilerin denetim planlamalarının riskli konuların tespiti için yeterli olduğuna dair görüşleri nelerdir?" sorusuna cevap arandığı belirtilmiştir. Şekil 5.8'de denetim planlaması konusunda denetçilerin yanıtları görülmektedir. Bu veriler ışığında tetkikçilerin görüşlerine göre denetim planlamalarında yetersizlikler olabileceği değerlendirilmektedir. Planlamada yaşanabilecek sorunlar mevcut olan uygunsuzluk ve iyileştirilebilir alanların denetim ile tespit edilmemesine sebep olabilecektir. Tespit edilmeyen her bir husus siber güvenlik riski anlamına geldiği değerlendirilmektedir.

Öz (2010) tarafından yapılan çalışmada; denetimlerde görev alan kaynakların sınırlı olması nedeniyle, denetlenebilecek kapsamın önceliklendirilmesi, denetimlerin ve denetimde

kullanılacak kaynakların planlanabilmesi için son derece önemli olduğu sonucuna varılmıştır [100]. Denetim planlamasında önemli/riskli konuların kapsama alınması ve denetimde kullanılan kriterlerin netleştirilmesi açısından risk teşkil edecek durumların çözümü için denetçiler ve denetlenen kuruluş tarafından önlem alınması gerektiği düşünülmektedir.

5.3.5. İyileştirme ve bulgular

ISO 9001 Kalite Yönetim Sistemleri Temel Esaslar, Terimler ve Tarifler standardında iyileştirme "performansı artırmaya yönelik faaliyet", düzeltme "tespit edilmiş, bir uygunsuzluğun ortadan kaldırılması için yapılan faaliyet" ve düzeltici faaliyet "uygunsuzluğun sebebini ortadan kaldırmak ve tekrarını önlemek için yapılan faaliyet" olarak tanımlanmıştır [101]. ISO 27001 BGYS bu çalışmanın 3.4 bölümünde bahsedildiği gibi tespit edilen uygunsuzluklar için uygunsuzluğun sebebini ortadan kaldıran ve tekrarını önleyen düzeltici faaliyetler gerçekleştirilmesini istemektedir. Bu sebeple tespit edilen uygunsuzluğun ilgili birimlere iletilmesi ve tekrar oluşmasını engelleyecek şekilde kök sebebini giderici faaliyetler gerçekleştirilmesi gerekmektedir.

Uygunsuzluklar siber güvenlik zafiyetleri ile ilgili olabileceği gibi, standardın idari süreçleri ile ilgili olabilmektedir. Kök sebebi giderilerek kapatılan uygunsuzlukların, ilgili oldukları konularda iyileştirme sağlaması beklenmektedir. Örnek olarak denetlenen kurum/kuruluşun web sitesinde bir güvenlik açıklığı tespit eden bir tetkikçi bu açıklığın sadece kapatılmasını sağlarsa düzeltme işlemi gerçekleştirmiş olacak, daha sonra benzer açıklıkların çıkması muhtemel olabilecektir. Tespit ettiği bulguyu, eğitim eksikliği, yazılımların devreye alınmadan önce analizlerinin gerçekleştirilmesi veya periyodik güvenlik testleri faaliyetleri gibi kök sebebini giderecek çalışmalar ile kapatılmasını sağladığında ise siber güvenlik risklerini anlamlı şekilde azaltabilecektir. Çizelge 5.5'de konu ile ilgili sorular ve cevap analizi bulunmaktadır.

Çizelge 5.5. Denetim sonuçları ile iyileştirme ve bulgu yönetimine dair sorular ve cevap analizi

Soru No	Soru	Genel			Kamu			Özel Sektör		
		ort	ss	bö	ort	ss	bö	ort	ss	bö
28	Tespit ettiğim bulgular tüm ilgili birimlere iletiyor.	4,06	1,19	Çok İyi	3,93	1,24	İyi	4,39	0,96	Çok İyi
29	Raporladığım bulgular için acil aksiyonlar alınıyor.	3,86	1,25	İyi	3,71	1,26	İyi	4,29	1,15	Çok İyi
30	Raporladığım bulgular kök sebepleri giderilerek tekrar oluşmayacak şekilde kapatılıyor.	2,90	1,38	Zayıf	2,67	1,31	Zayıf	3,54	1,35	İyi
31	Gerçekleştirdiğim denetimler sayesinde denetlenen birimlerin bilgi güvenliği farkındalığı artıyor.	4,05	1,10	Çok İyi	4,08	1,12	Çok İyi	3,96	1,04	İyi
32	Gerçekleştirdiğim denetimler sayesinde siber güvenlik açıklıklar kapatılarak riskli alanlar kapatılıyor.	3,79	1,19	İyi	3,76	1,18	İyi	3,86	1,21	İyi

Çizelge 5.5'de görüldüğü üzere denetim sonucu bulguların ilgili birimlere iletilmesi durumunun ölçüldüğü 28. soru; genel sonuçlara göre 4,06 ortalama ile "Çok iyi" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 3,93 ortalama ile "İyi" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 4,39 ortalama ile "Çok iyi" bağıl önem seviyesinde yanıtlanmıştır.

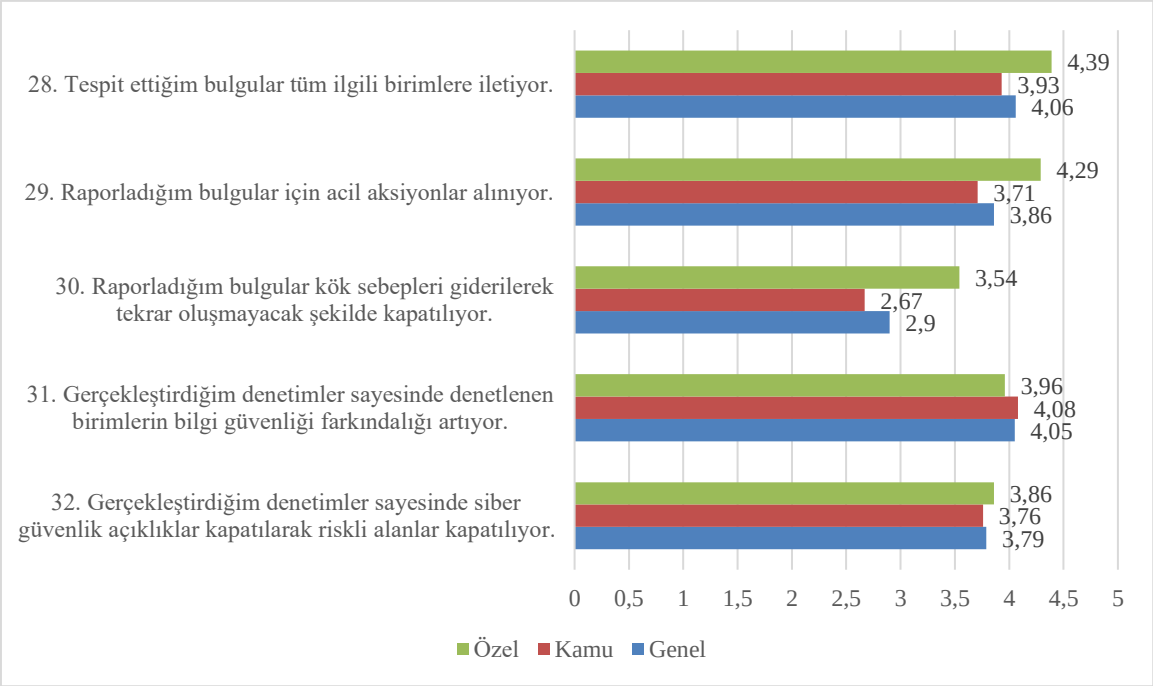
Tetkikçilerin denetim sonucu bulgular ile ilgili acil aksiyonların alındığına dair görüşlerinin ölçüldüğü 29. soru; genel sonuçlara göre 3,86 ortalama ile "İyi" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 3,71 ortalama ile "İyi" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 4,29 ortalama ile "Çok iyi" bağıl önem seviyesinde yanıtlanmıştır.

Tetkikçilerin denetim sonucu raporlanan bulgular ile ilgili kök sebeplerin giderilmesine dair görüşlerinin ölçüldüğü 30. soru; genel sonuçlara göre en düşük 3. değer olarak 2,90 ortalama ile "Zayıf" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 2,67 ortalama ile "Zayıf" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 3,54 ortalama ile "İyi" bağıl önem seviyesinde yanıtlanmıştır.

Tetkikçilerin denetimlerin bilgi güvenliği farkındalığının artmasına etkisi dair görüşlerinin ölçüldüğü 31. soru; genel sonuçlara göre 4,05 ortalama ile "Çok iyi" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 4,08 ortalama ile "Çok iyi" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 3,96 ortalama ile "İyi" bağıl önem seviyesinde yanıtlanmıştır.

Tetkikçilerin denetimlerin siber güvenlik açıklıklarının kapatılmasına etkisi konusunda görüşlerinin ölçüldüğü 32. soru; genel sonuçlara göre 3,79 ortalama ile "İyi" bağıl önem seviyesinde, kamuda görev alan ISO 27001 BGYS tetkikçileri özelinde 3,76 ortalama ile "İyi" bağıl önem seviyesinde, özel sektörde görev alan ISO 27001 BGYS tetkikçileri özelinde 3,86 ortalama ile "İyi" bağıl önem seviyesinde yanıtlanmıştır.

ISO 27001 BGYS tetkikçilerinin denetim sonuçlarının ilgili birimlere iletimi konusunda görüşlerinin genel olarak bağıl önem seviyesi "Çok iyi" olduğu görülmektedir. Denetim sonuçlarına göre acil aksiyonların alınması konusunda da tetkikçi görüşlerinin genel olarak bağıl önem seviyesi "İyi" olduğu; ancak denetim sonuçlarında raporlanan bulguların kök sebeplerinin giderilmesi konusunda yanıtlarda kamuda görev yapan tetkikçilerin "Zayıf" bağıl önem seviyesi ile öne çıkmakta olduğu görülmüştür. Özel sektördeki tetkikçiler ise bu konuda daha olumlu bir değerlendirme yapmıştır. Denetimlerin bilgi güvenliği farkındalığının artmasına etkisi ve siber güvenlik açıklıklarının kapatılmasına etkisi konularında genel olarak olumlu görüşler ifade edilmiştir. Bu sonuçlar, ISO 27001 BGYS denetimlerinde elde edilen bulguların etkili bir şekilde iletilmesi ve bu bulguların kök sebeplerinin giderilmesi için daha fazla çaba gerektiğini göstermektedir.



Şekil 5.9. İyileştirme ve bulgu konu başlıklarındaki soruların yanıt ortalamaları

Bu çalışmanın birinci bölümündeki araştırmanın amacı kısmında "3. İç tetkikçilerin denetim sonrası bulunan uygunsuzlukların raporlanması ve etkin şekilde çözümü için gerçekleştirilen faaliyetler ile ilgili görüşleri nelerdir?" sorusuna cevap arandığı belirtilmiştir. Şekil 5.9'da uygunsuzlukların etkin şekilde çözümü konusunda denetçilerin yanıtları görülmektedir. Tetkikçiler tarafından, denetimde tespit edilen uygunsuzluklar sonrası gerçekleştirilen faaliyetlerin siber güvenlik açıklıklarını kapatmakta olduğu, denetimde ve uygunsuzluklarda görev alan personelin bilgi güvenliği farkındalığını artırmakta olduğu düşünüldüğü görülmektedir. Ancak; tespit edilen uygunsuzlukların kök sebebinin giderilmesi ile ilgili eksiklikler olduğunu düşündükleri değerlendirilmektedir. Risk teşkil edecek bu durumun çözümü için denetçiler ve denetlenen kuruluş tarafından önlem alınması gerektiği düşünülmektedir.

6. SONUÇ, TARTIŞMA ve ÖNERİLER

6.1. Sonuç ve Tartışma

Gün geçtikçe kullanımı artan bilgi ve iletişim teknolojileri, olumlu katkılar sunmakla birlikte; bilgi güvenliği ve siber güvenlik konularında çok sayıda yeni tehdit ve zafiyeti getirmektedir. Söz konusu riskleri önlemek için BGYS standardı kapsamında yapılan çalışmalar önemli görülmesine rağmen, kağıt üzerinde kalan ISO 27001 BGYS belgesi kurum ve kuruluşlara fayda sağlamayacaktır. ISO 27001 çerçevesinde gerçekleştirilen faaliyetlerin, standartta da belirtilen şekilde, periyodik süreler ile iç tetkiklerinin etkin ve doğru şekilde gerçekleştirilmesi bilgi güvenliğinin ve siber güvenliğin sağlanmasında önem arz etmektedir.

Sonuç bölümünde öncelikle yapılan bu çalışmanın bulgularına göre, araştırma konusu hakkındaki sorunları ve eksiklikleri işaret edebilecek ISO 27001 denetimlerinde görev alan iç tetkikçilerin görüşlerini içeren yanıt ortalama değeri 3,00 altındaki ve bağıl önem seviyesi "Zayıf" değerlere sahip konu başlıkları değerlendirilerek vurgulanmıştır. Ayrıca; ISO 27001 BGYS konusunda kamuda görev alan tetkikçiler ile özel sektörde görev alan tetkikçiler arasında anlamlı farklılık gösteren hususlar belirtilmiştir.

Objektif ve bağımsızlık konu başlığında tetkikçilerin denetimlerini gerçekleştirdikleri birim yöneticileri ve/veya üst yöneticilerinin kendi yöneticisi olma durumu genel yanıtlar içerisinde çalışmanın en düşük değeri olan 2,58 ortalama ile, kamuda görev alan tetkikçiler için 2,68 ve özel sektörde görev alan tetkikçiler için 2,32 ortalama ile yanıtlandığı görülmektedir. Tetkikçilerin bir kısmının kendi yöneticisi ve/veya üst yöneticisine bağlı birimleri denetledikleri anlaşılmaktadır. Bu durum objektiflik ve bağımsızlığı direkt bozduğu söylenememekle birlikte tehlikeye atacaktır. Tetkikçinin objektifliğini bozabilecek bu durumda tespit ettiği uygunsuzlukları raporlayamaması ihtimal dahilindedir. Özel sektör tetkikçilerinin kendi çalıştıkları organizasyon içerisinde denetim için görevlendirilme durumlarını 2,64 ortalama ile yanıtladığı görülmekte olup; bu durum objektiflik ve bağımsızlık açısından riske sebep olacaktır.

Sürekli gelişim ve yetkinlik hususunda tetkikçilerin konu ile ilgili düzenli eğitim alması sorusu çalışmanın en düşük 2. değeri olan 2,77 ortalama ile, kamuda görev alan tetkikçiler

için 2,83 ve özel sektörde görev alan tetkikçiler için 2,61 ortalama ile yanıtlandığı görülmektedir. Bu yanıtlarda tetkikçilerin ISO 27001 BGYS denetimi ile ilgili düzenli ve yeterli eğitim almadıklarını düşündükleri anlaşılmaktadır. Eğitim tetkikçilerin gelişimi için tek yöntem olmadığı da kabul edilmekle birlikte; eğitim eksiklikleri denetimlerin etkinliği ve kalitesini etkileyebilecektir. Veri tabanı konusunda denetim gerçekleştiren tetkikçilerin bu konuda teknik bilgiye sahip olma durumu 2,99 ve yazılım geliştirme konusunda denetim gerçekleştiren tetkikçilerin bu konuda teknik bilgiye sahip olma durumu 3,00 genel ortalama ile yanıtlandığı görülmektedir. Teknik konularda denetim gerçekleştiren tetkikçilerin özel uzmanlık gerektiren bu konu başlıklarında teknik bilgilerinin eksik olduğunu düşündükleri anlaşılmaktadır. Bu sonuçlara göre, tetkikçilerin konu ile ilgili teknik bilgisi eksik olduğu durumlarda uygunsuzlukları tespit edememe riski bulunmaktadır. Kamuda görev alan tetkikçilerin denetim gerçekleştirdikleri yazılım geliştirme, network, veri tabanı ve işletim sistemi gibi teknik alanlarda teknik bilgi sahibi olma durumlarını, özel sektör tetkikçilerine göre daha az buldukları görülmüştür. Söz konusu durumlar denetim gerçekleştirilen teknik alanlarda siber güvenlik eksikliklerinin tespit edilmemesi açısından risk teşkil edecektir.

Denetim planlaması konu başlığında, ilgili riskli alanlar göz önüne alınarak denetim planlaması yapılması ile ilgili sorunun 2,90 ortalama ile, kamuda görev alan tetkikçiler için 2,97 ve özel sektörde görev alan tetkikçiler için 2,71 ortalama ile yanıtlandığı görülmektedir. Tetkikçilerin denetim planlamalarında riskli alanların dikkate alınarak denetim kapsamına alınması hususunda eksiklikler olduğunu düşündükleri anlaşılmaktadır. Riskli alanları tespit etmek için denetimlerde yeterli sayıda örnek üzerinden kontrol gerçekleştirilmesi ile ilgili sorunun 2,98 ortalama ile yanıtlandığı görülmektedir. Ayrıca, Tetkikçilerin yeterli örnek üzerinden denetimlerini gerçekleştirmeleri hususunda eksiklikleri olduğunu düşündükleri anlaşılmaktadır. Üst üste aynı birim veya sürecin denetiminin aynı kişi tarafından yapılması ile ilgili sorunun özel sektör için 2,71 ortalama ile yanıtlandığı görülmektedir. Bu sonuçlara göre; tetkikçilerin denetim planlaması veya örneklem seçimi sebebiyle, denetim kapsamında veya seçilen örneklerde olmayan konularda uygunsuzlukları ve siber güvenlik açıklıklarını tespit edememe riski bulunmaktadır.

Denetim sonrası tespit edilen bulguların kök sebeplerinin giderilerek tekrar oluşmayacak şekilde kapatılması ile ilgili sorunun 2,90 ortalama ile, kamuda görev alan tetkikçiler için 2,67 ve özel sektörde görev alan tetkikçiler için 3,54 ortalama ile yanıtlandığı görülmektedir.

Tetkikçilerin bulguların tekrar oluşmayacak şekilde faaliyetler gerçekleştirilerek kapatılmadığını düşündükleri anlaşılmaktadır. Bu sebeple tespit edilen uygunsuzlukların kapatılmasına rağmen tekrarlaması riski bulunmaktadır. Bu riskin kamu kuruluşlarında daha yüksek olduğu görülmektedir. Ayrıca kamuda görev alan tetkikçilerin denetimde kullandıkları soru/kontrol listesinin yeterliliğini daha az buldukları görülmekte olup, bu durum denetimde mevcut olan uygunsuzluk ve siber güvenlik eksikliklerinin denetim sonucu tespit edilememesine sebep olabilecektir.

Literatür araştırmasında, çok sayıda çalışma ISO 27001 standardının çeşitli faydalarını göstermekte; BGYS denetimlerinin yürütülmesinin, yönetim sisteminin sürekli ve etkin bir şekilde denetlenmesinin önemini vurgulamaktadır. Siber güvenlikle ilgili araştırmalar ve küresel raporlar, siber güvenliğin önemli bir endişe kaynağı olduğunu ve iç denetimlerin siber güvenlik önlemlerinin korunmasında çok önemli bir rol oynadığını göstermektedir. Denetimlerin etkinliği için denetim kaynakları, denetçilerin teknik yetkinlikleri, bağımsızlıkları ve objektiflikleri gibi kriterler öne çıkarılarak, bu hususların gelecekteki araştırma konuları arasında yer alması gerektiği vurgulanmıştır.

Bilgi ve iletişim teknolojilerinin artan kullanımı, bilgi güvenliği ve siber güvenlik alanlarında yeni tehdit ve zafiyetler ortaya çıkarmaktadır. Bu riskleri önlemek için BGYS standardı kapsamında yapılan çalışmalar önemli olmakla birlikte, standardın öngördüğü periyodik ve etkin iç denetimler, bilgi ve siber güvenliğin sağlanmasında kritik bir rol oynamaktadır. Yapılan çalışma, iç tetkikçilerin bağımsızlık ve objektifliği, tetkikçilerin sürekli gelişimi ve yetkinliği, denetimlerin planlaması ve bulguların kapatılması gibi alanlarda çeşitli eksiklikler olduğunu göstermektedir. Bu bulgular, ISO 27001 BGYS iç denetim süreçlerinin daha etkin ve doğru bir şekilde gerçekleştirilmesi gerektiğine işaret etmektedir.

Al-Karaki, Gawenmeh ve El-Yassami (2022) tarafından yayınlanan akıllı denetim ve sıralama kullanarak bir kuruluş bilgi sisteminin genel güvenlik duruşunun pratik durumu üzerine yapılan çalışmada; kuruluşların denetimleri etkin bir şekilde yürütecek vasıflı personel eksikliği nedeniyle zorluklarla karşılaşabileceği vurgulanmıştır [19]. Razikin ve Soewito (2022) tarafından yapılan risk analizi ve siber güvenlik çerçevesine dayalı karar destek modeli konulu çalışmada; kuruluşların ekipleri içinde siber güvenlik ve denetim süreçleriyle ilgili beceri boşluklarıyla karşılaşabilecekleri, denetimlerini gerçekleştirmek

için zaman ve personel gibi yeterli kaynakların tahsis edilmesinde zorluklar yaşayabilecekleri vurgulanmıştır [22]. Idayani, Nadlifatin, Subriadi, Janice ve Gumasing (2024) tarafından yayınlanan fintech kullanımı üzerine siber risklerin incelemesi konulu araştırmada; denetim sürecinin karmaşıklığı ve kaynak yoğunluğunun, kuruluşlar için zorluklar oluşturabileceği ve önemli ölçüde zaman, çaba ve uzmanlık gerektirdiği vurgulanmıştır [23]. İlgili çalışmalara paralel olarak araştırmamızda denetçilerin yetkinliği ile ilgili riskler bulunduğu ortaya koyulmuştur. Yetkin personeller tarafından denetimlerin gerçekleştirilmesi amacıyla öneriler sunulmakla birlikte bu önerilerin gerçekleştirilmesi için kuruluşların yönetimleri tarafından gerekli kaynağın sağlanması önem arz etmektedir.

Michalec, Shreeve ve Rashid (2023) geleceğin enerji sistemlerinde siber güvenlik vizyonu konulu araştırmada; hem personel hem de teknoloji açısından kaynak eksikliğinin, kuruluşların kapsamlı denetimler yapmasını zorlaştırabileceği vurgulanmıştır [24]. Denetimlerin planlanmasına riskli alanların dahil edilmesi ile ilgili yaşanan sorunlar bu çalışmanın sonuç bölümünde benzer olarak belirtilmiş olup kaynak eksiklikleri planlama konusunda yaşanacak sorunları doğrudan etkileyecektir. Yeterli kaynak olmaması durumunda riskli alanların denetim planına alınması zorlaşacaktır. Bu problemlerin çözümü için kuruluşların yönetimi tarafından gerekli kaynağın sağlanması önem arz etmektedir.

Durst, Hinteregger ve Zieba (2024) tarafından çevresel durumun siber güvenlik risk yönetimi ve organizasyonel dayanıklılık üzerindeki etkisi konulu çalışmada; kuruluşlardaki sınırlı kaynaklar ve uzmanlığın, ISO 27001 denetimlerinin başarılı bir şekilde yürütülmesini engelleyebileceği ve siber güvenlik önlemlerine ilişkin değerlendirmelerin derinliğini ve doğruluğunu etkileyebileceği vurgulanmıştır [25]. Araştırmamız sonucunda bu görüşe paralel olarak bulguların kök sebebi giderilerek kapatılması konusunda riskler bulunduğu raporlanmış olup; kaynak ve uzmanlık alanında eksikliklerin, tespit edilen uygunsuzlukların tekrar oluşmayacak şekilde kapatılmasını etkileyebileceği değerlendirilmektedir.

Slapničar, Vuko, Čular ve Drašček (2022) tarafından yapılan siber güvenlik denetiminin etkinliği konulu çalışmada; siber güvenlik denetim süreçlerinde çeşitli yöntemlerin kullanılması nedeniyle kanıt toplama kapsamının zorlayıcı olabileceği vurgulanmıştır [20]. Araştırmamız sonuç bölümünde benzer şekilde belirtilen denetim süreçlerinde yeterli örnek üzerinden kontrollerin gerçekleştirilmesinde riskler olduğu görüşü bulunmaktadır. Yeterli

örneklem kullanımı denetimlerdeki tespitlerin gözden kaçmasını engelleyebilmekle birlikte kaynak kullanımı açısından zorlayıcı olabilecektir.

Antunes, Maximiano ve Gomes (2022) tarafından bilgi güvenliği ve siber güvenlik denetiminin standartlara uygunluğunu yönetmek için özelleştirilebilir bir web platformu konusunda yapılan çalışmada; ISO 27001 denetim süreci ile ilişkin standardın katı olması ve denetim sürecinde fazla esnekliğe izin vermemesi sebebiyle farklı kurumsal ihtiyaçlara dayalı özelleştirmeyi sınırlandırdığı vurgulanmıştır [18]. Çalışmamızın öneriler bölümünde ISO 27001 denetim süreçleri ile ilgili bu sınırlılıklardan kaynaklı problemler için önerilerde bulunulmuştur. Orta ve büyük ölçekli kuruluşlarda bu önerilerin uygulanması için ISO 27001 iç tetkik sürecine dair kurallara eklemeler yapılması ve uygulanmasının zorunlu tutulmasının denetim sürecinin etkin yürütülmesi amacıyla özelleştirilmesini sağlayacağı değerlendirilmektedir.

Havelka ve Merhout (2013) tarafından bilgi teknolojileri denetim süreci hakkında yapılan çalışmada; bilgi teknolojisi denetim sürecini iyileştirmek için denetimlerin etkinlik, verimlilik ve kalite ile olan ilişkileri gelecekteki araştırma alanları olduğu sonucuna varılmıştır [31]. Çalışmamızda benzer olarak bu konuda tetkikçilerin gerçekleştirdikleri denetimlerin etkinliği, verimliliği ve kalitesi ile ilgili eksiklikler olduğunu düşündükleri görülmektedir.

Flora ve Rai (2015) tarafından yapılan çalışmada; iç denetçilerin siber güvenlik risklerinin uygun şekilde ele alınmasını sağlamak için organizasyonda tamamlayıcı bir rol oynamaları gerektiği; iç denetimin kuruluşun bilgi güvenliği programının etkili ve verimli olmasını sağlamada önemli bir rolü olduğu, iç denetimin kurumun risk toleransına dayalı olarak riski azaltmak için uygun kontrollere sahip olduğu konusunda güvence sağlayarak kuruma yardımcı olabileceği belirtilmektedir [32]. Çalışmamızda tetkikçilerin denetim süreçlerindeki eksiklikler ilgili düşünceleri sebebiyle, bu durumun iç denetimin rolünü etkileyebileceği, denetimlerin önemini riske atabileceği ve uygun kontrollere sahip olduğu konusunda sağladığı güvenceyi etkileyebileceği değerlendirilmektedir.

Steinbart, Raschke, Gal ve Dilla (2012) tarafından yapılan iç denetimler ve bilgi güvenliği hakkında ilişkiyi inceleyen çalışmada denetçi bağımsızlığı, denetçi nitelikleri, bilgi ve becerileri gibi çeşitli iç denetim kalitesi ölçütleri hakkında bilgi toplayamadıkları ve

durumun iç denetim ve bilgi güvenliği fonksiyonları arasındaki ilişkinin kalitesini önemli ölçüde etkilemesi muhtemel olduğu belirtilmektedir [44]. Çalışmamızda paralel olarak denetçi bağımsızlığı, denetçi nitelikleri, denetçi bilgi ve becerileri gibi çeşitli konularda tetkikçilerin denetim süreçlerinde ve kendilerinde eksiklikler gördükleri bu durumun da denetim sonuçlarını etkileyebileceği değerlendirilmiştir.

Bilgi güvenliği ve siber güvenlik denetimleri üzerine yapılan çeşitli çalışmalarda, denetimlerin etkin bir şekilde yürütülmesi için vasıflı personel eksikliği, kaynak yetersizliği ve zaman yoğunluğu gibi zorluklarla karşılaşılabileceği belirtilmektedir. Ayrıca, denetimlerde yeterli örneklem kullanımı ve planlama konusunda da sorunları vurgulamaktadır. Bu konular, denetimlerin etkinliğini ve dolayısıyla siber güvenliğin sağlanmasını olumsuz etkileyebilecektir. Bu durum kuruluşların denetim süreçlerini daha verimli hale getirmek için gerekli kaynak ve uzmanlığı sağlamalarının önemini de ortaya koymaktadır.

Bu araştırmada veri toplama aracılığıyla ISO 27001 BGYS ile ilgili görev alan tetkikçilerin görüşleri alınmıştır. Objektiflik/bağımsızlık, raporlama, sürekli gelişim/yetkinlik, denetim planlaması/kriterler ve iyileştirme/bulgular konu kategorilerinde gruplanan ve değerlendirilen sonuçlar içerisinde denetim süreçlerinin etkinliğini, kalitesini ve verimliliğini etkileyebilecek sonuçlar üzerinde durulmuştur. Çalışmanın içerisinde belirtildiği üzere denetim süreçlerinin etkinliği, kalitesi ve verimliliği kuruluşların siber güvenliğini doğrudan etkilemektedir. Tetkikçilerin görüşlerindeki sonuçlara göre tetkikçilerin kendi yöneticilerinin sorumluluğunda olan birimlerde görevlendirildikleri; tetkikçilerin denetim süreçleri ile ilgili düzenli eğitim almadıkları; yazılım geliştirme ve veritabanı gibi teknik konularda denetim gerçekleştiren tetkikçilerin teknik bilgilerinde eksiklikler olduğu; denetim planlamalarında riskli konuların tam olarak göz önünde bulundurulmadığı; denetimlerde yeterli sayıda örnek üzerinden kontrol sağlanamadığı; tespit edilen uygunsuzlukların kök sebebi giderilerek tekrar oluşmayacak şekilde tam olarak kapatılamadığı değerlendirilmektedir.

Sonuç olarak bu çalışmada bulgular değerlendirildiğinde, tetkikçilerin sürekli gelişimleri ve yetkinlikleri, denetimlerin objektiflik ve bağımsızlığı, denetimlerin planlaması ve denetim bulgularının yönetimi konularında eksiklikler olduğunu düşündükleri görülmektedir. Söz konusu eksiklikler bu çalışmanın bulgular bölümünde de örnekleri verilen siber olayların

yaşanmasına, gerçekleştirilen denetimlerde siber güvenlik zafiyetlerinin tespit edilememesine, tespit edilse dahi raporlanamamasına ve raporlanan bulguların ise tekrar oluşmayacak şekilde kapatılmamasına sebep olabileceği sonucuna varılmıştır.

BGYS iç tetkik sürecindeki olabilecek söz konusu risklerin azaltılması amacıyla, bu çalışmanın öneriler bölümünde 2022 yılında yayınlanmış Bilgi ve İletişim Güvenliği Denetim Rehberi, 2020 yılında yayınlanmış Bilgi ve İletişim Güvenliği Rehberi ve uluslararası ISO 31010 Risk Yönetimi - Risk Değerlendirme Teknikleri standardında bulunan esasların uygulanması ile ilgili öneriler sunulmuştur. Bu önerilerin uygulanması için kuruluşların yönetimi tarafından gerekli kaynağın ve desteğin sağlanması gerekmektedir.

6.2. Öneriler

Sonuç ve tartışma bölümünde belirtilen ISO 27001 denetimlerinde yaşanması muhtemel bu sorunların çözümü için genel olarak Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı (CBDDO) koordinasyonu ile hazırlanan Bilgi ve İletişim Güvenliği Rehberi'nde ve bu rehber için denetim çalışmalarının belirli bir metodolojide gerçekleştirilmesi amacıyla yayınlanan Bilgi ve İletişim Güvenliği Denetimi Rehberinde bulunan esaslardan yararlanılması önerilmektedir. Bu çalışmanın içerisinde söz konusu rehberlerle ilgili bilgi sunulmuştur.

Aşağıdaki konu başlıklarında, ilgili rehber, doküman ve standartlarda bulunan esasların kuruluşların iç tetkik süreçlerinde uygulanmasının zorunlu tutulması ve bu esasların uygulamasının kontrolünün yapılması, mevcut sorunların çözümüne öneri olarak sunulmaktadır.

<u>Objektiflik ve bağımsızlık</u>

Objektiflik ve bağımsızlık konuları ve denetim sürecinde örneklem seçimi ile ilgili; Bilgi ve İletişim Güvenliği Denetimi Rehberinin "3.2.3.1 Etkinlik Değerlendirmede Örneklem Seçimi" bölümünde tanımlı kuralların uygulanması, denetim planlamasında Bilgi ve İletişim Güvenliği Denetimi Rehberinin "EK - J: Tarafsızlık Taahhütnamesi Örneği" dokümanında bulunan görevlendirilen tetkikçilerin kendi çalıştıkları birimlerde ve yöneticisi/üst yöneticisi

aynı olan birimlerde görevlendirilmemeleri gibi kuralların belirlenmesi ve uygulanması önerilir [93].

Denetim kriterleri

Denetim kriterleri konu başlığı ile ilgili olarak Bilgi ve İletişim Güvenliği Rehberi içerisinde farklı konu başlıklarında 661 tedbir maddesi ile ilgili denetim soru önerisi ve denetim yöntem önerisi bulunmaktadır. Bu 661 tedbir ile ISO 27001 BGYS eşleştirme çalışması Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından gerçekleştirilmiş ve internet sitelerinde yayınlanmıştır. Denetimlerde kriter olarak bu soruların kullanılmasına dair kuralların belirlenmesi ve uygulanması önerilir [102].

Denetçi yetkinliği

Yetkinlik konu başlığında Bilgi ve İletişim Güvenliği Denetimi Rehberinin "3.1.1. Denetim Ekibinin Belirlenmesi" bölümündeki denetim ekibi üyelerinin sahip olması beklenen sertifikalara dair esasların ve özel uzmanlık gerektiren alanlarda tetkikçi harici uzman tecrübesinden yararlanılması gibi kuralların belirlenmesi ve uygulanması önerilir [93].

Denetim planlama ve örneklem seçimi

Planlama konu başlığı ile ilgili Bilgi ve İletişim Güvenliği Denetimi Rehberinin "3.1.3 Denetim Kapsamının Belirlenmesi" bölümünde "Risk değerlendirme sürecinde varlık grubunun gizliliği, bütünlüğü, erişilebilirliği ile etki alanları (bağımlı varlıklar, etkilenen kişi sayısı, kurumsal ve toplumsal sonuçlar, sektörel etki) dikkate alınmalıdır." gibi esaslara dair kuralların belirlenmesi ve uygulanması önerilir [93].

Örneklem seçimi ile ilgili Bilgi ve İletişim Güvenliği Denetimi Rehberinin "3.2.3.1 Etkinlik Değerlendirmede Örneklem Seçimi" bölümünde belirtilen kontrolün sıklığına bağlı örneklem büyüklüğü tablosundan faydalanılması, bu esaslara dair kuralların belirlenmesi ve uygulanması önerilir [93].

Denetim bulguları sonrası iyileştirme

İyileştirme konu başlığı ile ilgili olarak denetim süreçlerinde yazılan tüm uygunsuzluklar ile ilgili olarak ISO 31010 Risk Yönetimi - Risk değerlendirme teknikleri standardında bulunan kök neden analizi konu başlığında tanımlı esaslar çerçevesinde kuralların belirlenmesi ve uygulanması önerilir [103].

ISO 27001 denetimlerinde yaşanan sorunların çözümü için genel olarak Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı (CBDDO) tarafından hazırlanan Bilgi ve İletişim Güvenliği Rehberi ve Bilgi ve İletişim Güvenliği Denetimi Rehberi'nde bulunan esasların uygulanması önerilmektedir. Bu rehberlerin objektiflik ve bağımsızlık, denetim kriterleri, denetçi yetkinliği, denetim planlama gibi konularda belirlediği kuralların iç tetkik süreçlerinde zorunlu tutulması, mevcut sorunların çözümüne yardımcı olacaktır. Bu önerilerin küçük ölçekli işletmelerde uygulanması maliyetli olacağı değerlendirilmekle birlikte orta ve büyük ölçekli işletme/kuruluşlarda uygulanması için ISO 27001 iç tetkik sürecine dair kurallara eklenmesi ve uygulanmasının zorunlu tutulmasının denetim sürecinin etkin yürütülmesi ve bunun sonucu olarak kuruluşlarda siber güvenlik olgunluk seviyelerinin artmasına faydalı olacaktır.

KAYNAKLAR

1. İnternet: Digital 2024: Global Digital Overview. *DataReportal*. URL: https://datareportal.com/reports/digital-2024-global-overview-report, Son Erişim Tarihi: 12.02.2024.

2. İnternet: Risk in Focus Europe 2022. *IIA*. URL: https://www.eciia.eu/2021/09/risk-in-focus-2022-hot-topics-for-internal-auditors/, Son Erişim Tarihi: 12.02.2024.

3. İnternet: Risk in Focus Europe 2023. *IIA*. URL: https://www.eciia.eu/2022/09/risk-in-focus-2023-more-risky-uncertain-and-volatile-times-ahead/, Son Erişim Tarihi: 12.02.2024.

4. İnternet: Risk in Focus Europe 2024. *IIA*. URL: https://www.eciia.eu/wp-content/uploads/2023/09/CIIA-Risk-in-Focus-2024_final-web.pdf, Son Erişim Tarihi: 12.02.2024.

5. İnternet: 09. ISO Survey of certifications to management system standards - Full results. *ISO*. URL: https://www.iso.org/committee/54998.html?t=KomURwikWDLiuB1P1c7SjLMLEAgXOA7emZHKGWyn8f3KQUTU3m287NxnpA3DIuxm&view=documents#section-isodocuments-top, Son Erişim Tarihi: 12.02.2024.

6. İnternet: Siberay Sözlük. *Siber Suçlarla Mücadele Daire Başkanlığı*. URL: https://www.siberay.com/kurumlar/Siberay.com/SIBERAY-Sozluk.pdf, Son Erişim Tarihi: 12.02.2024.

7. Podrecca, M., Culot, G., Nassimbeni, G., Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, 142,

8. Shareef, M., Alkhazaali, M. (2023). The Security Issues in The Analysis of Information Management Systems. *Journal of Scientific Reports*, 5, 55-60.

9. Bolek, V., Romanová, A., Korček, F. (2023). The Information Security Management Systems in E-Business. *Journal of Global Information Management*, 31(1), 1-29.

10. Podrecca, M., Sartor, M. (2023). Forecasting the diffusion of ISO/IEC 27001: a Grey model approach. *The Tqm Journal*, 35(9), 123-151.

11. Kitsios, F., Chatzidimitriou, E., Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability*, 15, 5828.

12. Gazdağı, O., Çetinyokuş, T. (2020). Bankacılık Sektöründe Bilgi Güvenliği ve İş Sürekliğinin Sağlanması Amacıyla ISO/IEC 27001 ve ISO 22301 Standartlarının Uygulanmasına Yönelik Kavramsal İnceleme. *Journal of Humanities and Tourism Research*, 10(2), 475-491.

13. Yılmaz, H. (2014). TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi. *Kidder Denetişim,* 14(15), 45-59.

14. Marttin, V., Pehlivan, İ. (2010). ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme. *Mühendislik Bilimleri ve Tasarım Dergisi*, 1(1) 49-56.

15. Tarakçı, E., Gönül, A. M. (2023). Yönetim Sistemlerinde Siber Güvenlik için Risk Analizi ve Değerlendirme Çerçevesi. *OHS ACADEMY İş Sağlığı ve Güvenliği Akademi Dergisi,* 6(3). 165-172.

16. Durdu, A. Eren, A. (2021). ISO 27001 Bilgi Güvenliği Yönetim Sistemi Yazılım Tasarımı. *Bilişim Teknolojileri Dergisi,* 14(3), 255-265.

17. Çam, H., Aslay, F., Özen, Ü. (2019). Yükseköğretim Kurumlarında Bilgi Güvenliği Farkındalık Düzeylerinin Ölçümlenmesi. *Yönetim Bilişim Sistemleri Dergisi*, 5(2), 1-11.

18. Antunes, M., Maximiano, M., Gomes, R. (2022). A Customizable Web Platform to Manage Standards Compliance of Information Security and Cybersecurity Auditing, *Procedia Computer Science,* 196, 36-43.

19. Al-Karaki, J. N., Gawanmeh, A., El-Yassami, S., (2022). GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking, *Journal of King Saud University - Computer and Information Sciences*, 34(6), 3079-3095.

20. Slapničar, S., Vuko, T., Čular, M., Drašček, M. (2022). Effectiveness of cybersecurity audit, *International Journal of Accounting Information Systems,* 44,

21. McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models, *Computers & Security*, 144,

22. Razikin, K., Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework, *Egyptian Informatics Journal*, 23(3), 383-404.

23. Idayani, R. W., Nadlifatin, R., Subriadi, A. P. Gumasing, M. J. J. (2024). A Comprehensive Review on How Cyber Risk Will Affect the Use of Fintech, *Procedia Computer Science,* 234, 1356-1363.

24. Michalec, O., Shreeve, B., Rashid, A. (2023). Who will keep the lights on? Expertise and inclusion in cyber security visions of future energy systems, *Energy Research & Social Science*, 106,

25. Durst, S., Hinteregger, C., Zieba, M. (2024). The effect of environmental turbulence on cyber security risk management and organizational resilience, *Computers & Security*, 137,

26. Patterson, C. M., Nurse, J. R. C., Franqueira, V. N L. (2024). "I don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents, *Computers & Security*, 139,

27. Aktaş, K. (2020). *ISO 27001 Bilgi Güvenliği Yönetim Sistemi: Erişim Kontrol Politikası üzerine bir inceleme*, Yayımlanmamış Yüksek Lisans Tezi, Doğuş Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı, İstanbul.

28. Eulerich, M., Masli, A., Pickerd, C., Wood, D. A. (2023). The Impact of Audit Technology on Audit Task Outcomes: Evidence for Technology-Based Audit Techniques, *Contemporary Accounting*, 40(2), 981-1012.

29. Dumont, F., Jemai, S., Xu, Z., Felan, P. M., Farges, G. (2018). Sécurité de l'information:autodiagnostic selon l'ISO/IEC 27001. *IRBM News*, 2018, 39, 4-5.

30. Fidancı, Ö. Ş. (2022). *Kurumlar İçin Bilgi Güvenliği Yönetim Sisteminin Oluşturulması*, Yayımlanmamış Yüksek Lisans Tezi, KTO Karatay Üniversitesi Adli Bilişim Mühendisliği Anabilim Dalı, Konya.

31. 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.

32. Flora, P. E., Rai, S. (2015). Navigating Technology's top 10 Risks: Internal Audit's role. *The Institute of Internal Auditors Research Foundation*, Altamonte Springs,

33. İnternet: Risk in Focus Global 2024. *IIA*. URL: https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/risk-in-focus/risk-in-focus-survey-results-global-summary-2024.pdf, Son Erişim Tarihi: 12.02.2024.

34. İnternet: 2022 İç Denetimin Nabzı, Kuzey Amerika (Mart 2022). *IIA*. URL: https://www.theiia.org/en/content/research/pulse-of-internal-audit/2022/2022-north-american-pulse-of-internal-audit/, Son Erişim Tarihi: 12.02.2024.

35. İnternet: Morgan, S. 2022 Siber Güvenlik Yıllık Yayını: 100 Olgu, Rakamsal Veri, Kestirim ve İstatistiksel Veri (19 Ocak 2022). *Cybersecurity Ventures, Cisco*. URL: https://cybersecurityventures.com/cybersecurity-almanac-2022/, Son Erişim Tarihi: 12.02.2024.

36. İnternet: Küresel Bakış Açıları ve Anlayışlar 2022 Yılında Siber Güvenlik (Ağustos 2022). *IIA*. URL: https://www.tide.org.tr/file/documents/pdf/GPI_Cybersecurity_in_2022_Parts_1_3_Turkish.pdf, Son Erişim Tarihi: 12.02.2024.

37. İnternet: Küresel bakış açıları ve anlayışlar: siber güvenlik 2023. *IIA*. URL: https://www.tide.org.tr/file/documents/pdf/Q4_2023_GPI_Cybersecurity_Turkish.pdf. Son Erişim Tarihi: 12.02.2024.

38. Kohnke, A., Shoemaker, D., Sigler, K. E. (2016). The Complete Guide to Cybersecurity Risks and Controls. CRC Press, 9

39. Vitali, S., Giuliani, M. (2024). Emerging digital technologies and auditing firms: Opportunities and challenges, *International Journal of Accounting Information Systems,* 53,

40. Almaqtari, F. A., Farhan, N. H. S., Al-Hattami, H. M., Elsheikh, T., Al-dalaien B. O. A. (2024). The impact of artificial intelligence on information audit usage: Evidence from developing countries, Journal of Open Innovation: Technology, Market, and Complexity, 10(2).

41. Yıldız, A. (2021). İç Denetimin Uluslararası Mesleki Uygulama Çerçevesine Uyumu ve Etkinliği: Bakanlıklar Üzerinde Bir Araştırma, Yayımlanmamış Yüksek Lisans Tezi, Sakarya Üniversitesi İşletme Anabilim Dalı, Sakarya.

42. İnternet: Siber Güvenlik ve İç Denetimin Rolü - Acil Eylem Çağrısı 2017. *Deloitte Development LLC.* URL: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-cyber-ia-urgent-call-to-action.pdf, Son Erişim Tarihi: 12.02.2024.

43. Héroux, S., Fortin, A. (2013). The internal audit function in information technology: A holistic perspective. Journal of Information Systems, 27(1), 189-217.

44. Steinbart, PJ., Raschke, R. L., Gal, G., Dilla, W. N. (2012). The influence of a good relationship between the internal audit and information security functions on information security outcomes. International Journal of Accounting Information Systems, 13(3), 228-243.

45. İnternet: TDK(Türk Dil Kurumu) Sözlüğü. *TDK*. URL: https://sozluk.gov.tr/, Son Erişim Tarihi: 12.02.2024.

46. Gökçen, H. (2011). *Yönetim Bilgi / Bilişim Sistemleri: Analiz ve Tasarım* (İkinci Baskı). Ankara: Afşar Matbaacılık, 20

47. İnternet: Digital 2020: Global Dıgıtal Overview. *DataReportal*. URL: https://datareportal.com/reports/digital-2020-global-digital-overview, Son Erişim Tarihi: 12.02.2024.

48. Nazarov, A., Nazarov. D., Kovtun, D. (2021). Information security of territorial stability. 3S Web of Conferences, 291, 03018.

49. Somepalli, S. H., Tangella, S. K. R., Yalamanchili, S. (2020). Information Security Management. *HOLISTICA – Journal of Business and Public Administration,* 11(2), 1-16.

50. Canbek, G., Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, 9(3), 165-174.

51. Solms, B. (2006). Information Security - The Fourt Wave. *Computers & Security*, 25(3), 166-167.

52. Baykara, M., Daş, R., Karadoğan, İ. (2013). Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. *1st International Symposium on Digital Forensics and Security*, 20-21 May 2013, Elazığ, Turkey, 1(1)

53. Galinkin, E. (2021). Information Security Games: A Survey. *arXiv: Cryptography and Security*, 2103

54. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). ISO/IEC 27001 (2006). ISO/IEC:27001 Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler.

55. Paolini, A., Scardaci, D., Liampotis, N., Spinoso, V., Grenier, B., Chen, Y. (2020). Authentication, Authorization, and Accounting. *Towards Interoperable Research Infrastructures for Environmental and Earth Sciences*, 12003, Springer Cham, 247-271.

56. Soares, A. A. Z., Lopes, Y., Passos, D., Fernandes N.C., Muchaluat-Saade, D. C. (2021). 3AS: Authentication, Authorization, and Accountability for SDN-Based Smart Grids. *IEEE Access*, 9,

57. Divya, K. S., Roopashree, H. R., Yogeesh A. C. (2022). Non-Repudiation-based Network Security System using Multiparty Computation. *International Journal of Advanced Computer Science and Applications(IJACSA)*, 13(3)

58. İnternet: CVE-2014-6271 Detail. *NIST(National Institute of Standards and Technology)*. URL: https://nvd.nist.gov/vuln/detail/cve-2014-6271, Son Erişim Tarihi: 12.02.2024.

59. İnternet: CVE-2014-6332 Detail. *NIST(National Institute of Standards and Technology)*. URL: https://nvd.nist.gov/vuln/detail/CVE-2014-6321, Son Erişim Tarihi: 12.02.2024.

60. Paliwal, M. (2023). A review on cyber security. *AIP Conf. Proc*. 27 February 2023; 2427 (1)

61. Taherdoost, H. (2022). Cybersecurity vs. Information Security, *Procedia Computer Science*, 215, 483-487.

62. Bagó, P. (2023). Cyber security and artificial intelligence. *Economy & finance*, 10, 189-212.

63. Pour, M. S., Nader, C., Friday, K., Bou-Harb, E. (2023). A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security, *Computers & Security*, 128,

64. Hasan, M. K., Habib, A. K. M. A., Islam, S., Safie, N., Abdullah, S. N. H. S., Pandey. B. (2023). DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments, *Energy Reports*, 9(10), 1318-1326.

65. İnternet: Bilgi Teknolojileri Kurumu siber güvenlik mevzuatı. *BTK*. URL:https://www.btk.gov.tr/siber-guvenlik-mevzuat, Son Erişim Tarihi: 01.07.2024.

66. İnternet: Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi (Kararname Numarası: 1) (2018, 10 Temmuz). Resmi Gazete (Sayı: 30474). URL: https://www.resmigazete.gov.tr/eskiler/2018/07/20180710-1.pdf, Son Erişim Tarihi: 01.07.2024.

67. İnternet: Bilgi Teknolojileri Kurumu Siber Güvenlik Genel Bilgiler. *BTK*. URL:https://www.btk.gov.tr/siber-guvenlik-genel-bilgi, Son Erişim Tarihi: 01.07.2024.

68. İnternet: Cooperative Cyber Defence Centre of Excellence Locked Shields. *CDCOE*. URL:https://ccdcoe.org/locked-shields/, Son Erişim Tarihi: 01.07.2024.

69. İnternet: Kilitli Kalkan-2023 (Locked Shields-2023) Tatbikatı. *MSB*. URL: https://www.msb.gov.tr/Basin-ve-Yayin/Aciklamalar/985842bda91d49b7986792203ca5a602, Son Erişim Tarihi: 01.07.2024.

70. Seker, E. (2018). The concept of cyber defence exercises (cdx): Planning, execution, evaluation, *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1-9

71. Azinheira, B., Antunes, M., Maximiano, M. Gomes, R. (2023). A methodology for mapping cybersecurity standards into governance guidelines for SME in Portugal, *Procedia Computer Science*, 219, 121-128.

72. Stoica, L. A., Candoi-Savu, R. A. (2020). Math approach of implementing ISO 27001. *Proceedings of the International Conference on Business Excellence.* 14(1), 521-530.

73. Singgrit, P., Pamuji, G.C. (2020). The Use of ISO 27001 Framework for Government's Online E-Monitoring System Implementation. *International Journal of Education, Information Technology, and Others*, 3 (3),

74. Ersoy, E. V. (2012). *ISO/IEC 27001 Bilgi Güvenliği Standardı Tanımlar ve Örnek Uygulamalar (Birinci Baskı)*. Ankara: ODTÜ Yayıncılık, 8.

75. Calder, A., Watkins, S. (2008). Calder, A., Watkins, S. (2008). *IT Governance: A Managers Guide to Data Security and ISO 27001/ISO 27002 (4th edition).* Kogan page, 33.

76. Vural, Y., Sağıroğlu, Ş. (2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. *Journal of the Faculty of Engineering and Architecture of Gazi University*, 23(2), 507-522.

77. Ersoy, E. V. (2012). *ISO/IEC 27001 Bilgi Güvenliği Standardı* (Birinci Baskı). ODTÜ Yayıncılık, Ankara, 14.

78. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). ISO/IEC 27001 (2022). ISO/IEC:27001 Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler.

79. İnternet: ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection Information security controls. (2022). *ISO*. URL: https://www.iso.org/standard/75652.html, Son Erişim Tarihi: 12.02.2024.

80. İnternet: ISO/IEC 27004:2016 Information technology Security techniques Information security management. (2016), *ISO*. URL: https://www.iso.org/standard/64120.html, Son Erişim Tarihi: 12.02.2024.

81. İnternet: ISO/IEC TS 27006-2:2021 Requirements for bodies providing audit and certification of information security management systems. (2021). *ISO*. URL: https://www.iso.org/standard/71676.html, Son Erişim Tarihi: 12.02.2024.

82. İnternet: ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection Guidelines for information security management systems auditing. (2020). *ISO*. URL: https://www.iso.org/standard/77802.html, Son Erişim Tarihi: 12.02.2024.

83. İnternet: ISO/IEC 27013:2021 Information security, cybersecurity and privacy protection Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1. (2021). ISO. URL: https://www.iso.org/standard/78752.html, Son Erişim Tarihi: 12.02.2024.

84. İnternet: Elektronik haberleşme sektöründe şebeke ve bilgi güvenliği yönetmeliği (2014, 13 Temmuz). Resmi Gazete (Sayı: 29059). URL: https://www.resmigazete.gov.tr/eskiler/2014/07/20140713-4.htm, Son Erişim Tarihi: 12.02.2024.

85. İnternet: Elektrik Piyasası Lisans Yönetmeliği (2013, 02 Kasım). Resmi Gazete (Sayı: 28809). URL: https://www.mevzuat.gov.tr/MevzuatMetin/yonetmelik/7.5.18985.pdf, Son Erişim Tarihi: 12.02.2024.

86. İnternet: Kamunet Ağına Bağlanma ve Kamunet Ağının Denetimine İlişkin Usul Ve Esaslar Hakkında Tebliğ (2017, 21 Haziran). Resmi Gazete (Sayı: 30103). URL: https://www.resmigazete.gov.tr/eskiler/2017/06/20170621-15.htm, Son Erişim Tarihi: 12.02.2024.

87. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). ISO 19011 (2011). TS EN ISO 19011:2011 Yönetim sistemleri tetkik kılavuzu.

88. İnternet: IIA Uluslararası İç Denetim Standartları(2017, Ocak). IIA. URL: https://www.tide.org.tr/file/documents/pdf/UMUC-2017-updated.pdf, Son Erişim Tarihi: 12.02.2024.

89. İnternet: Bilgi ve İletişim Güvenliği Tedbirleri Konulu Genelge (2019, 6 Temmuz). Resmi Gazete (Sayı: 30823). URL: URL:https://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20190706-12.pdf, Son Erişim Tarihi: 01.07.2024.

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

91. Tulgar, M., Zaim A. H., Aydın, M. A. (2022). Ulusal Bilgi Ve İletişim Güvenliği Rehberi: Iot Güvenliği İçin Bir Uygulama Örneği. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, 21(42), 353-382.

92. İnternet: Bilgi ve İletişim Güvenliği Rehberi. *Cumhurbaşkanlığı Dijital Dönüşüm Ofisi.* URL: https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf, Son Erişim Tarihi: 12.02.2024.

93. İnternet: Bilgi ve İletişim Güvenliği Denetim Rehberi. *Cumhurbaşkanlığı Dijital Dönüşüm Ofisi.* URL: https://cbddo.gov.tr/SharedFolderServer/Projeler/File/BG_Denetim_Rehberi.pdf, Son Erişim Tarihi: 12.02.2024.

94. Alsultanny, Y. A. (2014). Evaluating Protesttin of Computer Network in Education Sector. *In Proceedings of the World Congress on Engineering and Computer Science*, San Francisco, USA, 1

95. Pallant, J. (2005). SPSS Survival Manual, 2nd Edn Buckingham

96. İnternet: Güvenilirlik ve Geçerlilik Testleri. Yöntem istatistik&analiz. URL: https://www.yontemistatistik.com/post/güvenilirlik-ve-geçerlilik-testleri, Son Erişim Tarihi: 01.07.2024.

97. Ercan, C. (2017). Denetçi Bağımsızlığına Yönelik Tehditler ve Korunma Önlemleri: Yeminli Mali Müşavirler Üzerine Bir Araştırma*. KSÜ Sosyal Bilimler Dergisi, 14(2), 261-284.

98. İnternet: Global Perspektifler ve Anlayışlar: Sayıların Ötesinde: İç Denetçinin Finansal Olmayan Raporlardaki Rolü (2015). IIA. URL: https://www.tide.org.tr/uploads/2015-1619%20GUI-Global%20Perspectives%20Nonfinancial%20Reporting-FNL-Lo.pdf, Son Erişim Tarihi: 12.02.2024.

99. Arslan, Y., Özbilger, H. İ. (2022). Ulusal Mevzuat Perspektifinde Bilgi İşlem Birimlerinin İç Denetiminde Bir Kontrol Listesi Önerisi. *Denetişim*, 26, 1-12

100. Öz, E. (2010). Denetim Evreninin Belirlenmesinde Alternatif Bir Yöntem: Analitik Hiyerarşi Prosesi. *Denetişim*, 4, 8-16

101. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). ISO 9001 (2015). TS EN ISO 9000:2015 Kalite yönetim sistemleri - Temel esaslar, terimler ve tarifler.

102. İnternet: TS ISO/IEC 27001:2017 Kontrolleri ile Bilgi ve İletişim Güvenliği Rehberi Eşleştirme Tablosu. Cumhurbaşkanlığı Dijital Dönüşüm Ofis. URL: https://cbddo.gov.tr/SharedFolderServer/Projeler/File/ISO27001%20-%20BGRehberEslestirmeTablosu.pdf, Son Erişim Tarihi: 12.02.2024.

103. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). ISO 31010 (2019) ISO EN 31010:2019 Risk management - Risk assessment techniques.

EKLER

EK-1. Araştırma Soruları

ISO 27001 Bilgi Güvenliği Yönetim Sistemi İç Tetkik/Denetim Anketi

Bu anket çalışması ile ulaşılan veri ve bilgiler Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Bölümünde yürütülen Yüksek Lisans Tez çalışmasında bilimsel araştırma amacıyla kullanılması amaçlanmaktadır.

Bu çalışma "ISO 27001 Bilgi Güvenliği Yönetim Sistemi İç Tetkiklerinin/Denetimlerinin etkinliği ve siber güvenliğe etkilerini" ölçmek amacıyla gerçekleştirilmektedir.

Bu anket siz değerli katılımcıların yaklaşık 8-10 dakikasını alacaktır.

Anket çalışmasında cevaplar doğru sonuçlara ulaşılabilmesi için önem arz etmektedir. Çalışma tamamen akademik amaçlı yapılmakta ve verdiğiniz hiçbir bilgi bireysel veya firma/kurum bazında açıklanmayacaktır.

Katılımlarınız için teşekkür ederim.

Emrah BALCILAR

Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Bölümü Yüksek Lisans Öğrencisi

1. Çalıştığınız Kurum/Şirket?
   ☐Kamu ☐Özel Sektör

2. Çalıştığınız Kurumdaki/Şirketteki pozisyonunuz?
   ☐Yönetici ☐Çalışan ☐İç Denetçi/Müfettiş

3. Çalıştığınız Kurumdaki/Şirketteki çalışan sayısı?
   ☐1-10 ☐11-50 ☐51-250 ☐251 ve üzeri

4. ISO 27001 Bilgi Güvenliği Yönetim Sistemi Tetkiki/Denetimi ile ilgili Eğitim aldınız mı?
   ☐Evet ☐Hayır

5. Hangi sayıda ISO 27001 Bilgi Güvenliği Yönetim Sistemi Tetkiki/Denetimine katıldınız?
   ☐1-2 ☐3-5 ☐6 ve üzeri

Aşağıdaki tüm sorular ISO 27001Bilgi Güvenliği Yönetim Sistemi İç Denetim/Tetkikleri kapsamında sorulmaktadır. Denetim ve Tetkik kelimeleri eş anlamlı olarak kabul edilerek sorular hazırlanmıştır.

No	Soru	Kesinlikle Katılmıyoru	Katılmıyoru	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
6	Şirketimde/Kurumumda ISO 27001 "Bilgi Güvenliği Yönetim Sistemi" belgesi alınmıştır ve uygulanmaktadır.					
7	Gerçekleştirdiğim denetimlerde bağımsızlığı sağlamak amacıyla kendi birimim dışındaki birimlerin denetiminde görevlendiriliyorum.					
8	Denetimlerini gerçekleştirdiğim birim ve süreçlerin yöneticileri ve/veya bir üst yöneticileri benim yöneticim değil.					
9	Şirketimde/Kurumumda ISO 27001 BGYS iç denetimleri objektif bir şekilde gerçekleştiriliyor.					
10	Denetim sonuçları ve bulguları kurum/şirket üst yönetimine iletiliyor.					
11	Gerçekleştirdiğim denetimlerde bulgularım ile ilgili herhangi bir baskıya maruz kalmıyorum.					
12	ISO 27001 BGYS Denetimi/Tetkiki ile ilgili düzenli eğitimler almaktayım.					
13	Gerçekleştirdiğim denetimleri için gerekli bilgi, beceri ve vasıflara sahibim.					
14	Denetlediğim birimler ile ilgili denetimi gerçekleştirebilecek teknik bilgiye sahibim.					
15*	Yazılım geliştirme konusunda denetim gerçekleştiriyorum ve bu konuda teknik bilgiye sahibim.					
16*	Veritabanı konusunda denetim gerçekleştiriyorum ve bu konuda teknik bilgiye sahibim.					
17*	Network konusunda denetim gerçekleştiriyorum ve bu konuda teknik bilgiye sahibim.					
18*	İşletim Sistemleri konusunda denetim gerçekleştiriyorum ve bu konuda teknik bilgiye sahibim.					
19	Şirketimde/Kurumumda riskli alanlar göz önünde bulundurularak iç denetim planlaması yapılmaktadır.					
20	Şirketimde/Kurumumda riskli alanları tespit etmek için yeterli periyotlarda denetim gerçekleştiriliyor.					
21	Şirketimde/Kurumumda riskli alanları tespit etmek için yeterli denetim zamanı denetçilere veriliyor.					
22	Üst üste aynı birim/süreçlerin denetimi aynı kişi tarafından gerçekleştirilmiyor.					

23	Şirketimde/Kurumumda riskli alanları tespit etmek için denetimlerde yeterli sayıda örnek üzerinde kontrol sağlanabiliyor.					
24	Şirketimde/Kurumumda denetime ön hazırlık yapabilmek için yeterli zaman denetçilere sunuluyor.					
25	Denetlediğim birimler ile ilgili ön hazırlık gerçekleştiriyorum.					
26	Şirketimde/Kurumumda denetim için soru ve kontrol listeleri riskli alanları tespit etmek için yeterli.					
27	Tespit ettiğim bulguları raporlayabiliyorum.					
28	Tespit ettiğim bulgular tüm ilgili birimlere iletiyor.					
29	Raporladığım bulgular için acil aksiyonlar alınıyor.					
30	Raporladığım bulgular kök sebepleri giderilerek tekrar oluşmayacak şekilde kapatılıyor.					
31	Gerçekleştirdiğim denetimler sayesinde denetlenen birimlerin bilgi güvenliği farkındalığı artıyor?					
32	Gerçekleştirdiğim denetimler sayesinde siber güvenlik açıklıklar kapatılarak riskli alanlar kapatılıyor.					
33	Eklemek istediklerinizi.					

* Cevap verilmesi zorunlu tutulmayan sorular.

EK-2. Etik Kurulu Onayı

Evrak Tarih ve Sayısı: 03.11.2022-E.499354

T.C.
GAZİ ÜNİVERSİTESİ REKTÖRLÜĞÜ
Etik Komisyonu

Sayı : E-77082166-302.08.01-499354 03.11.2022
Konu : Bilimsel ve Eğitim Amaçlı

Dağıtım Yerlerine

Üniversitemiz Bilişim Enstitüsü Adli Bilişim Ana Bilim Dalı **Yüksek Lisans Öğrencisi Emrah BALCILAR'ın, Doç.Dr. Çelebi ULUYOL'un,** danışmanlığında yürüttüğü ***"ISO 27001 Bilgi Güvenliği Standardı Denetimlerinin Siber Güvenliğe Etkileri Üzerine Bir İnceleme"*** adlı tez çalışması ile ilgili konu Komisyonumuzun **18.10.2022** tarih ve **17** sayılı toplantısında görüşülmüş olup,

İlgilinin çalışmasının, yapılması planlanan yerlerden izin alınması koşuluyla yapılmasında etik açıdan bir sakınca bulunmadığına oybirliği ile karar verilmiş ve karara ilişkin imza listesi ekte gönderilmiştir.

Bilgilerinizi rica ederim.

Araştırma Kod No: 2022 - 1144

Prof. Dr. İsmail KARAKAYA
Komisyon Başkanı

Ek:1 Liste
DAĞITIM
Gereği:
Sayın Doç. Dr. Çelebi ULUYOL

Bilgi:
Bilişim Enstitüsü Müdürlüğüne

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : BALCILAR, Emrah

Uyruğu : T.C.

Doğum tarihi ve yeri :

Telefon :

e-mail :

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Doktora	Gazi Üniversitesi / Adli Bilişim	Devam ediyor
Lisans	Başkent Üniversitesi / Bilgisayar Mühendisliği	2006

İş Deneyimi

Yıl	Yer	Görev
2010-Halen	Türksat A.Ş.	Müfettiş
2008-2010	Natek Bilişim	Proje Yöneticisi/Danışman
2007-2008	Sebit A.Ş.	Yazılım Geliştirici

Yabancı Dil

İngilizce,

Yayınlar

GAZİLİ OLMAK AYRICALIKTIR.