KOCAELİ SAĞLIK VE TEKNOLOJİ ÜNİVERSİTESİ
2009

T.C

KOCAELİ SAĞLIK VE TEKNOLOJİ ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ISO/IEC 27001:2022 VE KAMU BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ ARASINDAKİ BOŞLUK ANALİZİ

TUĞBA PAMUK

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ PROGRAMI

TEZLİ YÜKSEK LİSANS PROGRAMI

KOCAELİ–2025

T.C

KOCAELİ SAĞLIK VE TEKNOLOJİ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ISO/IEC 27001:2022 VE KAMU BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ ARASINDAKİ BOŞLUK ANALİZİ

TUĞBA PAMUK

YÜKSEK LİSANS TEZİ
BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ PROGRAMI

KOCAELİ-2025

Onay Sayfası

Bu tez Kocaeli Sağlık ve Teknoloji Üniversitesi Lisansüstü Eğitim Enstitüsü tarafından onaylanmıştır.

_____
Unvan ve İsim
Enstitü Müdürü

Bu tezin Kocaeli Sağlık ve Teknoloji Üniversitesi, Bilişim Sistemleri Mühendisliği Yüksek Lisans derecesinin tüm gerekliliklerini karşıladığını onaylıyorum.

_____
Unvan ve İsim
Bölüm Başkanı

TUĞBA PAMUK tarafından teslim edilen ISO/IEC 27001:2022 ve Kamu Bilgi ve İletişim Güvenliği Rehberi Arasındaki Boşluk Analizi başlıklı bu tezin kapsam ve kalite bakımından Yüksek Lisans derecesi için yeterli olduğunu değerlendirmektedir.

_____
Unvan ve İsim
Danışman

Tez Jürisi Üyeleri: (1. isim: Jüri başkanı; 2. isim: Danışman)
Dr. Öğr. Üyesi Burcu KIR SAVAŞ
Mühendislik Fakültesi, Kocaeli Üniversitesi
Dr. Öğr. Üyesi Mehmet KARA
Mühendislik ve Doğa Bilimleri Fakültesi, Kocaeli Sağlık ve Teknoloji Üniversitesi
Dr. Öğr. Üyesi Fulya AKDENİZ
Mühendislik ve Doğa Bilimleri Fakültesi, Kocaeli Sağlık ve Teknoloji Üniversitesi

Tarih:

ORJİNALLİK SAYFASI

İşbu belge ile tezimde yer alan tüm bilgilerin akademik ve etik kurallara uygun olarak elde edildiğini ve sunulduğunu beyan ederim. Bu tez çalışması, bilimsel araştırma ve yazım etik kurallarına uygun olarak tarafımca hazırlanmıştır. Tezin bazı bölümlerinin hazırlanmasında, içerik önerisi, dil sadeleştirme amacıyla OpenAI tarafından geliştirilen ChatGPT adlı yapay zekâ destekli dil modelinden faydalanılmıştır.

Ayrıca, kurallar gereği bu çalışmada özgün olmayan tüm materyal ve sonuçlar için ilgili kaynakların verildiğini beyan ederim.

Ad, Soyadı: Tuğba PAMUK

İmza:

ABSTRACT

GAP ANALYSIS BETWEEN ISO/IEC 27001:2022 AND THE TURKISH PUBLIC INFORMATION AND COMMUNICATION SECURITY GUIDE

PAMUK, Tuğba,

Information Systems Engineering Master's Program with Thesis

Supervisor : Asst. Prof. Mehmet KARA

July 2025, 93 pages

Increasing digitalization on a global scale has transformed information security from a mere technical requirement for public institutions into a strategic management area. With this transformation, the integration of international standards in a manner compatible with institutional structures has become critical for the protection of information assets. In this thesis, the structural compatibility, discrepancies, and application differences between the ISO/IEC 27001:2022 Information Security Management System standard and the Public Information and Communication Security Guide published by the Presidency of the Republic of Turkey's Digital Transformation Office have been examined using a holistic approach.

Through a gap analysis conducted as part of the research, the security controls of both structures were compared in detail, and the relationship between the standard's systematic, risk-based approach and the guide's normative regulations specific to the public sector was evaluated. The findings provide a roadmap for public institutions to establish a sustainable information security infrastructure that is compliant with national legislation and open to international audits. The study aims to contribute to the literature and corporate governance not only through theoretical comparisons but also through practical strategic conclusions.

Keywords: ISO/IEC 27001, Public Information and Communication Security Guide, ISO/IEC 27001 Annex – A, ISO/IEC 27002, Information Security, Audit

ÖZ

ISO/IEC 27001:2022 VE KAMU BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ ARASINDAKİ BOŞLUK ANALİZİ

Tuğba PAMUK

Bilişim Sistemleri Mühendisliği Tezli Yüksek Lisans

Tez Yöneticisi: Dr. Öğr. Üyesi Mehmet KARA

Temmuz 2025, 93 sayfa

Küresel ölçekte artan dijitalleşme, bilgi güvenliğini kamu kurumları için sadece teknik bir gereklilik olmaktan çıkarıp, stratejik bir yönetim alanına dönüştürmüştür. Bu dönüşümle birlikte, uluslararası standartların kurumsal yapılarla uyumlu bir şekilde entegre edilmesi, bilgi varlıklarının korunması açısından kritik hâle gelmiştir. Bu tezde, ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi standardı ile Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayımlanan Kamu Bilgi ve İletişim Güvenliği Rehberi arasındaki yapısal uyum, örtüşmeyen noktalar ve uygulama farklılıkları bütüncül bir yaklaşımla incelenmiştir.

Araştırma kapsamında gerçekleştirilen boşluk analizi (gap analysis) ile her iki yapının güvenlik kontrolleri detaylı biçimde karşılaştırılmış; standardın sistematik, risk temelli yaklaşımı ile rehberin kamu özelinde normatif düzenlemeleri arasındaki ilişki değerlendirilmiştir. Elde edilen bulgular, kamu kurumlarının hem ulusal mevzuata uygunluklarını sağlarken aynı zamanda uluslararası denetimlere açık, sürdürülebilir bir bilgi güvenliği altyapısı oluşturabilmeleri için bir yol haritası sunmaktadır. Çalışma, yalnızca teorik bir karşılaştırma değil, aynı zamanda uygulamaya dönük stratejik çıkarımlar da içermesi bakımından literatüre ve kurumsal yönetişime katkı sağlamayı hedeflemektedir.

Anahtar Kelimeler: ISO/IEC 27001, Kamu Bilgi ve İletişim Güvenliği Rehberi, ISO/IEC 27001 Ek – A, ISO/IEC 27002, Bilgi Güvenliği, Denetim

TEŞEKKÜR

Tez çalışma sürecimin tamamında bilgi birikimi, deneyimi ve engin tecrübeleriyle yol göstericim olan ve her adımda rehberlik eden kıymetli tez danışmanım Dr. Öğr. Üyesi Mehmet KARA' ya,

Eğitimim ve tez çalışmam süresince desteklerini hiçbir zaman esirgemeyen ve her anımda yanımda olan sevgili aileme tüm benliğimle teşekkür ediyorum.

İÇİNDEKİLER

TABLO LİSTESİ

TABLOLAR

ŞEKİL LİSTESİ

ŞEKİLLER

SEMBOL/KISALTMA LİSTESİ

BİT	Bilgi ve İletişim Teknolojileri
UYAP	Ulusal Yargı Ağı Bilişim Sistemi
MERNIS	Merkezi Nüfus İdaresi Sistemi
MHRS	Merkezi Hekim Randevu Sistemi
GİB	Gelir İdaresi Başkanlığı
YÖKSİS	Yükseköğretim Bilgi Sistemi
CBDDO	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
E-Devlet	Elektronik Devlet
ETSI	European Telecommunication System Institute
ISO	International Organization for Standardization
IEC	Uluslararası Elektroteknik Komisyonu
ISA	Uluslararası Otomasyon Derneği
ENISA	Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı
ITU	International Telecommunication Union
SOME	Siber Olaylara Müdahale Ekibi
IoT	Internet of Things
BGYS	Bilgi Güvenliği Yönetim Sistemi
SOCI	Kritik Altyapı Güvenliği Yasası
CVE	Common Vulnerabilities and Exposures
NIST	National Institute of Standards and Technology
CSF	Cybersecurity Framework
NCS	National Cyber Security Center
BSI	British Standards Institution
JISC	Japanese Industrial Standards Committee
KVKK	Kişisel Verileri Koruma Kanunu
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
DORA	Digital Operational Resilience Act
GDPR	General Data Protection Regulation

BÖLÜM 1: GİRİŞ

Çağımızda dijitalleşme hem kamu hem özel sektör kuruluşlarının operasyonel süreçlerinde kaçınılmaz bir dönüşüm alanı hâline gelmiştir ve bu da yalnızca sanayi ve hizmet sektörlerini değil; sağlık, e-ticaret ve tarım gibi alanları da derinden etkilemiş ve dönüştürmüştür. Bu dönüşüm, hem hizmet sunum biçimlerinde hem de süreç yönetimlerinde köklü değişimlere yol açmıştır.

Dijitalleşme ile birlikte kamu ve özel sektör kuruluşlarında bilgiye dayalı süreçlerin artması, bilgi güvenliğini kurumlar için hayati bir konu haline getirmiştir. Özellikle kişisel verilerin, kurumsal bilgilerin ve kritik altyapılara ilişkin verilerin dijital ortamlarda işlenmesi, bu verilerin gizliliği, bütünlüğü ve erişilebilirliğini koruma gereksinimini ortaya çıkarmıştır.

Dijitalleşmenin hız kazanması e-ticaret üzerinde alışveriş deneyiminin kişiselleştirilmesinden tedarik zincirinin yeniden yapılandırılmasına kadar geniş bir yelpazeyi kapsamaktadır. Yapay zeka ve makine öğrenimi teknolojileri, müşterilere özel ürün önerileri sunarak alışveriş süreçlerini optimize etmekte; chatbotlar ve sanal asistanlar, 7/24 müşteri hizmetleri sağlayarak kullanıcı deneyimini geliştirmektedir.

Bu gelişmeler, müşteri memnuniyetini artırmış, pazar erişimini küreselleştirmiş, işletmelerin operasyonel maliyetlerini düşürmüş ve veri analitiği sayesinde daha etkin stratejik kararlar alınmasını sağlamıştır.

Sağlık sektöründe ise dijital teknolojilerin adaptasyonu daha erişilebilir, hızlı ve etkili sağlık hizmetine erişime olanak sağlamıştır. Yapay zeka destekli tanı sistemleri, özellikle görüntüleme alanında, hastalıkların daha erken ve doğru teşhis edilmesini sağlamaktadır [1].

Bu gelişmeler, sağlık hizmetlerinin kalitesini artırmakta, hizmet sunum süreçlerini hızlandırmakta ve tedavi maliyetlerini azaltarak sağlık sistemlerinin genel verimliliğine katkıda bulunmaktadır [2].

Günümüz teknolojileri sağlık hizmetleri için yeni tıbbi teknoloji biçimleri ve uygulamaları alanında gelişmektedir. Sağlık hizmeti teknolojisinin sürekli gelişmesine

rağmen, bir hasta sağlık kayıt sisteminin uygulanması ve sistemlerin hassasiyeti nedeniyle hala önemli bir zorluk teşkil etmektedir. Bilgi, sağlık kurumlarının varlıklarını devam ettirebilmeleri açısından hayati öneme sahiptir ve bilgi güvenliği yönetimi süreciyle güvence altına alınması zorunludur [3].

Yapay zekâ, sağlık profesyonellerinin tanı ve tedavi süreci belirlemesine, hastaya özgü tedavi süreci ayarlanmasına, hastanın semptomlarına göre ilaç hazırlamada oldukça fayda sağlamaktadır [4].

Tarım sektörü de dijital teknolojilerden önemli ölçüde etkilenmiştir ve "akıllı tarım" kavramı ortaya çıkmıştır. Sensörler, dronlar ve uydu sistemleri aracılığıyla tarım arazilerinin verileri toplanmakta ve analiz edilmektedir. Bu dijital gelişmeler sonucunda tarımsal üretimde verimlilik artmış, çevresel etkiler azalmış, çiftçilerin gelir düzeyleri yükselmiş ve gıda güvenliğine yönelik toplum güveni artmıştır.

Gelecek için öngörülen en önemli üç stratejik kaynak olarak gıda/tarım, temiz su ve yenilenebilir enerji söylenebilir. Sürdürülebilir tarımsal kalkınma için bu kaynakların daha kontrollü kullanılması artık bir zorunluluktur. Verimi arttırmak için hızla dijital ve akıllı teknolojilerin geliştirilerek tarımda kullanılabilir hale getirilmesi gerekmektedir. Dijital tarım daha verimli, daha çevreci ve veriye dayalı karar verme olanağı sağlayan bir yoldur. Böylece daha güvenilir, daha uzun soluklu ve verimi yüksek üretimle nüfusun ihtiyacı daha rahat karşılanabilecektir. Yapılan yeniliklerle tarım sektöründe karşılaşılan zorlu koşullar daha rahat aşılabilir [5].

Bankacılık sektöründe ise dijital dönüşüm; teknolojik gelişmelerle birlikte yasal düzenlemeler, regülasyonlar, müşteri beklenti ve baskısı ve maliyet yönetimi gibi aktörlerle de yönetilmektedir. Günlük hayatımızın artık ayrılmaz parçaları olan mobil bankacılık, yapay zeka ve chatbotlar vb. konular temel uygulama alanlarındandır.

Ülkemizde kamu dijitalleşme süreci 2000'li yılların başından itibaren hız kazanmış, özellikle e-Devlet Kapısı (**www.turkiye.gov.tr**) üzerinden birçok hizmet dijital platformlara taşınmıştır. E-Devlet hizmetiyle birlikte vatandaşlar kamu hizmetlerine tek noktadan dijital erişimini sağlamaya başlamıştır. Elektronik Devlet (E-Devlet), kamu hizmetlerinin Bilgi ve İletişim Teknolojileri (BİT) kullanılarak dijital platformlar aracılığıyla vatandaşlara, kamu çalışanlarına sunulmasıdır [6,7].

Ulusal Yargı Ağı Bilişim Sistemi (UYAP) ile adli işlemlerin dijital ortamda yürütülmeye başlanması, Merkezi Nüfus İdaresi Sistemi (MERNİS) ile nüfus bilgileri elektronik ortama taşınarak kurumlar arası veri paylaşımının mümkün hale gelmesi, KamuNET ile de kamu kurumları arasında güvenli ağ iletişiminin sağlanması hedeflenerek e-devlet kamu hizmetlerinin sürekliliği sağlanmaya çalışılmıştır. E-Nabız gibi vatandaşların sağlık kayıtlarına ve tedavi geçmişlerine çevrimiçi ulaşabilmelerini sağlayan, Merkezi Hekim Randevu Sistemi (MHRS) gibi hastaların hastaneye gitmeden doktor randevusu almalarına olanak sağlayan sistemler sağlıkta çok önemli dijital değişim ve dönüşümdür. Bunların yanı sıra mali işlemler için İnteraktif Vergi Dairesi (GİB), eğitim için Okul Yönetim Bilgi Sistemi (E-Okul), Yükseköğretim Kurulu Başkanlığı Yükseköğretim Bilgi Sistemi (YÖKSİS) gibi elektronik sistemler ilgili vatandaşların verilere ulaşabilmesini sağlayarak devletin dijital kapasitesini artırmıştır ve hizmetlerin hızlı ve kesintisiz verilmesini, vatandaş memnuniyeti ve katılımını artırmayı ve veri güvenliği ve kurumlar arası entegrasyonu sağlamayı hedeflemiştir.

Kamuda dijital hizmetlerin yaygınlaştırılması ile birlikte kamu hizmetlerine erişim kolaylaştı, verimliliği artırmak hedeflenmiştir. Bu sürdürülebilirliğin sağlanabilmesi için insan kaynağı kapasitesi artırılarak, güvenlik önlemleri güçlendirilmeli ve kurumsal entegrasyon sağlanmalıdır [8].

Dijitalleşmenin getirdiği şeffaflık kamu hizmetlerinin kalitesini artırmada oldukça kritik faktördür. Kamu hizmetlerinde dijitalleşmenin başarılı bir şekilde gerçekleştirilmesi için bazı zorluklar ve engellerle karşılaşılabilmektedir. Veri güvenliği, bilgi gizliliği, dijital eşitsizlik, teknoloji altyapısının yetersizliği ve personelin yeterli dijital becerilere sahip olmaması gibi sorunlar dijital dönüşümde aşılması gereken kritik sorunlardandır. Bu nedenle kamu yönetimi teknolojisinin dijital dönüşüm sürecindeki başarısı için çözümler geliştirilmesi gerekmektedir [9].

Dijitalleşme hem kurum hem de ülkeler için büyük kolaylıklar ve faydalar sağlamaktadır ancak bu süreçte verilerin fiziksel ortamdan elektronik ortama aktarılması, bu ortamda saklanması işlenmesi ve iletilmesi kurum için önemli riskler oluşturmaktadır. Çünkü bilgisayar korsanları ya da düşman ülkeler gerekli güvenlik önlemi alınmadığında bu sistemlerde bulunan verilere atak yaparak maddi manevi çok

büyük zararlar verebilmektedir. Bu yüzden dijital ortama aktarılan verilerin korunması gerekmektedir.

Bu tezde bilgi sistemlerinin korunması için geliştirilmiş ISO/IEC 27001 standardı ve Türkiye Cumhuriyeti Cumhur Başkanlığı Dijital Dönüşüm Ofisi tarafından kamu bilgi sistemlerindeki verilerin korunması için oluşturulmuş Kamu Bilgi ve İletişim Güvenliği Rehberinin güvenlik bakış açısı analiz edilmiştir.

Devletler hizmetlerinin dijital ortamda sunulmasını, vatandaşlarının devletle olan etkileşim süreçlerini kolaylaştırmayı, bürokrasiyi azaltmayı ve şeffaflık ile verimliliği arttırmayı amaçladıkları için ülkemizdeki e-devlet hizmetini halka sunmaktadır.

1.1.E Devlet Uygulamalarının Durumu

Dünyadaki pek çok ülke ülkemizde olduğu gibi dijital hizmetlerini artırmaktadır. Bu konularda Güney Kore, Singapur, Hindistan, Estonya, İngiltere ön plana çıkmaktadır.

1.1.1. Güney Kore / E-Government

Güney Kore, e-devlet uygulamalarında oldukça ilerlemiş bir ülkedir. 2000'li yılların başında başlatılan e-devlet dönüşümü, ülkenin dijitalleşme oranını arttırmış ve bu da kamu hizmetlerini verimli hale getirmiştir.

Government24 adlı bir platform e-devletin merkezi aracıdır. Güney Kore vatandaşları vergi ödemelerinden, sağlık bilgilerine kadar birçok hizmete bu platform üzerinden erişebilir. Dijital imza ve kimlik uygulaması ile yine Güney Kore vatandaşları devlet ile olan işlemlerini yapabilirler. E-Health uygulaması da bizde kullanılan E-Nabız uygulaması gibi vatandaşların sağlık geçmişlerine dijital ortamda çevrimiçi ulaşmalarını sağlamaktadır [10].

1.1.2. Singapur / E-Government

Singapur, e-devlet hizmetleri konusunda dünyada öncü bir ülkedir. Singapur hükümeti, vatandaşlarına dijital ortamda kolay erişilebilen hizmetler sunarak, devletle olan etkileşimi daha verimli hale getirmiştir. GovTech ile hükümet dijital hizmetlerini halka sunmaktan sorumludur.

SingPass; Singapur'un dijital kimlik doğrulama sistemidir. Bu uygulama vatandaşların çeşitli kamu hizmetlerine çevrimiçi erişim sağlamak için kullanabileceği bir dijital kimliktir. Bu sistem, e-devlet portalı ile entegrasyon halindedir. GovTech ise Singapur'un dijital dönüşümünü yöneten hükümet organıdır. (Bizdeki Cumhurbaşkanlığı Dijital Dönüşüm Ofisi - CBDDO). E-Health ise bizdeki E-Nabız gibi sağlık hizmetlerini dijitalleştirerek, hastaların tıbbi geçmişlerine çevrimiçi olarak erişmelerini sağlar. Bu çevrimiçi uygulamalar vergi ödemeleri, araç kayıtları, sağlık hizmetleri, eğitim hizmetlerine başvuru gibi işlemler dijital platformlar üzerinden yapılır.

1.1.3 Hindistan / Digital India

Hindistan, geniş nüfusuyla e-devlet uygulamalarını hızla genişletmiştir. Digital India programı, ülkedeki dijitalleşmeyi hızlandırmayı hedefler ve devletle etkileşimleri dijital ortamda sunar. Hindistan'ın en büyük dijital kimlik sistemi olan Aadhaar, vatandaşların kimlik doğrulama işlemleri için kullanılır. Aadhaar, kamu hizmetlerine erişim için anahtar rol oynar. E-District ve E-Services gibi platformlarla, vatandaşların bölgesel yönetimle olan ilişkilerini dijital hale getirmiştir. Bu platformlar, başvuru, hizmet talebi ve ödeme işlemleri gibi pek çok devlet işlemini dijital ortamda gerçekleştirmektedir. M-Government (Mobil Hükümet): Hindistan, mobil cihazlar üzerinden devletle olan etkileşimi kolaylaştırmak amacıyla M-Government uygulamalarını başlatmıştır. Vatandaşlara, vergiler, sosyal yardım başvuruları, sağlık hizmetleri, eğitim gibi alanlarda dijital çözümler sunmaktadır [11].

1.1.4. Estonya / E-Estonia

Estonya, e-Devlet konusunda dünya çapında en ileri düzeydeki ülkelerden biridir. Estonya'nın e-devlet altyapısı, dijital kimlik ve dijital hizmetlerin entegrasyonu ile tanınır. Ülkede, vatandaşlar ve şirketler devlet hizmetlerine kolay erişim sağlayabilir.

Estonya, tüm vatandaşları için zorunlu dijital kimlik kartları sağlar. Bu dijital kimlik, e-devlet platformlarına erişimin anahtarıdır. Estonya'nın merkezi dijital altyapısı olan X-Road, devlet daireleri arasındaki veri paylaşımını güvenli bir şekilde sağlar. Kamu ve özel sektör arasındaki veri alışverişi bu altyapı ile yapılır. E-Residence (E-İkamet)

Estonya, dünyanın dört bir yanındaki girişimcilere, dijital kimlik alarak Estonya'da sanal bir işletme kurma imkânı sunar. E-Health, Sağlık hizmetleri dijitalleştirilmiş ve tüm vatandaşların sağlık verilerine çevrimiçi erişimi vardır.

Vergi beyanı, seçimler, sağlık hizmetleri, eğitim, araç kayıtları gibi pek çok işlem dijital ortamda yapılabilmektedir [12].

1.5 İngiltere / e- Government

İngiltere'de gov.uk platformu üzerinden vatandaşlar, devletle olan işlemlerini çevrimiçi olarak gerçekleştirebilirler. Bu platform üzerinden vergi ödemeleri, pasaport başvuruları, sosyal güvenlik işlemleri yapılabilir. Bu uygulamalar devlet hizmetlerini platform üzerinden halka sunarak; vatandaşların daha hızlı, güvenli ve verimli şekilde devlet hizmetlerinden yararlanmalarını sağlar.

Ülkelerin dijitalleşme hamleleri, kamu hizmetlerinin elektronik ortama taşınmasını ve büyük veri temelli karar alma süreçlerinin benimsenmesini beraberinde getirmiştir. Bu gelişmeler, bilginin kurumsal ve ulusal düzeyde kritik bir varlık olarak konumlanmasını sağlamış; dolayısıyla bilgi güvenliği, dijitalleşmenin ayrılmaz bir bileşeni haline gelmiştir. Bu bağlamda, dijitalleşme ile birlikte fiziksel ortamdan dijitale taşınan bilgilerin muhafaza edilmesi için bilgi güvenliğine geçiş süreci, sadece teknolojik değil; aynı zamanda yönetsel ve stratejik bir dönüşüm olarak değerlendirilmelidir.

BÖLÜM 2: BİLGİ GÜVENLİĞİ İHTİYACI

Bilgi; dijital ya da fiziksel ortamlar üzerine kaydedilmiş anlamlı veriler bütünüdür. Enformasyon verinin üst versiyonu olduğu için ‘’ anlamlandırılmış veri’’ olarak tanımlanabilir.

Bilgi Güvenliği ise; özellikle bilgi teknolojileri kullanılarak saklanan, iletilen bilgilerin veya işlenen verinin yetkisiz erişim, değiştirme veya yok edilmesine karşı korunmasını sağlayan disiplindir. Bir bilgi sisteminin faaliyetlerini yerine getirirken kesintisiz, kaliteli ve güvenli bir hizmet sunumunun sağlanmasını hedeflemektedir. Diğer yandan kurumsal imaj ve güvenirliğin sağlanması, eldeki bilgi varlıklarının korunumu ve yetkisiz erişimlerin önlenmesi de bilgi güvenliğinin temel amaç ve öncelikleri arasındadır [13].

Bilgi güvenliğinin zaruriyeti ve önemi hem kişisel hem de kurumsal alanda gün geçtikçe her sektörde, her organizasyonda giderek artmaktadır. Bu duruma artan siber saldırılar, veri ihlalleri ve bilgi güvenliği alanında yapılan yasal düzenlemelerin getirdiği cezai yaptırımlar neden olmuştur.

Bilgi güvenliğinin başlıca amaçları üç temel güvenlik ilkesi etrafında şekillenir: Gizlilik, bilginin yalnızca yetkili kişi ve sistemler tarafından erişilebilir olmasını sağlar; Bütünlük, bilginin doğruluk, tutarlılık ve güvenilirliğini korumayı hedefler; Erişilebilirlik ise bilginin ihtiyaç duyulduğu anda ulaşılabilir olmasını garanti altına alır. Bu üçlü yapı, bilgi güvenliğinin teknik ve yönetsel uygulamalarının temel çerçevesini oluşturur. Bununla birlikte, güvenlik ilkelerine günümüzde sıklıkla inkâr edilemezlik, hesap verebilirlik ve kimlik doğrulama gibi tamamlayıcı hedefler de eklenmektedir [14].

Bilgi güvenliğini sağlamanın adımlarından ilki güvenlik için hangi unsurlara ihtiyaç duyulacağının belirlenmesidir. Bilginin güvenliğini sağlamak için ikinci adım ise kurumda bilgi güvenliği kültürü anlayışının yerleştirilmesidir. Bilgi güvenliği kültürü; kurumsal bilgi güvenliği politikası, bilgi güvenliği yönetimi ve uygulanan uluslararası standartlar ile mümkündür. Üçüncü adım ise bilgi güvenliğinin en zayıf halkası olan insan için bilinçlendirme ve yetkinleştirme çalışmalarıdır [15].

Bilgi güvenliğinin amaçları, organizasyonun yapısı, faaliyet alanı ve yasal yükümlülükleri doğrultusunda çeşitlenebilir. Örneğin; bir kamu kurumunda bilgi güvenliği, vatandaş verilerinin gizliliğini ve hizmet sürekliliğini sağlamaya odaklanırken, bir finans kuruluşunda ise dolandırıcılıkların önlenmesi ve finansal verilerin bütünlüğü ön planda olabilir. Bu nedenle bilgi güvenliği, kurumun misyonu, vizyonu ve iş hedefleriyle doğrudan ilişkilendirilmelidir. Etkili bir bilgi güvenliği yönetimi; kurumun iç tehditlere (örneğin; yetkisiz erişim, insan hatası) ve dış tehditlere (örneğin; kötü amaçlı yazılımlar, APT'ler, sosyal mühendislik saldırıları) karşı direnç göstermesini sağlayan politikalar, prosedürler ve kontroller bütünü olarak tasarlanmalıdır. Ayrıca bilgi güvenliği, sadece riskleri azaltmayı değil; aynı zamanda yasal ve düzenleyici gereksinimlere uyumu sağlamayı da amaçlar.

Bilgi güvenliğinin amacı yalnızca saldırılardan korunmak değil; bilgiye dayalı süreçlerin sürekliliğini ve güvenilirliğini sağlamak, kurumsal sürdürülebilirliği desteklemek ve paydaş güvenini artırmaktır. Bu bağlamda bilgi güvenliği, teknik önlemlerle sınırlı olmayan; stratejik, yönetsel ve hukuki yönleri olan bütüncül bir yönetim alanıdır.

Bilgi ve iletişim teknolojilerinin yaygınlaşması, veri odaklı çalışma modellerinin artması ve elektronik hizmetlerin ön plana çıkması, dijital varlıkların korunmasını stratejik bir gereklilik haline getirmiştir. Bu bağlamda, bilgi güvenliği sadece teknolojik bir ihtiyaç değil, aynı zamanda kurumsal itibar, yasal uyumluluk ve vatandaş/müşteri güveni açısından da kritik bir unsur hâline gelmiştir. Dolayısıyla, bilgi güvenliği yönetim sistemlerinin etkin kurulumu ve sürdürülebilirliği, dijitalleşme sürecinin temel bir bileşeni olarak değerlendirilmelidir.

Avrupa Telekomünikasyon Standartları Enstitüsüne göre (ETSI) siber güvenlik standartları, saldırıları ilk etapta önleme ve saldırıların etkilerini azaltma yönündeki kolektif çaba için kritik öneme sahiptir. Bu nedenle çeşitli standart kuruluşları, kuruluşların veri ve sistemlerini güvence altına almalarına yardımcı olacak en iyi uygulamaları, kılavuzları ve diğer kaynakları geliştirmek için proaktif bir yaklaşım benimsemiştir. Bu anlayış neticesinde Uluslararası Standardizasyon Örgütü (ISO), Uluslararası Elektroteknik Komisyonu (IEC), Uluslararası Otomasyon Derneği (ISA),

ETSI, Uluslararası Telekomünikasyon Birliği-(ITU-T) Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA) gibi kuruluşlar arasında siber güvenlik standartlarının oluşturulması ve uygulanması konusunda geniş bir iş birliği yapılmasını sağlamıştır [16].

2.1. Türkiye'de Kurumsal Bilgi Güvenliği

İnternetin gelişmesine paralel olarak saldırılan artması ile birlikte tüm dünyada olduğu gibi ülkemizde de hem iyi bilinen güvenlik önlemeleri uygulanmış hem de yasal düzenlemeler yapılmaya başlanmıştır. Bu kapsamda aşağıdaki yasalar oluşturulmuştur.

- 5237 Sayılı Türk Ceza Kanunu
- 5809 Sayılı Elektronik Haberleşme Kanunu
- 5070 Sayılı Elektronik İmza Kanunu
- 5846 Sayılı Fikri ve Sanat Eserleri Kanunu
- 6698 Sayılı Kişisel Verilerin Korunması Kanunu
- 7545 Siber Güvenlik Kanunu

10 Temmuz 2018 tarihinde Cumhurbaşkanı tarafından belirlenen amaç, politika ve stratejilere uygun olarak kamunun dijital dönüşümüne öncelik etmek, e-devlet hizmetlerinin sunumuna aracılık etmek, kurumlar arası iş birliğini artırmak ve bu alanlarda koordinasyonu sağlamak amacıyla Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) kurulmuştur. Bu kuruluş kamu kurum ve kuruluşlarının dijital ortama geçmesini, siber güvenlik ve yapay zeka gibi konuları koordine etmekle görevlendirilmiştir.

Kamu hizmetlerinin dijitalleştirilmesi, e-Devlet altyapısının geliştirilmesi, ulusal siber güvenlik politikalarının oluşturulması, büyük veri, yapay zekâ ve blok zincir gibi yeni teknolojilerin kamuya entegrasyonu, Kamu Bilgi ve İletişim Güvenliği Rehberinin hazırlanması gibi görevleri bulunan bu yapı; Bilişim ve Bilgi Toplumu Dairesi Başkanlığı gibi daha önce farklı kurumlarda dağınık yürütülen görevleri merkezi bir otorite altında toplamıştır.

Kuruluşun görev süresi boyunca Dijital Türkiye Stratejisi ve "Ulusal Yapay Zekâ Stratejisi" hazırlanmıştır, kullanıcı sayısı 65 milyona e-devlet kapısı hizmet çeşitliliği açısından büyütülmüş, Kamu Bilgi ve İletişim Güvenliği Rehberi yayınlanarak kamu kurumlarının bilgi sistemleri güvenliğine dair kriterler belirlenmiştir ve Kamu Siber Olaylara Müdahale Ekipleri (SOME) koordinasyonu ülkemizin dijitalleşme sürecine yön veren pek çok stratejik çalışmalardan öne çıkanlardır. 2025 yılının Mart ayında yayımlanan bir Cumhurbaşkanlığı Kararnamesi ile kurumsal görev çakışmalarının önlenmesi, daha entegre ve merkezi bir dijital güvenlik politikası ihtiyacının oluşması ve siber tehditlere karşı daha hızlı karar alma ve uygulama kapasitesinin artırılması gerekçeleri ile CBDDO resmen kapatılmış, görev ve yetkileri Siber Güvenlik Başkanlığı'na devredilmiştir. Bu değişiklik ile birlikte Siber Güvenlik Başkanlığı, yalnızca güvenlik odaklı bir kurum olmaktan çıkmış, dijital dönüşümün genel koordinasyonunu üstlenen merkezi otorite hâline gelmiştir [17].

Dijitalleşme süreci, yalnızca veri ve işlemlerin elektronik ortama taşınmasıyla sınırlı kalmayıp, yapay zekâ, nesnelerin interneti (IoT), büyük veri analitiği ve bulut bilişim gibi ileri teknolojilerle bütünleşerek derinleşmektedir. Gelecek dönemde dijitalleşmenin yönü; daha otonom sistemlerin, yapay zekâ destekli karar mekanizmalarının ve uçtan uca dijital güvenliğin ön plana çıktığı bir yapıya doğru evrilmektedir. Bu evrim, bilgi güvenliği yönetim sistemlerinin yalnızca koruyucu değil, aynı zamanda proaktif ve dinamik yapılarla desteklenmesini zorunlu kılmaktadır. Bu bağlamda, dijitalleşmenin geldiği bu yeni aşamada, bilgi güvenliği standartlarının (örneğin ISO/IEC 27001:2022) ve ulusal regülasyonların (örneğin: Kamu Bilgi ve İletişim Güvenliği Rehberi) önemi daha da artmıştır.

Bilgi güvenliği alanında yapılan akademik çalışmalar, son yıllarda özellikle dijitalleşmenin hız kazanmasıyla birlikte artış göstermiş ve disiplinler arası bir karakter kazanmıştır. Literatürdeki çalışmalar; siber tehditlerin evrimi, saldırı tespit sistemleri, güvenlik farkındalığı, şifreleme yöntemleri, erişim kontrolleri, güvenlik olgunluk modelleri ve Bilgi Güvenliği Yönetim Sistemlerinin (BGYS) uygulanabilirliği gibi çeşitli alt başlıklar etrafında şekillenmektedir.

Kuruluşlar artık dijital varlıklarını sadece yönetmekle kalmayıp, bu varlıklar üzerinden yeni iş modelleri ve hizmetler üretmektedir. Dijitalleşmenin geldiği noktada, güvenlik, mahremiyet ve veri bütünlüğü gibi kavramlar stratejik öncelik hâline gelmiştir.

Ülkelerin toplumsal düzenleri ve kamu hizmetleri de incelendiğinde kritik altyapı çalışmalarında hizmet devamlılığı esas alınmıştır. Kritik altyapıların kapsamı ülkeden ülkeye değişmektedir. Amerika Birleşik Devletleri (ABD) hükümeti kritik altyapıların korunması çalışmalarını Ulusal Güvenlik kapsamına aldığı için kritik altyapıları "Ulusal Altyapı Koruma Planı" ile belirlemiştir, Avrupa Birliği'nin (AB) kritik altyapıların korunmasına bakışı üye ülkelerinde ikamet eden vatandaşların sağlık, emniyet, güvenlik ve ekonomik refahı ile üye ülke hükümetlerinin etkin işleyişinin korunması açısından bakmaktadır. Ülkemizdeki kritik altyapıların korunması çalışmaları ise önümüzdeki yıllarda hazırlanması muhtemel siber güvenlik stratejilerinin, ulusal seviyedeki siber güvenlik çalışmalarının ana temasının "kritik altyapıların korunması" olacağı değerlendirilmektedir. Bu kapsamda ülkemizdeki en önemli çalışmaların başında Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Ulusal Siber Güvenlik Stratejisi yer almaktadır [18].

Kritik altyapıların korunması uygulama çerçevesi Şekil 2.1'de gösterilmiştir.

Kritik Altyapı Sektörleri(KAS)	KAS Belirleme Sorumluluk	KAS Güvenlik Sorumluluk (Sektör Bazında)	KAS Güvenlik Sorumluluk (Tesis Bazında)	KAS Koordinasyon Sorumluluk
Enerji	EPDK, Enerji Bakanlığı, TAEK, AFAD	EPDK	İşletme Sahibi (Özel Sektör)	AFAD
Ulaştırma	UDHB, AFAD	UDHB,	İşletme Sahibi (Özel Sektör)	AFAD
Su Yönetimi/Barajlar	Orman ve Su işleri Bakanlığı, AFAD	Orman ve Su işleri Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD
Haberleşme	BTK, UDHB, AFAD	BTK, UDHB	İşletme Sahibi (Özel Sektör)	AFAD
Bankacılık ve Finans	BDDK,SPK, Hazine Müsteşarlığı, Maliye Bakanlığı, AFAD	BDDK,SPK, Hazine Müsteşarlığı, Maliye Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD
Kritik Kamu Hizmetleri	İçişleri Bakanlığı, AFAD	İçişleri Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD
Kritik Üretim/Ticari Tesisler	Bilim, Sanayi , ve Teknoloji Bakanlığı, Gümrük ve Ticaret Bakanlığı, AFAD TOBB	Bilim, Sanayi ve Teknoloji Bakanlığı, TOBB	İşletme Sahibi (Özel Sektör)	AFAD
Sağlık	Sağlık Bakanlığı, AFAD	Sağlık Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD
Tarım ve Gıda	GTHB, AFAD	GTHB	İşletme Sahibi (Özel Sektör)	AFAD
Kültür ve Turizm	Kültür ve Turizm Bakanlığı, AFAD	Kültür ve Turizm Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD

Şekil 2.1. Kritik Altyapıların Korunması Uygulama Çerçevesi

Siber güvenlik artık yalnızca ağ ve sistem koruması sağlayan teknik bir alan olmanın ötesine geçerek kurumsal risk yönetimi, iş sürekliliği ve yasal uyumluluk süreçlerinin ayrılmaz bir parçası hâline gelmiştir. Gelişen tehdit ortamı karşısında, geleneksel sınır temelli güvenlik yaklaşımlarının yetersiz kaldığı görülmekte ve bunun yerine, her erişim talebinin sürekli doğrulandığı Sıfır Güven (Zero Trust) mimarileri ön plana çıkmaktadır. Zero Trust mimarisi 'asla güvenme, daima doğrula' ilkesiyle çalışmaktadır. Bu yaklaşıma göre ağ içindeki kullanıcılar ve cihazlar bile güvenilmez kabul edilir, her erişim talebi, kimlik doğrulama, cihaz durumu ve konum gibi faktörlerle değerlendirilir, Kimlik ve erişim yönetimi, mikro segmentasyon ve sürekli izleme gibi mekanizmalarla desteklenir. Zero Trust; iç tehditlere karşı yüksek koruma, veri ihlallerinin sınırlandırılması, uyumluluk (compliance) gereksinimlerine katkı, esnek ve güvenli uzaktan erişim imkânı sunması açısından faydalıdır.

İnternet üzerinden yapılan büyük saldırılardan bir tanesi "Mirai: İnternetin düşüşü" olmuştur. Bu saldırıda nesnelerin internetinin (IoT) yeni ortaya çıkması ile botnetlerde hiçbir antivirüs programı olmamasından dolayı bu cihazları hedef alan bir botnet saldırısıdır. Japonca'da "gelecek" anlamına gelen Mirai; Linux tabanlı sistemler üzerinde çalışan IoT cihazları hedefleyen bir kötü amaçlı yazılım (malware) üzerinden kurulan bu zombi donanma ile yapılan büyük bir DDoS saldırısına dayanmaktadır. Bu saldırı ile güvenlik önlemlerinin alınması gerektiği bir kez daha görülmüştür [19].

İlk ulusal siber güvenlik stratejisini 11 Eylül 2001 yılında yaşadığı terör saldırısından kendine pay çıkaran ABD; 2003 yılında yayınlamıştır. Birleşik Krallık ise böylesi büyük bir farkındalıkta geç kalarak 2007 yılında Estonya'ya karşı gerçekleştirilen siber saldırılardan etkilenerek ancak 2009 yılında ilk siber güvenlik strateji belgesini yayınlamıştır.

Tüm dünyanın siber güvenlik saldırılarından gittikçe korkmasına sebep olan Stuxnet saldırıları; Birleşik Krallık'a kritik alt yapı güvenliğinin önemini bir kez daha hatırlatmıştır. Stuxnet; kötü amaçlı yazılım üzerinden İran'ın nükleer tesislerine yönelik gerçekleştirilen siber saldırıların sorumluluğunu hiçbir grup veya ülke üstlenmemesine rağmen uzmanlar gelişmiş ve karmaşık yapısı üzerinden Stuxnet'in bir devlet tarafından geliştirilmiş olabileceğine inanmışlardır. Bu bağlamda ABD,

İsrail, Birleşik Krallık, Rusya, Çin ve Fransa gibi devletler Stuxnet'i geliştirebilecek maddi ve teknik becerilere sahip ülkeler arasında değerlendirilmektedirler.

Stuxnet saldırısı enerji ve diğer birçok endüstriyel kontrol merkezindeki sistemlerin ve kritik alt yapı unsurlarının ne kadar savunmasız olduğunu ve siber saldırılara karşı güçlendirilmesi gerektiğini ortaya çıkarmıştır [20].

Dünya genelinde hükümetler, kritik altyapılara yönelik artan siber saldırılara karşı siber güvenlik önlemlerini zorunlu kılmak üzere tasarlanmış mevzuatla bu alanda güçlendirme çalışmalarını yaptıklarını ortaya koymaktadırlar. Avustralya'da federal hükümet 2018 Kritik Altyapı Güvenliği Yasası **(**SOCI) kapsamında kritik endüstri sektörlerini dörtten on bire çıkarmıştır. Bu mevzuat endüstrilerin siber güvenlik önlemlerini nasıl uygulamaları gerektiğine ilişkin düzenlemeleri de içermekte ve uyulmaması halinde ağır para cezaları öngörmektedir.

Yapay zekâ destekli tehdit tespiti, güvenlik otomasyonu, tehdit istihbaratı yönetimi ve uç nokta koruma teknolojileri gibi yenilikçi yöntemler, siber güvenlik stratejilerinin temel bileşenleri hâline gelmiştir. Siber saldırıların karmaşıklığının artması, fidye yazılımı tehditlerinin yaygınlaşması ve devlet destekli siber casusluk faaliyetlerinin çoğalması yalnızca teknik değil aynı zamanda yönetsel ve stratejik bilgi güvenliği politikalarının geliştirilmesini zorunlu kılmaktadır. Bu çerçevede bilgi güvenliği, sadece bilgi teknolojileri birimlerinin sorumluluğunda değil, kurumsal risk yönetimi ve yönetişim anlayışı içinde ele alınması gereken bütüncül bir yaklaşıma dönüşmüştür.

Güvenlik teknolojisi hem yazılım hem de donanım tabanlı olabilmektedir. Fakat günümüzde her şey yazılımla yapılmaya çalışıldığı için genellikle donanım soyutlanıp yazılımla yapılmaya çalışılmaktadır. Güvenlik geliştirmeleri var olan güvenlik özellikleri üzerinde yapılan düzenlemelerden oluşmaktadır. Güvenlik algoritmaları yoğun hesaplama gerektirdiği için önemli miktarda işlemci gücü ve bellek ihtiyacı olur. Bundan dolayı etkin güvenlik algoritmalarının tasarlanmasına ihtiyaç vardır. Daha önceki örneklerinde başlangıç seviyesinde olan siber savaş Rusya – Ukrayna savaşında fiziksel savaşla eş güdümlü olarak yürütülmektedir. Savaşın siber tarafında 50'den fazla Common Vulnerabilities and Exposures (CVE) kullanılmış ve 70'e yakın hükümet web sitesine saldırıldığı kayıt altına alınmıştır [21].

2022 yılı siber güvenlik mesleği için oldukça biçimlendirici bir yıl olmuştur. Jeopolitik ve makroekonomik çalkantılarla günümüzdeki şeklini alan ve her geçen günde şekillenmeye devam eden ve tanımlanan modern siber güvenlik kararlılıkla kendini göstermektedir. Büyüyen küresel siber güvenlik tehditleri ile bu tehditlere karşı mücadele edecek, kritik görevleri üstlenecek profesyonellerdeki boşluk da artmaktadır.

2022 yılında gerçekleşen ve oldukça ses getiren siber olaylardan bazıları şu şekildedir:

Google'ın saniyede 46 milyon istek ile bugüne kadar yapılmış en büyük HTTPS DDoS saldırısını engelleyerek rekor kırması, Conti fidye yazılımı çetesi, yüksek profilli bir siber saldırı ile Kosta Rika hükümetinin sistemimi ihlal ederek hükümetin sistemlerine girip, çok değerli verileri çalarak, 20 milyon dolar talep ederek Orta Amerika hükümetini olağanüstü hâl ilan etmeye zorlaması, Avustralya'nın en büyük sağlık sigortası sağlayıcılarından biri olan Medibank Private Ltd; 1.8 milyon uluslararası müşteri dahil olmak üzere 9,7 milyon eski ve mevcut müşteriye ait verilere yetkisiz bir tarafça erişildiğinin doğrulanması, Yandex Taksinin bilgisayar korsanları tarafından ele geçirilerek Moskova'da bulunan tüm taksilerin aynı noktaya yönlendirilmesi ile büyük bir trafik sıkışıklığına yol açması bu örnek siber olaylardandır [22].

Bir kuruluşta bilgi güvenliği yönetim sistemlerinin kurulmuş olması veya ISO/IEC 27001 standardına sahip olunması, kurum süreçlerinde bilgi güvenliğinin %100 sağlandığı anlamına gelmemektedir. Uygulanan bilgi güvenliği yönetim sistemlerinin ve uyumlanmaya çalışılan standartların kullanılabilir ve sürdürülebilir olması kuruluşlar için çok önemlidir [23].

2.2. Bilgi Güvenliği Standart, Anaçatı ve Regülasyonları

Bilgi güvenliği hem ulusal hem de uluslararası standartlar, ana çatılar ve regülasyonlar ile korunmaktadır. Bu standart ve regülasyonlar kurumlara bilgi güvenliği politika ve prosedürlerini yönetebilme, uygulayabilme, sürekli olarak iyileştirebilme imkânı sağlar. Bu imkanlar sayesinde de kurumlar bilgi güvenliği konusunda daha etkili ve tutarlı bir yaklaşım benimserler. National Institute of Standards and Technology (NIST) Siber Güvenlik Çerçevesi ana çatıya, ISO/IEC 27001 standartlara, Kamu Bilgi

ve İletişim Güvenliği Rehberi de regülasyonlara verilebilecek en önemli örneklerdir. Bu standartlar, yalnızca teknik kontrolleri değil; aynı zamanda organizasyonel yapı, insan faktörü ve süreç güvenliğini de kapsayan bir güvenlik kültürünün inşasını hedeflemektedir.

Bilgi güvenliği ve siber güvenlik alanlarında, ülkeler farklı standartlar, mevzuatlar ve çerçeveler geliştirerek ulusal düzeyde güvenlik politikalarını oluşturmuşlardır. Amerika Birleşik Devletleri'nde, NIST tarafından yayımlanan Cybersecurity Framework (CSF),. Avrupa Birliği ülkelerinde, Directive on Security of Network and Information Systems (NIS Direktifi) ve NIS2 Direktifi, Birleşik Krallık'ta Cyber Essentials programı, bunlara örnektir. [24].

Almanya'da BSI Grundschutz adı verilen bilgi güvenliği standardı, Japonya'da ise JIS Q 27001 ile bilgi güvenliğine kurumsal bir yaklaşım kazandırmıştır. Bu çabalar, bilgi güvenliği standartlarının küresel ölçekte farklı yöntemlerle geliştirilmekte olduğunu ve ülkelerin kendi risk profilleri, mevzuat gereksinimleri ve ulusal güvenlik stratejileri doğrultusunda özelleştirmeler yaptığını göstermektedir.

Ülkeler kendi siber güvenlik stratejileri doğrultusunda bilgi güvenliğini sağlamak amacıyla çeşitli yasal düzenlemeler (regülasyonlar) ve uygulama çerçeveleri (anaçatılar) geliştirmiştir. Söz konusu düzenlemeler, hem yerel ihtiyaçlara hem de uluslararası standartlara uyumlu olacak şekilde yapılandırılmıştır. Böylece, bilgi sistemlerinin gizliliği, bütünlüğü ve erişilebilirliği güvence altına alınarak dijital dönüşüm süreçlerinin güvenli temeller üzerine inşa edilmesi hedeflenmektedir. Bu doğrultuda 2018 yılında Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) öncülüğünde Kamu Bilgi ve İletişim Güvenliği Rehberi; yasalarımız, ISO/IEC 27001 ve diğer ilgili ülkelerdeki uygulamalar dikkate alınarak hazırlanmış ve yayınlamıştır. Dünyanın önde gelen ülkelerinde kullanılan düzenleme ve anaçatı dokümanları, ilk yayınlanma ve güncellenme yılları, yayınlayan kurum bilgileri Tablo 2.1'de görülmektedir.

Tablo 2.1 Ülkelerin Uyguladıkları Regülasyonlar ve Anaçatılar

Ülke	**Güvenlik Çerçevesi**	**Açıklama**	**Yıl**	**Yayınlayan Kurum**
ABD	NIST Cybersecurity Framework (CSF) ve NIST SP 800-53	Kritik altyapıların korunması ve siber risk yönetimi için rehber sağlar.	2014/2020	NIST
Avrupa Birliği	NIS ve NIS2 Direktifleri Network and Information Security Directive	Üye ülkeler arasında siber güvenlik uyumunu sağlamak için standartlar ve düzenlemeler oluşturur.	2016/2022	Avrupa Komisyonu
Birleşik Krallık	Cyber Essentials	Temel siber güvenlik önlemlerini zorunlu hale getirir ve siber güvenlik olgunluğu düzeyini artırır.	2014/2023	National Cyber Security Centre (NCSC)
Almanya	BSI Grundschutz (IT-Grundschutz-Kompendium)	ISO/IEC 27001 ile uyumlu, ulusal bilgi güvenliği yönetim sistemi standardıdır.	1994/2023	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Japonya	ISMS (Information Security Management System) (JIS Q 27001)	Bilgi güvenliğini kurumsal bir yapı içinde yöneten ve ISO/IEC 27001'e dayanan bir sistemdir.	2014/2023	Japanese Industrial Standards Committee (JISC)

Türkiye	Kamu Bilgi ve İletişim Güvenliği Rehberi	Kamu kurumlarının bilgi güvenliği için bir rehber ve ISO/IEC 27001 ile uyumlu bir modeldir.	2020	T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı

2.2.1. NIST Siber Güvenlik Anaçatısı

ABD Ticaret Bakanlığı'na bağlı Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından tüm sektörler için geçerli risk temelli bir siber güvenlik çerçevesi yayınlamıştır.

Bu ana çatı kuruluşlara siber güvenlik yeteneklerini geliştirme, riskleri etkin bir şekilde yönetme, kritik varlıkları koruma ve yasal düzenleyici uyum sağlama konularında kapsayıcı bir kılavuz sunar. 5 temel işlev üzerine kuruludur.

- Tanımlama
- Koruma
- Tespit etmek
- Cevaplama
- İyileşmek

Bu işlevler yönetişim ve kurumsal güvenlik politikalarının ele alındığı yeni bir işlev olan Yönetişim (Govern) de eklenmiştir. Her işlev, daha ayrıntılı kategorilere ve bu kategoriler de alt kategorilere bölünerek uygulama kolaylığı sağlar. Anaçatı, organizasyonların mevcut siber güvenlik seviyelerini değerlendirmelerine yardımcı olmak için dört olgunluk katmanı (kısmi, risk odaklı, tekrarlanabilir ve uyarlanabilir) sunar.

NIST SP 800- 53 federal bilgi sistemleri ve organizasyonlar için kapsamlı bir güvenlik ve gizlilik kontrolleri setidir. Bu çerçeve, kamu kurumları başta olmak üzere bilgi güvenliği ve gizliliğini sağlamak isteyen tüm kurumlar için uygulanabilir durumdadır. NIST SP 800-53 bilgi sistemleri üzerinde uygulanması gereken kontrolleri tanımlar ve bu kontroller aracılığıyla organizasyonların sistemlerini yetkisiz erişim, veri sızıntısı,

kötü amaçlı yazılım ve diğer siber tehditlere karşı korumasını sağlamanın yanı sıra ağlara ve verilere yönelik siber güvenlik risklerini yönetmeye ve azaltmaya yardımcı olur.

Ülkemizde uygulanmak üzere 2020 yılında Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (şu an Siber Güvenlik Başkanlığına devredildi) tarafından yayınlanmış olan Kamu Bilgi ve İletişim Güvenliği Rehberi hazırlanma aşamasında NIST ile birlikte ülkemiz kurumsal altyapısı ve altyapı uyumu da dikkate alınan durumlardır. Her iki rehber de teknik detaylarla donatılmıştır. NIST erişim kontrolü, şifreleme, eğitim, izleme gibi konulara değinirken Kamu Bilgi ve İletişim Güvenliği Rehberi ise kullanıcı yönetimi, erişim, ağ güvenliği, log yönetimi, fiziksel güvenlik gibi konulara değinmiştir.

2.2.2. NIS Direktifi (Network and Information Security Directive)

Avrupa Birliği, 2016 yılında NIS Direktifi'ni (EU 2016/1148**)** kabul etmiştir. Bu direktif, Avrupa genelinde ağ ve bilgi güvenliği önlemleri konusunda bir çerçeve oluşturmayı amaçlamaktadır. NIS Direktifi, özellikle kritik altyapı sağlayıcıları ve kamu hizmeti sunan kuruluşları hedef almaktadır. Kamu sektöründeki kuruluşlar, bu direktife uyum sağlamak için güvenlik risklerini yönetmek, güvenlik açıklarını raporlamak ve siber saldırılara karşı dayanıklılığı artırmak zorundadırlar ve ayrıca bu direktif, üyeleri arasında ortak güvenlik politikalarının ve standartlarının oluşturulmasını sağlamaktadır.

Siber güvenlik tehditlerinin arttığı bir dönemde, daha kapsamlı bir güvenlik yaklaşımı getirmek amacıyla bu direktif NIS2 Direktifi olarak güncellenmiştir. Bu yeni direktif, eski direktife göre daha sıkı güvenlik gereksinimleri getirir ve kamu sektöründeki hizmet sağlayıcıların daha güçlü güvenlik önlemleri almasını zorunlu kılar. Ayrıca, kamu sektörü ve özel sektör arasındaki iş birliğini daha da güçlendirir [25].

2.2.3. Cyber Essentials

İngiltere Ulusal Siber Güvenlik Merkezi (National Cyber Security Centre -NCSC) tarafından 2014 yılında oluşturulmuş işletmelerin temel siber güvenlik önlemlerini aldığını belgeleyen bir sertifikasyon programıdır. Bu sertifika programı güvenlik duvarları ve internet geçitleri, güvenli yapılandırma, kullanıcı erişimi kontrolü, zararlı yazılımdan korunma, güncellemeler ve ama yönetimi gibi konulara değinmiştir.

Cyber Essentials uluslararası ya da ulusal bir standart, rehber gibi geniş kapsamlı olmadığı için ülkemizde uygulanmamaktadır, ancak bize ait olan Kamu Bilgi ve İletişim Güvenliği Rehberi, ISO/IEC 27001 ve KVKK ile uyumlu yaklaşımları mevcuttur.

Ülkemizde Cyber Essentials'e birebir örnek olmasa dahi TÜBİTAK BİLGEM'in kurumsal bilgi güvenliği politikasındaki temel kontroller, Bilgi Teknolojileri ve İletişim Kurumu (BTK) ve Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) rehberleri gibi örnek ve uygulamalar ülkemizdeki uygulamalara örnek gösterilebilir.

2.2.4. BSI Grundschutz

BSI IT-Grundschutz, Almanya Federal Bilgi Güvenliği Dairesi (BSI - Bundesamt für Sicherheit in der Informationstechnik) tarafından geliştirilen ve bilgi sistemlerinde sistematik, yapılandırılmış ve uygulanabilir bilgi güvenliği önlemleri sunan bir çerçevedir.

Kurumların bilgi güvenliğini sağlamak için uygulanabilir, somut önlemler sunmak, özellikle kamu kurumları ve kritik altyapı sağlayıcıları için bir rehber ve sertifikasyon zemini oluşturmak, ISO/IEC 27001 ile entegre olabilecek bir ulusal güvenlik yaklaşımı sağlamak BSI Temel Koruma Kataloğunun temel amaçlarındandır [26].

BSI IT-Grundschutz'un en önemli farkı, bilgi güvenliğini sadece teknik bir mesele olarak değil, aynı zamanda organizasyonel, fiziksel ve insan faktörleriyle birlikte ele alması; bu çok boyutlu yapısıyla kurumların bilgi güvenliğini entegre şekilde yönetmesine olanak tanımasıdır. Ayrıca, sistematik kataloglar ve uygulama modülleri sayesinde, kullanıcı dostu ve sürdürülebilir bir uygulama süreci teşvik etmektedir.

2.2.5. JIS Q 27001

Japonya'da Bilgi Güvenliği Yönetim Sistemleri ve İş sürekliliği Yönetim Sistemi (BGYS/ISMS) için kullanılan ulusal standarttır ve ISO/IEC 27001'in Japon endüstriyel sistemine adapte edilmiş versiyonudur.

"JIS" = Japanese Industrial Standards (Japon Endüstri Standartları)
"Q" = Quality Management (Kalite Yönetimi alanı)
"27001" = ISO/IEC 27001 ile birebir uyumludur.

2006 yılında ilk kez yayınlanan standart, ISO/IEC 27001 ne zaman revize edilse ona uygun şekilde güncellenmektedir. En son 2023 yılında ISO/IEC 27001:2022 ile uyumlu hale getirilen son sürüm yayımlandı. Bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi süreçlerini kapsar. Tıpkı ISO 27001 gibi, risk temelli yaklaşımı esas alır [27].

Ulusal bilgi güvenliği standartları ve uygulamaları, ülkelerin kendi regülasyonları ve kurumsal ihtiyaçlarına göre şekillense dahi bireylerin kişisel verilerinin korunması artık küresel düzeyde ortak bir hassasiyet alanı haline gelmiştir. Bu bağlamda, yalnızca kurumsal bilgi güvenliğini değil, bireysel veri mahremiyetini de odağına alan yasal düzenlemeler ön plana çıkmaktadır. Özellikle General Data Protection Regulation (GDPR), bireylerin kişisel verilerinin korunmasına ilişkin standartları belirleyerek global ölçekte bir çerçeve sunarken; Avrupa Birliği Siber Güvenlik Ajansı (ENISA), siber tehditlere karşı teknik rehberlik, politika geliştirme ve kapasite oluşturma alanlarında temel kurumsal yapı olarak öne çıkmaktadır. Öte yandan, dijital finans sektöründeki artan siber riskler ve operasyonel tehditler doğrultusunda geliştirilen Dijital Operasyonel Dayanıklılık Yasası (DORA) ise finansal sistemin bütünlüğünü siber saldırılara karşı korumaya yönelik kapsamlı bir düzenleme olarak devreye alınmıştır. Bu üç yapı; veri koruma, siber güvenlik yönetimi ve dijital operasyonel risk başlıklarında AB'nin çok katmanlı yaklaşımını temsil etmekte, aynı zamanda üye ve aday ülkeler açısından uyum süreçlerinde rehber niteliği taşımaktadır.

2.2.6. AB Genel Veri Koruması Düzenlemesi

Avrupa Birliği, bireylerin kişisel verilerinin korunmasını sağlamak amacıyla 2018 yılında Genel Veri Koruma Tüzüğü'nü (GDPR) yürürlüğe koymuştur. Bu düzenleme kapsamında, özellikle kamu kurumları başta olmak üzere tüm veri sorumluları; kişisel verilerin toplanması, işlenmesi ve saklanması süreçlerinde yüksek düzeyde teknik ve idari güvenlik önlemleri almakla yükümlüdür [28,29].

GDPR'ın temel amacı, AB vatandaşlarının kişisel verilerini dijital çağda daha etkin şekilde korumaktır. Bu düzenleme, kişisel verilerin toplanması, işlenmesi, saklanması ve aktarılmasına ilişkin süreçleri sıkı kurallara bağlayarak veri sahibinin haklarını merkeze almaktadır. GDPR, yalnızca veri korumasını değil, aynı zamanda bireylerin

özel yaşamlarına saygının sağlanmasını, veri sorumlularının şeffaflık ve hesap verebilirlik ilkeleri çerçevesinde hareket etmelerini ve bireylerin kendi verileri üzerindeki kontrolünü artırmayı hedeflemektedir.

Veri işleme kurallarında; veri işlemede şeffaf ve hukuka uygun olması, verilerin ilişkili olduğu amaçla sınırlanması, veri kalitesi, doğruluğu ve hesap verilebilirliği olması, ilgili verinin tutulmasındaki zaman kısıtlanması ve verinin gizliliği ve bütünlüğü korunmasını örnek verilebilir [30].

GDPR'nin uygulanma amacı, sadece AB vatandaşlarının haklarını korumakla sınırlı değildir. Aynı zamanda, küresel ölçekte faaliyet gösteren veri sorumlularına da AB sınırları içinde veri işleme durumunda yükümlülükler getirerek veri güvenliği ve mahremiyetin uluslararası düzeyde standartlaşmasını hedeflemektedir.

Ülkemizde Kişisel Verilerin Korunmasına Yönelik yasal çerçeve (KVKK), 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile oluşturulmuştur. 2016 yılında yürürlüğe giren bu kanun, bireylerin temel hak ve özgürlüklerini korumayı ve kişisel verilerin işlenmesinde uyulması gereken ilke ve yükümlülükleri düzenlemeyi amaçlamaktadır. KVKK, veri sorumlularına aydınlatma yükümlülüğü, açık rıza alma zorunluluğu ve veri güvenliğine ilişkin teknik ve idari tedbirleri uygulama sorumluluğu getirmektedir. Aynı zamanda bireylere, verilerine erişme, düzeltme, silme ve işlenmesini sınırlama gibi çeşitli haklar tanımaktadır. Bu yönüyle KVKK, Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ile yapısal benzerlikler gösterse de, Türkiye'ye özgü düzenlemeler ve uygulama mekanizmalarıyla şekillenmiştir.

Siber güvenlik alanında yapılan çalışmalardan bir diğeri olan European Union Agency for Cybersecurity (Avrupa Birliği Siber Güvenlik Ajansı- ENISA)' nin temel amacı, Avrupa Birliği genelinde siber güvenliğin artırılması, üye ülkeler arasında bilgi paylaşımının teşvik edilmesi, siber tehdit analizlerinin yapılması ve kriz yönetimi kapasitesinin geliştirilmesidir [31].

Ülkemizde ise benzer işlevi yürüten başlıca yapı T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisidir (CBDDO). T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi 10 Temmuz 2018 tarihinde yayımlanan 1 No'lu Cumhurbaşkanlığı Kararnamesi ile kurulmuştur. Bu kararname ile Türkiye'de dijitalleşme, veri yönetimi, siber güvenlik

ve e-Devlet hizmetleri tek bir çatı altında koordineli şekilde yürütülmeye başlanmıştır. CBDDO ise strateji oluşturmanın yanı sıra uygulayıcı ve yönlendirici role sahiptir ancak 2025 yılının Mart ayında yayımlanan bir Cumhurbaşkanlığı Kararnamesi ile CBDDO resmen kapatılmış, görev ve yetkileri Siber Güvenlik Başkanlığı'na devredilmiştir [32, 33].

2020 yılında güncellenen Kamu Bilgi ve İletişim Güvenliği Rehberi, kamu kurumlarında bilgi güvenliği asgari gereksinimlerini belirleyen en önemli politika belgesidir. Her iki yapı da siber güvenlikte farkındalık oluşturma, eğitim faaliyetleri yürütme ve stratejik rehberlik sağlama gibi konularda benzer fonksiyonlara sahiptir.

Avrupa finans sektörünün siber saldırılar ve Bilgi Teknolojileri (BT) risklerine karşı dayanıklılığını artırmak için hazırlanan Digital Operational Resilience Act (Dijital Operasyonel Dayanıklılık Yasası- DORA) ise 28 Kasım 2022 tarihinde Avrupa Birliği Resmî Gazetesi'nde yayımlanan kapsamlı bir düzenlemedir. DORA' nın temel hedefi, finansal kuruluşların bilgi ve iletişim teknolojileri (ICT) altyapısında meydana gelebilecek kesinti, siber saldırı ya da teknik arızalar gibi risklere karşı hazırlıklı olmalarını sağlamak; bu kapsamda risk yönetimi, siber güvenlik, ICT üçüncü taraf risklerinin yönetimi, test süreçleri ve olay raporlama gibi alanlarda uyumluluk zorunluluğu getirmektir [34].

Türkiye'de ise doğrudan DORA' ya denk gelen tekil bir düzenleme bulunmamakla birlikte, benzer amaca hizmet eden çeşitli yasal ve kurumsal yapılar mevcuttur. DORA'nın Türkiye'deki en yakın kurumsal karşılığı Bankacılık Düzenleme ve Denetleme Kurumu (BDDK)'dır. Özellikle BDDK tarafından yayınlanan Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik (2020) ile bankaların bilgi sistemleri güvenliği, hizmet sürekliliği, yedekleme, veri merkezleri kullanımı ve dış hizmet sağlayıcılarla ilişkileri detaylı olarak düzenlenmiştir [35,36].

Banka sistemlerinde etkili bir bilgi güvenliği ve iş sürekliliği alt yapısının oluşturulabilmesi için öncelikle BGYS ve İş sürekliliği Yönetim Sistemi (İSYS) yapısının oluşturulması gerekir. Bilgi güvenliği ve iş sürekliliği organizasyonların işlevlerine göre uygun yöntem, nitelikli iş gücü, politika, yazılım ve donanım desteği

gerçekleştirilebilir. Özellikle kritik sistemlerde iş sürekliği ve bilgi güvenliğinin sağlanması maddi, manevi kayıpların önüne geçilmesinde önemlidir [37].

ISO/IEC 27001; Bilgi Güvenliği Yönetim Sistemi kurmak isteyen kuruluşların bağlamları, temel gereksinimleri, liderlik ve altyapı koşulları hakkında genel kuralları belirleyen uluslararası alanda kabul görmüş standarttır. Standarda tabii olmak için gönüllülük esastır, herhangi bir zaruriyet yoktur ama uyulması gereken prensipler net olarak açıklanmıştır. Bütün uluslar nazarında kabul gördüğü için risk yönetimi konusunda rehber niteliğindedir; Kamu Bilgi ve İletişim Güvenliği Rehberi, kamu kurumlarının bilgi güvenliği yönetim sistemi kurmaları, yönetmeleri ve güvenliğini sağlamaları için rehberlik sunan bir regülasyondur.

Bu çalışma; ISO/IEC 27001 standardı ile Kamu Bilgi ve İletişim Güvenliği Rehberi arasındaki önemli boşluklar incelenip, her iki belgenin genel yaklaşımı, kapsam ve uygulama alanları, risk yönetimi, denetim ve değerlendirmesi, hedef kitleleri, yönetime yaklaşımları ve teknik detayları analiz edilerek bunları anlamak ve uygulanabilir çözümler bulmak amaçlanmaktadır. Bu kapsamlı analiz, her iki standardın farklılıklarını ve benzerliklerini derinlemesine belirlemeyi ve her birinin uygulama alanlarını daha iyi anlamayı hedeflemektedir. Ayrıca bu standart ve regülasyonun farklı mevzuatlara, risk yönetimi stratejilerine, süreç yönetimi tekniklerine, denetim sistemlerine ve dokümantasyon yaklaşımlarına ilişkin yönlerinin detaylı bir şekilde incelenmesi de bu raporun kapsamını oluşturarak önemli bir yer tutmaktadır. Bu bağlamda, her iki standardın ne şekilde etkileşimde bulunduğu ve hangi alanlarda birbirlerini desteklediklerı açık kalan noktalar analiz edilecektir.

BÖLÜM 3: ISO/IEC 27001

ISO/IEC 27001, Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmak, uygulamak, sürdürmek ve sürekli iyileştirmek isteyen kuruluşlar için uluslararası geçerliliğe sahip bir standarttır. BGYS'nin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için uluslararası kabul görmüş bir standart olarak uzun yıllardır kullanılmaktadır. İlk olarak 2005 yılında yayınlanan bu standart, 2013 ve 2022 yılında kapsamlı revizyonlar geçirmiştir. Yayınlanan ISO/IEC 27001:2022 versiyonu, önceki versiyona göre daha sadeleştirilmiş ve güncellenmiş kontrol setleri ile dijitalleşen dünyaya daha etkili bir risk yönetimi yapılmasını mümkün kılmıştır.

Standart; kuruluşun bağlamı, liderlik, risk temelli düşünce, destek, operasyon, performans değerlendirme ve iyileştirme gibi temel yönetim sistemi ilkeleri üzerine kuruludur. ISO/IEC 27001'in amacı, kuruluşların bilgi varlıklarını sistematik bir şekilde koruyarak gizlilik, bütünlük ve erişilebilirlik ilkeleri doğrultusunda bilgi güvenliğini sağlamaktır. Uygulaması yasal bir zorunluluk olmasa da, risk yönetimi süreçlerinde küresel ölçekte rehber olarak kabul edilmektedir [38].

Bir kurum ve kuruluşta bilgi güvenliği yönetim sistemi içi elzem olan kurulum, uygulama, sürdürülmesi ve sürekli iyileştirilmesi için geliştirilmiştir. Kurum içinde ya da dışından art niyetli ve doğru olmayan kullanımlara karşı bilginin muhafaza edilmesi gerekliliklerini tanımlar. Sektör ya da işletme büyüklüğü ayırt etmeksizin (ticari işletmeler, devlet kurumları, mikro işletmeler, çokuluslu şirketler, perakendecilik, bankacılık, savunma, sağlık, eğitim kurumları vb.) tüm kuruluşların yararlanabilmesi üzerine geliştirilmiştir [39].

ISO/IEC 27001 standardının kökeni, 1995 yılında İngiliz Standartları Enstitüsü (British Standards Institution - BSI) tarafından yayımlanan BS 7799 standardına dayanmaktadır. BS 7799, bilgi güvenliği yönetimi konusunda iyi uygulama örneklerini içermekteydi. 1999 yılında bu standardın ikinci kısmı olan BS 7799-2 yayımlanmış ve bilgi güvenliği yönetim sistemleri için özel gereksinimleri tanımlamıştır. Bu belge, aynı zamanda bilgi güvenliği yönetimi alanında sertifikasyon yapılabilmesini de mümkün kılmıştır. 2005 yılında ise bu standart, ISO tarafından kabul edilerek ISO/IEC

27001 adıyla uluslararası düzeye taşınmıştır. ISO/IEC 2700'in tarihsel gelişimi Şekil 3.1'de görülmektedir.

Şekil 3.1. ISO 27001 / 27002 Tarihsel Gelişimi

2013 yılında, ISO/IEC 27001 standardı önemli bir revizyondan geçirilmiştir ve bu revizyon sayesinde risk yönetimi ve sürekli iyileştirme konularına daha fazla vurgu yapılmıştır. 2022 yılında, ISO/IEC 27001 standardı yeniden güncellenmiştir. Bu güncelleme ile yeni teknolojiler ve ortaya çıkan tehditler karşısında standardın etkinliğini artırması hedeflenmiştir.

ISO/IEC 27001 her türlü ve her boyuttaki organizasyon için uygun olan genel bir standarttır. Küçük, orta ve büyük ölçekli işletmeler, finansal kuruluşlar, sağlık sektörü, kamu kurumları, üretim ve hizmet sektörleri gibi farklı sektörlerde faaliyet gösteren her kuruluş, ISO/IEC 27001'i uygulayabilir. Bu standart, bilgi varlıklarının korunmasını ve risksiz ya da yönetilebilir derecede düşük riskli bir ortamın sağlanmasını hedefler ve gizlilik, bütünlük ve erişilebilirlik ilkelerini korumayı içerir.

ISO/IEC 27001 kuruluşların yasal ve düzenleyici gereksinimlere uyum sağlamasına yardımcı olur. Bu konu özellikle veri koruma yasaları ve düzenlemeleri açısından önemlidir. Bu standardın kurallarının kapsayıcı ve koruyuculuğu kurumun güven ve itibarını arttırmasını sağlar. Bu temel ilkeler risk tabanlı yaklaşımı teşvik ederek standarda tabi kuruluşların riskleri değerlendirmesini, yöneterek uygun kontrolleri seçmesini sağlar. Standart aynı zamanda temel ilkeleri ile ona tabii olan kuruluşların bilgi güvenliği yönetim performanslarını ve sürekli iyileştirme süreç yönetimlerini izleme, iş sürekliliği ve risk yönetimi konularında kurumlara fayda sağlamaktadır. Bu

sayede, kurumlar veri güvenliği konusunda önemli adımlar atar ve potansiyel tehlikelere karşı daha hazırlıklı olurlar.

ISO/IEC 27001'in içeriği, standartta yer alan başlıca gereklilikleri ve kuruluşların bu gereklilikleri nasıl yerine getireceklerini ayrıntılı bir şekilde açıklar. Standart, kuruluşlardan risk analizi yapmalarını, bilgi güvenliği politikaları oluşturmalarını, personelin eğitim ihtiyaçlarını belirlemelerini ve sürekli gözden geçirme faaliyetleri yapmalarını ister ve ayrıca; ISO/IEC 27001'in içeriği belgelendirme denetimleri için hangi dokümantasyonun gerektiğini ve kuruluşların sürekli iyileştirme için neler yapmaları gerektiğini detaylı bir şekilde açıklar.

27000 ailesinin diğer bir standardı olan ISO/IEC 27002, ISO/IEC 27001'in gereksinimlerini detaylandıran bir rehber standarttır. ISO/IEC 27001 ve ISO/IEC 27002 arasında da sıkı bir ilişki bulunmaktadır. Çünkü ISO/IEC 27002, bilgi güvenliğinin yönetimini sağlamak için pratik öneriler sunar ve ISO/IEC 27001 ile uyumlu bir şekilde kullanılır. ISO/IEC 27001'e uygunluk sağlamak isteyen kuruluşlar, ISO/IEC 27002'nin yönergelerine başvurarak bilgi güvenliği kontrollerini etkili bir şekilde uygulayabilirler.

Genel Veri Koruma Yönetmeliği (GDPR) ve ISO/IEC 27001 arasında da sıkı bir ilişki bulunmaktadır. GDPR, kişisel verilerin korunması ve işlenmesi konusunda kuruluşlara yönelik standartları belirlerken ISO/IEC 27001, bilgi güvenliği yönetim sistemi standartlarını ortaya koymaktadır. Bu nedenle, GDPR kapsamında uyumlu olmak isteyen kuruluşlar, ISO/IEC 27001 standardına uygunluk sağlayarak bilgi güvenliği konusunda gereken adımları atabilirler.

Bilgi güvenliği trendleri, teknolojinin hızlı değişimi ve dijital dönüşüm süreciyle doğrudan ilişkilidir. Dijital sistemler üzerinde, bir dokümanda, depolama cihazlarında, bilgisayarlarda veya telefonlarda, e-postalarda olmak üzere hemen hemen her yerde bilgi bulunabilmektedir. Bilgi güvenliği, kurumlardaki çalışanlar ile hareket edilerek, iş süreçlerinin desteklenmesinde, işin sürekliliğinin güvenli bir şekilde sağlanmasında, kurumun dış veya iç tehditlerden korunmasında önemli bir role sahiptir [40].

Bulut bilişim, yapay zeka, mobil teknolojiler, nesnelerin interneti, ve artan veri analitiği gibi konular bilgi güvenliği alanını etkileyen temel trendler arasında yer

almaktadır. ISO/IEC 27001 standardı, bu trendlere adaptasyon sürecinde kritik bir rol oynamakta ve kurumların bilgi varlıklarını bu yeni tehditlere karşı korumalarını sağlamak için gerekli yönergeleri sunmaktadır. Bu sayede ISO/IEC 27001, bilgi güvenliği trendleriyle uyumlu bir şekilde geliştirilerek, organizasyonların bilgi güvenliği stratejilerini güncel tutmalarını desteklemektedir.

Bu standardın temel yaklaşımı, sürekli iyileştirmeyi ve risk tabanlı bir yaklaşımı benimsemeyi içerir.

3.1. ISO/IEC 27001 Temel Maddeleri

ISO/IEC 27001 standardı 10 maddeden oluşmaktadır. Standardın ilk 3 maddesi olan Kapsam, Bağlayıcı Atıflar, Terimler ve Tanımlar ISO standart ailesi içinde yer alan genel ifadelerdir. 4. Madde sonra standardın detayları yer alır. Bu maddeler ve temel hedefleri aşağıda yer almaktadır.

- **Kuruluşun Bağlamı**: Bilgi Güvenliği Yönetim Sistemi kurulmadan önce, kuruluşun iç ve dış çevresi ile ilişki içinde değerlendirilmesi gereken önemli bir konudur. ISO/IEC 27001 standardına göre, bir kuruluşun bağlamını anlamak, bilgi güvenliği yönetim sisteminin etkin bir şekilde tasarlanabilmesi, uygulanabilmesi ve sürdürülmesi için kritik öneme sahiptir. Kuruluşun bilgi güvenliği hedeflerinin belirlenmesinde rehberlik eder, kaynakların doğru şekilde tahsis edilmesini sağlar ve risklerin yönetilmesine yardımcı olur bununla birlikte; bağlamın doğru şekilde anlaşılması, yasal uyumluluğun sağlanması ve kuruluşun itibarının korunması açısından da kritik bir adımdır. Kuruluşun bağlamını anlamak, aynı zamanda ISO/IEC 27001'in sürekli iyileştirme yaklaşımını benimsemesi için önemlidir. Bu bağlamda yapılan analizler, organizasyonun karşılaştığı değişikliklere hızlı bir şekilde adapte olabilmesini sağlar.

- **Liderlik:** Kuruluşun üst düzey yöneticilerinin ve liderlerinin, bilgi güvenliği yönetim sistemine olan bağlılıklarını, desteğini ve katılımını sağlamak için gerekli olan liderlik ve yöneticilik faaliyetlerini içerir. Liderlik; bilgi güvenliği ile ilgili net ve açık politikaların oluşturulmasına

öncülük etmelidir. Bu politikalar, organizasyonun bilgi güvenliği stratejilerini, hedeflerini ve taahhütlerini açık bir şekilde belirtir. Üst düzey yönetimin kararlılığı ve liderliği, organizasyonun bilgi güvenliğine nasıl yaklaşacağını belirler ve bu yaklaşımın organizasyon genelinde yayılmasını sağlar.

- **Planlama**: Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) başarılı bir şekilde kurulması, uygulanması ve sürdürülmesi için kritik bir aşamadır. Stratejik ve operasyonel düzeyde belirli adımların atılmasını sağlar. Planlamanın en temel bileşenlerinden biri risk yönetimi süreçleridir. Bilgi güvenliği hedeflerine ulaşmak için gerekli olan insan kaynakları, finansal kaynaklar, teknolojik altyapı ve zaman gibi kaynakların planlanması gerekmektedir. Bu, BGYS'nin uygulanabilirliğini ve sürdürülebilirliğini sağlamak için kritik bir adımdır. Organizasyonun bilgi güvenliği yönetim sistemine dair bir yol haritası oluşturulmasını sağlar.

- **Destek**: Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulamalarının etkin bir şekilde sürdürülebilmesi için gerekli olan kaynaklar, yetkinlikler ve altyapının sağlanması sürecidir. Sistemin doğru bir şekilde çalışabilmesi, güvenlik hedeflerine ulaşılabilmesi ve sürekli iyileştirme sağlanabilmesi için gereken tüm destek unsurlarını kapsar.

- **İşletim**: Organizasyonun BGYS'nin işleyişi için gerekli olan operasyonel faaliyetlerin nasıl gerçekleştirileceğine dair gereksinimleri belirler. Bu süreç, hem günlük faaliyetlerin sürdürülebilirliğini hem de bilgi güvenliğine dair risklerin etkin bir şekilde yönetilmesini sağlar. İşletim aşamasında, risklerin yönetilmesi ve risk yanıtlarının uygulanması kritik bir rol oynar.

  Bilgi güvenliği politikalarının, prosedürlerinin ve kontrollerinin etkin bir şekilde uygulanmasını, izlenmesini ve sürekli olarak iyileştirilmesini öngörerek, etkin bir işletim süreci, organizasyonun güvenlik tehditlerine

karşı dayanıklı olmasını sağlar ve bilgi güvenliğini uzun vadede sürdürülebilir hale getirir.

- **Performans Değerlendirmesi**: Bu aşama Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulamalarının etkinliğini ölçmek ve izlemek için yapılan süreçtir. BGYS' nin hedeflerine ne ölçüde ulaşıldığını belirlemek, sürekli iyileştirmeyi sağlamak ve organizasyonun bilgi güvenliği konusundaki başarısını değerlendirmek amacıyla gerçekleştirilir.

- **İyileştirme**: Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulamalarının etkinliğini sürekli olarak artırmak ve güvenlik risklerini minimize etmek için yapılan süreçtir. İyileştirme, organizasyonun bilgi güvenliği hedeflerine ulaşabilmesi için sürekli bir çaba gerektirir ve bu, sistemin zayıf noktalarının belirlenip düzeltilmesi, yeni güvenlik tehditlerine karşı önlemler alınması, ve daha iyi performans için değişiklikler yapılması anlamına gelir.

  İyileştirme sadece mevcut eksikliklerin giderilmesi değil, aynı zamanda organizasyonun gelecekteki güvenlik risklerine karşı daha dayanıklı hale gelmesi için sürekli bir süreçtir. Sürekli gelişim ilkesine dayanır ve organizasyonların güvenlik açıklarını erken tespit etmelerini, güvenlik önlemlerini iyileştirmelerini ve potansiyel tehditlere karşı hızlı bir şekilde tepki vermelerini sağlar.

  Düzeltici ve önleyici aksiyonlar (gelecekte meydana gelebilecek potansiyel sorunları önlemek amacıyla alınan önlemler), sürekli iyileştirme döngüsü, iç denetimler ve yönetim gözden geçirmeleri, organizasyonların BGYS'lerini etkin bir şekilde iyileştirmelerine yardımcı olur. Bu süreç, organizasyonun güvenlik tehditlerine karşı daha dirençli hale gelmesini sağlar ve bilgi güvenliğini sürdürülebilir bir şekilde yönetmeye olanak tanır.

3.2. ISO/IEC 27001 EK-A

ISO/IEC 27001:2022 Ek bilgi güvenliği kontrolleri için yönetim sistemi olan bir rehberdir ve standardın ana gerekliliklerini tamamlayıcı niteliktedir. Ek-A, ISO/IEC 27002 standardı ile uyumlu olarak hazırlanmıştır ve kuruluşların bilgi güvenliği risklerini yönetmek için uygulayabileceği 93 kontrolü içerir. Bu ek, organizasyonun bilgi güvenliği politikası, hedefleri, prosedürleri ve yönetim taahhütleri hakkında detaylı bilgiler içerir. Organizasyonun iç ve dış bağlamını, risk yönetimini ve belgelendirme sürecini de içeren Bilgi Güvenliği Yönetim Sistemi gerekliliklerine uygunluğunu gösterir. Kısacası, ISO/IEC 27001 Ek-A, temel olarak organizasyonun bilgi güvenliğine nasıl yaklaşması gerektiği ve bu konuda neleri yapması gerektiğini gösterir.

Ek-A'da listelenen kontroller, kuruluşların bilgi güvenliği risklerini azaltmak için uygulayabileceği pratik önlemler sunar. Örneğin, erişim kontrolü, şifreleme, fiziksel güvenlik gibi alanlarda rehberlik sağlar.

Ek-A'daki kontroller, kuruluşların yasal ve düzenleyici gerekliliklere uyum sağlamasına yardımcı olur. Örneğin, KVKK (Kişisel Verilerin Korunması Kanunu) veya GDPR (Genel Veri Koruma Tüzüğü) gibi düzenlemelere uyum için gerekli önlemleri içerir ve Ek-A'daki kontroller, kuruluşun büyüklüğüne, sektörüne ve risk profiline göre özelleştirilebilir. Her kontrolün uygulanması zorunlu değildir; sadece kuruluşun risk değerlendirmesi sonucunda belirlenen ihtiyaçlara göre seçilir.

ISO/IEC 27001 standardı ile 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) arasında doğrudan bir bağlantı bulunmamakla birlikte, bu standart ve yasaya göre kurumların bilgi güvenliği süreçlerini yapılandırmasında tamamlayıcı roller üstlenmektedir. ISO/IEC 27001, bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurarak bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini sağlamak üzere risk temelli teknik ve idari kontroller sunarken; KVKK, bireylerin kişisel verilerinin korunmasını anayasal bir hak olarak tanımlamakta ve kurumlara bu doğrultuda hukuki yükümlülükler getirmektedir. ISO/IEC 27001'in içerdiği erişim kontrolleri, şifreleme mekanizmaları, veri sınıflandırma, fiziksel güvenlik, tedarikçi ilişkileri yönetimi gibi uygulamalar, kişisel verilerin güvenli şekilde işlenmesi ve korunması için KVKK' ya teknik uyum açısından destek sağlar. KVKK' ya uymak zorunda olan kurumlar için

ISO/IEC 27001 yalnızca bir standart değil, aynı zamanda risklerin azaltılması, veri ihlallerinin önlenmesi ve hukuki yaptırımlardan kaçınılması için etkili bir uygulama aracı olarak değerlendirilmektedir [41].

ISO/IEC 27001 standardı kişisel verilerin korunmasına doğrudan odaklanmamıştır fakat kişisel verilerin güvenliğini sağlamak için gerekli bilgi güvenliği kontrollerini içeren genel bir çerçeve sunar. Bu nedenle, kişisel verilerin korunmasına dolaylı olarak katkı sağlar. Standart verilerin türünü ayrıştırmaz; kişisel veriler de bilgi varlıkları olarak kabul edilir. Bu nedenle, bir kurum ISO/IEC 27001'e uygun bir sistem kurduğunda, kişisel veriler de güvenlik kontrolleri kapsamına girer.

Ek-A kontrol seti içinde KVKK ile ilgili olabilecek maddelere örnek verilebilir.

A.5.12: Bilgi sınıflandırma
A.5.15 Erişim kontrolü
A.8.24: Şifreleme
A.5.34: Gizliliğin korunması ile ilgili mevzuat ve sözleşme yükümlülükleri

ISO/IEC 27001 Ek-A, bilgi güvenliği yönetim sistemi (BGYS) için bir dizi referans kontrolü ve rehber ilkesi içerir. 2022 yılında yapılan değişiklikle Ek-A'daki kontrol grupları yeniden düzenlenerek 14 ana tema 114 kontrol maddesi yerine 4 ana tema ve 93 kontrol maddesi olacak şekilde gruplandırılmıştır. Kontroller ve bu kontrollere ilişkin madde sayıları Tablo 3.1'de yer almaktadır.

Tablo 3.1 ISO/IEC 27001 EK-A Kontrolleri ve Madde Sayıları

Kontrol	Madde Sayısı
Kişi kontrolleri	8
Kurumsal kontroller	37
Teknolojik kontroller	34
Fiziksel kontroller	14

Ek-A, ISO/IEC 27001 standardının zorunlu bir parçasıdır. Ancak, standardın ana gerekliliklerini tamamlayıcı nitelikte olduğu için büyük önem taşır. Örneğin; ISO/IEC 27001, risk temelli bir yaklaşım benimser. Kuruluşlar, risk değerlendirmesi sonucunda

belirledikleri riskleri azaltmak için Ek-A'daki kontrolleri seçebilir. Bu nedenle, Ek-A'nın uygulanması, kuruluşun risk profiline bağlıdır.

ISO/IEC 27001 kuruluşlara yasal ve düzenleyici gereksinimlere uyum sağlama konusunda destek olmaktadır. Bunun yanı sıra ISO/IEC 27001 Ek-A'nın uygulanması, iş sürekliliği sağlama ve potansiyel tehlikelere karşı hazırlıklı olma konusunda önemli katkılar sağlamaktadır.

ISO/IEC 27001 Ek-A'nın kuruluşlara sağladığı önemli katkılardan biri ise müşteri güveni ve pazar rekabeti konusunda avantaj sağlamasıdır. Kuruluşlar; bu standardı benimseyip uygulayarak potansiyel müşterilerde güven oluşturup, rekabet avantajı elde edebilirler. Uluslararası geçerli bir standart eki olduğu için ISO/IEC 27001 Ek-A uygulanması sayesinde kuruluşlar, yasal ve mevzuat gerekliliklerine daha sıkı ve kolay bir şekilde uyum sağlayabilir, bu da iş sürekliliği ve itibarlarının artmasına yardımcı olabilir.

3.3. ISO 27002

ISO 27002 standardı; bilgi güvenliği yönetimi için en iyi uygulamaları içeren bir dayanak noktası olarak kabul edilmektedir. Bu standart, bilgi varlıklarını korumak ve bu konudaki süreçleri etkili bir şekilde yönetmek için organizasyonlara ISO/IEC 27001 sürecinde yol göstermesi ve bilgiyi koruma süreçlerinden dolayı bir rehber niteliğindedir.

ISO/IEC 27002, bilgi güvenliği kontrollerine ilişkin bir dizi rehber ilke ve en iyi uygulama sunan uluslararası bir standarttır. Bu standart, ISO/IEC 27001 kapsamında tanımlanan kontrollerin nasıl uygulanacağına dair detaylı açıklamalar sağlar ve kuruluşlara risk temelli yaklaşımla güvenlik tedbirlerini seçme, uygulama ve sürdürme konusunda destek olur. Standart; bilgi güvenliği politikaları, insan kaynakları güvenliği, fiziksel ve çevresel güvenlik, erişim kontrolü, kriptografi, operasyonel güvenlik gibi çok sayıda alanda öneriler sunar [38].

ISO 27002 standardı maddeleri Ek–A ile bire bir aynı olup Ek–A’ da tanımlanan gereksinimlerin nasıl karşılanacağını ve nasıl uygulanacağını göstermektedir. Standardın yapısı, organizasyonların bilgi güvenliği risklerini belirlemelerine, yönetmelerine ve azaltmalarına yardımcı olan kontrol hedeflerini ve kontrolleri içerir.

Ayrıca standart; organizasyonların bilgi güvenliği politikalarını, prosedürlerini ve süreçlerini geliştirmeleri için yönergeler sunar. Örn : Madde: 5 Liderlik, Üst yönetim, BGYS'nin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi konusunda aktif rol almak ve bunu açıkça desteklemekle yükümlüdür.

ISO/IEC 27002 uygulamasının adımları; belirlenen bilgi güvenliği politikalarının ve risk yönetimi süreçlerinin organizasyon içinde etkin bir şekilde hayata geçirilmesini içerir. Bilgi varlıklarının envanterinin çıkarılması, risk yönetimi sürecinin uygulanması, uygun güvenlik kontrollerinin seçimi ve uygulanması, personelin eğitimi ve farkındalığının artırılması başlıca adımlardandır. Bu rehberin uygulanması, kuruluşlara rekabet avantajı sağlayarak müşteri memnuniyetini artırabilir ve iş başarısını destekleyebilir. Ayrıca, ISO/IEC 27001 standardına uygunluk sağlandıktan sonra sürekli iyileştirme ve gözden geçirme adımları da süreçte kritik öneme sahiptir.

BÖLÜM : 4 KAMU BİLGİ VE İLETİŞİM GÜVENLİĞİ

Kamu Bilgi ve İletişim Güvenliği Rehberi, kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerin bilgi ve iletişim güvenliği kapsamında genel olarak alması gereken tedbirleri belirlemek için Cumhurbaşkanlığı Dijital Dönüşüm Ofisi koordinasyonunda paydaşların katılımıyla hazırlanan rehberdir [42]. Doküman bundan sonra rehber olarak ifade edilecektir.

Rehber oldukça fazla teknik tedbirin yer aldığı, hemen hemen bilgi teknolojilerindeki her alana dokunduğu, güvenlik tedbirlerinin ürün ve teknolojiden bağımsız seçimine olanak verdiği, ortak mutabakat ile hazırlanması ve ulusal / uluslararası mevzuat ve standartlara uyumlu olması gibi özellikleri ile güçlü bir rehber niteliğindedir [43].

Rehberin Kapsamı; bilgi işlem birimi barındıran veya bilgi işlem hizmetlerini sözleşmeler çerçevesinde üçüncü taraflardan alan, devlet teşkilatı içerisinde yer alan kurum ve kuruluşlar ile kritik altyapı hizmeti veren işletmeleri kapsamaktadır.

Rehberin uygulanması sonucu elde edilmesi beklenenler somutlaştırılarak 12 hedef olarak tanımlanmıştır:

1. Yerli ve milli ürün kullanımının teşvik edilmesi ,
2. Rehberi uygulayacak kurum ve kuruluşlarda yapılacak mükerrer çalışmaların ve yatırımların önüne geçilmesi ,
3. Güvenlik tedbirlerinin üç seviyeli olacak şekilde derecelendirilmesi ve varlık gruplarına güvenlik dereceleri ile uyumlu asgari güvenlik tedbirlerinin uygulanması,
4. Rehberin güvenlik tedbirleri ile ilgili detayların izlenebilirliğinin sağlanacak şekilde yapılandırılması ,
5. Güvenlik tedbirlerinin ürün ve teknoloji bağımsız olarak uygulanabilir olması ,
6. Güvenlik tedbirlerinin uygulanıp uygulanmadığının denetlenebilmesi ,
7. Güvenlik tedbirlerinin birbirinden bağımsız şekilde uygulanabilirliğini sağlayacak şekilde gruplandırılması ve rehberin modülerliğinin sağlanması ,
8. Tedbirlerin teknik olarak tüm kurum ve kuruluşlar tarafından uygulanabilir olması ,

9. İhtiyaçlar, gelişen ve değişen şartlar dikkate alınarak rehberin sürdürülebilirliğinin sağlanması,

10. Rehberin format ve içeriğinin özgün olması ,

11. Rehberin hem güvenlik tedbirlerini uygulayacak personele hem de bu tedbirlerin uygulanıp uygulanmadığını kontrol edecek denetçilere hitap etmesi ,

12. Rehber içeriğinin bilgi güvenliği çerçevesinde oluşturulmuş mevzuat ve rehberler ile ulusal/uluslararası standartlara uyumlu olması.

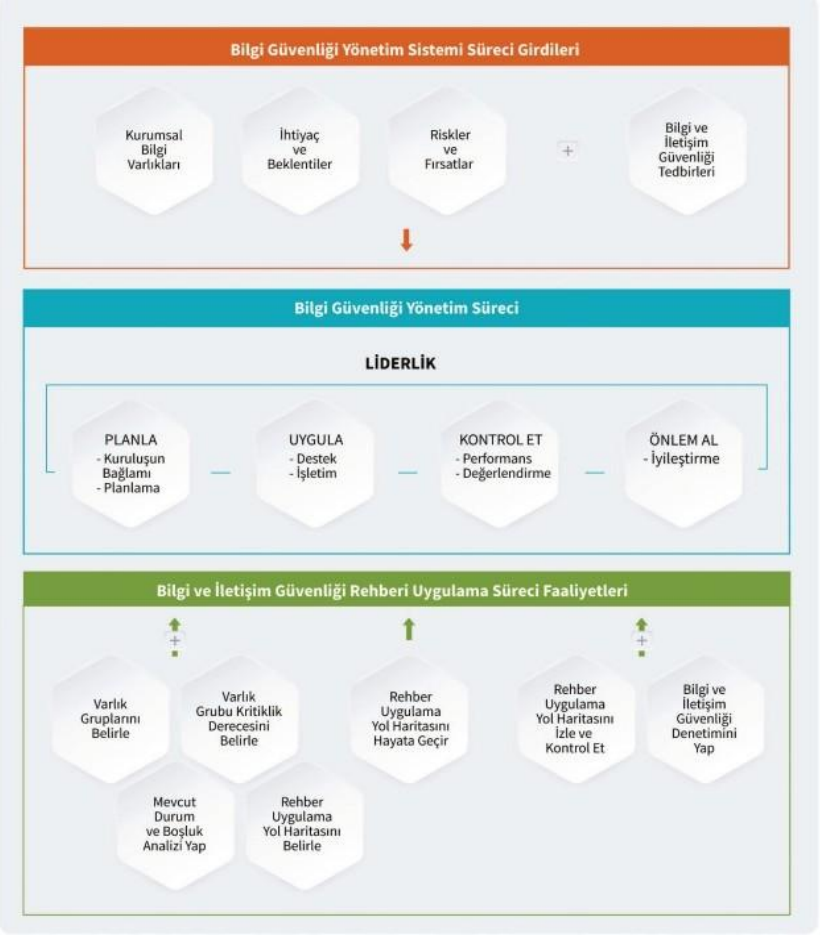
Bilgi ve iletişim güvenliğinin kavramını, önemini, temel ilkelerini, tehditlerini, standartlarını ve iyi uygulama örneklerini ele alan bu rehberle kamu kurumlarının bilgi ve iletişim güvenliği konusundaki ihtiyaçlarını analiz etmek, çözüm seçenekleri bulmak ve bu alanda en iyi uygulamaları teşvik etmek temel amaçtır. Rehberin 12 temel hedefi Şekil.4.1'de yer almaktadır [42].

Şekil 4.1. Bilgi ve İletişim Güvenliği Rehberi'nin hedefleri

Kuruluşlar günümüzün internet dünyasında hem kurum içi hem de kurum dışı tehditler karşısında savunmasız hale gelebiliyorlar. Özellikle kamuya açık sistemlerdeki güvenlik açıkları kuruluş için hayati etkilere sahip olabilir. Yaygınlaşan bilgisayar sistemleri, mobil uygulamalar, e-posta ve tüm haberleşme uygulamaları, web siteleri bunlardan örnek olarak verilebilir. Kuruluşun mevcut bilgilerini

koruyamaması ve uygun güvenlik yönergelerini seçme ve uygulamadaki yetersizlikleri itibar kaybına sebep olabilmektedir. [44].

Rehber, bilgi güvenliği politikaları, bilgi sınıflandırma ve işleme yöntemleri, ağ güvenliği, fiziksel güvenlik tedbirleri, bilgi güvenliği eğitimleri gibi konuları detaylı bir şekilde ele almasının yanında ayrıca bilgiye erişim yetkilendirmesi, güvenli iletişim teknolojileri ve güvenli yazılım uygulamaları gibi konulara da değinmektedir. Kamu çalışanlarının bu rehberi kullanarak bilgi ve iletişim güvenliğini sağlamaları ve korumaları hedeflenmektedir. Bu kapsamda, bilgi güvenliği, veri bütünlüğü, erişilebilirlik, gizlilik ve güvenlik gibi temel ilkeler dikkate alınır. Ayrıca, standartlar ulusal ve uluslararası kuruluşlardan alınan öneriler ve kabul görmüş güvenlik protokolleriyle uyumlu olmalıdır. Kamu Bilgi ve İletişim Güvenliği Rehberi ve Bilgi Güvenliği Yönetim Sistemi ilişkisi Şekil.4.2 ‘de aşağıda yer almaktadır [42].

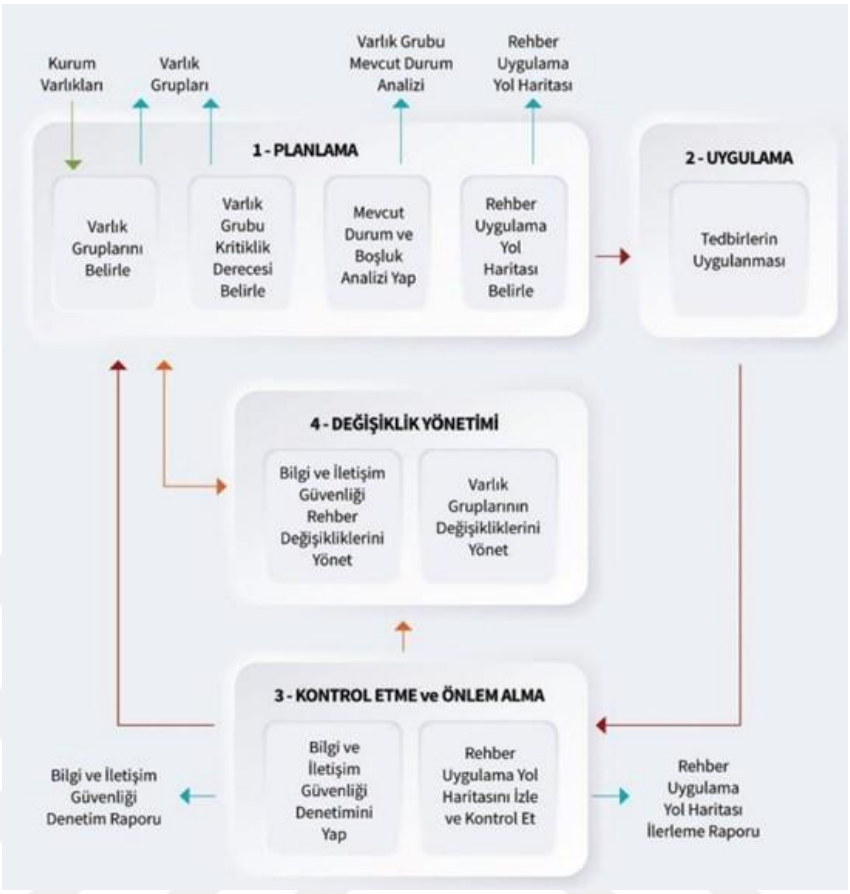


Şekil 4.2. Rehber ve Bilgi Güvenliği Yönetim Sistemi ilişkisi

Kamu Bilgi ve İletişim Güvenliği Rehberi'nin uygulama alanları oldukça geniştir. Kamu kurumları ile bağlı ve ilgili kuruluşlar, Ulusal Siber Güvenlik Stratejisinde belirlenen kritik altyapı sektörlerinde bulunan işletmeler bu rehberin kapsam alanındadır. Elektronik haberleşme, enerji, finans, ulaştırma, su yönetimi, kritik kamu hizmetleri bu işletmelere verilebilecek önemli örneklerdir.

Bu rehber, kamu kurumlarının operasyonel sürekliliğini sağlamak, güvenliği artırmak ve yasal düzenlemelere uygun hareket etmelerine yardımcı olmanın yanında; çalışanların bilinçlenmesi ve eğitilmesi yoluyla kurum içi veri güvenliği kültürünün oluşturulmasına katkı sağlamaktadır. Güncel tehditlere karşı korunma sağlayarak kurumların itibarını ve güvenilirliğini arttıran bu rehber, veri gizliliğini koruyarak kamu hizmetlerinin kesintisiz bir katkı sağlamaktadır.

Rehberin önceliği kamu kurumları ve çalışanlarının hassas bilgilerinin korunması gerekliliğidir. Kamu hizmetlerinin kesintisiz bir şekilde sürdürülmesi için bilgi ve iletişim güvenliğinin sağlanması zorunludur. Her geçen gün siber saldırıların artmasıyla oluşan bilgi sızıntılarının olumsuz etkileri göz önüne alındığında kamunun güvenliğinin sağlanması zorunluluktur. Şekil.4.3.'te rehberin uygulanma süreci tüm detaylarıyla görselleştirilmiştir [42].



Şekil 4.3. Bilgi ve İletişim Güvenliği Rehberi uygulama süreci

Rehberde dikkat çeken önemli unsurlardan biri, sadece donanım ve yazılım temelli tedbirlerin değil, aynı zamanda kurumsal farkındalık, erişim kontrol politikaları, loglama, eğitim faaliyetleri ve olay müdahale prosedürlerinin de sistematik bir biçimde tanımlanmasıdır. Bu çerçevede, erişim yetkilerinin rol bazlı verilmesi, veri yedeklerinin güvenli alanlarda tutulması, kullanıcı aktivitelerinin kayıt altına alınması, veri sınıflandırma sistemleriyle bilgi varlıklarının etiketlenmesi, ve personelin bilgi güvenliği konusunda düzenli eğitimlere tabi tutulması gibi birçok uygulama, rehberin temel uygulama başlıkları arasında yer alır. Ayrıca rehber, yalnızca mevcut durumun korunmasını değil, aynı zamanda gelişen teknolojik tehditlere karşı dinamik bir güvenlik yaklaşımının benimsenmesini önermektedir. Bu bağlamda, yapay zekâ, bulut bilişim, büyük veri ve nesnelerin interneti (IoT) gibi güncel teknolojilerin kullanımı sırasında doğabilecek yeni tehdit türlerine karşı rehberin revize edilmesi gerektiği belirtilmektedir. Bu da rehberin statik değil, sürekli güncellenmesi gereken yaşayan bir belge olduğunu göstermektedir.

Kamu Bilgi ve İletişim Güvenliği Rehberi esnek ve modüler yapısıyla güvenlik bilgilerini, milli güvenliğe özel olarak toplar ve bu şekilde birimlerden bağımsız olarak kullanılabilir şekilde tasarlanmıştır. Bununla birlikte, rehberdeki uygulamanın uygulanıp uygulanmadığını değerlendirme amacıyla inceleme, gözden geçirme, sızma testi ve kaynak kod analizi gibi çeşitli düzenlemelerin yapılmasına, işletilmesine, kontrol ve denetimlerinin yapılmasına olanak sağlar gerçek bir rehber gibi Türkiye Cumhuriyeti kurum ve kuruluşlarına kılavuz olacak bir dokümandır.

Kamu Bilgi ve İletişim Güvenliği Rehberi ülkemizde kamu kurumlarında bilgi güvenliğini sağlamak amacıyla hazırlanmış kapsamlı bir çerçeve sunmakta ve kişisel verilerin korunmasını bilgi güvenliği yönetiminin ayrılmaz bir parçası olarak ele almaktadır. Özellikle kişisel verilerin işlenmesi, saklanması, erişilmesi ve imhası süreçlerine dair kontroller getirerek, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile uyumlu bir güvenlik altyapısı oluşturulmasını teşvik etmektedir.

Güvenlik zafiyeti oluşması durumunda yasal yaptırımlara neden olabilecek, içeriğinin yetkisiz personel veya kişiler tarafından görülmesinin kuruma çok ciddi maddi veya manevi zarar vereceği her türlü bilgi/veri, kritiklik derecesi 3 olarak hesaplanan varlıkların işlediği veriler, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan özel nitelikli kişisel veriler yaklaşımı ile standartlardan ayrılarak doğrudan sonuçları yasalara bağlamaktadır. Yukarıdaki tanım rehberin "Kritik Bilgi/Veri" başlığı altında yer almakta olup, kişisel verilerin korunmasına verilen önemi vurgulamaktadır. Ayrıca rehber Türkiye'de kamu kurumlarının bilgi güvenliği yönetimini bir standarda bağlamayı amaçlayan ve kamu kurumlarını ilgilendirdiği için doğrudan yasal yaptırımlar içeren stratejik bir belgedir.

Rehberin temelinde, gizlilik, bütünlük ve erişilebilirlik ilkeleri çerçevesinde bilgi varlıklarının güvenliğinin sağlanması yer alır. Bu kapsamda, kişisel veriler, özellikle de KVKK kapsamında tanımlanan özel nitelikli kişisel veriler, "kritik bilgi/veri" olarak tanımlanmış ve diğer bilgi türlerinden ayrıştırılmıştır. Rehber, ISO/IEC 27001 gibi uluslararası standartlarla uyumlu şekilde hem teknik hem de idari tedbirler seti önermektedir. Ayrıca, veri minimizasyonu ilkesi doğrultusunda, sadece görev tanımı kapsamında gerekli olan kişisel verilere erişim yetkisi verilmesi gerektiği vurgulanmaktadır. Fiziksel ve elektronik ortamda tutulan kişisel veriler için erişim

yetkilendirmesi, yetkisiz erişime karşı koruma, yedeğin şifrelenmesi gibi teknik ve idari tedbirlerin alınması zorunlu hale getirilmiştir. Bu kapsamda, rehber sadece teknik güvenlik önlemleriyle sınırlı kalmayıp, aynı zamanda farkındalık eğitimi, bilgi güvenliği politikaları ve denetim mekanizmaları aracılığıyla kamu personelinin kişisel veri güvenliği konusundaki bilinç düzeyini artırmayı hedeflemektedir. Böylece, rehber hem KVKK'ya uyumun sağlanmasını desteklemekte hem de kamu kurumlarında kişisel verilerin bütünlük, gizlilik ve erişilebilirlik ilkeleri çerçevesinde korunmasına zemin hazırlamaktadır.

Ülkeler tarafından vatandaşlara sunulan birçok hizmet, gelişen bilgi teknolojileri bünyesinde internet üzerinden sağlanmaktadır. Söz konusu sistemler, kamu kurumlarının yanı sıra enerji ulaşım, haberleşme gibi kritik altyapı sektörlerinde yaygı bir şekilde kullanılmaktadır. Bu sistemler gerek sunulan hizmetlerin kalitesine gerekse ilgili kurum/kuruluşun daha verimli çalışmasına katkıda bulunmaktadır. Kurum ve kuruluşların uhdesinde bulunan bilgi-verinin tam güvenliği sağlanmış şekilde korunması gerekmekte olup söz konusu sistemlerin güvenliğinin sağlanması ulusal güvenlik açısından büyük bir önem oluşturmaktadır [45].

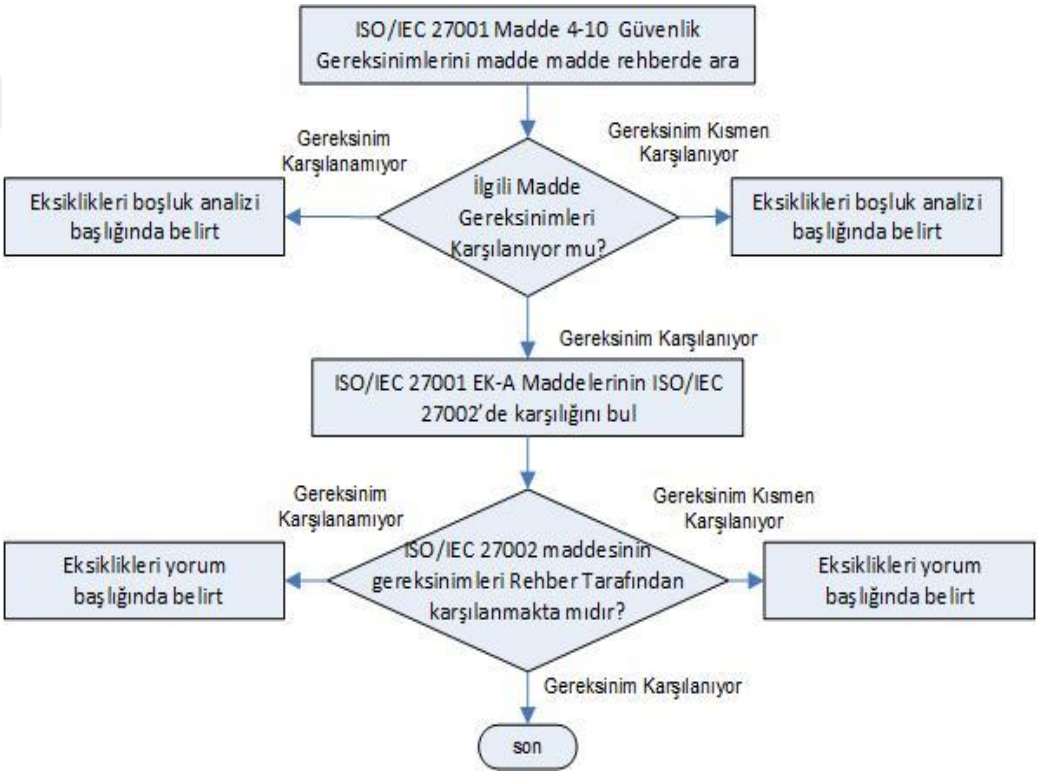
Uluslararası iş birliği ve standartlar, kamu bilgi ve iletişim güvenliği rehberi açısından da son derece önemlidir. Uluslararası standart kuruluşları tarafından belirlenen standartların ve en iyi uygulama örneklerinin takip edilmesi, uluslararası düzeyde iş birliği yapılması gerekmektedir. Özellikle bilgi ve iletişim dünyasının sınırları aşan doğası dikkate alındığında, uluslararası iş birliği ve ortak standartlar oluşturulması kaçınılmaz hale gelmektedir. Bu kapsamda, ISO, NIST, Institute of Electrical and Electronics Engineers (IEEE) gibi kuruluşlar tarafından oluşturulan standartların takip edilmesi, farklı ülkelerin bir araya gelerek ortak projeler yürütmesi, bilgi ve iletişim güvenliği alanındaki gelişmelerin küresel düzeyde etkili olmasını sağlayacaktır. Bu sayede, uluslararası düzeyde bilgi ve iletişim güvenliği standartlarının uyumlu bir şekilde uygulanması ve bu alanda ortak bir dil oluşturulması mümkün olacaktır.

Rehber, ISO/IEC 27001 gibi uluslararası standartlarla uyumlu şekilde hem teknik hem de idari tedbirler seti önermektedir. Erişim yetkilendirme, şifreleme, loglama, veri sınıflandırması, yedekleme ve imha konusunda teknik detaylara değinmiştir.

BÖLÜM 5: ISO/IEC 27001 VE KAMU BİLGİ SİSTEMLERİ VE İLETİŞİM GÜVENLİĞİ REHBERİ BOŞLUK ANALİZİ

ISO/IEC 27001 ve Kamu Bilgi ve İletişim Güvenliği Rehberi bilgi güvenliğini bütüncül olarak ele almaya çalışmakla birlikte yayınlaya kurumlar, nihai hedefleri ve uygulama durumları farklılıklar göstermektedir.

Şekil 5.1'de ISO/IEC 27001/27002 ve Kamu Bilgi ve İletişim Güvenliği arasındaki boşluk analizinin akış diyagramı yer almaktadır.



Şekil 5.1. ISO/IEC 27001/27002 ve Kamu Bilgi ve İletişim Güvenliği Rehberi arasındaki boşluk analizinin akış diyagramı

ISO/IEC 27001/27002 standardının 4–10. maddeleri ile Kamu Bilgi ve İletişim Güvenliği Rehberi arasındaki gereksinim uyum analizinde izleme karar verme süreci akış şeklinde sunulmaktadır. Yöntem, öncelikle standardın ilgili maddelerinin rehberdeki karşılıklarının sistematik olarak taranmasıyla başlamaktadır. Her bir gereksinim, "karşılanmıyor", "kısmen karşılanıyor" veya "karşılanıyor" kategorilerinden birinde sınıflandırılmakta; eksiklikler, yorumlar ve öneriler ise analizin ilgili bölümlerinde ayrıntılı olarak raporlanmaktadır.

Gereksinimlerin tamamen karşılandığı durumlarda süreç, ISO/IEC 27001 Ek-A maddelerinin ISO/IEC 27002 standardındaki kontrollerle eşleştirilmesi adımı ile ilerlemektedir. Bu aşamada da benzer şekilde karşılanma durumu değerlendirilmekte ve olası uyumsuzluklar ve eksiklikler tespit edilmektedir. Böylelikle, standart ile rehber arasındaki güvenlik gereksinim boşlukları ortaya konulmaya çalışılmıştır. ISO/IEC 27001 ve rehbere ait temel özellikler Tablo 5.1'de yer almaktadır.

Tablo 5.1. ISO/IEC 27001 ve Kamu Bilgi ve İletişim Güvenliği Rehberi Temel Özellikleri

Özellik	**ISO/IEC 27001:2022**	**Kamu Bilgi ve İletişim Güvenliği Rehberi**
Yayınlayan Kuruluş	ISO (International Organization for Standardization)	Siber Güvenlik Başkanlığı (Eski adıyla Cumhurbaşkanlığı Dijital Dönüşüm Ofisi – CBDDO)
Kapsam	Tüm kuruluşlar için evrensel; özel sektör ve kamu dahil	Yalnızca Türkiye'deki kamu kurum ve kuruluşları
Amacı	Herhangi bir kurumda Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmak, uygulamak, sürdürmek ve sürekli iyileştirmek	Kamu kurumlarında bilgi ve iletişim sistemlerinde güvenliğin sağlanması
Yapı	Ana metin (10 Madde) + EK-A (93 kontrol, 4 ana tema)	4 ana başlık, 17 temel ilke, 41 alt başlık

Bu iki belgeyi de detaylı incelediğimizde bilgi güvenliği açısından örtüşen ve farklılaşan yönler taşımakta olup, aralarındaki uyumsuzluk ve tamamlayıcılık ilişkilerinin değerlendirilmesi, kurumsal güvenlik uygulamalarının etkinliği açısından kritik öneme sahiptir.

ISO/IEC 27001 Ek-A kapsamında yer alan 93 kontrol, organizasyonel, teknolojik, fiziksel ve insan kaynaklı tehditlere karşı koruma sağlamakta iken; Kamu Bilgi ve İletişim Güvenliği Rehberi tedbir türlerine göre 4 ana başlık altında (Bilgi ve iletişim güvenliği uygulama süreci, varlık gruplarına yönelik tedbirler, uygulama ve teknoloji alanlarına yönelik tedbirler ve sıkılaştırma tedbirleri) 149 kontrol maddesi bulundurur; bu kontroller, kamuya özgü operasyonel gereksinimler (örn. USOM, e-Devlet, millî kriptografi vb.) çerçevesinde şekillenmektedir. Boşluk analizleri, güvenlik seviyesinin daha dengeli kurulabilmesi için öneme sahiptir.

ISO/IEC 27001 ile Kamu Bilgi ve İletişim Güvenliği Rehberi arasında hedeflenen güvenlik seviyeleri açısından benzerlikler olmakla birlikte, uygulama detayları, zorunluluk düzeyi ve yerel bağlam bakımından ciddi farklılıklar olduğunu ortaya koymuştur. Bu durum, her iki standarda eş zamanlı uyum sağlamak isteyen kamu kurumları açısından bazı zorluklar yaratmaktadır. Bu nedenle Kamu kurumlarında ISO/IEC 27001 standardı uygulanırken Kamu Bilgi ve İletişim Güvenliği Rehberi'nin gereksinimleri mutlaka dikkate alınmalı, ikili bir entegrasyon modeli geliştirilmelidir ayrıca ulusal rehberin, ISO/IEC 27001 standardı ile eşgüdümlü biçimde güncellenmesi, uyumlaştırma açısından fayda sağlayacaktır. Rehberin uygulama esaslarının her kurumun risk profiline göre yeniden yapılandırılmasına izin verilmesi, ISO/IEC 27001'in esnekliğine yaklaşılması açısından önemlidir.

5.1. ISO/IEC 27001 Standart Maddeleri Boşluk Analizi

5.1.1. Kuruluşun Bağlamı Maddesinin Boşluk Analizi

Kamu Bilgi ve İletişim Güvenliği Rehberinde 'Kuruluşun Bağlamı' ifadesini açıkça belirtmemiştir fakat, çeşitli bölümlerinde bu kavramı içeren açıklamalara yer verilmiştir.

ISO/IEC 27001'in 4. maddesi, bilgi güvenliği yönetiminin kurumsal bağlam ve paydaş analizine dayalı olarak şekillendirilmesini şart koşarken, Kamu Bilgi ve İletişim Güvenliği Rehberi daha çok iç yapıya ve uygulama kontrollerine odaklanmaktadır. Kamu Bilgi ve İletişim Güvenliği Rehberinde özellikle dış çevre analizi, ilgili tarafların beklentilerinin belirlenmesi ve süreç etkileşimlerinin tanımlanması gibi

alanlarda eklemeler yapılabilir. Bu da bunun regülasyon olması ve kamu kurumları tarafından doğrudan uygulanacak olmasından kaynaklanmaktadır.

ISO/IEC 27001:2022'nin dördüncü maddesi, bilgi güvenliği yönetim sisteminin yalnızca teknik önlemlerle sınırlı kalmayıp, kuruluşun operasyonel, hukuki, sosyal ve teknolojik çevresel koşullarıyla doğrudan ilişkilendirilmesi gerektiğini savunur. Bu madde, yönetişim süreçlerinin bağlamsal farkındalık temelinde inşa edilmesini, yani bilgi güvenliği önlemlerinin kurumun gerçek yaşam döngüsüne uyumlu hâle getirilmesini öngörür. Kuruluşun dış ve iç konuları analiz edilerek BGYS' nin amacına ulaşmasına etkisi olan faktörlerin belirlenmesi gerekir. (yasal düzenlemeler, sektörel tehditler, teknolojik değişimler, organizasyon yapısı…). Sınırlar, faaliyet alanları ve kapsam net şekilde tanımlanmalıdır. Bu nedenle ISO/IEC 27001'de kuruluşun bağlamı risk-temelli düşünme, paydaş yönetimi ve stratejik hizalama açısından kritik önemdedir.

Kamu Bilgi ve İletişim Güvenliği Rehberi her ne kadar "bağlam" kavramını doğrudan sistemli bir başlık altında ele almasa da, kılavuzun giriş ve kapsam bölümlerinde kurumun faaliyet yapısına özgü güvenlik önlemleri belirlenmesini teşvik eder. Rehber, bilgi varlıklarının önem derecesine, teknolojik altyapıya ve kurumsal hedeflere göre güvenlik sorumluluklarının şekillendirilmesini önererek, "kurumsal bağlam" düşüncesini dolaylı biçimde hayata geçirmektedir. Bu yönüyle, ISO/IEC 27001'in stratejik çerçevesi ile Kamu Bilgi ve İletişim Güvenliği Rehberi'nin sektörel uygulama odağı arasında içeriksel bir uyum yakalamak mümkündür.

Kamu kurumlarının kendi özel durumlarına uygun politika geliştirmesi gerektiği belirtilir. Yönetişim yapısı ve kurumsal sahiplenme bağlamın anlaşılmasını zorunlu kılar. Kurumun hizmetlerinin niteliği dikkate alınarak kritik sistemlerin tanımlanması istenir.

5.1.2. Liderlik Maddesinin Boşluk Analizi

ISO/IEC 27001 liderlik maddesi; Bilgi Güvenliği Yönetim Sisteminin (BGYS) etkin şekilde uygulanabilmesi için üst yönetimin kararlı liderliğini, sistemin sahiplenilmesini ve gerekli kaynakların sağlanmasını zorunlu kılar. Üst yönetim, BGYS' nin etkinliğini sağlamak ve sürdürmek için aktif rol almalıdır. Bu madde,

liderliğin yalnızca onay değil, katılım ve yönlendirme içermesini şart koşar. BGYS rollerinin açık şekilde tanımlanması ve bu rollerin ilgili kişilere iletilmesi gereklidir. Üst yönetim, bu dağılımın uygun şekilde yapıldığından emin olmalıdır.

Kamu Bilgi ve İletişim Güvenliği Rehberinde ise görev dağılımının yapılmasını ve bilgi güvenliği sorumlularının atanmasını öngörür. Kurumların kendi özgün yapılarına uygun olarak bilgi güvenliği politikalarını oluşturması ve üst yönetimin bu süreci yönlendirmesi gereklidir. Kurum içindeki bilgi güvenliği rollerinin açık şekilde belirlenmesi ve bu rollerin kurumsal yapıya entegre edilmesi gerektiği ifade edilir.

ISO/IEC 27001, liderliği bilgi güvenliği yönetim sisteminin omurgası olarak konumlandırır. Liderlik, yalnızca yönetimsel bir görev değil; stratejik yönelim, kaynak tahsisi, politika onayı ve sistematik iyileştirme gibi işlevleri içeren kapsamlı bir sorumluluk alanıdır. Kamu Bilgi ve İletişim Güvenliği Rehberi ise liderlik konusunu daha çok yönetsel sorumluluk boyutunda ele alır. Üst yönetimin rolü tanımlanmış olsa da, ISO/IEC 27001'in öngördüğü stratejik liderlik anlayışı rehberde net ve kapsamlı biçimde yer almaz. Bu da rehberin, kamu kurumlarında bilgi güvenliği kültürünün oluşturulması ve sürdürülebilirliği açısından bir boşluk içerdiğini göstermektedir. Rehbere ISO/IEC 27001'deki gibi "liderlik" başlığı altında, yönetimin bilgi güvenliğine olan taahhüdü, sistematik liderlik rolü ve stratejik yönetişim katkısını içeren bölümler eklenmesi gerekmektedir.

Kamu Bilgi ve İletişim Güvenliği Rehberinde ise liderlik rolünü "üst yönetim" kavramı üzerinden tanımlar. Ancak burada vurgu, yalnızca teknik önlemler değil; kamu kurumlarının görev ve sorumluluk zinciri içerisindeki tüm karar alıcıların aktif katılımına yöneliktir. Kamuya özgü hiyerarşik yapı göz önünde bulundurularak, kurumsal güvenliğin yönetici inisiyatifinden bağımsız sürdürülemeyeceği açık biçimde ifade edilmiştir.

Liderlik ifadesi Rehber ve Bilgi Güvenliği Yönetim Sistemi ilişkisi resminde geçmekte ve tüm süreci ele alan rol olarak gösterilmekle birlikte doküman içerisinde yetkinlikleri, sorumlulukları ve yapacağı faaliyetler hakkında bilgi yer almamaktadır

5.1.3. Planlama Maddesinin Boşluk Analizi

ISO/IEC 27001 Planlama maddesi bilgi güvenliği yönetim sisteminin (BGYS) etkili şekilde kurulması ve sürdürülmesi için gerekli olan stratejik planlama adımlarını kapsar. Varlık temelli ya da senaryo temelli risk değerlendirme yöntemleri önerilerek risk kriterleri belirlenmeli ve riskler analiz edilerek kabul edilebilir seviyeler tanımlanmasını öngörür. Standarda göre yalnızca ön hazırlık değil, sistematik bir risk yönetimi, stratejik hedef belirleme ve süreç entegrasyonu faaliyetidir.

Rehberde ise tehdit etki seviyesi ve risk değerleri bağlamında kritik sistemlerin değerlendirilmesi yapılmalıdır, Risklerin yönetilmesi amacıyla güvenlik önlemleri belirlenmelidir. Rehberde planlama faaliyetleri daha çok "risklerin belirlenmesi" ve "kontrollerin seçimi" süreçlerine indirgenmiştir.

Risk ve fırsat analizleriyle başlayan süreç, ölçülebilir hedeflerin belirlenmesi, risklerin işlenmesi ve kaynak planlaması ile devam eder. Bu yapı, bilgi güvenliği yönetim sisteminin sürdürülebilirliğini sağlar. Planlama, yalnızca teknik önlemlerin sıralanması değil; sistemin sürdürülebilirliğini sağlayan stratejik bir süreçtir.

Rehberde planlama varlık gruplarının ve kritiklik dereceklerinin belirlenmesi, mevut durum boşluk analizinin yapılması rehber uygulama adımlarının çıkarılması aşamalarını içermektedir. Bu haliyle bilgi güvenliğine bütüncül bir bakış açısı olmasa da teknik önlemlerin tespit edilmesi ve uygulanmasını içermektedir.

Rehberde risk değerlendirme sonuçlarının, alınacak önlemlere temel oluşturacağı ifade edilir fakat bilgi güvenliği hedefleri doğrudan bir başlık olarak yer almaz. Ancak bazı teknik önlemler (örn. loglama, kullanıcı erişim sınırlandırması) hedefe yönelik faaliyet olarak değerlendirilebilir. BGYS kapsamında değişiklik yönetimi 2.4 maddede rehber değişikliklerinin yönetilmesi ve varlık gruplarının değişikliklerinin yönetilmesi ele alınmıştır.

5.1.4. Destek Maddesinin Boşluk Analizi

ISO/IEC 27001'in 7. maddesi, bilgi güvenliğinin teknik önlemlerle sınırlı kalmaması gerektiğini vurgular. Kurumsal kaynakların etkin kullanımı, personel yeterliliği, farkındalık artırıcı faaliyetler ve belgelenmiş bilgi yönetimi, BGYS' nin

sürdürülebilirliğini sağlayan yapı taşlarıdır. Bu bağlamda standart, bilgi güvenliğini sadece bir teknik mesele değil, aynı zamanda bir kurumsal kültür ve iletişim konusu olarak ele almaktadır.

BGYS için gerekli olan kaynaklar sağlanmalıdır (insan gücü, teknik altyapı, yazılım, donanım vb.), BGYS kapsamında görev alan personelin bilgi güvenliği konusunda yeterliliği, eğitimi ve tecrübesi sağlanmalıdır, BGYS kapsamında iç ve dış iletişim gereklilikleri belirlenmeli, kimlerle, ne zaman, nasıl iletişim kurulacağı net olmalıdır, BGYS politikaları, prosedürleri, kayıtları ve belgeleri uygun şekilde oluşturulmalı, sürdürülmeli ve kontrol edilmelidir. ISO/IEC 27001'de "destek" sadece bir hazırlık aşaması değil, bilgi güvenliği sisteminin işlerliğini sürdüren temel bir altyapı bileşenidir.

Kamu Bilgi ve İletişim Güvenliği Rehberi ise bu destekleyici unsurları çeşitli maddelerde ele alır. Özellikle kullanıcı farkındalığı ve organizasyonel yapılanma bölümleri, ISO/IEC 27001'in bazı beklentileriyle örtüşür, ancak rehber kaynak yönetimi, yetkinliklerin ölçülmesi ve sistematik iletişim planları gibi konularda açık ve ölçülebilir gereklilikler sunmamaktadır.

Kurumun bilgi güvenliği ile ilgili dokümantasyon oluşturması ve bu belgeleri yönetmesi önerilir, destekleyici bazı teknik ve yönetsel kontrollerin varlığı burada da ima edilir, rehberde destek maddesi alt bileşenleri çeşitli bölümlerde detaylandırılmamış biçimde bulunur.

ISO/IEC 27001, bilgi güvenliği yönetim sisteminin etkinliği için gerekli destek unsurlarını (kaynaklar, yetkinlik, dokümantasyon, iletişim vb.) detaylı ve bütüncül biçimde tanımlar ve kurumsal düzeyde bilgi güvenliğini sürdürülebilir kılmak için sistematik, ölçülebilir ve denetlenebilir bir yapı sunar. Kamu Bilgi ve İletişim Güvenliği Rehberi ise bu destek unsurlarına yer verse de, bunları dağınık, yönlendirici düzeyde ele alır. Bağlayıcılığı sınırlıdır ve birçok konuda uygulama detayları ISO/IEC 27001'in gerekliliklerini kısmi şekilde karşılar. Kurumların farklı düzeylerde uygulama geliştirmesine açık kapı bıraksa da, bu durum standardizasyon eksikliğine yol açabilir. Kaynak yönetimi, yetkinlik değerlendirme ve iletişim planlamasında bu boşluklar farkedilmektedir.

5.1.5. İşletim Maddesinin Boşluk Analizi

ISO/IEC 27001'in 8. maddesi, bilgi güvenliği uygulamalarının sürdürülebilirliği açısından kritik bir bölümdür. Özellikle operasyonel planlama, risk değerlendirme ve işleme gibi süreçlerin bütünsel ve döngüsel bir yaklaşımla ele alınması beklenir.

Kuruluş, bilgi güvenliği süreçlerini ve bunların çıktısını kontrol edecek şekilde planlamalı, uygulamalı ve sürdürmelidir. Uygulama sırasında gerekli kontroller tanımlanmalı, prosedürler belgelenmeli ve süreç boyunca dokümantasyon yönetimi sağlanmalıdır. Riskler, yeni tehditler veya değişen durumlar ışığında yeniden analiz edilmelidir. Belirlenen risklere karşı uygun kontroller uygulanmalı ve bu işlemler izlenebilir biçimde belgelenmelidir. ISO/IEC 27001, işletim aşamasında planların sistemli biçimde uygulamaya dökülmesini, risk temelli kararların dokümante edilmesini ve kontrollerin aktif olarak yürütülmesini zorunlu kılar.

Kamu Bilgi ve İletişim Güvenliği Rehberi, "işletim" kavramını içeriğinde bilgi güvenliği faaliyetlerinin uygulanmasına yönelik birçok teknik ve yönetsel kontrol maddeleriyle ele almıştır. Sistem yapılandırması, izleme, yedekleme ve log yönetimi gibi uygulama düzeyinde kontroller içerir.

ISO/IEC 27001'in işletim yaklaşımı, risk temelli kontrollerin uygulanmasını planlı, ölçülebilir ve dokümante edilmiş süreçlerle desteklerken; rehberde bu kontroller çoğunlukla eylem bazlı kalmakta, bütüncül bir işletim modeli sunulamamaktadır. Bu durum, kamu kurumlarında uygulama farklılıklarına ve sürdürülebilirlik sorunlarına yol açabilecektir.

5.1.6. Performans Değerlendirmesi Maddesinin Boşluk Analizi

ISO/IEC 27001 standardının 9. maddesi, Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) etkinliğini değerlendirmeye yönelik performans izleme, iç denetim ve yönetim gözden geçirme süreçlerini kapsamaktadır. Bilgi Güvenliği Yönetim Sistemlerinin olgunlaştırılması ve sürdürülebilirliğini sağlamak adına yönetsel geri besleme mekanizmalarına önem vermektedir.

Kuruluş, bilgi güvenliği performansını izlemek için neyin ölçüleceğini, ne zaman ve nasıl ölçüleceğini, hangi araçların kullanılacağını ve kimin sorumlu olacağını önceden

tanımlamalıdır. Kuruluş, BGYS'nin gerekliliklere uygunluğunu ve etkinliğini değerlendirmek için planlı aralıklarla iç denetimler gerçekleştirmelidir, Denetim sonuçları belgelenmeli ve üst yönetime raporlanmalıdır. ISO/IEC 27001'de performans değerlendirme, sürekli iyileştirme döngüsünün veri temelli ve sayısal göstergelerle desteklenir.

Rehber, bilgi güvenliğinin operasyonel uygulanışına odaklanırken, performans göstergelerinin belirlenmesi, izlenmesi veya analizi gibi yönetsel mekanizmalara dair sistematik bir yapı sunmamaktadır. Bunun yanında kamu kurumlarında iç denetimin yapılması gerekliliğini belirtmekte, denetim sıklığı ve sorumlulukları tanımlamaktadır. Dolayısıyla bu alt madde, rehber tarafından büyük ölçüde karşılanmaktadır.

ISO/IEC 27001'in önerdiği risk odaklı, kanıta dayalı denetim yaklaşımına rehberde kısmi olarak değinilmiştir. Kamu Bilgi ve İletişim Güvenliği Rehberi ise iç denetim dışında bu yapıları sistematik biçimde sunmamakta, daha çok teknik ve operasyonel kontrollerin uygulanışına odaklanmaktadır. Rehber'in denetimi için CBDDO tarafından 2021 yılında Bilgi ve İletişim Güvenliği Denetim Rehberi yayınlanmıştır [43].

Bilgi ve İletişim Güvenliği Denetim Rehberi'nin amacı kurumun Rehber'e uyumunun denetlenmesi olarak belirlenmiştir. Bu dokümanda rehberdeki isterleri baz aldığı için rehberde eksik olan madde büyük olasılıkla denetimde de eksik olacaktır. Diğer taraftan denetimi yapacak kişilerin ISO/IEC 27001 baş denetçi sertifikasına ya da TSE tarafından verilen baş denetçi sertifikasına sahip olması gerektiği belirtilmiştir. Bu da denetimin yetkin ekip tarafından yapılmasına sağlatacak ve ISO/IEC 27001 bakış açısı rehbere de uygulanmış olacaktır.

5.1.7. İyileştirme Maddesinin Boşluk Analizi

ISO/IEC 27001 standardının bu maddesi Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) sürekli olarak iyileştirilmesini ve tespit edilen uygunsuzlukların etkin biçimde ele alınmasını zorunlu kılar. Bu madde, sistemin çevikliği, dirençliliği ve öğrenen bir yapı haline gelmesi açısından kritik önem taşır.

ISO/IEC 27001 10.1 Uygunsuzluk ve Düzeltici Faaliyet maddesi ile meydana gelen uygunsuzlukların nedenlerinin analiz edilmesini, tekrarının önlenmesi amacıyla

düzeltici faaliyetlerin planlanması ve uygulanmasını gerektirir. 10.2 Sürekli İyileştirme maddesi ise bilgi güvenliği yönetim sisteminin çevresel değişiklikler, iç/dış denetimler, olaylar ve performans verileri doğrultusunda sürekli olarak gözden geçirilmesini ve iyileştirilmesini hedefler.

ISO/IEC 27001, bu yaklaşımı Planla – Uygula – Kontrol Et – Önlem Al (PUKÖ) döngüsü çerçevesinde ele alır. Rehberde daha çok kontrollerin uygulanması ve teknik güvenlik önlemleri üzerinde durulmaktadır.

Genel çerçevede bakıldığında 10. madde bir BGYS' nin sadece kurulmasını değil, değişen koşullara göre evrilmesini, gelişmesini ve dirençli bir yapıya dönüşmesini hedeflemektedir. Bu bağlamda sürekli iyileştirme ve düzeltici faaliyetler, sistemin canlılığını koruması açısından stratejik öneme sahiptir. Kamu Bilgi ve İletişim Güvenliği Rehberi, teknik odaklı bir yapı sunduğu için, iyileştirme döngüsü ve yönetişim temelli öğrenme süreçlerini büyük ölçüde geniş bakış açısıyla ele almamaktadır.

BGYS'nin uygunluk, yeterlilik ve etkinliği sürekli olarak iyileştirilmelidir. Bu süreç, denetim bulguları, performans değerlendirme sonuçları, kullanıcı geri bildirimleri gibi girdilerden beslenmelidir.

ISO/IEC 27001'de iyileştirme, sistemin yaşam döngüsünü sürdüren ve kalite yönetim sistemleriyle uyumlu bir "geri bildirim ve düzeltme mekanizması" olarak ele alınır. Kamu Bilgi ve İletişim Güvenliği Rehberi, iyileştirme faaliyetlerini doğrudan başlıklandırmaz, ancak çeşitli maddelerde "güncelleme", "gözden geçirme" ve "tedbir alma" ifadeleriyle bu konuya dolaylı olarak değinilir. Bilgi güvenliği süreçlerinin periyodik olarak gözden geçirilmesi gerektiği belirtilir fakat, gözden geçirme sonuçlarının nasıl eyleme dönüştürüleceği açıklanmaz. Uygulanan kontrollerin etkinliği izlenmeli, ihtiyaç halinde yeni önlemler alınmalıdır. Ancak bu faaliyetler planlı, belgeye dayalı ve sistematik biçimde sunulmaz. Rehberde iyileştirme faaliyeti daha çok "güncelleme" kavramına indirgenmiştir.

5.2 ISO/IEC 27002 Güvenlik Kontrolleri ile Kamu Bilgi Sistemleri ve İletişim Güvenliği Rehberi Karşılaştırılmalı Boşluk Analizi

ISO/IEC 27001'in güvenlik gereksinimleri Ek-A'da yer almaktadır. Ek-A'da bilgi güvenliği için yapılması gerekenler tanımlanmaktadır. Bu başlık altında ISO/IEC 27001 Ek-A'da yer alan 93 kontrol maddesi kurumsal, teknolojik, fiziksel ve kişi olmak üzere dört kategoriye ayrılmıştır. Ek-A maddelerindeki gereksinmeleri karşılamak için neler yapılabileceği ise ISO/IEC 27002 dokümanında tanımlanmaktadır. Bu başlık altında Ek-A'da bulunan her bir kategorinin gereksinimleri ayarı ayrı çıkarılmış ve bu gereksinimlerin rehber tarafından karşılanıp karşılanmadığı kontrol edilmiştir. Bu karşılaştırma ISO/IEC 27001 Ek-A maddesi, rehberdeki karşılığı ve boşluk analizi sütunlarından oluşmaktadır. Birinci sütunda doğrudan ISO/IEC 27001 EK-A maddesi yer almaktadır. 2. Sütunda bu 1. Sütundaki maddenin rehberde karşıladığı madde veya maddeler yer almaktadır. Birden çok maddeyi içeriyorsa .x işareti ile çoklu madde işaretlenmiştir. Son sütunda ise madde gereksinimleri karşılamaktadır kısmen karşılamaktadır ya da karşılamamaktadır ifadesi ile durum tespit edilmişti. Kısmen karşılanan veya karşılanmayan durumlar ise tablodan altında güvenlik kontrolü için yorumlar başlıkları altında verilmiştir.

Ek-A başlık organizasyonu ve rehber başlık organizasyonu oldukça farklı yapıdadır. Bu yüzden doğrudan eşleştirmek kolay olmamaktadır. Burada yapılan kontroller ISO/IEC 27002:20022 güvenlik kontrol maddeleri referans alınarak yapılmıştır. İki doküman arasındaki başlık bilgilerinin çok farklı organizasyon altında verilmesi bilgi güvenliğine bütüncül bakmayı engellemektedir. İkisi de bilgi güvenliğini ele almaktadır fakat konuya bakış açıları ve kontrol noktaları oldukça farklıdır.

5.2.1 Kurumsal Güvenlik Kontrollerdeki Boşluk Analizi

Bu başlık altında standardın (ISO/IEC 27002) Kurumsal Güvenlik Kontrollerine karşılık rehberin güvenlik tedbirleri incelenmiştir. Kurumsal kontrollere yönelik karşılaştırmalı boşluk analizi detayları Tablo 5.2'de yer almaktadır.

Tablo 5.2 Kurumsal Güvenlik Kontrol Maddeleri

ISO 27001:2022 EK-A Maddesi	**Rehberdeki Karşılığı**	**Boşluk Analizi**
A.5.1 Bilgi güvenliği için politika seti	3.1.1.3, 3.5.1.9, 3.5.3.1	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.5.2 Bilgi güvenliği rolleri ve sorumlulukları	3.1.10.1, 3.1.13.8, 3.1.13.14, 3.5.1.7, Tablo 2	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.5.3 Görevler arası ayrım	3.1.9.8, 3.1.11.5	Bu maddenin gereksinimleri kısmen karşılanmıştır.
A.5.4 Yönetim Sorumlulukları	Tablo 2	Bu maddenin gereksinimleri kısmen karşılanmıştır.
A.5.5 Yetkililerle İletişim	3.1.10.3, 3.1.12.9, 4.5.2.14	Bu maddenin gereksinimleri karşılanmıştır.
A.5.6 Özel İlgi Gruplarıyla İletişim	3.1.10.2,	Bu maddenin gereksinimleri karşılanmıştır.
A.5.7 Tehdit İstihbaratı	3.1.10.4, 4.5.2.13	Bu maddenin gereksinimleri kısmen karşılanmıştır.
A.5.8 Proje Yönetiminde Bilgi Güvenliği	2.1.4, 3.2.6.1, 3.2.3.8	Bu maddenin gereksinimleri karşılanmıştır.
A.5.9 Bilgi envanteri ve diğer ilgili varlıklar	3.1.1. x, 3.1.2.x	Bu maddenin gereksinimleri karşılanmıştır.
A.5.10 Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı	2.1.1, 3.1.1, 3.1.2, 3.1.3.10, 3.5.1.2	Bu maddenin gereksinimleri karşılanmıştır.
A.5.11 Varlıkların iadesi	3.1.14.1, 3.5.1.8, 4.3.1.11	Bu maddenin gereksinimleri karşılanmıştır.
A.5.12 Bilgilerin sınıflandırılması	3.1.7.	Bu maddenin gereksinimleri karşılanmıştır.
A.5.13 Bilgilerin etiketlenmesi	3.1.2.3, 3.6.2.10 (Kısmi değinilmiş)	Bu maddenin gereksinimleri kısmen karşılanmıştır.
A.5.14 Bilgi transferi	3.1.6.36, 3.2.7.4, 3.6.1.10, 3.6.2.2, 5.3.1.15	Bu maddenin gereksinimleri karşılanmıştır.
A.5.15 Erişim Kontrolü	3.1.1.7, 3.1.3.9, 4.4.2.5, 3.1.4.19, 3.1.6.x, 3.1.12, 3.1.14.1x, 3.3.2.5, 3.4.1.7, 5.1.2.8	Bu maddenin gereksinimleri karşılanmıştır.
A.5.16 Kimlik yönetimi	3.1.12.13, 3.1.12.14, 5.1.1.18	Bu maddenin gereksinimleri karşılanmıştır.

A.5.17 Kimlik doğrulama bilgileri	3.1.12.x, 3.1.4.x, 3.2.1.x,3.4.3,x	Bu maddenin gereksinimleri karşılanmıştır.
A.5.18 Erişim hakları	3.1.14.1, 5.1.3.1, 5.2.1.17, 5.2.1.18	Bu maddenin gereksinimleri karşılanmıştır.
A.5.19 Tedarikçi ilişkilerinde bilgi güvenliği	3.2.6.3, 3.5.3.x	Bu maddenin gereksinimleri kısmen karşılanmıştır.
A.5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması	3.1.1.2, 3.1.2.2, 3.2.6.3, 3.5.3.1, 3.5.3.3, 3.5.3.9	Bu maddenin gereksinimleri karşılanmıştır.
A.5.21 Bilgi ve iletişim teknolojisi (BİT) tedarik zincirinde bilgi güvenliğini yönetme	3.5.3.4, 3.5.3.10	Bu maddenin gereksinimleri kısmen karşılanmıştır.
A.5.22 Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişiklik yönetimi	3.5.3.9	Bu maddenin gereksinimleri kısmen karşılanmıştır
A.5.23 Bulut hizmetlerinin kullanımı için bilgi güvenliği	4.3.1.x	Bu maddenin gereksinimleri karşılanmıştır.
A.5.24 Bilgi güvenliği ihlal olayı yönetimi planlaması ve hazırlığı	3.1.10, 3.1.10.8, 3.1.12.18, 3.4.5.2, 3.5.1.6, 3.5.1.7, 3.5.2.2, 4.1.1.10, 4.4.2.10	Bu maddenin gereksinimleri karşılanmıştır.
A.5.25 Bilgi güvenliği ihlal olaylarını değerlendirme ve karar verme	3.5.1.6 , 3.5.2.2	Bu maddenin gereksinimleri karşılanmıştır.
A.5.26 Bilgi güvenliği ihlal olaylarına yanıt verme	3.1.10.1, 3.1.10.5, 3.1.10.7, 3.5.1.6	Bu maddenin gereksinimleri karşılanmıştır.
A.5.27 Bilgi güvenliği ihlal olaylarından ders çıkarma	3.1.10.x	Bu maddenin gereksinimleri karşılanmıştır.
A.5.28 Kanıt toplama	4.4.2.10	Bu maddenin gereksinimleri karşılanmıştır.
A.5.29 Kesinti sırasında bilgi güvenliği	3.1.13.12, 3.6.2.7, 4.5.3.1	Bu maddenin gereksinimleri karşılanmıştır.
A.5.30 İş sürekliliği için BİT hazırlığı	3.1.6.7, 3.1.13.6, 3.1.13.7, 4.3.1.9, 4.5.3.8	Bu maddenin gereksinimleri karşılanmıştır.
A.5.31 Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler	3.1.8.1, 3.1.9.2, 3.1.13.6, 3.5.1.1, 3.5.1.6, 4.4.2.10	Bu maddenin gereksinimleri karşılanmıştır.
A.5.32 Fikri Mülkiyet Hakları	3.1.2.2, 3.1.14.1	Bu maddenin gereksinimleri kısmen karşılanmıştır.

A.5.33 Kayıtların korunması	3.2.1.4, 3.2.5.3, 3.4.5.5, 3.6.1.8, 5.3.1.16	Bu maddenin kısmen gereksinimleri karşılanmıştır.
A.5.34 Kişiyi tespit bilgisinin (PII) gizliliği ve korunması	4.1.1.1	Bu maddenin gereksinimleri karşılanmıştır.
A.5.35 Bilgi güvenliğinin bağımsız gözden geçirilmesi	2.3.2	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.5.36 Bilgi güvenliğine yönelik politikalar, kurallar ve standartlara uygunluk	3.5.1.9, 3.5.3.1	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.5.37 Dokümante edilmiş işletim prosedürleri	3.1.6.16, 3.1.6.1, 3.1.9.7, 3.1.10.x, 3.1.11.x, 3.1.13.8, 3.1.13.13, 3.2.1.9, 3.2.5.3, 3.2.7.20, 3.2.9.7, 3.5.3.x, 4.4.2.13	Bu maddenin gereksinimleri karşılanmaktadır.

Ek-A Kurumsal Güvenlik Kontrolleri İçin Yorumlar

A.5.1: Cihazların kurum ağına bağlanması, eski cihazların imha edilmesi, kurumda kullanılacak yazılımların onaylanması, zararlı yazılımların engellenmesi, yama yönetimi, uzaktan bağlanma, erişim kontrolü, sosyal medya, mobil cihaz kullanımı gibi teknik konularda politika ve prosedür geliştirilmesi istenmektedir. Organizasyon iş stratejisi regülasyon, yasa ve anlaşmalara uyum, risk yönetimi gibi teknik olmayan organizasyonel politikaların ele alınmadığı görülmektedir. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.5.2: Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci için Sorumluluk Atama Matrisi tanımlanmış. Ama üst yönetimin sorumlulukları net belirtilmemiş. Bu matriste tüm işlemler için onay görevi verilmiştir. Oysa ISO/IEC 27002'de rol ve sorumlulukları belirleme, yasalar ve regülasyonlarla uyum, bilgi güvenliği politikalarını belirleme ve uygulama gibi kritik görevler verilmiştir. Bu maddenin gereksinimleri kısmen karşılanmıştır.

A.5.3: Test ortamı, siber olaylara müdahale gibi spesifik görevler için görevler ayrılığı ilkesi ifade edilmiş oysa tüm bilgi sistem rol ve sorumluluklarında (yazılım geliştirme, sistem yönetimi, cihaz yönetimi, veri tabanı yönetimi vb.) görevler ayrılığı prensibinin vurgulanması gerekir. Bu maddenin gereksinimleri kısmen karşılanmıştır.

A.5.4: Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci için Sorumluluk Atama Matrisi tanımlanmış ve bu matriste tüm işlemler için onay görevi verilmiştir. Oysa ISO/IEC 27002'de rol ve sorumlulukları belirleme, yasalar ve regülasyonlarla uyum, bilgi güvenliği politikalarını belirleme ve uygulama gibi kritik görevler verilmiştir. Bu maddenin gereksinimleri kısmen karşılanmıştır

A.5.5: Bu maddenin gereksinimleri karşılanmıştır.

A.5.6: Üreticileri sayfaları takip edilmeli, USOM ve diğer tehdit istihbarat kurumlarından alınan bildirimler doğrultusunda gerekli önlemlerin alınması gerektiği ifade edilmiştir. Bu maddenin gereksinimleri karşılanmıştır

A.5.7: Tehdit istihbaratı SOME ve enerji sektörüne özel güvenlik gereksinimleri bölümlerinde ifade edilmiştir. Oysa bilgi güvenliğinin her aşamasında stratejik, taktik ve operasyonel tehdit istihbaratının yapılıp gerekli eylemlerin alınması gerekmektedir. Bu maddenin gereksinimleri kısmen karşılanmıştır.

A.5.8: Rehber proje yönetimi başlığı altında konuyu bize vermese dahi uygulama yol haritası belirlenmesi aşamasında tüm yasal, düzenleyici ve sözleşmeden doğan gereksinimleri dikkate alarak ilerler. Güvenli yazılım geliştirme projelerinde de güvenlik gereksinimlerinin tanımlanması, güvenli yazılım geliştirme süreçlerinin uygulanması aşamalarında bilgi güvenliği gereksinimlerinin karşılanması gerektiği belirtilmiştir.

A.5.9: Bilgi ve diğer varlıkların tanımlanması, sınıflandırılması ve güvenlik önlemlerinin alınması açısından standart ile uyumludur.

A.5.10: Varlık gruplarının belirlenmesi, kullanıcıların bilgi varlıklarını uygun ve güvenli şekilde kullanmasına dair kuralların belirlenmesi gerekliliği ile doğrudan örtüşür.

A.5.11: İşten ayrılma ve görev değişikliğinde kurum varlıklarının iadesi zorunluluğu doğrudan belirtilmemiştir ancak ilgili süreçler dolaylı olarak sorumluluğu kapsamaktadır.

A.5.12: Rehber kurum verilerinin sistematik olarak kategorilere ayrılması ve sınıflandırılması için politikalar oluşturulmasını belirtmektedir ve standart ile uyumludur.

A.5.13: Rehber kurumun envanterinde yalnızca üreticisinin destekleyeceği yazılımlar olması gerektiğini belirtir ve bunlar içerisinde üretici desteği bitenlerin etiketlenmesi gerektiğini vurgulamaktadır. Kablolamanın da gerektirdiği düzende yapılarak kabloların tek tek etiketlenmesi gerektiğini belirtir ancak bu etiketleme tüm bilgi varlıkları için detaylandırılmamıştır.

A.5.14: Rehber düzenli veri aktarımı yapılması gereken durumlarda hangi yolların izleneceği, transferi kimin yapacağı, çalışma alanlarının izinsiz transfere engel olacak şekilde güvenli düzenlenmesi gerekliliği, transfer yapılırken kullanılacak maksimum ve minimum hız belirlenmesi gibi detayları açıkça belirtmiştir. Standart ile uyumludur.

A.5.15: Rehber genel çerçevede teknik detaylara değinmiş olduğu için erişim kontrolü konusunda da birden fazla yerde bu konuyu ele almıştır. Standart ile uyumludur.

A.5.16: Rehber kimlik doğrulama sistemleri ve kimlik yönetimi uygulamalarına, bunların merkezi olarak yürütülmesi ve e-devlet ile entegre olması gerekliliğine değinmiştir. Her kullanıcıya özgü hesap tanımlanması, kimlik yaşam döngüsü yönetimi, merkezi sistem entegrasyonu gibi unsurları açısından standart ile uyumludur.

A.5.17: Parola politikaları, kullanıcı tanımlama ve güçlü doğrulama yöntemleri, çok faktörlü kimlik doğrulama ve bilgilerin güvenli yönetimi konularına rehber oldukça detaylı şekilde değinmiştir. Standart ile uyumludur.

A.5.18: Uzaktan çalışmanın sona ermesi durumunda; yetki ve erişim haklarının iptali ve kullanılan teçhizatın iadesi, erişim haklarının görev tanımına göre verilmesi, belirli sistemlere erişimin yeterli en düşük haklarla güvenli şekilde yapılmasının belirtilmesi ve kullanıcı haklarının en az yetki prensibinde tanımlanması ve ihtiyaç dışı erişimlerin kaldırılması hükümleri standart ile uyumludur.

A.5.19: Rehber tedarikçi seçimi, sözleşmelerde güvenlik yükümlülükleri, izleme ve denetleme gereklilikleri konusunda standart ile uyumludur. Tedarikçilerle çalışırken

yapılan iş birliklerini ve sözleşmelere bilgi güvenliği gereksinimlerinin eklenmesini doğrudan belirtmektedir.

A.5.20: Rehber; tedarikçi ilişkilerinde sözleşmelerin onaylı olup olmadığına, yazılım geliştirme anlaşmalarında şartlar dahilinde güvenlik zafiyeti içermediğine dair taahhütname alınmasına, tedarikçi ilişkilerinde bilgi güvenliği politikasının tanımlanması ve dokümante edilmesine dair detaylara yer verdiği için standart ile uyumudur.

A.5.21: Alt yüklenici yönetimi ve tedarikçi güvenliği değerlendirilse de, zincir boyunca izlenebilirlik ve teknik kontroller net biçimde tanımlanmamıştır. İlgili güvenlik gereksinimleri sözleşme içeriğine eklenmelidir ifadesi yer alsa da hangi gereksinimlerin ekleneceği, donanım/yazılım bileşenlerinde güvenlik izleme, Kod güvenliği, tedarik kaynağı zinciri izlenebilirliği gibi teknik detaylara açıkça yer verilmemiştir.

A.5.22: Tedarikçilerin izlenmesi ve denetlenmesi doğrudan yer alır ancak değişiklik yönetimi süreçleri detaylarıyla tanımlanmamıştır. Değişiklik planı, etki analizi, onay ve izleme mekanizmasında ayrıntı belirtilmemiştir.

A.5.23: Rehber bulut hizmetin nasıl kullanılacağı, güvenliğinin nasıl sağlanacağı, hizmet alımından sonra erişimin nasıl sonlandırılacağına .vb. detaylara değinmiştir. Teknik detaylar tedbir olarak dokümante edildiği için standart ile uyumludur.

A.5.24: Rehber; kurumların ihtiyaç halinde şüpheli ağ trafiklerini takip etmesini, şüpheli hesap kullanımı durumlarında kullanıcı rolü, yetki seviyesi değişiklikleri yapılabilmesini, ihlal durumunda cihaz erişimi kısıtlaması yapılmasına yönelik tanımlamalar yapmıştır. Bir güvenlik ihlali yaşanmadan önce olası ihlal senaryolarına karşı yol haritası hazırlanarak dokümante edilebilir ve personel eğitimlerinde buna da yer verilebilir.

A.5.25: Rehberde bilgi güvenliği ihlali konusuna değinilmiştir fakat olayların teknik analizle sınıflandırılması, olay ayrımının yapılması gibi detaylar rehberde açıkça belirtilmemiştir.

A.5.26: SOME ekiplerinin nasıl yanıt vereceğine dair adımlar dokümante edilmiştir, hazırlık aşamalarında tatbikat yapılmasına dair detaylar vardır, müdahalede görev alacak kişilerin rol ve sorumluluklarının dokümante edilmesi gerektiği belirtilmiştir. Standart ile uyumludur.

A.5.27: Siber Güvenlik Olay Yönetimi başlığı altında ele alınmıştır. Bu maddenin gereksinimleri karşılanmaktadır.

A.5.28: Rehberde kanıt, delil gibi kavramlar doğrudan tanımlanmamıştır. Dijital delillerin toplanmasına dair teknik veya organizasyonel talimat, delil bütünlüğü ya da zincirleme kayıt gibi adımlara dair bir tanımlama yapılmamıştır. Özellikle dijital delil toplama, saklama ve nasıl yapılacağına dair prosedür oluşturularak, eğitimleri verilebilir. Bu maddenin gereksinimleri karşılanmaktadır.

A.5.29: Rehberde felaket senaryolarından kurtarma planının hazırlanmasına yönelik adımlar verilmiştir, destekleyici alt yapı hizmetlerinde işlem detayları açıklanmış ve bu durumlarda hizmetin aksamaması için gerekli farkındalık çalışmalarına da değinilmiştir. Standart ile uyumludur.

A.5.30: Rehber kurumun internete açık hizmetleri için koruma adımlarına değinerek, iş sürekliliği kapsamını tanımlamıştır ve bunun sürdürülmesi için kapsamları açıkça belirtmiştir. Standart ile uyumludur.

A.5.31: Rehber denetim kayıtlarının yasalara uygun saklanması, gelecek ihtiyaç planlamalarında yasal yükümlülükler tanımlanması, faaliyet alanının yasal ve sözleşmeden doğan yükümlülükleri, ve diğer süreçler için yasalar ve sözleşmelere uygun tanımlama yapılması gerektiğini açıkça belirtmiştir. Standart ile uyumludur.

A.5.32: Rehber telif hakları, yazılım lisansı, yasal içerik kullanımı gibi fikri mülkiyet konularına rehberde yer verilmemektedir. Telif haklarına uyum için kontrol mekanizması ve lisans yönetimi süreçleri tanımlanmamıştır. Bu konuda yasalar ışığında tanımlama yapılabilir.

A.5.33: Kullanıcı bilgilerinin fiziksel güce dayanıklı kriptografik yöntemlerle korunması, uygulama kurumlarının izole ortamlarda yapılması gerektiği, tersine mühendisliğe karşı korunma detayları, sunucunun korumalı kurulumuna dair

açıklamalar yer almaktadır. Sözleşme, politika ayrı bir kayıt süreci yok ve saklama süresi belirleme kayıt bütünlüğünün kontrolü gibi gerekliliklere yer verilmemiştir.

A.5.34: PII için özel teknik kontrollerin (örneğin maskeleme, şifreleme, takma adlandırma) ayrıntıları rehberde açıklanmamıştır. Bu maddenin gereksinimleri karşılanmaktadır.

A.5.35: Rehbere uyum yılda en az bir defa olmak üzere iç denetim yoluyla Siber Güvenlik Başkanlığı tarafından yayınlanan Bilgi ve İletişim Güvenliği Denetim Rehberi esas alınarak denetlenir. Rehber denetimlerinde gerektiğinde ISO/IEC 27001 maddelerinin denetimlerde sorgulanmasının yardımcı bir denetim aracı olarak sorulmasının yolu da açılmalıdır. Bu maddenin gereksinimleri karşılanmaktadır.

A.5.36: Tedarikçi ilişkilerinde politika tanımlaması açıklanmış fakat diğer durumlar için bilgi güvenliği politikası detaylandırılmamıştır. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.5.37: Prosedürlerin dokümante edilmesi, kontrolü ve güncellenmesi rehberde detaylarıyla açıklanmıştır. Standart ile uyumludur. Bu maddenin gereksinimleri karşılanmaktadır.

5.2.2 Kişi Güvenlik Kontrollerinin Boşluk Analizi

Bu başlık altında standardın (ISO/IEC 27002) Kişi Güvenlik Kontrollerine karşılık rehberin güvenlik tedbirleri incelenmiştir. Kişi Güvenlik Kontrollerine yönelik karşılaştırmalı boşluk analizi detayları Tablo 5.3'te yer almaktadır.

Tablo 5.3 Kişi Güvenlik Kontrol Maddeleri Boşluk Analizi

ISO 27001:2022 EK-A Maddesi	**Rehberdeki Karşılığı**	**Boşluk Analizi**
A.6.1 Tarama	3.5.1.x	Bu maddenin gereksinimleri karşılanmıştır.
A.6.2 İstihdam şartları ve koşulları	3.5.1.8	Bu maddenin gereksinimleri karşılanmıştır.
A.6.3 Bilgi güvenliği farkındalığı, eğitim ve öğretim	3.1.14.4, 3.3.1.3, 3.5.2.1	Bu maddenin gereksinimleri kısmen karşılanmıştır.

A.6.4 Disiplin süreci	3.5.1.6	Bu maddenin gereksinimleri kısmen karşılanmıştır.
A.6.5 İstihdamın sona ermesinden veya değiştirilmesinden sonraki sorumluluklar	3.5.1.x	Bu maddenin gereksinimleri karşılanmıştır.
A.6.6 Gizlilik veya ifşa etmeme anlaşmaları	3.1.11.1, 3.5.1.x 3.5.3.x	Bu maddenin gereksinimleri kısmen karşılanmıştır.
A.6.7 Uzaktan çalışma	3.1.14x	Bu maddenin gereksinimleri kısmen karşılanmıştır.
A.6.8 Bilgi güvenliği olayı raporlanması	3.1.10.x, 4.4.2.16	Bu maddenin gereksinimleri karşılanmıştır.

Ek-A Kişi Güvenlik Kontrolleri İçin Yorumlar

A.6.1: Tarama bölümü tümden işe alım ve iş yerinde görevleri sırasındaki kontroller ayrıntılı bir şekilde ele alınmıştır. Kamu görevlisi olurken alına güvenlik kontrolleri de göz önüne alındığında ayrıntılı bir şekilde tanımlandığı değerlendirilmektedir. 3.5.2'de tanımlanan farkındalık kontrolleri ile görevlerini etkin bir şekilde sürdürmeleri hedeflenmiştir.

A.6.2: İşten ayrılma ve içten çıkarma için gerekli kontrolleri içermektedir. Bu maddenin gereksinimleri karşılanmıştır.

A.6.3: ISO/IEC 27002'de üst yönetimin de bilgi güvenliği farkındalık çalışmalarına katılması gerektiği vurgulanmıştır. Bu maddenin gereksinimleri kısmen karşılanmıştır.

A.6.4: Rehberde genel olarak taahhütnamelere atıfta bulunmakta ancak açık bir disiplin süreci tanımı, örneğin: uyarı, kınama, işten çıkarma, vb. gibi aşamalı bir model belirtilmemiştir. Olayın soruşturulması, kanıtlanması gibi ayrıntılar ifade edilmemiştir. Bu maddenin gereksinimleri kısmen karşılanmıştır.

A.6.5: Bu maddenin gereksinimleri karşılanmıştır.

A.6.6: Personel, işten ayrılma ve tedarikçilerle ilişkiler başlıklarında hassas verilerin korunması ifade edilmiştir. Fakat verilerin tedarikçi tarafında nasıl etiketlenip, nasıl

koruncağı dair detaylı kontroller bulunmamaktadır. Bu maddenin gereksinimleri kısmen karşılanmıştır.

A.6.7: Uzaktan çalışma Ağ ve Sistem Güvenliği başlığı altında ele alınmıştır. Daha çok sistem yöneticilerin ağa erişim ve video konferansı tanımlamaktadır. Bu tür çalışmalarda önemli olan olay kayıtlarının tutulması, yetkisiz erişimlerin kontrol edilmesi, uzaktaki sisteme erişim yönetimi, uzaktaki cihazların sigortalanması, uzaktaki cihaz getirildiğinde uygulanacak prosedür konularına değinilmemiştir. Bu maddenin gereksinimleri kısmen karşılanmıştır.

A.6.8: Siber Güvenlik Olay Yönetimi bölümü altında ayrıntılı bir şekilde siber olay müdahalesi ele alınmıştır. Bu maddenin gereksinimleri karşılanmıştır.

5.2.3 Fiziksel Güvenlik Kontrollerdeki Boşlukların Analizi

Bu başlık altında standardın (ISO/IEC 27002) Fiziksel Güvenlik Kontrollerine karşılık rehberin güvenlik tedbirleri incelenmiştir. Fiziksel Güvenlik Kontrollerine yönelik karşılaştırmalı boşluk analizi detayları Tablo 5.4'te yer almaktadır.

Tablo 5.4 Fiziksel Güvenlik Kontrol Maddeleri Boşluk Analizi

ISO 27001:2022 EK-A Maddesi	**Rehberdeki Karşılığı**	**Boşluk Analizi**
A.7.1 Fiziksel güvenlik sınırları	3.6.1.1, 3.6.1.4, 3.6.1.8	Bu maddenin gereksinimleri karşılanmıştır.
A.7.2 Fiziksel giriş	3.1.6.3, 3.1.6.9, 3.1.6.911, 3.6.2.11	Bu maddenin gereksinimleri karşılanmıştır.
A.7.3 Ofislerin, odaların ve tesislerin güvenliğini sağlama	3.6.1.7, 3.6.1.9, 3.6.1.10, 3.6.1.14, 3.6.2.6, 3.6.2.11	Bu maddenin gereksinimleri kısmen karşılanmıştır.
A.7.4 Fiziksel güvenlik izleme	3.6.1.2, 3.6.1.3, 3.6.1.3, 3.6.1.9,3.6.1.9,3.6.1.12, 3.6.2.3, 3.6.2.5, 3.6.2.7, 3.6.2.12	Bu maddenin gereksinimleri karşılanmıştır.
A.7.5 Fiziksel ve çevresel tehditlere karşı koruma	3.6.1.8, 3.6.2.8	Bu maddenin gereksinimleri kısmen karşılanmıştır.
A.7.6 Güvenli alanlarda çalışma	3.6.1.3,3.6.1.10. 3.6.2.3, 3.6.2.3	Bu maddenin gereksinimleri karşılanmıştır.

A.7.7 Temiz masa ve temiz ekran	3.5.1.3,3.3.1.11, 3.3.1.10, 3.3.1.5	Bu maddenin gereksinimleri karşılanmıştır.
A.7.8 Ekipman konumlandırma ve koruma	3.6.1.1,3.6.1.7, 3.6.1.8, 3.6.1.11, 3.6.3.2, 4.5.2.12, 4.5.3.8, 4.5.3.9, 3.3.1.15	Bu maddenin gereksinimleri kısmen karşılanmıştır.
A.7.9 Kuruluş dışındaki varlıkların güvenliği	3.1.1.6, 3.1.1.9, 3.1.2.3, 3.1.2.4, 3.2.7.4	Bu maddenin gereksinimleri kısmen karşılanmıştır.
A.7.10 Depolama ortamı	3.3.2.x, 3.1.1.6.	Bu maddenin gereksinimleri karşılanmaktadır.
A.7.11 Destekleyici altyapı hizmetleri	3.6.1.8,3.6.1.11, 3.6.2.2, 3.6.2.5, 3.6.2.7, 3.6.2.8	Bu maddenin gereksinimleri karşılanmaktadır.
A.7.12 Kablo güvenliği	3.6.1.7, 3.6. 2.10	Bu maddenin gereksinimleri karşılanmaktadır.
A.7.13 Ekipman bakımı	3.1.1.6, 6.2.9, 3.6.2.15	Bu maddenin gereksinimleri karşılanmaktadır.
A.7.14 Ekipmanın güvenli bir şekilde yok edilmesi veya tekrar kullanılması	3.4.1.4, 3.3.2.1	Bu maddenin gereksinimleri karşılanmaktadır.

Ek-A Fiziksel Güvenlik Kontrolleri İçin Yorumlar

A.7.1: Genel Güvenlik Tedbirleri başlığı altında tüm teknik ve yönetimsel güvenlik hususları ele alınmıştır.

A.7.2: Genel Güvenlik Tedbirleri başlığı altında tüm teknik ve yönetimsel güvenlik hususları ele alınmıştır. Rehberde prosedürel veya kontrole yönelik ek maddeler de bulunmaktadır. Ziyaretçilere refakatçi sağlanması vb. İki madde birbiri ile uyumludur

A.7.3: Ofis odaları ve tesislerin güvenliğine yönelik gerekli önlemler tanımlanmıştır fakat kritik binaların veya ofislerin göz önünde olmayacak şekilde tasarlanması, içerdeki faaliyetler görünmeyecek şekilde önlemler alınması ifade edilmemiştir. Fiziksel kontrole yönelik maddeler rehberde 3.6. Fiziksel Mekanların Güvenliği başlığı altında yer almaktadır. Bu başlık altında Genel Güvenlik tedbirleri, Sistem Odası/Veri Merkezine Yönelik tedbirler ve Elektronik Bilgi Kaçaklarından Korunma Yöntemleri başlıkları altında ele alınmıştır. Bu maddelerde Ek-A maddelerinin

ötesinde yönetimsel, prosedürler denetime yönelik hususlar ayrıntılı bir şekilde ele alınmıştır. Örneğin Elektromanyetik ve Bilgi kaçaklarından Korunma Yöntemleri başlığında ele alınan maddeler askeri düzeyde güvenlik gerektirecek kurumlara uygulanabilecek nitelikte detaylı güvenlik gereksinimlerdir. Fiziksel kontrol maddelerinin denetimine ilişkin maddeler de tanımlanmıştır. Bu maddenin gereksinimleri kısmen karşılanmıştır.

A.7.4: Fiziksel ortamın izlenmesi rehberde ayrıntılı bir şekilde ele alınmıştır. Sadece gereksinimler değil denetim adımları da tanımlanmıştır. ISO/IEC 27002'de üst seviyeden 3 madde ile ifade edilirken rehberde 9 kontrol maddesi ile ifade edilmiştir. Bu madde gereksinimleri karşılanmıştır.

A.7.5: Fiziksel ve çevresel koşulları kontrol edilmektedir. Rehber sürekli var olan bina ve altyapının güvenliğinden bahsederken ISO /IEC 27001 Ek-A tasarım konusunda da gereksinimleri (binanın dışarıdan görünümü, suç bölgesine yakınlığı vb.) ortaya koymaktadır. Bu maddenin gereksinimleri kısmen karşılanmıştır.

A.7.6: Kritik cihaz ve verilerin bulunduğu güvenli alanlara ait çalışma kriterleri ayrıntılı bir şekilde tanımlanmıştır. Tanımlanan kriterler yanında bu maddelere ilişkin prosedür ve denetim maddeleri de rehberde yer almaktadır.

A.7.7: Buradaki bazı maddeler fiziksel güvenlik yanında personel güvenliği bölümü altında ele alınmıştır.

A.7.8: Endüstriyel ortamlardaki varlıkların özel koşullarına ilişkin ayrıntılı maddeler bulunmamaktadır. Endüstri koşulları ile ilgili önlemler enerji sektörü özelinde güvenlik gereksinimlerinde belirtilmiştir. Bu maddenin gereksinimleri kısmen karşılanmıştır.

A.7.9: Kuruluş dışı varlıkların güvenliği konusu rehberde doğrudan ve kapsamlı şekilde ele alınmamıştır. Donanım Varlık Envanteri Yönetimi ve Yazılım Varlık Envanteri başlıkları altında yer almaktadır. Dışarıya aktarılan verilerin nasıl korunacağı, karşı taraftan beklenen güvenlik önlemleri gibi kritik kontroller yer almamaktadır. Bu maddenin gereksinimleri kısmen karşılanmıştır.

A.7.10: Tanışabilir bilgisayarın disk güvenliğine yönelik maddelerin birçoğu bu madde gereksinimlerini karşılamaktadır ancak taşınabilir bilgisayarın imhası veya el değiştirmesi durumundaki güvenlik önlemleri ifade edilmiştir. Bu maddenin gereksinimleri karşılanmıştır.

A.7.11: Bu maddenin gereksinimleri karşılanmaktadır.

A.7.12: Bu maddenin gereksinimleri karşılanmaktadır.

A.7.13: Bu maddenin gereksinimleri karşılanmaktadır.

A.7.14: Bu maddenin gereksinimleri karşılanmaktadır.

Rehber Ek-B'de uluslararası standartlar ve yayımlı kılavuzlar ile eşleştirilmesini gösteren bir tablo yer almaktadır. Bu tabloda ISO/IEC 27001'de yer almaktadır fakat eşleştirme çok üst seviyeden ve rehberin sıkılaştırmalar dışındaki tüm maddelerinin standartla uyumlu olduğu gösterilmektedir.

5.2.4. Teknolojik Güvenlik Kontrollerdeki Boşluk Analizi

Bu başlık altında standardın (ISO/IEC 27002) Teknolojik Güvenlik Kontrollerine karşılık rehberin güvenlik tedbirleri incelenmiştir. Teknolojik Güvenlik Kontrollerine yönelik karşılaştırmalı boşluk analizi detayları Tablo 5.5'te yer almaktadır.

Tablo 5.5 Teknolojik Güvenlik Kontrol Maddeleri Boşluk Analizi

ISO 27001:2022 EK-A Maddesi	**Kamu Bilgi ve İletişim Güvenliği Rehberinde Karşılığı**	**Boşluk Analizi**
A.8.1 Kullanıcı uç nokta cihazları	3.2.x, 3.3.x, 3.4.x-	Bu maddenin gereksinimleri karşılanmaktadır
A.8.2 Ayrıcalıklı erişim hakları	3.2.3.3, 3.2.7.12, 3.2.7.1, 5.1.3.5, 5.1.3.6	Bu maddenin gereksinimleri kısmen karşılanmaktadır
A.8.3 Bilgi erişim kısıtlaması	3.5.1.x, 3.6.1.x, 3.6.2.x, 4.1.2x	Bu maddenin gereksinimleri karşılanmaktadır.
A.8.4 Kaynak koduna erişim	3.2.6.x	Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.5 Güvenli kimlik doğrulama	3.1.12.x	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.6 Kapasite yönetimi	3.1.9.2, 3.6.2.15	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.7 Kötü amaçlı yazılıma karşı koruma	3.1.3.2, 3.1.4.7, 3.1.5.x, 3.1.6.32, 3.1.9.4	Bu maddenin gereksinimleri kısmen karşılanmaktadır
A.8.8 Teknik açıklıkların yönetimi	3.1.3.x	Bu maddenin gereksinimleri kısmen karşılanmaktadır
A.8.9 Konfigürasyon (yapılandırma) yönetimi	3.1.1.x, 3.1.2.x	Bu maddenin gereksinimleri kısmen karşılanmaktadır
A.8.10 Bilgi silme	3.1.1.6, 3.1.1.9, 3.1.9.3, 4.3.1.11	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.11 Veri maskeleme	4.1.2.6, 4.1.4.2, 5.3.2.5	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.12 Veri sızıntısı önleme	3.1.7.8, 3.1 14.17	Bu maddenin gereksinimleri karşılanmaktadır.
A.8.13 Bilgi yedekleme	4.1.5.x, 3.3.1.1,3.1.3.x	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.14 Bilgi işleme tesislerinin yedekliliği	3.1.3.x	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.15 Olay Kayıtları (Log tutma)	3.1.8.x	Bu maddenin gereksinimleri kısmen karşılanmaktadır
A.8.16 İzleme faaliyetleri	3.1.7.8, 3.1.12.9, 3.6.2.5, 3.6.2.12	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.17 Saat senkronizasyonu	4.5.2.11, 3.1.8.3	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.18 Ayrıcalıklı destek programların kullanımı	5.1.3.6	Bu maddenin gereksinimleri karşılanmamaktadır.
A.8.19 İşletim sistemlerine yazılım kurulumu	3.1.2.x, 3.2.5.x,	Bu maddenin gereksinimleri karşılanmaktadır.
A.8.20 Ağ güvenliği	3.1.6.x	Bu maddenin gereksinimleri karşılanmaktadır.
A.8.21 Ağ hizmetlerinin güvenliği	3.1.6.x	Bu maddenin gereksinimleri karşılanmaktadır.
A.8.22 Ağların ayrımı	3.1.6.6	Bu maddenin gereksinimleri karşılanmaktadır.

A.8.23 Web filtreleme	3.1.6.20, 3.1.6.21, 3.1.6.22	Bu maddenin gereksinimleri karşılanmaktadır.
A.8.24 Kriptografi (şifreleme) kullanımı	4.4.x	Bu maddenin gereksinimleri karşılanmaktadır.
A.8.25 Güvenli geliştirme yaşam döngüsü	3.2.6	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.26 Uygulama güvenlik gereklilikleri	3.2.x	Bu maddenin gereksinimleri karşılanmaktadır.
A.8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri	3.1.6.x, 3.2.6.x	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.28 Güvenli kodlama	3.2.6.x	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.29 Geliştirme ve kabul aşamasında güvenlik testleri	3.2.6.x, 4.6.x	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.30 Dış kaynak yoluyla geliştirme	3.2.4.2, 4.3.1.10, 4.3.1.1	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.31 Geliştirme, test ve canlı (gerçek) ortamlarının ayrılması	3.1.11.17, 3.2.6.2, 3.2.7.7	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.32 Değişiklik yönetimi	2.4, 3.1.3.3	Bu maddenin gereksinimleri karşılanmaktadır.
A.8.33 Test bilgisi	3.2.6.2, 3.2.7.7	Bu maddenin gereksinimleri kısmen karşılanmaktadır.
A.8.34 Denetim sırasında bilgi sistemlerinin korunması	2.3.2.	Bu maddenin gereksinimleri karşılanmaktadır.

Ek-A Teknolojik Güvenlik Kontrolleri İçin Yorumlar

A.8.1: Rehber, Uygulama ve veri Güvenliği, Taşınabilir Cihaz ve Ortam Güvenliği, Nesnelerin İnterneti (IoT) Cihaz Güvenliği bölümlerinde uç cihaz güvenliğini kapsamlı bir şekilde ele almıştır. Bu maddenin gereksinimleri karşılanmaktadır.

A.8.2: Rehberde erişim yetkileri Yetkilendirme başlığı altında ele alınmıştır. Ayrıcalıklı erişimlerin büyük bir kısmı ifade edilmiş. Bunun yanında yetkilerin sınırlı

bir süre için verilmesi, yetkilerin linkle çoklu paylaşılmaması gibi standardın istediği ayrıntılar rehberde yer almamaktadır. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.3: Bilgiye erişim kısıtlaması farklı başlıklar altında ele alınmıştır. Bu maddenin gereksinimleri karşılanmaktadır.

A.8.4: Rehberde Güvenli Yazılım Geliştirme bölümü olmasın karşın standardın spesifik olarak istediği kaynak koda erişimlerin sınırlandırılması, geliştiricilerin doğrudan kaynak koda depolarına erişmemesi, güvenli geliştirme araçlarının belirlenmesi gibi spesifik gereksinimler tanımlanmamıştır. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.5: Kimlik doğrulama Ağ ve Sistem Güvenliği Başlığı altında ele alınmış. Oysa bu konu bilgi güvenliğinin tüm alanlarını etkileyen geniş kapsamlı bir konu ve bu tür bilgilerin farklı yerlerde verilmesi bilgi güvenliğine bütüncül bakmayı engellemektedir. İkisi de bilgi güvenliğini ele almaya çalışıyor fakat bakış açıları çok farklı. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.6: Sanallaştırma, Klima altyapısı gibi maddelerde yerli kapasitenin sağlanması gerektiği ifade edilmesine karşın tüm teknik ve personel altyapı yeterliliğini sorgulayan maddeler bulunmamaktadır. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.7: Zararlı Yazılımlardan Korunma başlıklı bir bölüm bulunmaktadır. E-posta güvenliği gibi özel bölümeler altında zararlı yazılıma karşı korunma ele alınsa da atak durumlarında sistemin izole edilmesi, zararlı yazılımlar konusunda bültenler çıkarılması gibi ayrıntıları içermemektedir. Zafiyetli sistem için güncellemenin mümkün olmadığı durumda ne yapılacağı net olarak ortaya konulmamıştır. Ayrıca tehdit ve zafiyet yönetimi ile olay yönetimin bağlanması gerektiği açıkça ifade edilmemiştir. Bu bilgi Siber Güvenlik Olay Yönetimi başlığı altında da ele alınmamıştır. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.8: Bu maddenin gereksinimleri kısmen karşılanmamaktadır. Zafiyetli sistem için güncellemenin mümkün olmadığı durumda ne yapılacağı net olarak ortaya konulmamıştır. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.9: Konfigürasyon yönetimin bazı başlıkları Donanım Varlıklarının Envanter Yönetimi ve Yazılım Varlıklarının Envanter Yönetimi başlıkları altında ele alınmıştır. Ama gereksiz servislerin kapatılması, ortak zaman bilgisi kullanımı, konfigürasyon dosyası değişikliklerinin tutulması gibi maddeler bu başlıklarda yer almamaktadır. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.10: Donanım Varlıklarının Envanter Yönetimi ve Yazılım Varlıklarının Envanter Yönetimi başlıkları altında gereksiz bilgilerin geri döndürülmeyecek şekilde silinmesi ifade edilmiş fakat bunlara ait olay kayıtlarının tutulması gibi ayrıntılar bulunmamaktadır. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.11: Kişisel verileri güvenliği bölümünde veri maskelemeden bahsedilmektedir. Standart ise hassas verilerin maskelenerek saklanması gerektiğini belirtiyor ve maskeleme teknikleri konularında örnekler veriyor. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.12: Veri kaçağı önleme standarda yeni bir kontrol maddesi olarak eklenmiştir. Rehber de aynı başlığı içermektedir. 3.1.7 ‘de ve 4.1.8’de ve 4.4.1.x’de standardın maddeleri ele alınmıştır. Bu maddenin gereksinimleri karşılanmaktadır.

A.8.13: Rehberde yedekleme bütüncül bir bakış açısıyla ele alınmamış. Genel olarak Felaketten Kurtarma ve İş Sürekliliği bölümünde ele alınmakla birlikte, bazı bölümün içinde ilgili verilerin yedeğinin alınması, saklanması ve gerektiğinde imha edilmesi ifade edilmeye çalışılmıştır. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.14: Rehberde bilgi işlem tesis yedekliliği genel olarak Felaketten Kurtarma ve İş Sürekliliği bölümünde ele alınmıştır. Bu bölümlerde yedek merkezinin fiziksel olarak uzak bir yerde bulunması öncesinde internet servis sağlayıcılarla anlaşılması gibi standardın spesifik belirlediği hususlar sorgulanmamaktadır. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.15: Rehberde İz ve Denetim Kayıtlarının Tutulması ve izlenmesi altında tüm olay kayıtlarına ait gereksinimler ifade edilmiştir. Alt bölümlerde de sistemler ait olay kayıtlarının tutulması gerekti ifade edilmiştir. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.16: İzleme ve olay kayıtlar benzer başlıklar altında ele alınmış ve izleme maddeleri ilgili bölümlerin altına eklenmiştir. Maddeler birbiri ile uyumludur. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.17: Zaman bilgisinin onaylı sunuculardan alınması gerektiği belirtilmiştir. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.18: Ayrıcalıklı programları ele alan maddeler bulunmamaktadır. Bu maddenin gereksinimleri karşılanmamaktadır.

A.8.19: Sistem yazılım yüklenmesi Yazılım Varlık Envanteri Yönetimi, Güvenli Kurulum ve yapılandırma başlıkları altında ele alınmıştır. İşletim sistemine yönelik gereksinimler değil tüm yazılımlara yönelik gereksinimler ele alınmıştır. Bu maddenin gereksinimleri karşılanmaktadır.

A.8.20: Genel ağ cihaz ve sistemleri yanında, Wi-Fi, IP Telefon, içerik kontrolü gibi güvenliğe yönelik diğer sistemler ait güvenlik gereksinimleri de belirtilmiştir. Bu maddenin gereksinimleri karşılanmaktadır.

A.8.21: Ağ Güvenliği başlığı bu gereksinimler de karşılanmıştır. Bu maddenin gereksinimleri karşılanmaktadır.

A.8.22: Bu maddenin gereksinimleri karşılanmaktadır

A.8.23: Bu maddenin gereksinimleri karşılanmaktadır.

A.8.24: Bu maddenin gereksinimleri karşılanmaktadır.

A.8.25: Standart tüm BT ürünlerinin güvenli getirilmesini ele alırken, rehber sadece güvenli yazılım geliştirme gereksinimlerini tanımlamıştır. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.26: Uygulama Güvenliği 3.2 bölümünde kapsamlı bir başlık olarak alınmıştır. Bu maddenin gereksinimleri karşılanmaktadır.

A.8.27: Güvenli Yazılım Geliştirme, Ağ Mimarisi gibi bölümler olsa da Güvenli Sistem Mimarisi ve Mühendislik ilklerini içeren genel bir başlık bulunmamaktadır. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.28: Güvenli yazılım geliştirme bölümünde kaynak kodu analiz, uygulama güvenli testler, güvenli yazılım geliştirme metodolojisi gibi üst seviye ifadeler kullanılmıştır. Standart bu konularda SQL Enjeksiyonu, Hata Mesajı kontrolü gibi daha spesifik gereksinimleri tanımlamıştır. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.29: Güvenli Yazılım Geliştirme ve Yeni Geliştirmeler ve Tedarik bölümünde testlere ilişkin ifadeler yer almaktadır. Standartta ise güvenlik sistemi geliştirme ve testinin çok ayrıntılı ele alındığı görülmektedir. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.30: Rehber daha çok bu konularda politika, prosedür geliştirip onlar aracılığıyla sürecin güvenliğinin sağlanmasını ifade etmektedir. Standart ise doğrudan yapılması gerekenleri ifade etmektedir. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.31: Test, geliştirme ve canlı sistem ayrılması gerektiği ve nasıl ayrılması gerektiği net bir şekilde ifade edilmemiştir. Kamu kurumu olduğu için genel sistem geliştirmeyeceği varsayılmış olabilir. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.32: Rehberin etkin bir şekilde uygulamasını tanımlayan Değişiklik Yönetim bölümü bulunmasına cihaz, sistem ve yazılımlar üzerindeki değişikliklerin izlenmesi her varlık başlığı altında incelenmiştir. Bu maddenin gereksinimleri karşılanmaktadır.

A.8.33: Rehber sadece yazılım geliştirme için bir ortamdan bahsetmekte o da sınırlı kontrol içermektedir. Bu maddenin gereksinimleri kısmen karşılanmaktadır.

A.8.34: Rehber bilgi sistem denetime ait ayrıntılı bilgi vermemiştir. Bilgi ve İletişim Güvenliği Denetim Rehber'ine göre yapılacağını belirtmiştir. Bu maddenin gereksinimleri karşılanmaktadır.

BÖLÜM 6: SONUÇ ve ÖNERİLER

Günümüzde dijitalleşme hem kamu hem özel sektör kuruluşlarının operasyonel süreçlerinde kaçınılmaz bir dönüşüm alanı hâline gelmiştir. Bu da yalnızca sanayi ve hizmet sektörlerini değil; devlet, sağlık, ticaret ve tarım gibi alanları da derinden etkileyip ve dönüştürmektedir. Bu dönüşüm, hem hizmet sunum biçimlerinde hem de süreç yönetimlerinde köklü değişimlere yol açmıştır.

Dijitalleşme ile birlikte kamu ve özel sektör kuruluşlarında bilgiye dayalı süreçlerin artması, bilgi güvenliğini kurumlar için hayati bir konu haline getirmiştir. Özellikle kişisel verilerin, kurumsal bilgilerin ve kritik altyapılara ilişkin verilerin dijital ortamlarda işlenmesi, bu verilerin gizliliği, bütünlüğü ve erişilebilirliğini koruma gereksinimini ortaya çıkarmıştır. Söz konusu bilişim sistemleri güvenliğinin sağlanması için standartlar, anaçatılar ve regülasyonlar geliştirilmiştir.

ISO/IEC 27001; Bilgi Güvenliği Yönetim Sistemi kurmak isteyen kuruluşların bağlamları, temel gereksinimleri, liderlik ve altyapı koşulları hakkında genel kuralları belirleyen uluslararası alanda kabul görmüş standarttır. Standarda tabii olmak için gönüllülük esastır, herhangi bir zaruriyet yoktur ama uyulması gereken prensipler net olarak açıklanmıştır. Bütün uluslar nazarında kabul gördüğü için risk yönetimi konusunda rehber niteliğindedir. Kamu Bilgi ve İletişim Güvenliği Rehberi, ise CBDDO tarafından yayımlanmış, Türkiye'deki kamu kurumlarındaki bilişim sistemleri güvenliğini sağlamak için hazırlanmış bir regülasyondur. kamu kurumlarının bilgi güvenliği yönetim sistemi kurmaları, yönetmeleri ve güvenliğini sağlamaları için rehberlik sunan bir regülasyondur.

Bu tez çalışmamda uluslararası düzeyde kabul görmüş bir bilgi güvenliği yönetim sistemi standardı olan ISO/IEC 27001:2022 ile Türkiye'de kamu kurumlarının uyması gereken ulusal bir çerçeve niteliğindeki Kamu Bilgi ve İletişim Güvenliği Rehberi arasında kapsamlı bir boşluk analizi gerçekleştirilmiştir. Analiz kapsamında ISO/IEC 27001 Ek A'da yer alan kontrol maddeleri ile rehberin ilgili bölümleri ve maddeleri karşılaştırılmış; aralarındaki örtüşen yönler, eksiklikler ve uygulama farkları sistematik biçimde değerlendirilmiştir. Standart ve rehberin her ikisi de gizlilik bütünlük ve erişilebilirliği korumayı hedeflemesine rağmen güvenliği farklı başlıklar

altından ele aldıkları için karşılaştırmak zor olmuştur. Rehberin daha çok bilgi güvenliği varlıkları üzerinde önlemler alarak güvenliği sağladığı gözlemlenmiştir.

Kamu Bilgi ve İletişim Güvenliği Rehberi ile ISO/IEC 27001:2022 Ek-A kontrolleri arasında hem kapsam hem derinlik açısından farklar bulunduğu gözlemlenmiştir. Rehber özellikle teknik kontrollerde ISO/IEC 27001 ile genel çerçevede örtüşmekle birlikte; yönetişim, sürekli iyileştirme, politika yaşam döngüsü, tedarikçi güvenliği, risk temelli yaklaşım gibi alanlarda kısmi boşluklar içermekte ve bu çalışma da bu boşlukları analiz etmek için hazırlanmıştır.

Elde edilen bulgular,

- Standart, liderliği bilgi güvenliği yönetim sisteminin omurgası olarak konumlandırır. Liderlik, yalnızca yönetimsel bir görev değil; stratejik yönelim, kaynak tahsisi, politika onayı ve sistematik iyileştirme gibi işlevleri içeren kapsamlı bir sorumluluk alanıdır. Kamu Bilgi ve İletişim Güvenliği Rehberi ise liderlik konusunu daha çok yönetsel sorumluluk boyutunda ele alır. Rehberde üst yönetimin rolü tanımlanmış olsa da, standardın öngördüğü stratejik liderlik anlayışı rehberde net ve kapsamlı biçimde yer almaz. Bu da rehberin, kamu kurumlarında bilgi güvenliği kültürünün oluşturulması ve sürdürülebilirliği açısından bir boşluk içerdiğini göstermektedir. Rehbere ISO/IEC 27001'deki gibi "liderlik" başlığı altında, yönetimin bilgi güvenliğine olan taahhüdü, sistematik liderlik rolü ve stratejik yönetişim katkısını içeren bölümler eklenmesi gerekmektedir.

- Standardın planlama maddesi bilgi güvenliği yönetim sisteminin (BGYS) etkili şekilde kurulması ve sürdürülmesi için gerekli olan stratejik planlama adımlarını kapsar. Varlık temelli ya da senaryo temelli risk değerlendirme yöntemleri önerilerek risk kriterleri belirlenmeli ve riskler analiz edilerek kabul edilebilir seviyeler tanımlanmasını öngörür. Rehberde ise planlama faaliyetleri daha çok "risklerin belirlenmesi" ve "kontrollerin seçimi" süreçlerine indirgenmiştir.

- Standardın işletim yaklaşımı, risk temelli kontrollerin uygulanmasını planlı, ölçülebilir ve dokümante edilmiş süreçlerle desteklerken; Rehberde bu

kontroller çoğunlukla eylem bazlı kalmakta, bütüncül bir işletim modeli sunulamamaktadır. Bu durum, kamu kurumlarında uygulama farklılıklarına ve sürdürülebilirlik sorunlarına yol açabilecektir.

- Rehberin amacı kurumun rehbere uyumunun denetlenmesi olarak belirlenmiştir. Bu doküman da rehberdeki istekleri baz aldığı için rehberde eksik olan madde büyük olasılıkla denetimde de eksik olacaktır. Diğer taraftan denetimi yapacak kişilerin ISO/IEC 27001 baş denetçi sertifikasına ya da TSE tarafından verilen baş denetçi sertifikasına sahip olması gerektiği belirtilmiştir. Bu da denetimin yetkin ekip tarafından yapılmasına olanak sağlayacak ve ISO/IEC 27001 bakış açısı rehbere de uygulanmış olacaktır.

- Standardın iyileştirme maddesi BGYS' nin sadece kurulmasını değil, değişen koşullara göre evrilmesini, gelişmesini ve dirençli bir yapıya dönüşmesini hedeflemektedir. Bu bağlamda sürekli iyileştirme ve düzeltici faaliyetler, sistemin canlılığını koruması açısından stratejik öneme sahiptir. Rehber ise teknik odaklı bir yapı sunduğu için, iyileştirme döngüsü ve yönetişim temelli öğrenme süreçlerini büyük ölçüde geniş bakış açısıyla ele almamaktadır.

- Rehberin çoğu temel bilgi güvenliği kontrol alanını kapsadığını, özellikle teknik kontroller (ağ güvenliği, erişim kontrolleri, güvenlik testleri vb.) açısından ISO/IEC 27001 ile büyük ölçüde uyumlu olduğunu göstermektedir. Ancak analiz, Kamu Bilgi ve İletişim Güvenliği Rehberi'nin yönetişimsel düzeyde yani politika oluşturma, risk temelli yaklaşım, belgelendirme ve sürekli iyileştirme gibi alanlarda ISO/IEC 27001'in sistematik yapısından belirgin şekilde farklılaştığını ve detaylandırma konusunda zayıf kaldığı tespit edilmiştir.

- Rehberi uygulayan kurum kamu kurumu olacağı için tabi olduğu yasa ve düzenlemeler çerçevesinde gerekli dokümantasyon, rol sorumlulukları tanımlıyor olabileceği göz önüne alınmalıdır.

- Rehber tarafında KVKK ile daha sıkı bir bağlantı kurulmaya çalışılmıştır. Standartta bu durum genel bir başlık olarak ele alınmıştır.

- ISO/IEC 27001'de yer alan birçok kontrol maddesi için risk yönetimi temelli detaylı bir yaklaşım önerilirken, rehber daha çok "uygulanacak tedbirler" şeklinde yönlendirici ama operasyonel düzeyde kalmaktadır. Bu durum, kamu kurumlarının bilgi güvenliği uygulamalarında belirli bir düzeyin üzerinde stratejik bütünlük sağlamakta zorlanabileceğini göstermektedir. Bu kurumların devletle olan bağından kaynaklanabilecek bir durumda olabilir. Çünkü kamu kurumları özel sektör kuruluşları gibi tamamen kendi vizyon ve misyonunu belirleyecek durumda değildir.

- Rehber'in yazılı prosedürler, rollerin tanımlanması, disiplin süreçleri, sözleşmesel yükümlülükler ve dış kaynak yönetimi gibi standardın yönetimsel kontrolleriyle ilgili kısımlarda sınırlı kaldığı yönündedir. Bu boşluklar, bilgi güvenliği uygulamalarında hesap verilebilirlik, sürdürülebilirlik ve denetlenebilirlik açısından riskler oluşturabilir fakat kamu kurumunun tabi olduğu kanun ve regülasyonlar bu riskleri ortadan kaldırma ya da azaltmada etken olabilir.

- Rehber, temel teknik kontrollerin uygulanması açısından yeterli bir yapı sunmakla birlikte, bilgi güvenliği yönetiminin kurumsal süreçlere entegre edilmesi bakımından ISO/IEC 27001 ile tam anlamıyla uyumlu değildir. Teknik anlamda ve uygulama konularında her ne kadar detaylara değinilmiş olsa da bu durum, Türkiye'deki kamu kurumlarının uluslararası standartlara uygunlukta ve sertifikasyon süreçlerinde çeşitli zorluklar yaşayabileceğini göstermektedir. Bu nedenle, rehberin gelecekteki güncellemelerinde ülkemizdeki kanun, yönetmelik ve diğer regülasyonlara daha etkin bağlantı kurularak boşluklar giderilebilir.

- ISO/IEC 27001 standardıyla olan farkların kapatılmasına yönelik daha bütünsel ve risk temelli bir yaklaşımın benimsenmesi, hem uyumluluğu hem de kurumsal bilgi güvenliğinin etkinliğini artıracaktır.

- Olay müdahale süresinde SOME, USOM ve yetkili kurumlarla iletişim tanımlanmasına karşın, basınla iletişim, toplumla iletişim net ifade edilmemiştir

- Alt yüklenici ve tedarikçilerle yapılan çalışmada temel ihtiyaçlar tanımlanmakla birlikte onlara teslim edilen verilerin nasıl korunacağı, onların denetimleri nasıl yapılacağı gibi güvenlik zincirinin tüm halkalarını ele alınmamıştır.

- Telif hakları, yazılım lisansı, yasal içerik kullanımı gibi fikri mülkiyet konularına rehberde yer verilmemektedir. Telif haklarına uyum için kontrol mekanizması ve lisans yönetimi süreçleri tanımlanmamıştır. Bu konuda yasalar ışığında tanımlama yapılabilir.

- Uzaktan çalışma Ağ ve Sistem Güvenliği başlığı altında ele alınmıştır. Daha çok sistem yöneticilerin ağa erişim ve video konferansı tanımlamaktadır. Bu tür çalışmalarda önemli olan olay kayıtlarının tutulması, yetkisiz erişimlerin kontrol edilmesi, uzaktaki sisteme erişim yönetimi, uzaktaki cihazların sigortalanması, uzaktaki cihaz getirildiğinde uygulanacak prosedür konularına değinilmemiştir.

- Ofis odaları ve tesislerin güvenliğine yönelik gerekli önlemler tanımlanmıştır fakat kritik binaların veya ofislerin göz önünde olmayacak şekilde tasarlanması, içerdeki faaliyetler görünmeyecek şekilde önlemler alınması ifade edilmemiştir. Ayrıca binanın suça yakın yerlerde kurulmaması gibi çevresel etkenler de ifade edilmemiştir.

- Endüstriyel ortamlardaki varlıkların özel koşullarına ilişkin ayrıntılı maddeler bulunmamaktadır. Endüstri koşulları ile ilgili önlemler enerji sektörü özelinde güvenlik gereksinimlerinde belirtilmiştir.

- Kimlik doğrulama, yetkilendirme, olay kaydı genel güvenlik önlemleri Rehber'de cihaz veya varlık bazlı verilmiştir. Oysa bunların sistemdeki tüm varlıklar için tanımlanması gerekir.

- Personel yetkinliği ve yeterliliği bilgi sistemlerinin tamamı için verilmemiştir. Olay müdahale gibi spesifik bazı roller için verilmiştir.

- Güvenli Yazılım Geliştirme ve Yeni Geliştirmeler ve Tedarik bölümünde testlere ilişkin ifadeler yer almaktadır. Standartta ise güvenlik sistemi

geliştirme ve testinin çok ayrıntılı ele alındığı görülmektedir. Bu maddenin gereksinimleri karşılamaktadır.

Bu çalışma Standart ve Rehber üzerinden yapılmıştır. Kamu kurumlarındaki uygulama sonuçlarından yola çıkılarak bilgi güvenliği uygulamalarında eksik kalan veya geliştirilmesi gereken kısımlar daha net ifade edilebilir.

Bazı kamu kurumlarında, (Bankalar, vakıf üniversiteleri vb.) tabi oldukları regülasyonlardan dolayı aynı anda hem rehber hem de standarda uyma zorunluluğu olabilmektedir. Bu kurumlardan birinde standardın ve rehberin aynı anada uygulanmasının getirdiği avantajlar ve iş yükü analiz edilebilir.

Rehberin gereksinimlerinin birçoğunun yasa ve diğer regülasyonlarla bağlantısı bulunmaktadır. Bunlardan sadece KVKK ile ilgili gereksinimlere değinilmiştir. Diğerleri de ayrı bir çalışmada ele alınarak yasalar ve regülasyonlarla olan ilişkisi daha net ortaya konulabilir.

KAYNAKÇA

[1] McKinsey & Company, The state of AI in 2021. McKinsey & Company, 2021. [Online]. Erişim: 28 Tem.2025.Available: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Analytics/Our%20Insights/Global%20survey%20The%20state%20of%20AI%20in%202021/Global-survey-The-state-of-AI-in-2021.pdf

[2] World Health Organization, Global strategy on digital health 2020–2025. World Health Organization, 2021. [Online]. Erişim: 28 Tem.2025. Available: https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf

[3] H. Soysal, ISO/IEC 27001 Kapsamında Bilgi Güvenliği Yönetim Farkındalığının Değerlendirilmesi: Ankara İli Sağlık Kurumları Bilgi İşlem Birimi Çalışanları Örneği, Yüksek lisans tezi, T.C. Necmettin Erbakan Üniversitesi, Sağlık Bilimleri Enstitüsü, Konya, 2023.

[4] G. Y. Tarcani, P. Y. Balçıki, and N. B. Sebik, "Türkiye ve Dünyada Sağlık Hizmetlerinde Yapay Zekâ," Lokman Hekim Tıp Tarihi ve Folklorik Tıp Dergisi, vol. 14, no. 1, pp. 50–60, 2024, doi: 10.31020/mutftd.1278529.

[5] H. Şahin, "Dijital Tarım, Tarım 4.0, Akılı Tarım, Robotik Uygulamalar ve Otonom Sistemler," Tarım Makinaları Bilimi Dergisi, vol. 18, no. 2, pp. 68–83, Oct. 2022.

[6] E. Çeliksoy and A. Akça, "Türkiye'de Kamu Yönetiminde Yaşanan Dijital Dönüşüm Süreci," Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, vol. 15, no. 2, pp. 445–486, Jul. 2024.

[7] OECD, The e-Government Imperative, OECD e-Government Studies, OECD Publishing, Paris, 2003, doi:10.1787/9789264101197-en.

[8] Y. Uysal, S. Kurban, and M. Z. Çığm, "Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve E-Yönetişim," Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, no. 78, pp. 211–231, 2023, doi: 10.51290/dpusbe.1337001.

[9] H. Uslu, “Dijital Dönüşüm ve Kamu Hizmetleri: Yönetimde Yenilikçi Yaklaşımlar ve Zorluklar,” Uluslararası Politik Araştırmalar Dergisi, vol. 8, no. 2, pp. 45–60, 2023.

[10] J. Kim, J. Oh, G. Gim, and Y. Kim, “An Empirical Study on E-Government Service Using Web Standard Policy,” in AI and Metaverse, R. Lee, G. Gim, and J. Kim, Eds., Studies in Computational Intelligence, vol. 1160, Cham: Springer, 2024, pp. 75–85. doi: 10.1007/978-3-031-61163-6_7.

[11] B. Thangjam, K. K. Jha, and S. Sharma, "Scale development for measuring the farmers' attitude towards sustainable agricultural practices," The Journal of Research ANGRAU, vol. 52, no. 2, pp. 139–147, 2024.

[12] V. I. Espinosa and A. Pino, “E-government as a development strategy: The case of Estonia,” International Journal of Public Administration, vol. 48, no. 2, pp. 86–99, Feb. 2024, doi: 10.1080/01900692.2024.2316128.

[13] M. Yıldız, Kurumlar için bilgi güvenliği yönetim sisteminin oluşturulması, Yüksek lisans tezi, Konya Karatay Üniversitesi, 2022.

[14] O. M. Christopher and G. Osazuwa, "Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature," International Journal of Innovative Science and Research Technology, vol. 8, no. 12, Dec. 2023, doi.org/10.5281/zenodo.10464076.

[15] S. Nezgitli and Ş. Gökçearslan, Kamu Kurumu ve Özel Sektöre Yönelik Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme, Instructional Technology and Lifelong Learning, 2022, Cilt 3, Sayı 1, s. 19-44

[16] F. Djebbar, "A comparative analysis of industrial cybersecurity standards," IEEE Access, vol. 11, pp. 102119–102136, Aug. 2023.

[17] Cumhurbaşkanlığı, “Cumhurbaşkanlığı Kararnamesi, Sayı: 32354,” 28 Mart 2025.

[18] M. Kıran and İ. Soğukpınar, “Ulusal siber güvenlik stratejilerinin değerlendirilmesi,” Savunma Bilimleri Dergisi, vol. 19, no. 1, pp. 75–100, 2020.

[19] S. Nezgitli and R. Benzer, "Avrupa Birliği Siber Güvenlik Kanunu," Journal of Information Systems and Management Research, vol. 2, no. 1, pp. 10–17, 2020.

[20] İ. Ç. Erkul, “Birleşik Krallık’ın siber güvenlik politikasını güç ve caydırıcılık üzerinden anlamlandırmak,” Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi, cilt 2, sayı 1, ss. 1–21, 2023.

[21] TÜBİTAK BİLGEM, Rusya-Ukrayna Savaşı Siber Güvenlik Değerlendirme Raporu, 2022.

[22] M. Tunçbilek, "2022 Yılında Yaşanan Gelişmeler Doğrultusunda Bilgi Güvenliğinde Risk Yönetiminin Artan Önemine İlişkin Bir Değerlendirme," Bilgi ve İletişim Teknolojileri Dergisi, 2024.

[23] R. Başar, “Türkiye’de ISO 27001 Bilgi Güvenliği Yönetim Sistemi Sertifikasına Sahip Çeşitli Kuruluşların BGYS Yaklaşımları Üzerine Bir İnceleme,” Premium E-Journal of Social Sciences, 2022.

[24] National Cyber Security Centre, Cyber Essentials: Basic Technical Protection Against Cyber-Attacks, London, UK: NCSC, 2020. [Online]. Erişim: 28 Tem.2025. Available: https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf

[25] European Union, NIS2 Directive, 2022.

[26] Bundesamt für Sicherheit in der Informationstechnik (BSI), Lagebericht 2023, 2023.[Online]. Erişim: 28 Tem.2025.Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=8

[27] Japanese Industrial Standards Committee, JIS Q 27001:2023, 2023.

[28] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 – General Data Protection Regulation (GDPR), 2016. [Online]. Erişim: 28 Tem.2025. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[29] D. Pöhn, N. Mörsdorf, and W. Hommel, "Needle in the Haystack: Analyzing the Right of Access According to GDPR Article 15 Five Years after the Implementation," arXiv preprint arXiv:2308.15166, 2023.

[30] R. N. Savaş, A. H. Zaim, and M. A. Aydın, "KVKK ve GDPR Kapsamında Firmaların Mevcut Durum Analizi Üzerine Bir İnceleme," İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, vol. 19, no. 38, pp. 208–223, Dec. 2020.

[31] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2021, Heraklion, Greece: ENISA, 2021. [Online]. Erişim: 28 Tem.2025.Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[32] T.C. Cumhurbaşkanlığı, Cumhurbaşkanlığı Kararnamesi, Sayı: 32354, 28 Mart 2025.

[33] Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Dijital Türkiye Raporu, 2022.

[34] European Commission, Proposal for a Regulation on Digital Operational Resilience for the Financial Sector (DORA), 2022.

[35] Sermaye Piyasası Kurulu (SPK), Bilgi Sistemleri Rehberi, 2022.

[36] Türkiye Cumhuriyet Merkez Bankası, Ödeme Sistemlerinde Bilgi Güvenliği İlkeleri Rehberi, 2021.

[37] O. Gazdağı and T. Çetinyokuş, "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, vol. 10, no. 2, pp. 475–491, Jun. 2020, doi: 10.14230/johut781.

[38] International Organization for Standardization, ISO/IEC 27001, 2022.

[39] G. A. Korkmaz, ISO 27001 Bilgi Güvenliği Sistemi Konulu Yayınların WoS Veri Tabanına Dayalı Bibliyometrik Analizi, Düzce, Türkiye: 2023. [Çevrimiçi]. Erişim: 28 Tem.2025. Erişim adresi: https://www.researchgate.net/publication/369572814

[40] M. B. Yazıcıoğlu, “ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi kapsamında bilgi güvenliği risk yönetimi ve risk analizi,” Bilgisayar Bilimleri ve Teknolojileri Dergisi, vol. 5, no. 2, pp. 1–13, 2024 .

[41] T.C. Kişisel Verileri Koruma Kurumu (KVKK), Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), Ankara, Türkiye: KVKK, 2018. [Çevrimiçi]. Erişim: 28 Tem.2025.Erişimadresi: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5

[42] T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Kamu Bilgi ve İletişim Güvenliği Rehberi, Ankara, Türkiye: Cumhurbaşkanlığı DDO, 2020. [Çevrimiçi]. Erişim: 28 Tem.2025.Erişim adresi: https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf

[43] M. Tulgar, A. H. Zaim, and M. A. Aydın, “Ulusal Bilgi ve İletişim Güvenliği Rehberi: IoT güvenliği için bir uygulama örneği,” İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, vol. 21, no. 42, pp. 353–382, 2022.

[44] R. Özkan, ISO 27001 Bilgi Güvenliği Yönetim Sistemleri Standartlarının Uygulanması: Gıda Sektöründe Bir Uygulama, Yüksek lisans tezi, [Üniversite Adı], Karaman, 2024.

[45] T. Özbilen, A. Çağlar, “Türk kamu sektöründe bilgi ve bilişim güvenliği,” Kamu Yönetimi ve Teknoloji Dergisi - , no. 1, 2020.