İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

Veri Güvenliğinin İyileştirilmesi Sürecinde Risk Tabanlı Küresel Standart, Çerçeve ve En İyi Uygulama Yaklaşımları

Onur KORUCU
115691023

Prof. Dr. Şule IŞINSU ÖZMEN

İSTANBUL
2021

Veri Güvenliğinin İyileştirilmesi Sürecinde Risk Tabanlı Küresel Standart, Çerçeve ve En İyi Uygulama Yaklaşımları

Risk Based Global Standard, Framework and Best Practice Approaches in Data Protection Improvement Process

Onur Korucu
115691023

Tez Danışmanı : **Prof. Dr. Şule IŞINSU ÖZMEN** (İmza) .....
İstanbul Bilgi Üniversitesi

Jüri Üyeleri : **Dr. Öğr. Üyesi Mehmet Bedii KAYA** (İmza) .....
İstanbul Bilgi Üniversitesi

Prof. Dr. Cem Sefa SÜTCÜ (İmza) .....
Marmara Üniversitesi

Tezin Onaylandığı Tarih : 30.01.2021
Toplam Sayfa Sayısı : 146

Anahtar Kelimeler (Türkçe)
1) Veri Güvenliği
2) Bilgi Güvenliği
3) Risk Yönetimi
4) Bilgi Teknolojileri Yönetişimi
5) Uyum

Anahtar Kelimeler (İngilizce)
1) Data Protection
2) Information Security
3) Risk Management
4) Information Technology Governance
5) Compliance

ÖNSÖZ

Bu çalışmada amaçlanan, son yılların ve günümüzün en önemli konularından veri güvenliği kavramının dünyaca kabul edilen küresel standart, çerçeve ve en iyi uygulama yaklaşımları yardımı ile risk tabanında değerlendirilebilen, geliştirilebilen ve sürdürülebilen bir algıya oturtulması, bununla birlikte farklılaşan ekonomik, sektörel ve kültürel gereksinimlerin ve konjonktürlerin ülke gerçekleri paralelinde ele alınarak teknoloji-hukuk-uyum güçlerinin entegrasyonu için yeni bir bakış açısı sunmaktır.

Bununla beraber değerli destekleri için başta aileme, arkadaşlarıma ve kıymetli öğretmenlerime teşekkür ederim.

Onur KORUCU

İÇİNDEKİLER

KISALTMALAR

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
ISACA	Bilgi Sistemleri Denetim ve Kontrol Kurumu (Information Systems Audit and Control Association)
API	Uygulama Programlama Ara yüzü / Application Programming Interface
APO	Align, Plan and Organize
APT	Advanced Persistent Threat
ATM	Automated Teller Machine
BAI	Build, Acquire and Implement
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BGYS	Bilgi Güvenliği Yönetim Sistemi
BT	Bilgi Teknolojileri
BTK	Bilgi Teknolojileri ve İletişim Kurumu
BS	Bilgi Sitemleri
CD	Compact Disc
COBIT	Bilgi için Kontrol Hedefleri ve İlgili Teknolojiler / Control Objectives for Information and related Technology
COVID-19	Coronavirus
DDI	Data Documentation Initiative
DDoS	Dağıtık Hizmet Engelleme / Distrubuted Denial of Service Attack
DLP	Data Loss Prevention software
DoS	Hizmet Engelleme / Denial of Service
DPIA	Veri Koruma Etki Değerlendirmesi / Data Protection Impact Assessment
DPC	Data Protection Commission
DPO	Veri Koruma Görevlisi / Data Protection Officer
DSS	Deliver, Service and Support

EDM	Evaluate, Direct and Manage
EDPS	European Data Protection Supervisor
GB	Gigabytes
GDPR	Genel Veri Koruma Yönetmeliği / General Data Protection Regulation
GRC	Yönetişim Risk ve Uyum / Governance Risk Compliance
GSM	Global System for Mobile Communications
ICO	Bilgi Komisyonu Ofisi / Information Commissioner's Office
IMF	International Monetary Fund / Uluslararası Para Fonu
IoT	Nesnelerin interneti / Internet of Things
ISO	Bilgi Güvenliği Yönetimi Koordinatörü / Information Security Officer
ISO	Uluslararası Standartlaştırma Örgütü / International Organization for Standardization
ISO 27001	ISO / IEC 27001:2013 Bilgi Güvenliği Yönetim Standardı
ITIL	Bilgi Teknolojileri Altyapı Kütüphanesi / The Information Technology Infrastructure Library
KRI	Key Risk Indicator
KRM	Ticari Nitelikli Kredi Bildirimi ve Paylaşımı
KVKK	Kişisel Verilerin Korunması Kanunu
MEA	Monitor, Evaluate and Assess
MB	Megabytes
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü / National Institute of Standards and Technology
POS	The Point of Sale
SEO	Arama Motoru Optimizasyonu / Search Engine Optimization
SLA	Service Level Agreement
SIEM	Security Information and Event Management
SWOT	Güçlü Yönler, Zayıf Yönler, Fırsatlar ve Tehditler / Strengths, Weaknesses, Opportunities and Threats
TB	Terabytes

TİDE	Türkiye İç Denetçiler Enstitüsü
UK	Birleşik Krallık Hükümeti
WHO	Dünya Sağlık Örgütü / World Health Organization

ŞEKİL LİSTESİ

TABLO LİSTESİ

ABSTRACT

Data protection notion has gained enormous importance, not only from corporate perspective but also nationally and internationally. In our world, one of the biggest risks around digitalization is to provide essential and sustainable data protection.

To be able to identify and prevent data protection risks and threats, global standards, frameworks and best practices are used in our country as well as globally to guide parties to make forecasting and maintain a uniform maturity level. Fast developing technology and technological changes made the requirement of data protection inevitable. Data protection can be accomplishable by identifying the threats in relation to the data before they materialize and taking required preventive measures into account. In light of this, risk-based data protection is a dynamic and disciplined system which helps data governance. This work presents a national and an international perspective in relation to technology and law connection to maintain data protection.

In the first part of this work, the definition, approach and technical aspects of data and data protection are addressed. The connection between data protection, cyber security and information security is evaluated. The technical terminology regarding data protection is explained. Comments in relation to data protection audits and its future are shared. The second part of this work addresses the definition of risk and risk evaluation approaches. Risk based global standards, frameworks and best practices are introduced and technical parts are mentioned. Risk based process and technology management methods are evaluated and the need of standardization is stated in relation to the regulations. The third part of this work discusses the aspects of risk-based approach as well as the aspects technology and law that support and complement each other from the data security point of view. Finally, with the help of global standards, best practices and frameworks, the relationship between data security audit approach and actual legislation examples discussed, illustrated in detail. The opinions which are believed to be useful are shared.

Keywords: Data, Data Types, Data Protection, Data Governance, Information Security, Risk Management, Risk Assessment, Risk Based Approach, Process Control,

Technology Audit, Information Technology Governance, Compliance, Global Standard, International Standards, Framework, Best Practice, ISO 27001, COBIT, NIST, ITIL, KVKK, GDPR.

ÖZET

Veri güvenliği kavramı günümüzde sadece kurumsal değil aynı zamanda kişisel, organizasyonel ve bütünleşik yaklaşım ile ulusal ve uluslararası büyük önem kazanmıştır. Dünyada dijitalleşme alanında en büyük risk veri güvenliğinin yeterli ve sürdürülebilir olarak sağlanamamasıdır.

Veri güvenliği hususunda görülen risk ve tehditlerin belirlenebilmesi ve önlenebilmesi için ülkemiz ve dünyada küresel standartlar, çerçeveler ve en iyi uygulama yaklaşımları yardımı ile gerekli öngörümleme ve yeknesak bir güvenlik olgunluğu sağlanması amaçlanmaktadır. Teknolojinin hızla gelişmesi ve değişmesi verinin yolculuğunda güvenliğinin sağlanmasını kaçınılmaz kılmıştır. Veri güvenliğinin sağlanması, verinin güvenliğine yönelik tehdit oluşturan unsurların gerçekleşmeden önce belirlenmesi ve gerekli önleyici tedbirin alınması ile mümkündür. Bu ifade ile risk tabanlı veri güvenliği, verilerin yönetişimini sağlayan dinamik ve disiplinli bir sistemdir. Mevcut çalışma, söz konusu veri güvenliğinin sağlanmasında teknoloji ve hukuk ilişkisine dair ulusal ve uluslararası bir bakış açısı ortaya koymaktadır.

Çalışmanın birinci bölümünde veri ve veri güvenliği tanımı, yaklaşımları ve teknik yönlerine değinilmiştir; bilgi güvenliği, siber güvenlik ve veri güvenliği ilişkisi incelenmiştir. Veri güvenliği kavramı hakkında bilinmesi gereken teknik ifadeler açıklanmıştır. Veri güvenliğinin denetimi ve geleceğine ilişkin görüşler paylaşılmıştır. Çalışmanın ikinci bölümünde risk tanımı ve risk değerlendirme yaklaşımlarına değinilmiştir, risk tabanlı küresel standart, çerçeve ve en iyi uygulama yaklaşımları tanıtılmış ve teknik yönleri paylaşılmıştır. Risk tabanlı süreç ve teknoloji denetimi yöntemlerinin neler olduğu tartışılmıştır, regülasyonlar ile ilişkisi bakımından standartlaşma ihtiyacı belirtilmiştir.

Çalışmanın üçüncü bölümünde Türkiye'de ve dünyada risk tabanlı yaklaşımın ve veri güvenliğinin sağlanması bakımından teknoloji ve hukukun birbirini destekleyen yönleri vurgulanmıştır. Küresel standart, çerçeve ve en iyi uygulama örnekleri yardımı ile, veri güvenliği denetimi ve güncel mevzuat örneklerinin ilişkisi detaylı şekilde

değerlendirilmiş, örneklendirilmiş ve uyum süreçlerinde faydalı olacağına inanılan görüşler paylaşılmıştır.

Anahtar Kelimeler: Veri, Veri Çeşitleri, Veri Güvenliği, Veri Yönetişimi, Bilgi Güvenliği, Risk Yönetimi, Risk Değerlendirmesi, Risk Tabanlı Yaklaşım, Süreç Denetimi, Teknoloji Denetimi, Bilgi Teknolojileri Yönetişimi, Uyum, Küresel Standart, Uluslararası Standartlar, Çerçeve, En İyi Uygulama, ISO 27001, COBIT, NIST, ITIL, KVKK, GDPR.

GİRİŞ

Yazılı olarak henüz kabulü gerçekleşmese bile yeni 'teknoloji çağı'na geçtiğimiz 20. yüzyılın ikinci yarısından günümüze dünyada ve ülkemizde bilişim teknolojilerinin yaygınlaşması, kullanımının hızla artması ve artık organizasyon ve kurumların dijital hayatı benimsemesi kaçınılmaz olmuştur. Farklı kategorilerdeki ve özelliklerdeki verilerimiz artık fiziksel ortamlardan çok dijital ortamlarda yoğun bir biçimde işlenmekte, paylaşılmakta ve saklanmaktadır. Mevcut süreçte yaşanan teknolojik, hukuki, ekonomik ve süreçsel değişkenler formülize edilecek olursa, gelecek kuşakların yaşamakta olduğumuz yılları, 20. yüzyılın ikinci yarısı öncesinden ayırt edici şekilde nitelemek için günümüzün çokça kullanılan dijitalleşme tanımına vurgu yapacakları öngörülebilir. 21. yüzyıla geldiğimizde dijitalleşme yaklaşımı, kişisel kullanım başlangıç noktasından kurumsala büyüyen bir eksende sadece iş yapma biçimimiz değil, yaşamın her alanına etki eden bir değişim olarak, belirgin bir şekilde kendini göstermektedir.

Günümüzde veri tanımı birbirinden farklı şekillerde yapılmaktadır. Bunun sebebi ise verinin, veriyi kullanan taraflar, kullanım amacı, türü vb. nitelik ve nicelik özelliklerine göre herkes için farklı anlam ifade etmesidir. Bilimsel bir yakınsama ile veri, ünlü bilim adamı Albert Einstein'ın kütlenin bir tür enerji olduğu çıkarımını dünyanın en ünlü formülü olarak nitelendirmesinde olduğu gibi, herhangi bir işleme tabi tutulmamış, gözlem veya ölçüm yöntemleri ile farklılaşan ortamlardan elde edilen her türlü değer olarak nitelendirilebilir. Veri, kişiler arasında sözlü ifadeler, yazılı fiziki belgeler veya dijital ortam saklanan bilgiler olarak karşımıza çıkabilmektedir. Farkında olarak ya da olmadan üretilen, kullanılan, paylaşılan ve saklanan verilerin; işlenmesi ve organize edilmesi ile bilgi elde edilmektedir. Elektronik ortamlarda verilerin veya bilgilerin işlenmesi, saklanması ve paylaşılması esnasında, bütünlüğü bozulmadan, izinsiz erişimlerden korunarak güvenli bir bilgi işleme ortamı oluşturma sürecindeki adımların bütününe veri güvenliği denmektedir. Bilgiye sürekli erişimin sağlanması, bilginin göndericiden alıcısına kadar gizlilik içerisinde, bozulmadan,

değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlük içerisinde güvenli bir şekilde iletimi bilgi güvenliği olarak tanımlanabilir.[1]

Bilgi güvenliği literatürüne göre risk, "gizlilik", "bütünlük" ve "erişebilirlik" olarak sıralanan bilginin korunması gereken temel niteliklerinin bir tehditle karşılaşması durumunda varlık üzerindeki bilinen zafiyet ya da zafiyetlerin kötü amaçlı kullanılmasıyla kuruma zarar verme, istenmeyen etki doğurabilme ihtimaline denir.[2]

Bilgi Güvenliği Yönetim Sistemi (BGYS), kurumların verilerini yönetebilmek amacıyla benimsedikleri sistematik bir yaklaşım olup temel amacı verilerin güvenliğini sağlamaktır. Bilgi güvenliği yönetim sistemlerinde risk yönetimi ise, hedeflere ulaşabilmek için her seviyede risklerin belirli bir yöntemle sistematik olarak belirlenmesini, değerlendirilmesini, kabul edilebilir seviyelerin denetlenmesini, risklerin etkilerini azaltmak için önlemlerin alınmasını ve işletilmesini sağlayacak süreklilik gerektiren bir süreçtir. Risk yönetimi, gelecekteki istenen veya istenmeyen olayların olasılığı ve uzlaşılan hedefler üzerindeki etkisini göz önünde bulundurarak karar vermeye yardımcı olur.[3] Risk yönetimi, kurumların veri güvenliğini tehdit eden riskleri ve bu risklerin olasılık ve etkilerini öngörmeye yardım edecek katmanlı bir çalışma gerektirmektedir. Risk tabanlı yaklaşım, kurumlara yasal gerekliliklere uymanın ötesine geçebilecek bir perspektif sağlayabilmekte, kurumların amaçları doğrultusunda mevcut durum analizi yaparak gerekli veri güvenliği tedbirlerini almaları hususunda yol gösterebilmektedir.

Verilerin dijital ortamda saklanması eğilimine paralel olarak farklı amaçlara hizmet eden teknolojilerin kullanımının ülkemizde ve dünyada hızla gelişip yaygınlaşması görülmektedir. Bu yaygın kullanılan teknolojilerin politika ve yöntem eksiklikleri sebebi ile etkin kullanımı konusunda yetersizlikler söz konusudur. Ülkemizde özellikle bankacılık gibi mevzuatla yönlenen sektörlerde, dünyaya oranla belirgin şekilde teknoloji kullanımı ve yatırımı eğilimi görülmektedir. Bankacılıkla birlikte, elektronik haberleşme, sağlık, elektronik ticaret, enerji, otelcilik vb. sektörlerde de veri

[1] Pfleeger, C.P, The fundamentals of information security, Software, IEEE, C.14, 1997, s.14.
[2] Demirci, M., Bilgi Güvenliği. Ankara : Kamu Hastaneleri Kurumu, 2015.
[3] Eskiyörük, D., BGYS Risk Yönetim Süreci Kılavuzu, Kocaeli: Tübitak, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, 2007.

güvenliği aynı şekilde önemlidir. Hukuki, ekonomik ve stratejik perspektiften benzer değerde görülen veriler, farklı sektör ve organizasyonel yapılardaki kurumlarda aynı şekilde işlense dahi, teknoloji kullanım ve dijitalleşebilme yatkınlığı her sektör ve kurumda farklılık gösterebilmektedir. Bu anlamda teknolojik çözümler veri güvenliğinin sağlanması konusunda kurumların işlerini kolaylaştırıp, hata oranını düşürse dahi, asıl ortak amaç tüm çalışanların bilinçlendirildiği ve her katmanda benimsenen bir bilgi güvenliği yönetim yapısı inşa edebilmektir.

Organizasyonel yapı, kültürel yaklaşım, mevcut değişkenler gibi parametreler söz konusu olduğunda hukuk ve uyum çerçevesinde regülasyonlara, dünyaca kabul gören standart, çerçeve vb. kurallara bakış dijital bir çözümü amaçlamazsa bilişim teknolojileri ile bu teknolojilerin hammaddesi olan verinin önemi tam olarak anlaşılamamış olacaktır. Eğer güvenlik teknolojileri aksak kalırsa, verinin bilgiye dönüşmesi sürecinde gerekli güvenlik koşullarının sağlanamayacaktır.

Kurumlar tarafından veri güvenliğine yönelik risk tabanlı yaklaşımların belirlenmesi ve kurumların kendilerine uygun stratejileri benimsemeleri farklılık göstermektedir. Farklılaşan iş modelleri, teknolojik tehdit etmenleri, sektörel faktörler, organizasyonel hedefleri göz önünde bulundurulduğunda kurumlar regülasyon ve kanunlara uyum çerçevesinde zorunlu bir veri güvenliği ortamı sağlama yükümlülüğündedir. Veri güvenliğinin sağlanması için ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Standardı (ISO 27001), Bilgi için Kontrol Hedefleri ve İlgili Teknolojiler (Control Objectives for Information and related Technology-COBIT), Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology-NIST), The Information Technology Infrastructure Library (ITIL) gibi bilgi yönetim standartları, çerçeveler ve en iyi uygulamalar mevcuttur. Kurumlar, bulundukları lokasyonlar, regülasyonların tavsiye ettiği kontroller, mevcut benimsenen veri güvenliği politikaları, güven ortamının sağlanması, kanuni zorunluklar gibi sebepler ile farklı kategorilerdeki verilerini bu standartları, çerçeveleri ve en iyi uygulamaları takip ederek sağlamayı hedeflemektedirler. Kurumlarda bilgi ve veri güvenliği yönetim sistemini oluşturmak için yol gösteren bu küresel standartlar, çerçeveler ve en iyi uygulamalar; sistematik bir risk analiz yöntemini önermektedir. Kurumların iş modellerine uygun risk değerlendirme yöntemlerinin oluşturulması ve bu sayede uyum süreçlerinin

mevzuatlara uygun şekilde tamamlanması temel veri güvenliği ihtiyacıdır. Buna paralel bir tutumla 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) veri güvenliğinin sağlanmasına ilişkin yükümlülükler getirilmiş olup, veri güvenliğinin sağlanmasına ilişkin gerekli tedbirlerin alınmaması durumunda idari para cezalarının gündeme geleceği yine ilgili mevzuat kapsamında öngörülmüştür. Veri güvenliğinin sağlanması sürecinde alınması gereken önlemler Kişisel Verileri Koruma Kurulu tarafından yayınlanan Kişisel Veri Güvenliği Rehberi ile teknik ve idari tedbirler olacak şekilde, KVKK uyarınca kişisel verilerin hukuka aykırı olarak işlenmesini ve kişisel verilere hukuka aykırı olarak erişilmesini önlemek ile kişisel verilerin muhafazasını sağlamak amacıyla veri sorumlularının alması gereken teknik ve idari tedbirlere ilişkin başlıca yöntemleri ayrı ayrı bölümler halinde açıklamakta olduğunu belirten ifadeler ile yayınlanmıştır.[4] Kişisel Veri Güvenliği Rehberi içerisinde bulunan idari tedbirler bölümünde, mevcut risk ve tehditlerin belirlenmesi ve risk analizi ifadesi açıkça belirtilmiş, ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı kaynak olarak gösterilmiştir. Nitekim KVKK'nın 12. Maddesi uyarınca veri sorumlusu; (i) kişisel verilerin hukuka aykırı olarak işlenmesini önleme, (ii) kişisel verilere hukuka aykırı olarak erişilmesini önleme, (iii) kişisel verilerin muhafazasını sağlama amaçlarıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türkü teknik ve idari tedbiri almak zorundadır.

Mayıs 2016'da kabul edilen ve 25 Mayıs 2018'de yürürlüğe giren Avrupa Birliği (AB)'nin veri koruma düzenlemesi Genel Veri Koruma Yönetmeliği (General Data Protection Regulation-GDPR) bir regülasyon olması bakımından yürürlüğe girmesi ve uygulanması eş zamanlı olmuştur. GDPR risk tabanlı bir yaklaşım benimsemekte ve bu risk yaklaşımına göre, veri işleme faaliyetindeki risk seviyesi arttıkça, hesap verilebilirliğe ilişkin yükümlülükleri de ağırlaşmaktadır. Risk tabanlı yaklaşım yöntemi mevcut mevzuata uyum sürecinde gerekli değerlendirme, ölçümleme ve orantılılık metodu olarak kullanılmıştır. GDPR 24. maddesi kapsamında, riskin gerçekleşme ihtimali ve riskin gerçekleşmesi durumunda doğuracağı etkilerin ölçümlenmesi gereksinimi ifade edilmiştir. GDPR'nin 32. maddesi verilerin işlemesi

[4] Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi, Teknik ve İdari Tedbirler. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf (Erişim tarihi: 04.01.2020)

sürecinde güvenliğin sağlanmasını kapsamaktadır ve bu süreçte oluşacak risklerle doğru orantılı olarak gerekli teknik ve idari tedbirleri alma yükümlülüğü getirilmektedir. GDPR'nin 35. maddesi kapsamında öngörülen veri koruma etki değerlendirmesi; kişisel verilerin gizliliğini etkileme ve ihlal etme potansiyeline sahip olan fiziksel etmenler ve bilişim sistemlerinin uygulama esnasında ve uygulamadan sonraki süreçte; verinin güvenliği bakımından kontrol edilmesine yönelik denetim mekanizması rolündedir. Veri Koruma Etki Değerlendirmesi (Data Protection Impact Assessment-DPIA) veri güvenliğine yönelik riskleri belirlemek ve olası tehditlere engel olmak amacıyla önleyici yolların belirlenmesi sürecidir. Bu tür risk analizleri; gelişmiş ülkeler başta olmak üzere dünya genelinde giderek yaygınlaşmaktadır. Risk tabanlı yaklaşım yöntemi mevcut mevzuata uyum sürecinde gerekli değerlendirme, ölçümleme ve orantılılık metodu olarak kullanılmıştır. Benzer veri güvenliği yaklaşımlarına Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yürürlüğe giren güncel mevzuatlar da örnek olarak verilebilir.

Bu çalışmada veri güvenliği ve risk değerlendirme kavramlarının teknik özellikleri üzerinde durulmuş ve bu kavramların detaylı incelemesi yapılmıştır. Çalışmanın son bölümünde veri güvenliğinin iyileştirilmesinde teknoloji ve hukuk uyum ilişkisinin, ulusal ve uluslararası bakışla risk tabanlı yaklaşım ile ele alınması amaçlanmıştır. Risk tabanlı yaklaşım küresel standart, çerçeve ve en iyi uygulama örnekleri kapsamında risk yönetimi kuralları ile temellendirilmiştir. Dünyada ve Türkiye'de veri güvenliğine ilişkin yürürlükte olan mevzuatlara atıflarda bulunarak teknoloji ve uyum perspektifinde risk analizi ve denetim güvence fonksiyonlarının yeterliliğine ilişkin değerlendirmeler ve görüşler paylaşılmıştır.

BİRİNCİ BÖLÜM

VERİ, VERİ GÜVENLİĞİ TANIMI, YAKLAŞIMLARI VE TEKNİK YÖNLERİ

1.1 VERİ TANIMI VE VERİ GÜVENLİĞİ YAKLAŞIMLARI

1.1.1. Veri Nedir?

Verinin İngilizce karşılığı olarak kullanılan "data", Latince "datum" kelimesinin çoğul halidir. Data "vermeye cesaret etmek" fiilinin geçmiş zamanı, dolayısıyla "verilen şey" anlamına gelmektedir. Latince "data" (dedomena) kavramının M.Ö. 300 yıllarında Öklid'in bir çalışmasında geçtiği bildirilmektedir.[5] Dilimizde de "verilen şey" anlamında, "veri" olarak kullanılmaktadır. Bilişim teknolojisi açısından veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller veya bit dizeleri olarak tanımlanabilir. Veri, gerçekleşen olgular ve aksiyona geçmiş olaylar hakkındaki birbirinden ayrı nesnel değerleri ifade etmek amacı ile kullanılır ve belli bir formatla kayıt altında tutularak anlamlı bilgiye dönüşür. Bir verinin tek başına bir anlamı ve işlevi bulunmamaktadır. Veriler toplandıktan sonra gruplanarak, sıralanarak ve özetlenerek, elle ya da bilgisayarla işlenip enformasyona dönüştürüldüklerinde anlam kazanmakta; ait oldukları bağlamı açıklama gücüne kavuşmaktadır. Problem çözme ya da karar verme gibi bir amaca hizmet edebilecek duruma gelmektedir.[6]

Başka bir ifade ile veri, analiz veya referans amacıyla toplanan değerler koleksiyonudur. Veriler, yazılı olmayan düşünsel kayıtlar, görsel ve işitsel kaynaklar, nümerik tablolar, nesnel formlar ve dijital kayıtlar gibi çeşitli formlarda bulunabilir. Günümüzde veri kavramı olguların ve rakamların sistematik olarak kümelenmesini temsil eden tekil veya toplu bir ifade olarak ele alınmaktadır.

[5] Canberk, Gürol, Şeref, Sağıroğlu, Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme Politeknik Dergisi, C.9, S.3, 2006 s. 165-174.

Veri kavramı, dijital verilerin oluşturulması ve bilgisayar, telefon, sunucu vb. elektronik ortamlarda işlenen, paylaşılan ve saklanan bilgilerin büyüyerek artması ile kalıcı olarak hayatımıza girmiştir. Dijital veriler, kişisel ya da kurumsal her tip ortamda masaüstü bilgisayarlar, dizüstü bilgisayarlar, cep telefonları, tabletler, sensörler vb. çeşitli elektronik cihazlar yardımı ile üretilir. Bugün iş hayatına yön veren, analitik yöntemlerle sistemli olarak işlenerek modeller ile yaratılan veriler, verileri üreten veya içeren elektronik depolama ortamlarında ikili değerlerin dizileri (0lar ve 1ler) olarak depolanmaktadır. Dijital verilere örnek olarak elektronik belgeler, e-postalar, e-kitaplar, dijital görüntüler, dijital sesler ve dijital videolar verilebilir.
Veri ve bilgi terimleri birbiriyle yakından ilişkilidir. Günümüzde bu terimlerin sıkça birbiri yerine kullanılması durumu görülmektedir. Veriler belirli bir düzen ve sistematik içinde işlenmesi ile bilgiye dönüştürülür. Veriler belirli bir bağlamda işlenip, kümelenip anlamlandırıldığında bu organize edilmiş veriye bilgi denmektedir. Bilgi yönetimi günümüzde büyük önem kazanmıştır. Artık doğru ilişkisel sistematik dizinli bilgiler ayrı bir iş kolu olarak veri analitiği kavramı ile karşımıza çıkmaktadır. Bilgiye sahip olmanın bir rekabet ve güç aracı olduğunu Stewart'ın "bilgi zenginliğin en önemli kaynağı haline geldiğine göre, bireylerin, şirketlerin ve ülkelerin bilgiyi üreten ve işleyen varlıklara yatırım yapması gerekir." sözleri vurgulamaktadır.[7]

Verilerin işlenmesi, kümelenmesi, analiz edilmesi kurumların iş modelleri ve süreç öngörümlemelerinde büyük önem taşır. Bu sayede kurumlar verilerden değer elde ederek kurumsal etkinliği sağlamak için istihbarat oluşturabilirler.

1.1.2. Veri Yönetimi

Kişisel yaşantımızda bir grup CD veya daha önceleri bir grup diskete sığan bilgilerimiz bugün nasıl TB'lık yüksek kapasiteli disklere sığamaz olmuştur. Bireyler kişisel veri birikimlerini sahip oldukları elektronik cihazlarda muhafaza etmek ve güvenliğini sağlamak zorunda kalmışlardır. Tıpkı bireylerin ihtiyaçları gibi kurumlar

[7] Stewart, Thomas A., Entelektüel Sermaye- Kuruluşların Yeni Zenginliği, Çev. Nurettin Elhüseyni, BZD Yayıncılık, İstanbul, 1997, 339s.

da önüne geçilemez bir hızla artan, değişen ve gelişen farklı fonksiyonlardaki verilerini kullanmak, organize etmek ve saklamak istemektedirler. Bu sayede veri yönetimi, kavram ve ihtiyaç olarak hayatımıza girmiştir.

Veri yönetimi, verinin güvenli, verimli ve uygun maliyetli bir şekilde toplanması, saklanması ve kullanılması uygulamasıdır. Veri yönetiminin amacı; insanların, kurumların ve bağlantılı araçların verileri politika ve düzenleme sınırları kapsamında kullanımını optimize etmelerine yardımcı olmaktır. Böylece kurumlar en yüksek düzeyde fayda sağlayacak kararlar alabilir ve bunları hayata geçirebilirler. Bu sebeple kurumlar değer yaratmak için maddi olmayan varlıklara giderek daha fazla güvendikleri için güçlü bir veri yönetimi stratejisi her zamankinden daha önemli hâle gelmektedir.[8]

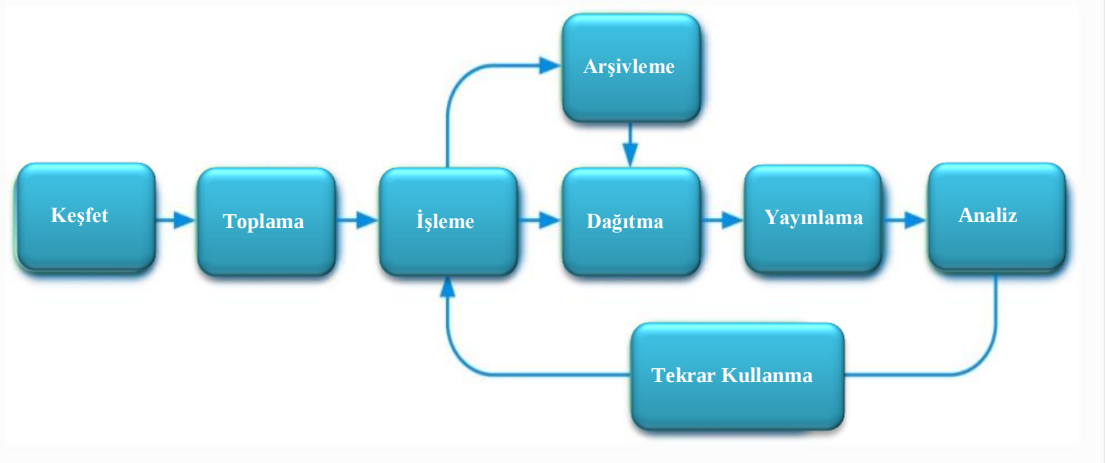
Veri yönetimi, veri miktarındaki hızlı artış sebebi ile yeni bir iş kolu haline gelmiştir. Veri artışının bu kadar hızlı olduğu bir ortamda verinin yeniden kullanımının sağlanmak üzere paylaşılması, anlaşılır ve iyi düzenlenmiş olması, bir diğer ifadeyle verinin iyi yönetilmesi ile mümkün olabilmektedir.[9] Veri yönetimi, verinin nasıl elde edileceği, nasıl toplanacağı ve kullanılacağı, verinin sürdürülebilirliği sağlanacak şekilde nerede depolanacağı ve arşivleneceği ve verinin yeniden kullanımını sağlamak üzere dağıtım ve paylaşımının nasıl yapılacağının planlanmasıdır. Verinin nasıl yönetileceğinin planlaması veri yaşam döngüleri kullanılarak ifade edilebilir. Verilerin yönetilebilmesi için verinin yaşam döngüsünün, türünün ve sınıflandırmasının doğru anlaşılması gerekmektedir. Bu sayede veri farklı amaçlara hizmet edecek şekilde farklı algoritmalarda anlamlı bilgiye dönüşebilir ve gereken kontrol ortamı sağlanarak güvenliğine ilişkin riskler belirlenebilir ve bu risklerin gerçekleşmesi önlenebilir. Veri yaşam döngüleri veri keşfi, veri toplama, veri işleme ve planlama, veri analizi, veriyi yayınlama ve paylaşma, verinin uzun vadede yönetimi ve yeniden kullanımı değerlendirmektedir. Veri yaşam döngüsü ilk olarak DDI (Data Documentation Initiative) tarafından dizayn edilmiştir. Bu dizayn ile verinin farklı amaçlarla, farklı

[8] https://www.oracle.com/tr/database/what-is-data-management/
(Erişim tarihi: 05.01.2021)

[9] Ross-Hellauer, T., Jones, S., Research data management: An introductory webinar, 2016, https://webinars.eifl.net/2016-05-26_ResearchDataManagementAnintroductoryWebi1/default.html
(Erişim tarihi: 05.01.2021)

elektronik ortam ve farklı algoritmalar içerisinde kullanılması yolculuğu ifade edilmiştir.

Şekil 1.1 Veri Yaşam Döngüsü



[10]Kaynak: DDI. (2018). Why use DDI (Data Documentation Initiative). https://www.ddialliance.org/training/why-use-ddi

Verilerin üretilmesi hızı öyle artmıştır ki artık bu hususta söylenmiş onca yeni söylem literatüre geçmiştir. Verinin nasıl ve ne kadar büyük hacimde üretildiğini anlayabilmek için günümüzün en büyük icadı olan internet üzerinde gerçekleşen aksiyonların değerlendirmeleri veri yönetimine olan ihtiyaca ya da daha büyük bir ifade ile enformasyon yönetimine dair bizlere fikir vermektedir. Cisco'nun yaptığı araştırmalar gösteriyor ki küresel nüfusun yaklaşık üçte ikisi 2023 yılına kadar internet erişimine sahip olacak, 2018'de 3,9 milyardan (küresel nüfusun yüzde 51'i) 2023 yılına kadar 5,3 milyar toplam internet kullanıcısı (küresel nüfusun yüzde 66'sı) olacak, 2018'de kişi başına 2,4 ağ bağlantılı cihaz olan kişi başına 3,6 ağ bağlantılı cihaz olacak, 2018'de 18,4 milyar iken, 2023'e kadar 29,3 milyar ağ bağlantılı cihaz

[10] Kaynak: DDI. (2018). Why use DDI (Data Documentation Initiative). Erişim adresi: https://www.ddialliance.org/training/why-use-ddi (Erişim tarihi: 05.01.2021)

olacak.[11] 2019 da dünyada günlük alınan ve gönderilen e-posta sayısı ortalaması 293,6 milyar ve bu sayının 2022'de 333,2 milyar olması bekleniyor. Sadece Amerika Birleşik Devletleri'nde günlük internet kullanımı 3,138,420 GB gerçekleşmektedir. Buna ek olarak dünya genelinde yapılan araştırmalara göre 2020'de her saniye başına yaklaşık 1.7MB veri üretilmekte ve üretilen veriler depolanmakta ya da paylaşılmaktadır. Bu değerler katlanarak artmaktadır. Thomas L. Friedman'ın ifadesi ile, internetin icadıyla tüm dünya nüfusu tek bir şirket haline dönüşmüş, küresel düzeyde bir iş birliği içindedir yani internet dünyadaki mesafeleri ortadan kaldırarak teknoloji oyun sahasını düz hale getirmiştir.[12]

Verilerin filtresiz şekilde üretimi ve dolaşımı sorunu verinin yönetimini daha da önemli kılmıştır. Bu anlamda altını ararken çokça taştan kurtulmak yani kıymetli bir veri kümesine ulaşmak için çöp diye tabir edilen veri yığınından kurtulmak gerekmektedir.

Bugün bu veri yönetimini iyi gerçekleştiren Google, Facebook, Youtube vb. firmaların ürün ve platformlarının özellikle günümüzde yaşanan uzun süreli pandemi etkisi ile de ekonomik olarak nasıl büyüdüğünü ve bu ticari işletmelerin veri akışında ne denli büyük pay sahibi olduklarını görmekteyiz.

Veri hacminin büyümesi, bilgi bolluğunun yaşanması ve hiç bir veri ve bilginin kaybedilmemesi gerektiği fikri birçok yeni sorunu da beraberinde getirmektedir. Bilginin dolaşımı sürecinde görev alan, bilgiyi toplayan, işleyen ve paylaşan elektronik ortam, cihaz ve aracı teknolojilerin sayılarının artmasına karşın var olan depolama kapasitesi toplanan bilginin çok altında kalmaktadır. Dünyada bulundurulmaya ve kullanılmaya çalışılan küresel bilgi hacmi, depolama kapasitesini uzun süredir aşmış bulunmaktadır.

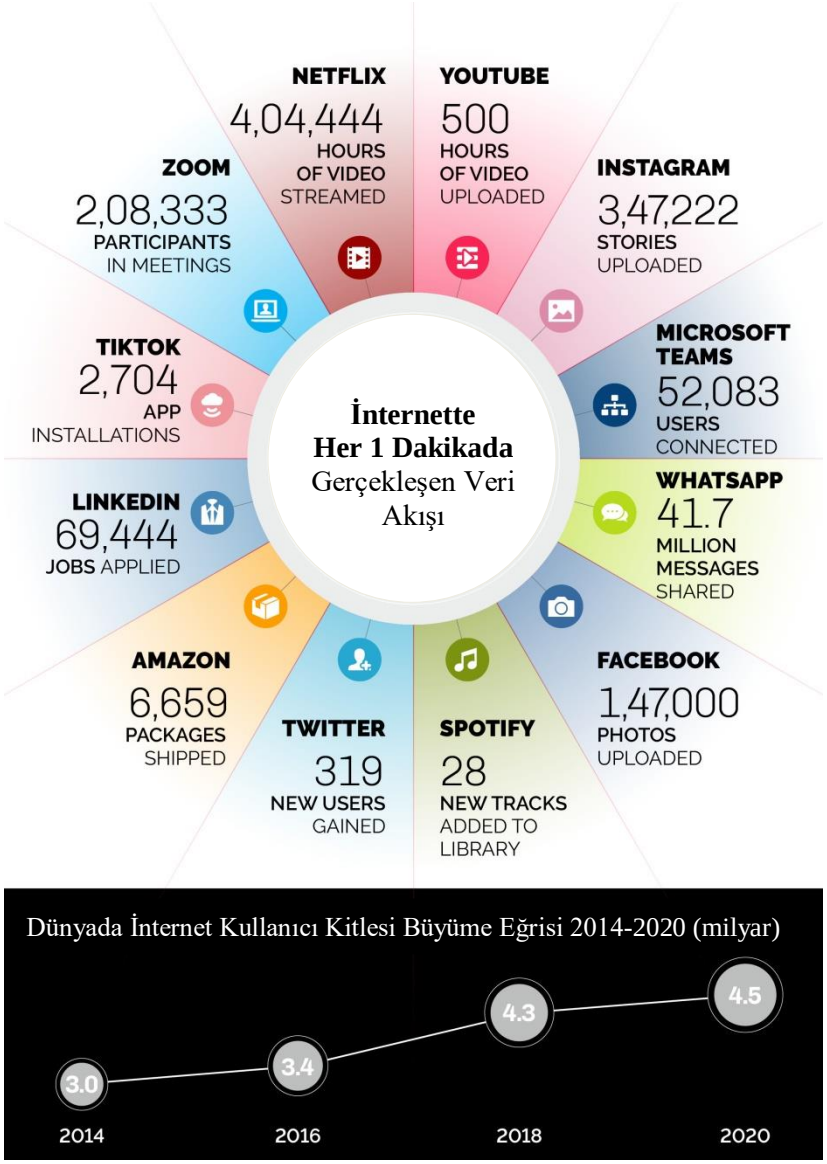
Geçirdiğimiz son bir yıl göstermiştir ki, çevresel risk faktörlerinden biri olan pandeminin yaşanması, birçok ülke ekonomisinde küçülmeye sebebiyet verirken,

[11] Cisco Annual Internet Report (2018-2023) White Paper, 2020.
https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
(Erişim tarihi: 05.01.2021)

[12] Thomas L. Friedman, Dünya Düzdür: Yirmi Birinci Yüzyılın Kısa Tarihi, Çevirmen: Levent Cinemre, Boyner Yayınları, 2006.

internet, bulut bilişim, teknoloji altyapısı vb. hizmetlerin yoğun sağlandığı ülke ekonomileri diğer ülkelerin aksine büyüme göstermiştir. Veriyi yönetebilen ülkeler bu ekonomik büyüme eğilimini sürdürebilecek, teknoloji oyun sahasında daha büyük bir paya sahip olacaklardır. Dünyanın veri yükünü taşıyan bu ülkelerde veri yönetiminin en önemli bileşenlerinden biri de veri güvenliğidir.

Şekil 1.2 2020'de İnternette Her 1 Dakikada Gerçekleşen Veri Akışı



Kaynak: https://www.statista.com/chart/17518/data-created-in-an-internet-minute/[13]

[13] Claire Jenik, A Minute on the Internet in 2020, Statista, Visual Capitalist, 2020.

Veri yönetimi yaklaşımının oluşmasıyla verilerin kategorize edilmesi ve verilerin farklı güvenlik gereksinimlerinin regülasyonlar ve kanunlar aracılığı ile tayin edilmesi söz konusudur. Verilerin kategorize edilebilmesi için belirlenmiş kriterler çerçevesinde verilerin sınıflandırılması gerekmektedir. Bu sınıflandırmalar sonucunda kurumlar ve hatta artık kişiler verilerine ilişkin gerekli güvenlik kontrollerini ve gereksinimlerini yerine getirebilirler, kategorik olarak mevcut risk ve tehditleri önceden belirleyebilirler. Bu anlamda verilerin farklı kategorik özelliklerini değerlendirebiliriz;

Kamusal Veri (Public Data): Devletler, devlet kurumları tarafından tutulan verilerdir. Kişisel bilgi olmayıp anonim hale gelen ya da kamu bilgisi değeri taşıyan bilgilendirici, araştırma değeri taşıyan halka açık paylaşılması hukuken uygun bulunmuş verilerdir. Elektronik, görsel, yazılı vb. yollarla kişilerin erişebileceği bir onaya tabi olmayan bilgilerdir. Kamusal veriler genellikle ham veya işlenmemiş veriler olduğundan bir telif hakkı uygulaması gerektirmemektedir.

Açık Veri (Open Data): Herhangi bir telif hakkına sahip olmayan, herkes tarafından kullanılabilen, düzenlenebilen ve dağıtılabilen veridir. Açık veride devletin şeffaflığı ve katılımı amaçlanmaktadır. Açık veri sayesinde devletler hem ekonomik hem de sosyal anlamda verimliliklerini artırabilir. Verilerin herkese açık ve özgürce kullanılabilir olması vatandaşların da farkındalığını ve bilgi sahibi olma düzeyini arttıracaktır. Açık veri üretiminin başlıca gerekliliği dijital formatlarda (CSV, XLS, JSON, XML vb) olmasıdır. Açık veriler lisanslı, sürekli yenilenen yani bütünlüğü bozulmamış, güvenli ve indeksli olmalıdır.[14] Anayasamızın 4982 sayılı Bilgi Edinme Hakkı Kanunu gereğince bütün vatandaşlar bilgi edinme hakkına sahiptir. Bilgi edinme hakkı hem kamusal algı hem de bireylerin fikri karakterini ifade edebilmesi anlamında öz gereksinimlerdendir. Devletin şeffaflığını amaçlayan bu kanun sayesinde bilgi almak istenilen bütün konular hakkında gerekli mercilere başvuru

https://www.statista.com/chart/17518/data-created-in-an-internet-minute/
(Erişim tarihi:05.01.2021)

[14] Açık veri nedir?,Haber odası, 2018
https://www.newslabturkey.org/acik-veri-nedir-veriye-nasil-ulasilir/
(Erişme tarihi: 05.01.2021)

yapılabilir ve mevcut bütün verilere ulaşım sağlanabilir. Dünyanın bilgi edinme özgürlüğüne destek veren, gelişmiş bazı ülkelerinde açık veriye erişim resmi olarak yürürlüktedir. Data.gov, Data.gov.uk ve Data.gov.ie gibi örnekler açık veri hükümeti girişimlerinin iyi örneklerindendir. Türkiye'de henüz açık veri için resmileşmiş bir kanal yoktur.

Stratejik Veri (Strategic Data): Tipik olarak stratejik veriler, işletmenin faaliyet gösterdiği sektörü çevreleyen bilgileri içerir ve endüstriyel veri olarak adlandırılır. Endüstriyel veriler, tedarikçi ve alıcı gücünü, tüketicilerin ürünü ikame etme kabiliyetini ve sektördeki rakiplerin sayısını içerebilir. Stratejik veriler, güçlü yönler, zayıf yönler, fırsatlar ve tehditler anlamına gelen SWOT analizi yapılmasında kurumlara yardımcı olur. SWOT analizi, şirketlerin işin stratejik yönünü tayin etmesi ve stratejik hedefler belirlemesine sağlar. Stratejik veriler ayrıca sektörel trendlere ayak uydurmasına yardımcı olur. İşgücü istatistikleri, çalışanlar arasındaki genel eğilimler konusunda üst yönetime bilgi verir ve iş gücünün kurumların stratejik hedeflerine bağlılığını sürdürmede yönetime yön gösterici kurumlara özel verilerdir.

Çevresel Veri (Data Exhaust): Çevresel veriler belirli kayıt aksiyonu gerekmeksizin, pasif bir şekilde toplanan ve toplanma ortamına ait duran veriyi anlatır. Verinin belirlenmiş bir toplanma amacı işlenmeden bir değeri olmayan veridir. Bu veriler farklı amaç için toplanmış başka veri kaynaklarıyla yeniden organize edilebilirler. Çevresel veriler günümüzde yeni teknolojilerin benimsenmesi ve kullanımı ile oldukça yoğun bir veri grubunu oluşturmaktadır. Bu verilere örnek olarak mobil cihazların kullanımının yaygınlaşması ile günlük faaliyetlerin ve ortamsal verilerin üretilmesi verilebilir. Kişiler, günlük hayatlarında ya da çalışma ortamlarında farkında olmadan pasif bir şekilde veri üretmeye devam etmektedir. . İnternet aramaları, telefon görüşmeleri ya da özel çağrı merkezleri bu türden veri üretmektedir. Çevresel veri doğası itibari ile büyük şirketlerin kolayca toplayıp büyük veriye dönüştürerek organize edilmiş stratejik veri modeli yardımı ile davranışsal bir algoritmaya ulaşabileceği bir veri tipidir.

Topluluk Verisi (Community Data): Toplumsal hayat ve iş hayatı içindeki sosyal eğilimleri anlayabilmek için dinamik ağların içerisindeki yapılandırılmamış veri kümeleri topluluk verileri oluşturur. Topluluk verisi, müşterilerin ürün değerlendirmeleri, hizmet memnuiyet bilgilendirmeleri, oylama butonlarını, sosyal medya veya elektronik ticaret bildirimlerini vb. geri bildirim metotları ile edinilen bilgidir. Bu veriler çokça gündemde olan örneklerde olduğu gibi gerek işleme, organize etme ve hatta manipülasyon yöntemleri ile sosyal yapıdaki kalıplardan süzülmüş sonuçlar çıkarmak amacı ile kullanılabilir.

Kişisel Veri (Personel Data): KVK Kanunu 3. maddesinde 'Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,[15] kişisel veri olarak tanımlamıştır. Bu bağlamda sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, motorlu taşıt plakası, sosyal güvenlik numarası, parmak izleri, genetik bilgiler vb. veriler dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel verilerdir.

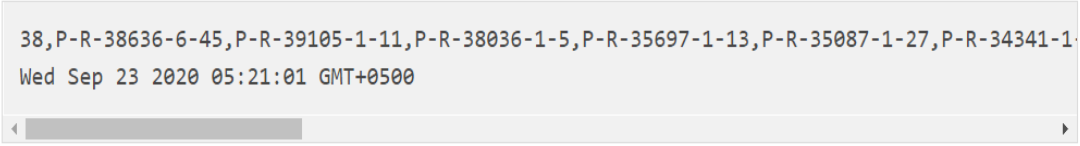
Yapılandırılmış Veri (Structured Data): Yapılandırılmış veriler düzenli olmayan verilerin özellikle arama motorlarının anlayabileceği şekilde organize edilmiş, anlamlı hale getirilmiş verilerdir. Yapılandırılmış veriler, biçimlendirilmiş ve iyi tanımlanmış bir veri modeline dönüştürülmüş bilgilerdir. Bu yapılandırılmış kodlar ya da veriler, arama motoru örümcekleri (botları) tarafından okunur ve ilgili içerik anlamlandırılır.

[15] Kişisel Verileri Koruma Kanunu
https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5
(Erişim tarihi:05.01.2021)

Yapılandırılmış verilerin ilişkisel modeli, veri artıklığını en aza indirdiği için belleği kullanmaktadır. Ancak bu aynı zamanda yapılandırılmış verilerin daha birbirine bağımlı ve daha az esnek olduğu anlamına gelir. Yapılandırılmış veriler hem insanlar hem de makineler tarafından üretilir. Barkodlar, POS (the point of sale) verileri gibi makineler tarafından oluşturulan çok sayıda yapılandırılmış veri örneği vardır. Yapılandırılmış verilerin organizasyonu nedeniyle, analiz etmek hem yarı yapılandırılmış hem de yapılandırılmamış verilere göre daha kolaydır. En temelde yapılandırılmış veriler Arama Motoru Optimizasyonu (Search Engine Optimization-SEO) süreçleri içerisinde kolaylıkla anlamlandırmasını sağlamaktır.

Yapılandırılmamış Veri (Unstructured Data): Yapılandırılmamış veriler, belirli bir formatta olmayan data kümesidir. Yapılandırılmamış verilere örnek olarak, elektronik kayıtlar (log) verilebilir. Elektronik çözüm sağlayan uygulamaların birçoğu uygulama üzerinde aktivite kaydı tutmaktadır. Ancak eğer bir kayıt yönetimi (log management) ürünü ile bu uygulama kayıtları anlamlı raporlara dönüştürülmezse elde edeceğimiz veriler aşağıdaki örnekte olduğu gibi görünür ve yapılandırılmadan anlamlı bir bilgi sağlayamaz.

Şekil 1.3 Yapılandırılmamış Bir Veri Örneği



Büyük Veri (Big Data): Büyük veri, verinin endüstriyel devrimi olarak kabul edilen kendi başına yeni iş kolları ve araştırma alanları yaratan, büyük teknoloji sağlayıcı markaların zenginleşmesinin en büyük destekçisi olarak günümüzün en gündemde konularındandır. Büyük verinin tanımı birçok farklı kaynakta başka ifadeler bulmuştur. En basit tanımıyla, büyük veri insan eliyle ve makineler tarafından sayısal olarak kodlanmış her türden kurumsal veri ile internet ve sosyal medya paylaşımları, yazılı mecralar, elektronik kaydı olan alışverişler vb. şekillerde oluşan kişisel verilerin anlamlı ve işlenebilir biçime dönüştürülmesi halidir. Yapılandırılmamış ve değersiz

olarak görülen veriler açık API (Application Programming Interface)'ler aracılığıyla, sayısal platformların kullanıcılarından elde ettikleri tüm bilgilere ulaşılabilmektedir. Uygulama Programlama Ara yüzü anlamına gelen API, herhangi bir uygulamanın belli işlevlerini diğer uygulamaların da kullanabilmesi için oluşturulmuş bir modüldür. Bu modül sayesinde verileri büyük hacimde analiz ederek algoritmik sonuçlara varan kurumlar verinin son halini pazarlama, satış, kitlelere ulaşma gibi amaçlarla kullanırlar.

Büyük hacimli verinin işlenip analiz edilmesi sadece teknolojik hayata değil, bizzat siyasi ve günlük yaşamın gidişatına da yön vermektedir. Buna verilecek dünyadaki en dikkat çekici örnek eski Amerika Birleşik Devletleri (ABD) başkanı Barack Obama'nın 2012 yılındaki seçimlerde büyük veri analizi sayesinde birçok seçmene ulaştığı, bu yaklaşımla farklı kaynaklardan birçok verinin derlenmesi ile elde edilen sonuçlar doğrultusunda seçmenlerle iletişim kurulduğunun belirlenmesi, olacaktır.[16] Yaşanan başarılı sonuçlardan hareketle benzer yöntem, 2016 yılındaki gerçekleşen seçimlerde de kullanılmış, bu sayede özellikle kişisel verilerin büyük çapta işlenmesi ve kişilere özel psikogramların oluşturulması alanında uzmanlaşmış olan Cambridge Analytica kuruluşu seçmenler üzerinde oluşturduğu detaylı ve ilginç çalışması ile adını duyurmuştur.[17]

1.1.3. Veri Güvenliği Nedir?

İnternet kullanımın yaygınlaşması, dijitalleşmenin bir kurumsal amaç haline dönüşmesi, ülkemizde çokça tartışılan ancak dünyanın yoğun şekilde bulut bilişim kullanmaya başlaması ve her geçen gün artan büyük hacimli verilerin bulut ortamına taşınması, teknolojiye ulaşımın ucuz ve kolay olması, uzaktan çalışma vb. sayılabilecek birçok unsur günümüzde hem kişisel hem de kurumsal veri güvenliğini kaçınılmaz kılmıştır.

[16] How Obama's data crunchers helped him win, 2016.
http://edition.cnn.com/2012/11/07/tech/web/obama-campaign-tech-team/
(Erişim tarihi: 05.01.2021)
[17] The Power of Big Data and Psychographics, 2016.
https://www.youtube.com/watch?v=n8Dd5aVXLCc
(Erişim tarihi: 05.01.2021)

Hızla gelişen, değişen, etki eden teknolojinin kişisel ve kurumsal alanda hayatı kolaylaştırması daha da önemlisi muadili olmayan zamandan tasarrufu sağlaması gibi sağladığı birçok olanak ile talebi her geçen gün daha da çoğalmakta, kişisel ve kurumsal bütçe payı da buna paralel şekilde artmaktadır. Günümüzde bilgi ve veri alışverişinin kolaylaşması, internetin sağladığı hizmet sayesinde yer ve zaman kavramı olmaksızın yararlanılabilmesi kişisel ve kurumsal teknoloji bağımlılığını gün geçtikçe arttırmaktadır. Teknoloji araçları ve ortamları, internet servisi ve elektronik paylaşım bağımlılığı arttıkça veri ve anlamlı veri kümesi anlamında bilgi güvenliği riskleri de beraberinde getirmektedir.

Bilgi güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür. Bunun sağlanması için, uygun güvenlik politikasının belirlenmeli ve uygulanmalıdır. Bu politikalar, faaliyetlerin sorgulanması, erişimlerin izlenmesi, değişikliklerin kayıtlarının tutulup değerlendirilmesi, silme işlemlerinin sınırlandırılması gibi bazı kullanım şekillerine indirgenebilmektedir.[18]

Kişisel veriler günlük hayatın içerisinde farklı amaçlarla işlenmekte, paylaşılmakta ve saklanmaktadır. Bireyler, kişisel veri yönetimlerinde kurumsal veri güvenliği yaklaşımında olamayacaklarından dijital ekosistemin veri güvenliği açısından en savunmasız aktörleri olarak karşımıza çıkmaktadır. Bu sebeple KVK Kanunu ile günümüzde birçok kullanıcı kişisel verilerinin güvenliğine önem vermek hususunda farkındalık kazanmıştır. Ancak kişisel veriler dijital ortamlarda tek bir giriş noktasında hayata geçse dahi, farklı amaç ve teknolojik katmanlı ara yüzler ile tek bir veri çıkışı olamamaktadır. Bu durumda veri güvenliği sağlama önlemleri de yetersiz kalabilmektedir.

Kurumsal ve kişisel bilgi güvenliği riskleri arasında çeşitli benzerlikler mevcuttur. Ancak kurumsal veri güvenliğinin gereksinimlerini karşılamaması durumunda kurumların iş fonksiyonlarını doğrudan etkileyerek para, zaman ve itibar kaybına,

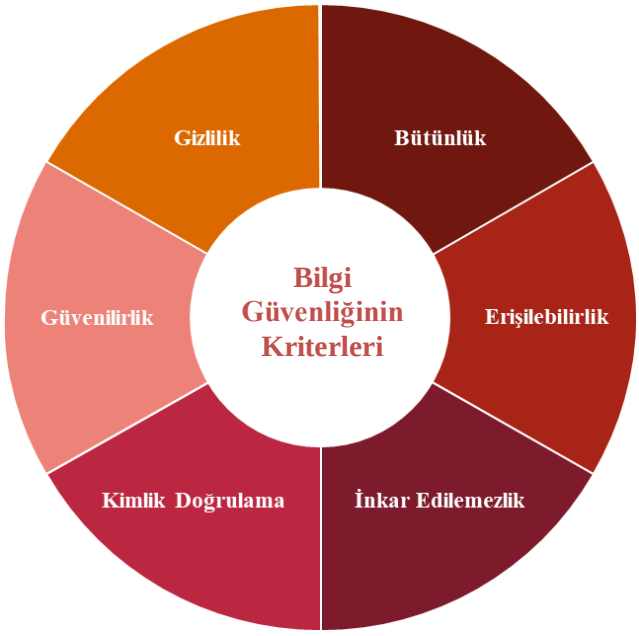
[18] Canberk, Gürol, Şeref, Sağıroğlu, Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme Politeknik Dergisi, C.9, S.3, 2006 s. 165-174.

daha ileri durumlarda ise yasal sorunlara ve hatta işletmenin çeşitli sebeplerle piyasada varlığını sürdürememesine sebep olabilir.

Kurumların bilgi güvenliği yönetimi konusunda gerçekleştirecekleri denetim ve iyileştirme faaliyetleri ölçeklerine, sektörlerine, çalışma yöntemlerine, iş modellerine vb. faktörlere göre değişiklik göstermektedir. Genel anlamda, ortam faktörleri ne olursa olsun her bilgi güvenliğinin sağlanabilmesi için küresel veri güvenliği politikalarıyla uyumlu bir yol haritası geliştirmeleri ve tüm çalışanlarını, fiziksel ve elektronik ortamlarını, cihazlarını, verilerini ve gizliliklerini kurum bilgi güvenliği yönetim standartları ve politikaları doğrultusunda güvenliğin sağlanması konusunda eğitmeleri şarttır.

Bilgi güvenliği, elektronik ortam, ürün, cihazlarda işlenmekte olan verilerin gizliliğini, bütünlüğünü ve sürekliliğini korumayı amaçlayan bir disiplindir.

Şekil 1.4 Bilgi Güvenliğinin Kriterleri



Gizlilik (Confidentiality): Gizlik prensibi bilginin yetkisiz kişilerin eline geçmesini engellemeyi amaçlamaktadır. Bilgi çalışan bilgisayarları, sunucular, her türlü veri

saklama ortamlarında, ağ üzerinde gönderici ve alıcı arasında paylaşılırken yetkisiz erişimlerden korunmalıdır. Gizlilik prensibi kurum içi farkındalık eksikliği veya iç atak yöntemleri ya da dış atak yöntemleri ile bir saldırgan aracılığı ile bozulabilir. Kurumların elektronik altyapılarında tespit edilen zafiyetler, yazılımsal hatalar, sosyal mühendislik gibi sebeplerle yetkisiz ve kötü niyetli taraflar verilere izinsiz olarak erişebilir.

Veri Bütünlüğü (Data Integrity): Bütünlük prensibi veriyi olması gerektiği şekilde tutmayı ve korumayı amaçlamaktadır. Kurumlarda kullanımda olan doğru ve mevcut bilginin bozulmasını, değiştirilmesini, yeni veriler eklenmesini, bilginin bir kısmının veya tamamının silinmesini engellemeyi hedefler. Verinin bütünlüğü verinin kullanılması sürecinde doğruluğunun muhafaza edilmesi prensibidir.

Erişilebilirlik (Availability): Erişilebilirlik prensibi bilginin her an ulaşılabilir ve kullanılabilir olmasını amaçlamaktadır. Elektronik ortamdaki doküman, altyapı, uygulamalar ve veritabanı erişimlerinin sürekli bir şekilde tam ve eksiksiz olarak erişilebilmesi aynı zamanda iş sürekliliğini de sağlayacaktır. İş sürekliği yaklaşımı, bilişim sistemlerini, kurumsal risklerin tespit edilmesi ve her türlü tehditin önlenmesini hedefler. İş sürekliliği hizmeti sayesinde, kullanıcılar, erişim yetkileri dahilinde olan verilere zamanında ve güvenilir bir şekilde ulaşabilmektedirler.

Kimlik Doğrulama (Accountability): Kimlik doğrulama prensibi elektronik ortam ve sistemler üzerinde gelişen her türlü olayın ihtiyaç halinde, daha sonra incelenmesine olanak sağlayan kayıt mekanizmasını hedefler. Kullanıcıların sistemlere giriş yapmaları, uygulamaların aktive edilmesi, e-posta alışverişi, onay işlemleri vb. bilgisayar sistemi veya ağ üzerinde meydana gelen bütün aktivite kayıtları bu kapsamda değerlendirilebilir. Özellikle adli bilişim vakalarında kanıt toplanması sürecinde önemli bir unsuru teşkil etmektedir. Sistemlerden toplanan aktivite kayıtları denetlenerek bilinen saldırı türlerine ait kayıtların varlığı yahut büyük ihtimalle yeni bir saldırıyı işaret eden sıra dışı kayıtların olup olmadığı incelenir.

Kimlik Doğrulama (Authentication): Kimlik doğrulama verilerin alıcı, verici, onaycı, kullanıcı olarak gerçek kimlikte olup olmadıklarını kontrol etmeyi amaçlar. Kimlik doğrulama günlük hayatımızda en sık karşılaştığımız kontrollerden parola güvenliği örneği ile karşımıza çıkmaktadır. Parola güvenliği, anahtar yönetimi, şifre ve kriptografik kontroller kimlik doğrulama sürecinin basitten daha karmaşık yapıya farklı halleridir. Bilgisayar ağları ve elektronik sistemlerin dışında fiziksel sistemler için de kimlik doğrulama oldukça sıkça kullanılan bir bilgi güvenliği denetleme yöntemidir. Akıllı kartlar, parmak izi okuyucular, retina tarayıcılar vb. biyometrik teknolojilere dayalı kimlik doğrulama sistemleri sıklıkla kullanılmaktadır.

Güvenilirlik (Reliability): Güvenilirlik prensibi sistemin öngörülen çıktısı ile elde edilen çıktısı arasındaki tutarlılık durumudur. Sistemin kendisinden beklenen şeyi eksiksiz veya bir ek olmadan her çalıştırıldığında tutarlı bir şekilde gerçekleştirmesini amaçlamaktadır.

İnkar Edilemezlik (Non-repudiation): İnkar edilemezlik prensibi verinin iletildiği gönderici ve alıcı arasında ortaya çıkabilecek iletişim sorunları ve anlaşmazlıkları en aza indirmeyi amaçlar. Sistemler arasında bir bilgi aktarımı yapılmışsa gönderen ve alıcı aktivitelerini reddedememelidir Özellikle gerçek zamanlı işlem gerektiren finansal sistemlerde kullanılmakta olup, elektronik imzalar bu prensibin örneklerindendir.

Veriler, veri güvenliği prensiplerine göre kurumsal olarak sınıflandırılır ve gerekli hallerde etiketlenir. Global olarak kabul görmüş güvenlik standart ve çerçevelerinden ISO 27001 ve COBIT sınıflandırma ve etiketleme kontrollerini detaylıca içermektedir. Veri sınıflandırma yöntemi, veri güvenliği prensipleri kullanılarak puanlandırılarak gerçekleştirdiler. Yapılan değerlendirme sonucunda veri sınıfları; halka açık, kuruma özel, gizli veya çok gizli olarak tayin edilir ve gerekli güvenlik önlemleri bu etiketlere göre sağlanır.

Halka Açık Veri: İçerdiği konu itibariyle, gizlilik değeri taşımayan ancak kurumun genel fonksiyonlarıyla ilişkili verileri içeren bilgi sistemleri dokümanlarına verilen veri sınıfıdır. Kurum dışında da kullanılabilir.

Kuruma Özel: İçerdiği konu itibariyle, kurumun iş modeli ve genel fonksiyonlarıyla ilişkili veri içeren bilgi sistemleri dokümanlarına verilen veri sınıfıdır. Kurum çalışanları tarafından kullanılması uygundur.

Gizli: Kurum bünyesinde kullanılan ancak kurum içerisinde tüm personel tarafından erişim hakkı olmayan verilerdir. Bu sınıftaki verilerin korunması, fiziki mekân güvenliği, erişime yetkili kişilerin belirlenmesi, iş sürekliliğinin sağlanması birinci derecede önemlidir. Bu kapsamda bu verilerin üretildiği elektronik ortam ve sistemler özel kullanıma haiz olması, sınırlı ve belirli sayıdaki yetkililerce erişilebilir olması ve korunması esastır.

Çok Gizli: İzinsiz açıklanması durumunda, organizasyona, operasyonlara, varlıklara, finansal tablolara ve çalışanlara çok önemli ya da olağanüstü etkisi olacak verilerdir. Bu sınıftaki verilerin korunması, fiziki mekân güvenliği, erişime yetkili kişilerin belirlenmesi, iş sürekliliğinin sağlanması birinci derecede önemlidir. Bu kapsamda bu verilerin üretildiği elektronik ortam ve sistemler özel kullanıma haiz olması, sınırlı ve belirli sayıdaki yetkililerce erişilebilir olması ve korunması esastır. Bu verilerin çalınması durumunda kurum finansal, hukuki, itibari zarar görecektir.

1.1.4. Veri Güvenliği Tehditleri

Siber güvenliğin en önemli unsurlarından biri olan veri güvenliği, elektronik, dijital ve iletişim sistemlerindeki verilerin yetkisiz ifşa ve değişikliklerden korunma yöntemleridir. Kavramsal olarak siber güvenlik ve koruduğu, tanımladığı varlıkların temelinde veri güvenliği bulunmaktadır.

Tehdit, "bir sistemin veya kurumun zarar görmesine neden olan istenmeyen bir olayın arkasındaki gizli neden" olarak tanımlanabilir.[19] Kurumlardaki güvenlik boşlukları tehditlere sebebiyet vereceği gibi değişen teknolojik, çevresel şartlardan doğan riskler de söz konusu olabilmektedir.

Tehditler, insan kaynaklı tehditler, fiziksel tehditler, yazılım kaynaklı tehditler, güvenlik boşlukları, eğitim ve bilinç eksikliğinden kaynaklanan tehditler olarak sınıflandırılabilir.

İnsan Kaynaklı Tehditler: İnsan kaynaklı tehditleri, bilinçli veya bilinçsiz olarak yapılan girişimlere göre iki ayrı grupta değerlendirebiliriz. Kurumlarda yeterli yönetişim bilinci, güvenlik farkındalığının olmaması ve denetleme eksiklikleri bu tehditleri oluşturan unsurlardır.

Kötü niyet olmayan çalışanlar tarafından oluşan tehditler iş hayatında sıkça karşılaştığımız durumlardandır. Kullanıcıların sistemleri bilinçsiz ve yetersiz bilgi ile kullanmaya çalışması, verilerin güvenlik prensiplerine uymaması, gerekli veri güvenliği farkındalık eğitimlerini almamış olmaları neticesinde yaşanan tehditlerin ortaya çıkmasını sağlamaktadır. Kurumlar veri güvenliği önlemlerini genellikle kurum dışından gelebilecek saldırı veya belirlenmiş zafiyetler için almaktadırlar. Ancak bugün gerçekleşen veri sızıntılarının %70 üzerindeki sebebi kötü niyetli olmayan çalışanların bilinçsiz tutumlarından kaynaklanmaktadır. Gereken güvenlik farkındalığını edinmemiş çalışanlar sistemlerde ve elektronik ortamlarda gerçekleşen anomali durumlarını da tespit edemezler ve gerekli bildirimi sağlayamazlar.
Kötü niyetli çalışanlar tarafından sisteme zarar verme amacıyla gerçekleşecek içeriden saldırı tipleridir. Bu tür tehditlerde saldırganlar tehdit kaynağı ve sistemde bulunan güvenlik boşluklarından yararlanırlar.[20]

[19] Bilişim Güvenliği Kitapçığı. ProG Bilişim Güvenliği ve Araştırma, s.7, 2008, http://www.pro-g.com.tr/whitepapers/bilisimguvenligi-v1.pdf
(Erişim tarihi:05.01.2021)
[20] Shephard, B., Information security-who cares?. Power System Management and Control, Fifth International Conference, Conf. Publ. No. 48, 2002, 126s.

Yazılım Tehditleri: İşletim sistemi, programlar, uygulamalar vb. sistemler aracılığı ile kullanıcı bilgisayarlarında veri kaybına sebep olabilecek tehditlerdir. Yazılımlar kötü amaçlı olarak tahrip edilebilir, değiştirilebilir, silinebilir veya kaza ile değişikliğe maruz kalabilir. Yazılımlar üzerinde gerçekleşen değişiklikler ancak kod analizi kontrolleri ile mümkündür. Kurumlar ISO 27001, COBIT, NIST vb. güvenlik yönetişim modellerini benimseyip gerekli denetim unsurlarını sağlarlarsa, ancak yazılım tehdit risklerini tespit edebilirler. Yazılımların kötücül kodlar ile sistemlerden veri sızdırmaları tehdidinin fark edilmesinin zor olmasının sebebi, yazılımın daha önceden yaptığı işi aynı şekilde yaparken bunun yanından saldırganın beklentisi olan ekstra işlemleri de yapacak şekilde değiştirilebilmesidir. Truva atı (trojan horse) programı, görünürde bir işi yaparken fark edilmeyen saldırgan aktivitesini arka planda sürdürmesini sağlayan programlardır. Virüsler kötü amaçlı yazılmış programlardır. Kurumlar virüslere karşı denetimler ve otomatik koruma programları kullanmaktadırlar. Arka kapı (BackDoor), oldukça tehlikeli bir saldırı tipi olup kullanıcısından habersiz gizli giriş noktaları bulunan programlardır. Bilgiye istenmeyen kişi veya programların erişmesini sağlarlar.

Güvenlik Zafiyetleri: Bilgisayar sistemlerinin güvenliğini tehlikeye sokan yazılım, donanım veya tasarım hatalarından kaynaklanan açıklıklardır. Bilgisayar sistemlerindeki güvenlik zafiyetleri virüs, trojan gibi zararlı yazılımlarla istismar edilerek veri açıklıkları meydana gelmektedir. Hizmet Engelleme (Denial of Service-DoS), Dağıtık Hizmet Engelleme (Distrubuted Denial of Service Attack- DDoS) internete bağlı bir hostun hizmetlerini geçici veya süresiz olarak aksatarak, bir makinenin veya ağ kaynaklarının asıl kullanıcılar tarafından ulaşılamamasını hedefleyen çok bilinen bir siber saldırı yöntemidir. Kaspersky 2020 raporuna göre Türkiye'de 2020 yılında en çok DDoS saldırısı belediyelere, eğitim kurumlarına ve sağlık kurumlarına düzenlenmiştir.

Veri Açıklıkları: Bilgisayar sistemlerinde verilerin istenmeyen şekilde kurum dışına sızmasına sebep olan olaylardır. Bu olaylar güvenlik zafiyetlerinin bilgisayar korsanları tarafından kullanılması, hedef odaklı siber saldırılar veya siber suç

kategorisine giren daha çok finansal çıkar amacı güden "hack" olaylarını kapsamaktadır.

Siber Casusluk ve Sürekli Tehditler (APT): Siber casusluk daha çok devletler veya büyük organizasyonlar tarafından büyük kaynaklarla uzun vadede yürütülen veri hırsızlığına verilen isimdir. "Advanced Persistent Threat (APT)" adıyla anılan tehditler de bu kategori altında değerlendirilir.

Mobil Tehditler: Cep telefonları, tabletler vb. mobil platformları etkileyen zararlı yazılımlar son yıllarda daha gündemdedir. Mobil zararlı yazılımlar daha çok kullanıcı verilerini tehdit etmektedir. Özellikle Android tabanlı platformların yaygınlaşması ve bu platformun resmi uygulama mağazalarının dışından uygulama yüklenmesine izin vermesi mobil tehditlerin artmasını hızlandırmıştır.

E-Posta Tehditleri ve Spam e-postalar: Kişisel ve iş e-posta adreslerinin amacı dışında paylaşılması ve kontrolsüz şekilde erişim sağlanan internet sitesi sayfaları üzerinden e-postalar alınması tehditidir. 2014 yılına baktığımızda en yüksek oranlara ulaşan saldırılara bakıldığında gönderilen her 243 e-postadan biri virüs içermekte, gönderilen her 10 e-postadan 1 tanesi zararlı sitelere bağlantı veren içerik barındırmakta olduğu görülmüştür. Siber casusluk girişimleri oltalama (phishing) e-postalar ile başlamıştır. Bu saldırı tipinde amaç kullanıcı parolalarını çalmaktır. E-postalardaki oltalama (phishing) oranının düşüşün sebebinin bu saldırıların daha çok sosyal medya araçlarına yönelmesiyle açıklanabilir.

Sosyal Medya Tehditleri: Sosyal medya platformları son yıllarda altın çağlarını yaşamakta ve şirket sahiplerini zengin etmektedir. Facebook, Twitter, Instagram vb. sosyal medya platformlarının kullanımının artmasıyla bu platformlara yönelik siber tehditlerde de artış gözlenmektedir. Bu platformlara yapılan en sık saldırı yöntemi sosyal mühendislik saldırılarıdır. Diğer yöntem ise oltalama (phishing) saldırılarıdır. Bu konu özellikle KVK Kanunu ve yurtdışında GDPR ile ilişkili olarak sıkça gündeme gelmektedir.

Bulut Teknolojileri Tehditleri: Son yılların ve geleceğin yükselen değeri bulut bilişim teknolojilerinde ortaya çıkan siber güvenlik tehditlerinde büyük oranda artış gözlemlenmiştir. Her türden veriyi barındıran bulut sistemleri yeni güvenlik regülasyonlarının ortaya çıkacağı sinyallerini vermektedir. Yaşanan bulut bilişim siber tehditlerine iyi örneklerden biri Apple'a ait iCloud platformundan ünlülere ait resimlerin çalınarak, internete sızdırılmasıdır. Apple firması bu saldırıda sorumluluk kabul etmemiş, veri kaybının kullanıcıların yanlış kullanımından kaynaklandığını ifade ederek kullanıcıları suçlamıştır.

1.2 VERİ GÜVENLİĞİNİN DEĞERLENDİRİLMESİ

1.2.1. Veri Güvenliği Politikaları

Güvenlik politikaları kurum veya kuruluşlarda kabul edilebilir güvenlik seviyesinin tanımlanmasına yardım eden, tüm çalışanların ve ortak çalışma içerisinde bulunan diğer kurum ve kuruluşların uyması gereken kurallar bütünüdür.[21]

Veri güvenliği bilgi güvenliğinin bir parçası olarak ifade edilir ve bilgi güvenliği politikaları, bir kurumun gizli, stratejik, kuruma özel bilgilerinin yönetimini, korunmasını, güvenli yollarla paylaşımını ve uyumunu düzenleyen kurallar ve uygulamalar bütünüdür.

Veri güvenliğinin sağlanması amacı ile oluşturulan kurumsal bilgi güvenliği politikaları, kurum ve kuruluşlarda bilgi güvenliğini yönetiminin sağlanması ve bilgi güvenliği çerçevesinin belirlenmesi için tüm bilgi güvenlik faaliyetlerini kapsayan ve yönlendiren kurallar bütünü olup kurumsal bilgi kaynaklarına ve ortamlarına erişim yetkisi olan tüm çalışanların, iş ortaklarının ve dış hizmet alım gerçekleştirilen kurum çalışanlarının uyması gereken talimatları içeren kurumsal dokümanlardır. Bilgi güvenliği politikaları kurum sistemleri üzerinden ilgili tüm tarafların en güncel formatına erişebilmesi gereken dokümanlardır. Bilgi güvenliği politikaları kurumların uyum gösterdiği standart, çerçeve, regülasyonlar vb. unsurlara göre farklılık

[21] Kalman, S., Web Security Field Guide. Indianapolis, 2003.

gösterebilir, ancak genellikle çalışanların sorumluluklarını, güvenlik denetim yöntemlerini, amaç ve hedeflerini, kurumsal bilgi varlıklarının yönetimini, korunmasını, dağıtımını ve önemli işlevlerin korunmasını düzenleyen kurallar ve uygulamaların açıklandığı genel ifadeleri içermektedir. Veri güvenliğine ilişkin kurumun gerçekleştirmesi gereken birçok kontrol hususu söz konusudur. Veri güvenliğinin kapsamında bulunan bu alt kontroller için ayrı alt prosedürler, talimatlar hazırlanmalıdır.

Günümüzde kurumların özellikle dikkat etmeleri gereken konu çalışanların veri güvenliğine ilişkin alt kontrol, prosedürler ve talimatlar hakkında yeterli bilgi edinebilmesi için koşulların sağlanması olmalıdır. Bir bilgi güvenliği yönetimi tüm çalışanları kapsayacağından en temel bilgi güvenliği yönetim sistem zorunluluğu tüm çalışanların sisteme dahil edilmesidir. Bununla birlikte kurumların dijitalleşme süreçleri ile artık yalnızca bilgi teknolojileri (BT) çalışanları değil, tüm çalışanları verilerin hayat döngüsü içerisinde rol almakta ve bilişim ortamlarına yetkilendirilmektedirler. Bu sebeple, çalışanlara kullanıcı hesaplarının oluşturulması ve yönetilmesi, şifre değiştirme, sınıflandırılmış verinin kullanımı ve ihlal bildirimi vb. durumlarda izlenmesi gereken adımlar ve kurallar alt prosedürler, talimatlar aracılığıyla açıklanmalıdır.

Bilgi Güvenliği Politikası, kurumun bilgi güvenliği ihtiyaçlarını ve bilgi güvenliği kavramını kurumun bilgi kaynaklarını kullanan her kişiye anlatma amacıyla hazırlanır. Kurumdaki bilgi güvenliği ihtiyacı, kurumun yaptığı işin gereği olarak ortaya çıkmış veya ilgili kanunlar ve düzenlemelerle belirlenmiş olabilir. Bu iş gerekleri ve varsa yasal zorunluluklar bu dokümanda net bir biçimde ortaya konmalıdır.[22]
Veri güvenliği ilkeleri;

- Verilerin ve bilgi varlıklarının güvenli bir ortamında kullanılmasını sağlamak,
- Verileri, sistemleri, yazılımları, iletişim ağlarını yetkisiz erişim ve suistimallere karşı koruma altına almak,

[22] Öztürk, Günce, Tübitak, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE), Bilgi Güvenliği Politikasi Oluşturma Kilavuzu, Doküman Kodu: BGYS-0005, S.1, 2008.

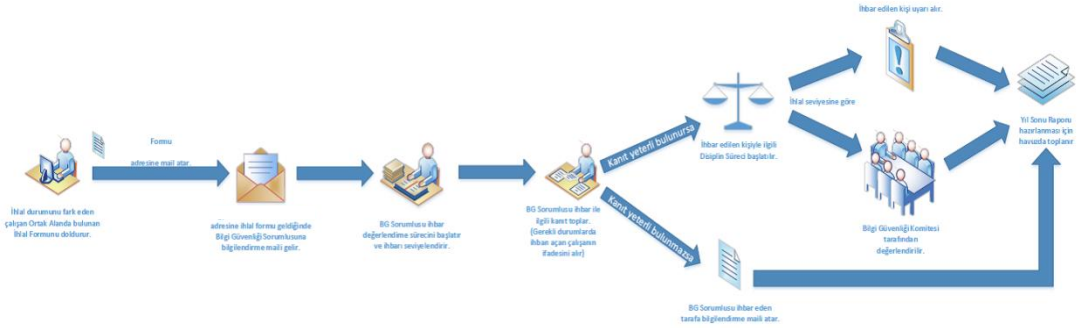
- Tüm kullanıcıların bilgi güvenliği politikası ve ilgili destekleyici prosedürlere, talimatlara bütünüyle uymalarını ve farkında olmalarını sağlamak,
- Tüm kullanıcıların kendi sorumluluklarını, yönetimlerinde olan ve/veya erişebildikleri verinin bütünlüğü ve gizliliğinin önemini anlamalarını sağlamak,
- Kurum bilgi güvenliğini tehdit edebilecek olayların oluşmasını engellemek, yönetim ve çalışanların bu amaçla yeterli seviyede bilgilendirilmesini sağlamak,
- Olası veri ihlallerinin bildirilebilmesi için uygun iletişim kanalları oluşturmak, bu iletişim kanallarını tüm çalışanlara duyurmak,
- Düzenli denetim ve sürekli veri güvenliği iyileştirme çalışmalarına destek olmak.

Kurumsal bilgi güvenliği politikaları kuruluşların ihtiyaçları doğrultusunda temel güvenlik unsurlarının (gizlilik, bütünlük, erişilebilirlik, vb.) bazıları üzerinde yoğunlaşabilir. Sektörel yaklaşımlar kurumların bilgi güvenliği hedeflerini etkilemektedir. Ancak kişisel verinin işlenmediği veya saklanmadığı bir kurum günümüzde olmadığından her kurum gizlilik prensibini, güvenlik bütünlüğünü sağlayabilmek için önemsemek zorundadır.

1.2.2. Veri Güvenliği İhlalleri

Kurumlarda gerçekleşebilecek veri güvenliği ihlal olaylarının tespiti ve gerekli düzeltici aksiyonun alınması süreci kurumdan kuruma değişkenlik gösterebilmektedir. Ancak veri güvenlik ihlal durumlarının tespiti her zaman çok kolay olmamaktadır.
Kurumlarda yaşanan hatalı veri kullanımı veya saldırıların aktivitelerinin tespitinde kullanıcıların, yöneticilerin ve teknik personelin sorumluluk ve görevleri, tespit edilen sorun ve saldırıların hangi sistemler üzerinde gerçekleştiği, zararın ne olduğunun tespiti yöntemi, ihlal durumuna müdahale edecek ekip ve aksiyon adımları önceden belirlenmelidir. İhlal durumlarında da çalışanlara izlemesi gereken yolu anlatacak ve yardımcı olacak kılavuzlara yer verilmelidir.

Şekil 1.5 Örnek bir Veri Güvenliği İhlal Bildirim Süreci



Veri güvenliği ihlallerinin belirlenmesi ve sınıflandırılması;

- Veri güvenliği ihlal yönetiminin bir parçası olarak belirlenmiş olayların raporlanması ve bu olayların sınıflandırılması için süreçlerin uygulanması,
- İhlal olaylarının sınıflandırılmasında kategori, etki, aciliyet ve öncelik gibi faktörlerin belirlenmesi,
- İhlal olaylarının ilişkili grup veya alana (örn. donanım, yazılım, destek yazılımı) göre sınıflandırılması,
- İhlal bildirim sürecinde ilişkili taraflarının organizasyonel sorumlulukların belirlenmiş olması ve gereken desteğin verilmesi, adımları için yöntem belirler.

Veri güvenliği ihlallerinin takibi ve çözümü;

- İhlal olayları yönetim sisteminde aşağıdakiler için tüm raporlanan olayların kök sebeplerinin izlenmesi, analiz edilmesi ve belirlenmesine imkân verecek şekilde uygun denetim izi oluşturması;
    - Tüm ilgili konfigürasyon maddeleri,
    - Bildirilen olaylar,
    - Problem eğilimlerini, sistemsel anomalilerin izlenmesi,

- Kök sebebe yönelik kalıcı çözümlerin belirlenmesi ve başlatılması,

- Çözüm süreci boyunca, olay yönetiminin problem ve hataları çözümlemek için değişiklik yönetiminden gelişim hakkında düzenli raporlar alması,
- Olay yönetiminin, kullanıcı hizmetlerindeki problemlerin ve bilinen hataların devam eden etkilerini izlemesi ve bu etkilerin önemli hale gelmesi durumunda, üst yönetime gerekli bildirimin sağlanması
- Hizmet seviyesi anlaşmaları (Service level agreement-SLA)'ler ile ilgili problemlerin çözümünün gelişiminin izlenmesi, adımları için yöntem belirler.

Veri ihlallerinin tespitinde SIEM (Security information and event management) adı verilen, güvenlik bilgi ve olay yönetimi araçları teknolojik çözüm olarak kullanılmaktadır. SIEM, belirlenen politika ve kuralların yardımıyla bağımsız gibi görünen olaylar arasında anlamlı bağlantılar kurarak muhtemel saldırıları tespit etmeye yardımcı olan korelasyon tekniğidir. SIEM ürünleri çevre birimlerden uç kullanıcılara kadar sistemlerin ürettiği logları merkezi olarak toplayan, saklayan ve analiz eden sistemlerdir. SIEM çözümleri, bir ağda gerçek zamanlı olarak bütünsel bir görünüm sağlar ve BT ekiplerinin güvenlik tehditlerine karşı mücadelede daha proaktif olmalarına yardımcı olur.

- SIEM çözümü iyi bir korelasyon ile kurum bilişim ortamında gerçekleşen milyonlarca olay içerisinden filtreleme yapar ve önemli olana odaklanılmasını sağlar.
- Bağımsız gibi görünen olayları birbiriyle bağlantılandırmak ya da olayları datayla ilişkilendirir.
- Aggregation (birleştirme) işlemi yaparak, olayların birden fazla kaydı tutulmuşsa bunları bir kayıta indirerek analiz edilecek verinin hacmini düşürmekte ve işlemleri hızlandırmaya yardımcı olmaktır.
- Bir kuruluşun bilgi güvenliği sistemlerinde gerçek zamanlı görünürlük sağlar.
- SIEM araçları, BT ortamınızdaki olayları anlama ve işleme konusunda verimliliği önemli ölçüde arttırır.
- SIEM araçları ana bilgisayarlar arasında üretilen günlük verilerini ilişkilendirip analiz etmesinden dolayı olayları tespit edebilir.

- Gerçek zamanlı çözümleyicidir.
- Kurumsal güvenlik standart ihlallerinin takibini yapabilir.

1.2.3. Veri Güvenliğinin Denetimi

Türkiye İç Denetçiler Enstitüsü (TİDE) tarafından yapılan tanımıyla iç denetim; bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence faaliyetidir. İç denetim, kurumun risk yönetim, kontrol ve kurumsal yönetim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur.[23]

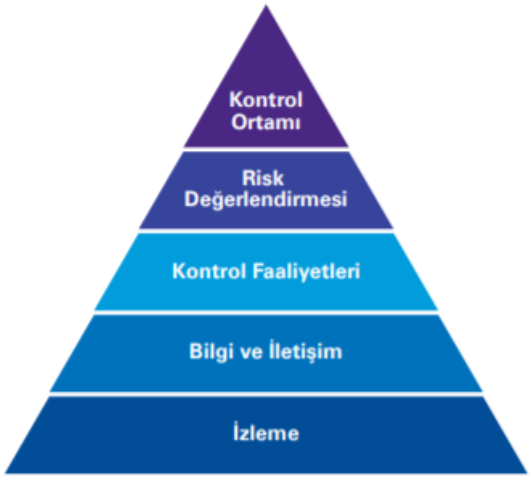
Kurumlarda gerçekleştirilen denetim faaliyetleri risk ve kontrol değerleme faaliyetlerine destek sağlar, kurumlar tarafından gerçekleştirilen operasyon ve bilgi teknoloji faaliyetlerini izler, faaliyetlere ilişkin risk değerlendirmesi yapar ve uygulanan kontrollerin etkinliğini ölçümler. Bu işlev ve kapsam özellikleri ile denetim; sisteminin güvenilirliği, bilgi güvenliği, yasa ve düzenlemelere uygunluk gibi alanlarda kurumsal hayatın önemli bir parçasıdır.

Denetim, kurumlarda kayıt yönetimi ve analiz çalışmalarına katkı sağlar ve olgunluk değerlendirmeleri yapabilmesi için destek olur. Zamanında gerçekleştirilen denetimler risk yönetiminin bir parçası olarak önleyici niteliktedir. Denetim, kurumların hedeflerine ulaşması ve misyonlarını gerçekleştirmesi; bu yolda ilerlerken önlerine çıkabilecek belirsizliklerin en aza indirilmesi amacıyla uygulanan süreçtir. Denetim ve iç kontrol, kurumların sürekli değişen çevre koşulları, hizmet alanların talepleri ve öncelikleri ile gelecekte ortaya çıkabilecek tehdit unsuru olan veya fırsatlar yaratabilecek risklerle başa çıkabilmeleri için yönetimi güçlendirir. Diğer bir ifadeyle denetim, kurumun yönetimi ve personeli tarafından hayata geçirilen, belirlenmiş hedeflere ulaşmasında ve misyonunu gerçekleştirmesinde makul bir güvence sağlamak üzere tasarlanmış ve kurumun genelini etkileyen bütünleşmiş bir süreçtir. İç kontrol standartları, iç kontrol sisteminin uygulama esnasında başvurduğu temel ilkelerdir.

[23] COSO, Enterprise Risk Management – Integrated Framework: Executive Summary, 2004.

Denetim modelini beş katman veya birbiri ile bağlantılı bileşenlerden oluşan bir piramit olarak tanımlamaktadır. Bu bileşenler:[24]

Şekil 1.6 Denetim Modeli Katmanları



Kaynak: The Committee of Sponsoring Organizations of the Treadway Commission's (COSO), "Internal Control-Integrated Framework",https://www.coso.org/Pages/default.aspx.[25]

Bilgi güvenliği yönetimi kurumların üst yönetimlerinin görevleri arasındadır, bu sebeple üst yönetim, güvenlik altyapısını oluşturarak ve gözlemleyerek verilerin güvenliğinin sağlanmasından birinci derece sorumludur. Denetim faaliyetleri bağımsız denetçiler tarafından gerçekleştirilmelidir. Bu sebeple kurumlarda veri güvenliği denetimini gerçekleştirecek ekipler BT ya da teknoloji iş kollarına değil doğrudan yönetime raporla yapmalıdır.

Kurumsal bilgi güvenliğinin uçtan uca sağlanabilmesi için bilginin üretildiği, işlendiği ve saklandığı her elektronik ve fiziksel ortamda denetim faaliyeti gerçekleştirilmelidir. Veri güvenliği denetimi, veriye teması bulunan her iş kolunun dahil olması ve

[24] https://assets.kpmg/content/dam/kpmg/tr/pdf/2018/05/bt-denetim-standartlari-ve-uygulamalari.pdf (Erişim tarihi:04.01.2021)
[25] The Committee of Sponsoring Organizations of the Treadway Commission's (COSO), "Internal Control–Integrated Framework", https://www.coso.org/ Pages/default.aspx.
(Erişim tarihi:04.01.2021)

sorumluluk alması gereken bir süreçtir. Denetimin amacına ulaşabilmesi için gereken örneklem ortamı oluşturulmalı ve denetimler periyodik olarak yapılmalıdır. Denetim kontrolleri temelde birbirinden ayrılmaktadır.

Önleyici Kontroller: Güvenlik duvarları (firewall), internet güvenlik sistemleri, saldırı önleme sistemleri, fiziksel ve mantıksal erişim kontrolü, cihaz konfigürasyonu ve şifreleme istenmeyen durumları önlemede en sık kullanılan yöntemlerdir.

Belirleyici Kontroller: Örneklem gruplarının incelendiği saldırı tespit sistemleri, zafiyet taraması, penetrasyon testleri ve kayıtlar olası sorun ve güvenlik olaylarını belirlemek için tasarlanmış kontrollere örnek olarak gösterilebilir.

Doğrulayıcı/Sorunların Çözümüne Yönelik Kontroller: Acil durum merkezleri, iş sürekliliği yönetimi, yama yönetimi sistemleri ise belirlenen sorunların çözümü için geliştirilen kontrollerin en yaygın kullanılan örneklerindendir.

Genel itibarıyla kritik BT ortamlarına sahip olması beklenen halka açık şirketler, bankalar, finansal hizmetler, telekomünikasyon ve enerji, vb. sektörlerinde yer alan kuruluşlar veya ciro, aktif büyüklük, vb. belirli bir finansal boyut açısından belirli bir eşiğin üzerinde yer alan kuruluşların BT denetimi uygulanması için en elzem kuruluşlar olacağı düşünülmektedir. Bu anlamda, tüm sektör ve kuruluşlara yaygın olası bir BT denetimi mevzuatının; halihazırda bağımsız denetimin zorunlu tutulduğu kuruluşlara benzer bir şekilde ciro, personel adedi vb. kriterlere dayanarak firmalar için aşamalı bir şekilde devreye alınabileceği düşünülmektedir.[26]

Veri güvenliği denetiminde uygulanacak diğer bir yöntem siber güvenlik denetiminin sağlanmasıdır. Siber güvenlik denetimlerinin en bilinen ve faydalı yaklaşımı penetrasyon testleridir. Penetrasyon Testi (Penetration Testing) sistem, ağ yapısı, uygulamalar, veritabanı üzerinde olası güvenlik açıkları belirlemek ve sistem

[26] https://assets.kpmg/content/dam/kpmg/tr/pdf/2018/05/bt-denetim-standartlari-ve-uygulamalari.pdf (Erişim tarihi:04.01.2021)

korumasını değerlendirmek için otomatik ya da manuel gerçekleştirilebilecek saldırıların simüle edilmiş kontrolleridir. Penetrasyon testi sayesinde kuruma bir saldırganın atak etmesi öncesi benzer senaryolar kurum tarafından kendine uygulanır. Penetrasyon testleri kurum tarafından belirlenen uygulamalar, veritabanları vb. bilişim yapılarında kurgulanmış siber atak simülasyonlarıdır.

Bu bağlamda güvenlik açığı, bir sistemin güvenlik mekanizmasındaki potansiyel bir zayıflıktır, risktir.

Veri güvenliği ve siber güvenlik ilişkisi açısından genel risklerin denetimler yolu ile belirlenmesi veri güvenliği iyileştirme adımları için yol gösterici olacaktır.

1.2.4. Veri Güvenliğinin Geleceği

Birçok kurum, müşteri verilerini kendi veri merkezlerinde ya da bulut ortamlarda bulundurmaktadırlar. Sanallaştırma yöntemi kullanarak ya da bulut bilişim hizmeti alınarak saklanan verilerin güvenliğinin sağlanması farklı tehditleri beraberinde getirmektedir.

Büyük verinin ortaya çıkışı ile alışılagelmiş veri güvenliği çözümleri yetersiz kalmaktadır. Büyük veri sistemlerinde ortaya çıkabilecek tehditlerin algılanması gerekmektedir ve gerekli noktalarda yüksek performanslı kriptografik uygulamalar kullanılmalıdır.

Nesnelerin interneti (Internet of Things-IoT) hayatımıza girişiyle, çevrimiçi eşyalardan altyapıları kontrol eden otomatize sistemlere kadar dünya çapındaki milyarlarca fiziksel cihazın internete bağlanabilmesini ve veri alıp iletmesi olağan hale gelmiştir. Ancak bu gelişen IoT teknolojisi ile kullanılan verilerin güvenliğinin sağlanması sahneye yeni saldırı tipleri çıkmasına sebep olmuştur. Nesnelerin interneti çeşitli haberleşme protokolleri sayesinde birbirleri ile haberleşebilen, birbirlerine bağlanıp veri paylaşan akıllı ağlar oluşturmaktadır. IoT sistemlerinin sahip olduğu açıklıkları örnek olarak; zayıf, tahmin edilebilir veya sabit kodlanmış parolalar, backdoor veya sistemlere yetkisiz erişime izin veren uygulamalar, güvensiz ağ servisleri, güvensiz ara yüz, bulut veya mobil sistem ara yüzleri, güvenli güncelleme mekanizmasının

eksikliği, güvensiz veri transferi ve depolaması, cihaz yönetimi eksikliği verilebilir. Tüm bu açıklıkların saldırmaya çalıştığı veriler internet kullanan nesnelerin üzerinde saklanan kişisel veriler olduğundan konuya ilişkin Türkiye'de KVK Kanunu IoT perspektifinde de en önemli etkiye sahip olacaktır.

Günümüzde tüm kurumlar müşteri verilerini kullanmakta, işlemekte ve saklamaktadır. En büyük markaların dahi bu verileri korumak konusunda zaman zaman yetersiz kalmakta ve hatta zaman zaman manipüle edilmiş amaçlarla bu verileri kendi çıkarları için kullandıkları görülmektedir. Bu büyük markalar yaşanacak herhangi bir veri saldırısı veya müşteri verilerinin zarar görmesinden dolayı çok büyük para cezalarıyla karşı karşıya kalabilmektedirler. Kurumların büyüklüğü ve finansal hacmi göz önünde bulundurulduğunda, birçok uluslararası marka büyük para cezalarını ödemeyi büyük ölçekli veri güvenliği yatırımları yapma aksiyonuna tercih edebilmektedir. Ancak KVK Kurulu gibi kanun uygulayıcı organizasyonların, kurumların almış olduğu cezalar ve bu cezalara sebep olan ihlalleri kamu ile paylaşıyor olmaları kurumlara itibar kaybı riski teşkil etmiş ve caydırıcı bir yaptırım olmuştur.

İKİNCİ BÖLÜM

RİSK, RİSK TABANLI KÜRESEL STANDART, ÇERÇEVE VE EN İYİ UYGULAMA YAKLAŞIMLARI

2.1 RİSK TANIMI VE DEĞERLENDİRİLMESİ

2.1.1. Risk Nedir?

Risk, ISACA'nın Terimler Sözlüğüne göre "Bir olay olasılığının ve sonuçlarının kombinasyonu." şeklinde açıklanmıştır.[27]

Risk kavramını daha detaylı tanımlamak gerekirse; olası şartlar içerisinden bir tehditin bir varlık üzerinde zafiyet açığa çıkarması ve kuruma zarar verebilecek başarılı bir atak gerçekleştirmesi olasılığıdır.

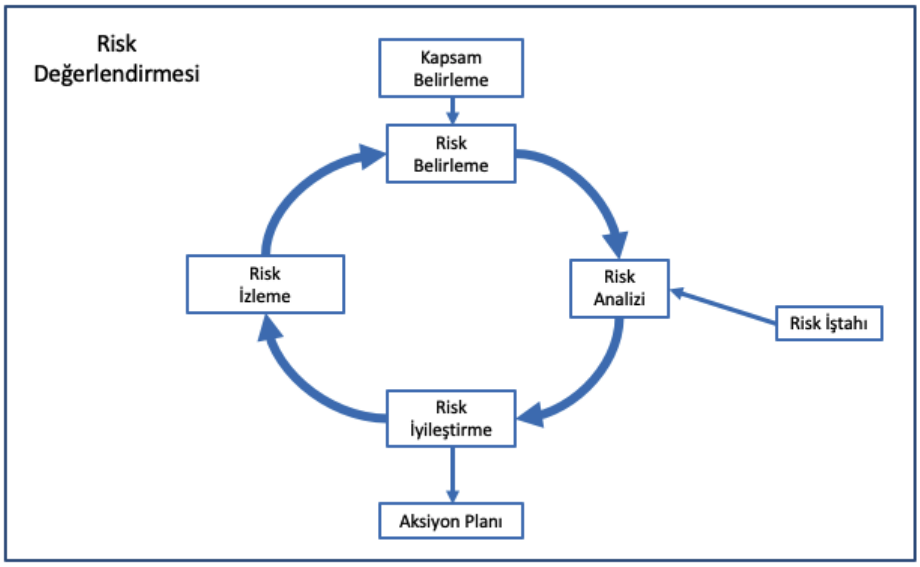
Zafiyetlerin oluşması sonucu, varlığın değeri düşebilir, erişebilirliği ve bütünlüğü bozulabilir veya varlık tamamen kullanılmaz hale gelebilir.

Risk Yönetimi Yaşam Döngüsü: Risk yönetimi diğer birçok süreç gibi döngüsel bir süreçtir. Risk yönetimi, kurumun karşısındaki gerçek tehditlerin risk değerlendirmesi sonucu ortaya çıkarılması ile oluşur.

Risk değerlendirmesinin sonuçları risk envanterine yelleştirilerek, güncel ve geçmiş risklerin takibi gerçekleştirilir. Bu sayede geçmişe dönük yaşanan olaylardan ders alınabilir, gelecekte olası tehditlere karşı önleyici faaliyetler geliştirilebilir. Risk envanteri kurumların zafiyetlerini gösteren kaynaklardır ve düzenli olarak değerlendirilmeli ve güncelliği korunmalıdır.

[27] ISACA® Glossary of Terms English – Turkish First Edition, 2018, https://www.isaca.org/resources/glossary (Erişim tarihi: 05.01.2021)

Şekil 2.1 Risk Yönetimi Yaşam Döngüsü



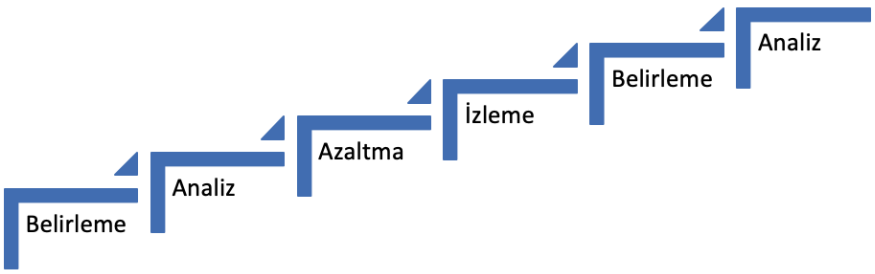
Kaynak: https://www.isaca.org/resources/glossary [28]

2.1.2. Risk Değerlendirilmesi Nedir?

Risk yönetiminin döngüsel olabilmesi için en önemli adımlarından biri risk değerlendirilmesidir. Risk değerlendirme periyodik olarak kurumun iş yapabilirliğine etki edecek bütün potansiyel risklerin değerlendirilmesidir. Risk değerlendirmenin içinde stratejik, program, proje ve operasyonel risklerin hepsi yer almaktadır. Bu sebeple kurumlara atanan BT ya da bilgi güvenliği yöneticisi olan çalışanların, çalışma hayatlarına başlandıklarında ilk yapması gereken şeylerden biri kuruma ait mevcut risk değerlendirme yapısını anlamaktır. ISACA bilgi güvenliği yönetim yaklaşımında etkin risk değerlendirme yapabilmenin sırrı kurumlara ait mevcut durumun iyi anlaşılması ve ulaşılmak istenen durumun gerçekçi şekilde tayin edilmesi, olarak vurgulanmıştır. Risk değerlendirmenin önemi hukuki pozisyonlama anlamında güncel mevzuatlarda da daha çok yer almaktadır.

[28] ISACA® Glossary of Terms English – Turkish First Edition, 2018, https://www.isaca.org/resources/glossary
(Erişim tarihi: 05.01.2021)

Şekil 2.2 Risk Değerlendirmesi Adımları



[29]Kaynak: https://www.isaca.org/resources/glossary

2.1.2.1 Risk Belirleme

Risk yönetiminin ilk aşaması, olası risklerin belirlenmesidir. Bu aşamada çeşitli yöntemler ve kaynaklar kullanılabilir. İlk olarak kullanılabilecek yöntemler şu şekilde sıralanabilir:

- Beyin fırtınası
- Kontrol listeleri
- Akış şemaları
- Kök neden analizleri
- Senaryo ve olasılık analizleri

Yukarıdakilere ek olarak farklı kaynaklar kullanılarak risk belirlenebilir, bunlar:

- Vaka araştırmaları
- Denetim raporları
- Zafiyet analizleri

[29] ISACA® Glossary of Terms English – Turkish First Edition, 2018, https://www.isaca.org/resources/glossary (Erişim tarihi: 05.01.2021)

Daha önce bir risk değerlendirme çalışması yapmamış kurumlar yukarıdaki gibi farklı yöntem ve kaynakları kullanarak risk belirleme adımında kurumun maruz kaldığı riskleri belirlemeye çalışmalıdırlar.

2.1.2.2 Risk Analizi

Risk analizi, risk yönetim çerçevesinin, ikinci adımıdır. Riskler belirlendikten sonra farklı karakteristik kategorilerine göre analiz edilir. Bu analiz asgari olarak aşağıdaki değerlendirmeleri içermelidir:

- Olayın gerçekleşme olasılığı; burada risk ile eşleştirilmiş olayın olma olasılığı hesaplanır. Bu genellikle bir yıl içerisinde gerçekleşebilecek olaylar sayısı olarak belirtilir.
- Olayın gerçekleşmesinde yapacağı etki; farklı olaylara ilişkin senaryolar incelenerek her birinin etkisi belirlenir.
- Azaltma; riskin boyutunun küçültülmesi için farklı metotlar üzerinde çalışılır. Riskin tipine göre pek çok farklı teknik kullanılabilir, süreç veya prosedürü değiştirmek, personeli eğitmek, mimariyi değiştirmek veya ayarını değiştirmek veya güvenlik yaması uygulamak vb.
- Öneri; risk analiz edildikten sonra, önerilen düzeltici veya önleyici aksiyonlar belirlenir.

2.1.2.3 Risk İyileştirme

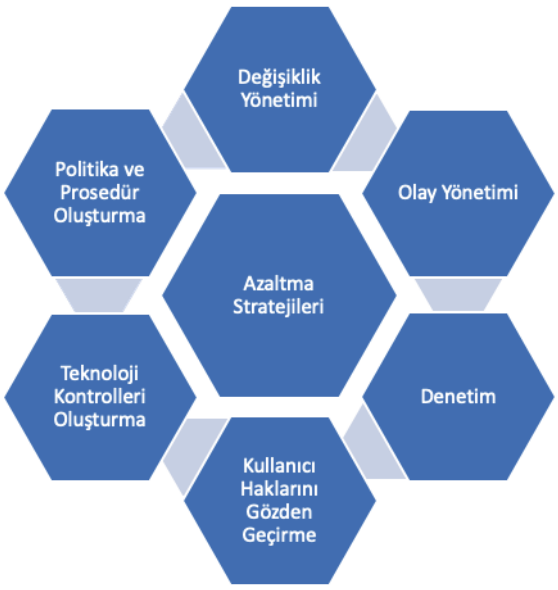
Risk iyileştirme, risk yönetimi yaşam döngüsünün son adımıdır. Bu adımda, belirlenen risklere ilişkin olarak kurumun ne yapacağı kararı verilir. Önde gelen risk iyileştirme adımları aşağıdaki gibidir:

Riski Kabul Etme: Kurum riski kabul ederek herhangi bir aksiyon almamayı seçer. Riskin kabul edilmesi, riskin mevcut etkisinin kurumun risk iştahının altında olması

veya düzeltici ya da önleyici faaliyetin riskin etkisinden daha maliyetli olması gibi gerekçelerle olabilir.

Riski Azaltma: Kurum bir aksiyon belirleyerek riskin gerçekleşme olasılığını düşürmeye veya riskin etkisini azaltmaya çalışır. Alınabilecek aksiyonlar; iş süreçlerini değiştirmek, sistemsel kriterleri değiştirmek, kontrol oluşturmak veya personeli eğitmek vb. olabilir.

Şekil 2.3 Risk Yönetimi Örnek Risk Azaltma Stratejileri



Riski Aktarma (Riski Transfer Etme): Riskin aktarımı veya transfer edilmesi genel olarak sigorta yolu ile gerçekleştirilir, fakat anlaşma ile üçüncü taraflara devretme gibi farklı yollar da kullanılmaktadır.

Riskten Kaçınmak: Kurum riskin oluşmasına neden olan faaliyeti veya faaliyetleri sonlandırır. Bu seçenek genellikle artık kar getirmeyen veya zaman aşımına uğramış iş süreçleri için kullanılır.

Risk azaltma yönteminin uygulanabilmesi için kurumun risk iştahı ve risk toleransını belirlemiş olması gerekmektedir. Risk iştahı; kurumun kabul etmeyi uygun gördüğü

risk miktarıdır. Risk toleransı ise; herhangi bir aksiyon gerekmeden kurumun tahammül edebileceği risk miktarıdır. Aralarındaki en önemli fark risk toleransının etrafta var olan risklere karşı bir aksiyon almadan önceki seviye olup, bunun yanında risk iştahının ise tespit edilen risklere karşı aksiyon alınmış veya alınmamış olmasının önemi olmamasıdır. Yeni tespit edilmiş bir risk ilk ortaya çıktığında risk iştahı olarak belirlenmiş seviye içerisinde olabilir veya bu seviyeye riski azaltmaya ilişkin bir aksiyon alındıktan sonra gelebilir.

2.1.2.4 Risk İzleme

Kurum içerisindeki varlıkların değerleri, tehditler, zafiyetler, etki ve gerçekleşme olasılığı sürekli izlenmeli ve gözden geçirilmelidir. Risk izleme aşağıdakileri içerir:

- Teknoloji mimarisindeki değişimler,
- Daha önce bilinmeyen yeni keşfedilmiş zafiyetler,
- Kanunlar ve regülasyonlarda değişiklikler,
- Yeni, değiştirilmiş veya kullanımı durdurulan varlıklar

2.1.3 Risk Değerlendirme Uygulama Örneği

Risklerin ölçümü için Etki-Olasılık-Olgunluk Analizi uygulanır. Bu analiz, kendi kendini değerlendirme yöntemi uygulanarak yapılır.

Risklerin meydana gelme olasılıkları ve meydana gelmeleri halinde yaratacakları etki düzeyi derecelendirilmekte ve bu risklere karşılık süreçlerin, altyapının ve kontrollerin olgunluğu değerlendirilmektedir.

Derecelendirilen risk etkisi ve olasılığı skorlarının ortalaması alınarak risk seviyesi hesaplanmaktadır. Bir sonraki aşamada ise bu riskler için süreç, altyapı ve kontrol bakış açısı kapsamında, uygulanan aksiyon planları ile bu planların yeterliliği değerlendirilerek olgunluk skoru belirlenmektedir.

Risk seviyesi ve olgunluk skorlarının çarpımı ile “Risk Puanı” belirlenmiş olur.

İlgili iş birimi yöneticileri tarafından her bir risk için, ilgili iş birimlerinin ilettiği etki, olasılık ve olgunluk skorlamaları gözden geçirilerek, gerekirse değişiklik yapılarak, risk seviyeleri belirlenir.

Puanlama kriterleri aşağıdaki seviyelerde değerlendirilmektedir:

Tablo 2.1 Risk Etkileri

RİSK ETKİSİ	
Felaket derecesinde güvenlik, yasal veya düzenleyici sorunu - şiddetli iş etkisi	10
Önemli derecede güvenlik, yasal veya düzenleyici sorunu - Önemli kayıplar ve müşteri şikayetleri	8
Tüketici/müşteri memnuniyeti ve yasal uyumun etkilenmesi - asgarinin üzerinde maliyet	6
Asgari derecede, tüketicinin/müşterinin fark etmeyeceği ölçüde ürün kalitesinin etkilenmesi - asgari maliyet	4
Ürün kalitesinin veya uyumun etkilenmemesi - asgari kayıp	2

Belirlenen risklerin gerçekleşmeleri durumunda oluşturacakları etkileri belirlemek amacıyla aşağıdaki kriterler göz önünde bulundurularak genel değerlendirme sağlanır.

- Finansal kayıplar,
- Stratejik değişiklikler,
- Operasyonların kesintiye uğraması,
- İtibar kayıpları (kurumsal imajın zarar görmesi ve müşteri memnuniyetsizliği),
- Müşteri/tüketici zararı,
- Yasal ve düzenleyici gereksinimlerin ve sözleşmelerin ihlalleri.

Karşılaşma olasılığının belirlenmesi, ilgili tehdidin oluşma ihtimalinin 5 seviyede derecelendirilmesidir. Tehditleri etkisi kadar gerçekleşme olasılığı da risk yönetimini yakından ilgilendirir.

Puanlama kriterleri aşağıdaki seviyelerde değerlendirilmektedir:

Tablo 2.2 Riskin Karşılaşılma Olasılığı

KARŞILAŞMA OLASILIĞI	
Sürekli sapmalar (> son 3 ay içerisinde 10 benzer durumun gerçekleşmesi)	10
Sık sık sapmalar (> son 1 yıl içerisinde 10 benzer durumun gerçekleşmesi)	8
Olası sapmalar (> son 1 yıl içerisinde 5 benzer durumun gerçekleşmesi)	6
Aralıklı sapmalar (> son 1 yıl içerisinde 1-5 benzer durumun gerçekleşmesi)	4
İlk defa karşılaşılan durumlar	2

Süreç, kontrol, altyapı olgunluğunun belirlenmesi, ilgili tehdidin tespit edilmesine veya önlenmesine karşılık süreç, altyapı ve kontrol bakış açısı ile uygulanan aksiyon planları ile bu planların yeterliliğinin 5 seviyede derecelendirilmesidir. Puanlama kriterleri aşağıdaki seviyelerde değerlendirilmektedir:

Tablo 2.3 Süreç/Kontrol/Altyapı Olgunluğu

SÜREÇ/KONTROL/ALTYAPI OLGUNLUĞU	
Problemi tespit etmeye yönelik bir sistemin olmaması	10
Seyrek kontroller - problem muhtemelen tespit edilemez.	8
Düzenli kontroller - problem tespit edilebilir.	6
Tespite yönelik otomatik olmayan kontroller	4
Neredeyse kesin olarak problemi tespit etmeye yönelik kontroller	2

Riskler, süreçlerin doğasından kaynaklanan (inherent) riskleri ve kalan (residual) riskleri de kapsar. Riskler ve Fırsatlar çalışmasında her süreç için risklere karşılık sorumlular, ilgili taraf (müşteri, tüketici, tedarikçi, personel, paydaş ve yasal mevzuat), iç/dış bağlam, etki-olasılık-olgunluk ve ilgili kontrol alanları doldurularak mevcut durum belirlenmektedir.

2.1.3.1 Risklerin ve Fırsatların Değerlendirilmesi

Risk değerlendirmesi, Bilgi Güvenliği Yönetimi Koordinatörü (Information Security Officer-ISO) koordinasyonunda süreç sorumluları tarafından, yıllık olarak risk ölçümlenme metodolojisine göre ilgili birim yöneticilerinin de gerekli desteği alınarak gerçekleştirilir. Risklerin ve fırsatların belirlenmesi ISO 27001 standardının ana bölümlerinden biridir. Bilgi güvenliği yönetim sisteminin kurum genelinde oluşturulmuş bir risk değerlendirme çalışması ile uygulanması hedeflenir. Risk ve fırsatların değerlendirilmesi farklı yöntemlerle gerçekleştirilebilir.

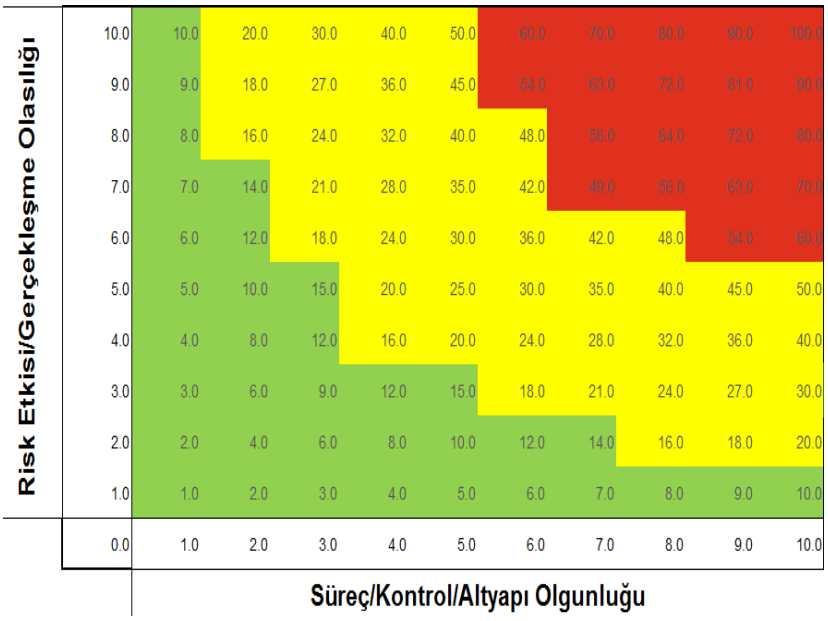
Risk değerlendirmesi çalışmalarında, riskler iş birimlerine ve yürütülen faaliyetlere göre farklılıklar gösterir. Riskleri belirlerken çalışanların görüşleri alınmalı ve değerlendirme sürecine katılmaları sağlanmalıdır. Risklerin belirlenmesi ve değerlendirmesi bir kurumun kendini ve iş süreçlerini ne kadar iyi tanıdığını gösteren çalışmalardır. Bu sebeple BT birimleri ve iş birimlerinin koordinasyonu çok önemlidir.

Kurumun risk iştahı ve buna bağlı olarak risk tolerans limitleri; kurumun stratejik hedefleri, kilit performans göstergeleri, mevcut yetki matrisleri ile hissedarların, üst yönetimin ve diğer paydaşların stratejilere ve kabul edilebilir risk seviyelerine ilişkin değerlendirmeleri dikkate alınarak belirlenir. Bu çalışma kapsamında risklerin sonuçları (örneğin finansal, yasal, itibar, insan, çevre) itibarıyla etki seviyelerinin değerlendirileceği etki değerlendirme seviyeleri ile olasılık seviyeleri oluşturulur.

Isı haritasında belirlenen kriterlere göre risk puanı için seviyeler belirlenmektedir. Isı haritasında bulunan renkler şöyle ifade edilmektedir:

- Yeşil: Süreçler etkin bir şekilde tasarlanmıştır ve çok az hata ile karşılaşılmaktadır. Sistem mevcuttur ve etkin bir şekilde çalışmaktadır.
- Sarı: Süreçler tasarlanmıştır ancak kalite hataları ile karşılaşılmaktadır. Sistem mevcuttur ve kısmen çalışmaktadır.
- Kırmızı: Süreçler tasarlanmamıştır. Sistem mevcut değildir/etkin bir şekilde çalışmamaktadır.

Şekil 2.4 Risk Isı Haritası



Fırsatlara ilişkin değerlendirme analizleri Bilgi Güvenliği Yönetimi Koordinatörü (ISO) tarafından konsolide edilerek yönetime iletilmektedir.

2.1.3.2. Risk Aksiyonlarının Belirlenmesi

Kurumun risk iştahı ve risk toleransı göz önünde bulundurularak, kabul edilebilir risk seviyeleri belirlenir. Kritik ve yüksek risk seviyesine sahip olduğu değerlendirilen risklere ilişkin etki ve/veya olasılık seviyelerini azaltmak amacıyla mevcut kontrollerin tasarım ve uygulama etkinliklerini artıracak aksiyonlar ile yeni kontrollerin tasarlanması ve uygulamaya alınmasına ilişkin aksiyonlar belirlenerek planlara bağlanır Isı haritasında "Kırmızı" ile belirlenen riskler kabul edilebilir sınırın üzerinde olan risklerdir ve bu riskler için alınacak düzeltici ve önleyici aksiyonlar ilgili iş birimi görüşü ile belirlenmeli, üst yönetimin bilgisi dahilinde takip edilmektedir. Ayrıca takip eden 3 risk değerlendirme çalışmasında "Sarı" ile belirlenen riskler kırmızı grup risklerde olduğu gibi ilgili iş birimi sorumlularının bilgilendirilmesi ile takip edilmelidir.

2.1.3.3 Risk ve Fırsatların Değerlendirme Sonuçlarının Yönetim ile Paylaşılması

Risk değerlendirme sonuçları yıllık olarak yönetim gözden geçirme toplantılarında yönetim ile paylaşılmaktadır. Belirlenmiş iyileştirme aksiyonları olarak fırsatlar, yine yönetim gözden geçirme toplantısında görüşülerek gerekli aksiyonlar belirlenir ve kaydedilir. Buradaki amaç kurumsal stratejilerin belirlenmesi ve uygulanmasında kurumsal risk yönetiminin önemini ortaya koyarak bilişim teknolojisindeki gelişmelerle birlikte gereken desteğin sağlanmasıdır.

Kurumsal yönetimin gerekliliklerini yerine getirebilmek için tutarlı ve etkin bir risk yönetim planı oluşturma ihtiyacı bulunmaktadır.[30]

2.2 BİLGİ TEKNOLOJİLERİ KAVRAMI, YÖNETİMİ VE YÖNETİŞİMİ

2.2.1. Bilgi Teknolojileri Kavramı

Küresel standart, çerçeve ve en iyi uygulamalara geçmeden önce, BT yönetişim ve ardından yönetim kavramlarına değinmemiz doğru olacaktır.

2.2.1.1. BT Yönetişimi Nedir?

BT yönetişimi sadece bir BT konusu olmadığı gibi, yine sadece BT fonksiyonlarının sorumluluğunda değildir. Geniş anlamda, kurumun genel yönetişiminin içerisinde yer almakla birlikte, bilgi teknolojilerinin yönetimi ve bilgi teknolojileri kontrolleri üzerine odaklanmış bir parçasıdır. Kurumun stratejisi ve genel yönetişim modelinden ayrı düşünülemez. Sonuç olarak BT yönetişimi yönetim kurulunun sorumluluğunda olup, BT ve diğer kritik aktivitelerin yönetişiminin doğru bir biçimde sağlandığından emin olur.

BT yönetişimi yönetim kurulunun sorumluluğundadır. BT yönetişimi, kurumun takip edeceği yol haritasını çizme, karar alma ve belirlenen yolda ilerlerken paydaşların performans takibi gibi konuları içerir. Kuruma aşağıdaki konularda destek olur:

[30] Kurumsal Risk Yönetimi, Marsh Risk Consulting

- Paydaşların ihtiyaçları, mevcut durumları ve seçeneklerinin dengeli, üzerinde anlaşılmış bir kurum stratejisi belirlemede en büyük değerlendirme ölçeği olması,
- Kurumun takip edeceği yönetişim planının önceliklendirme ve karar alma üzerine kurulu olması,
- Uyum ve performansın kabul edilen yol ve hedeflere uygun olarak izlenmesi.

BT yönetişimi, kurumlarda da gerçekleştirilen BT faaliyetlerinin kurumun stratejileri ile uyumlu olması anlamına gelmektedir. BT yönetişimini etkin biçimde uygulayan kurumlardaki BT birimleri, kurumun stratejik amaçlarına ulaşması ve hedeflerini yakalaması için bir destek birim olmak yerine stratejik iş ortağı olarak değerlendirilmektedir. BT işgücü kaynaklarının ve bütçelerinin kullanımı, üst yönetimin onayı ve katılımı ile karara bağlanmaktadır.

2.2.1.2. BT Yönetişimi Kapsamı

BT yönetişimi, BT yönetimine ilişkin organizasyon kültürü, politikalar ve uygulamaları kapsar ve beş anahtar bölümden oluşur:

- Hizalama: Bilgi teknolojileri için strateji belirleme ve bilgi teknolojileri ile iş birimi uyumunu amaçlar. Bunu yaparken organizasyon içerisindeki servisleri ve projeleri göz önünde bulundurur.
- Değer Katma: Bilgi teknolojileri ve iş birimi uyumunu ve bilgi teknolojilerinin iş birimine azami katkı sağlamasını amaçlar. Bilgi teknolojilerinin iş birimine kattığı değeri izler ve değerlendirir. Yatırımın getirisini değerlendirir.
- Risk Yönetimi: Riski en aza indirgemek ve yönetmek için süreçlerin oluşturulduğundan emin olur ve BT yatırımlarının risklerini değerlendirir.
- Kaynak Yönetimi: Kaynak ve BT kaynaklarının kullanımına ilişkin yönü belirler. İş gereksinimlerini karşılamak için yeteri kadar BT kapasitesi olduğundan emin olur.

- Performans Ölçümü: Stratejik uyumu doğrular. BT'nin iş birimlerine beklenen değeri katıp katmadığını denetler.

BT yönetişimi bir seferlik bir egzersiz değildir ve kurallar koyup onların üstünden geçerek elde edilemez. Kurumların kararlı bir şekilde, yönetim piramidinde en üst yönetimden en alt kadro çalışanlara kadar beraber hareket ederek, hızla değişen BT ortamında sürekli olarak sürdürmeleri gereken bir aktivitedir.

2.2.1.3. BT Yönetişiminin Önemi

BT yönetişimi aşağıda belirtilen sorunları ortadan kaldırarak kurumlara daha net bir yol haritası çizebildiği için önemlidir.

- BT servisleri ve projelerine ilişkin sorumluluklarda eksiklikler olması ve bu nedenle hesap verebilirlik kavramının olmayışı.
- BT fonksiyonlarının iş birimlerinin gereksinimlerine bakışı ve iş birimlerinin BT fonksiyonlarının verebileceği desteğe ilişkin beklentileri arasında her geçen gün büyüyen bir boşluk olması,
- Kurumların BT fonksiyonunun günlük operasyonlarda ne gibi desteğinin olduğu ve kattığı değeri daha iyi anlamaları gereksinimi,
- İş birimlerinin kurum içi veya kurum dışı BT ekiplerinin fonksiyonlarını daha iyi tanıması.
- Üst yönetimin, BT biriminin piyasadaki rakiplerine göre nerede olduğunu ölçmek istemesi,
- Yönetimin mevcut ve gelecekte kullanılacak teknoloji altyapısının iş birimi beklentilerini (teknoloji, insan ve süreç açısından) karşılamak adına yeterli olup olmayacağı,
- Her geçen gün kurumların BT bağımlılıklarının artması nedeniyle yönetimin kritik BT risklerinden haberdar olması ve bunların yönetilebildiğini görmesi ve bu risklerin kritik BT kararları alınırken önemli rol oynaması.

- Ve son olarak, kurumların BT'nin karmaşık ve sürekli değişen özel koşullara sahip olması nedeniyle iyi bir yönetim yaklaşımı ve kuvvetli kontrollerin uygulanmasının daha da gerekli olmasıdır.

BT yönetişimine ilişkin sektörel değerlendirmelere göre;

- Kurumların yalnızca %85'i değişiklik talepleri için olurluk incelemesi istemektedir.
- Onaylanmış projelerin sadece %40'ı geçerli (gerçekçi) fayda değerlendirmesine sahiptir.
- Kurumların %10'undan azı planlanan faydaların, proje tamamlandıktan sonra gerçekleşip, gerçekleşmediğini kontrol etmektedir.
- Kurumların %5'inden azı proje paydaşlarını hedeflere ulaşma konusunda sorumlu tutmaktadır.[31]

2.2.1.4. BT Yönetimi Nedir?

BT yönetimi, tüm iş birimlerinin kullanmadan iş göremediği sistemlerinin yönetilmesi ve güvenliğinin sağlanması için her türlü fonksiyonu içerir. BT bugün kurumda her çalışanı yakından ilgilendiren dijital yaşamın can damarıdır. Kısaca açıklarsak, yönetişim tarafından belirlenen doğrultuda, görevleri kontrol etme/yönetmeye yönetim denir. Üst yönetim BT yönetiminden de sorumludur. Başka bir deyişle yönetim planlar, gerçekleştirir, işletir ve izler. Bu aktivitelerin hepsini yönetişim tarafından belirlenen doğrultu ile uyumlu bir şekilde yapar.

BT yönetişimi ve yönetimi kurumların stratejilerini belirleme ve uygulama konusunda çok önemli yere sahiptirler. Verinin güvenliğinin sağlanması, ancak kurumların oturmuş BT yönetişim ve yönetim yapıları olması sayesinde gerçekleşebilir. Kurumların dayanıklı, değişime ayak uydurabilen bir yönetişim ve yönetim yapısı kurabilmeleri için küresel standart, çerçeve ve en iyi uygulamalar bulunmaktadır.

[31] Linenberg, Y. & Gudka, A. (2004). The learning organisation—the benefits of tracking project benefits. Paper presented at PMI® Global Congress 2004—EMEA, Prague, Czech Republic. Newtown Square, PA: Project Management Institute.

2.3 KÜRESEL STANDART, ÇERÇEVE VE EN İYİ UYGULAMALAR VE YAKLAŞIMLARI

2.3.1. Küresel Standart, Çerçeve ve En İyi Uygulama Nedir?

Küresel standart, çerçeve ve en iyi uygulamalar genel olarak BT yönetişimi içerisindeki süreçler ve aktiviteleri ana hatlarıyla belirlerken, BT yönetişim süreçlerini ve süreçlerin performansını izleme gibi konularda metotları da belirlerler. Küresel standart, çerçeve ve en iyi uygulamalar günümüzde veri koruma ve ilişkili mevzuatlarının da temelini oluşturmaktadır.

Standart: Standartlar genel olarak bir otorite (Uluslararası Standartlaştırma Örgütü (ISO) gibi) veya tanınmış bir dış standart kuruluşu tarafından onaylanmış zorunlu bir gereksinimdir. Genel olarak belirli bir kalite, seviye, sonuç elde etmek veya daha güvenli bir ortam yaratmak için kullanılırlar.

Çerçeve: Çerçeve buradaki kullanımımızla 'Yönetişim Çerçevesi', dünyadaki en tanınmış ve yaygın kullanılan yönetişim çerçevesini yapan kurum olan ISACA'ya göre: "Bir çerçeve, karmaşık sorunları çözmek veya adreslemek için kullanılan kavramsal bir temel yapıdır. Bir yönetişim gerçekleştiricisidir. Bir şeyin nasıl ele alınabileceğini veya anlaşılabileceğini tanımlayan kavramlar, varsayımlar ve uygulamalar bütünüdür, ilgili taraflar arasındaki ilişkileri belirler, ilgili kişilerin rollerini belirtir ve sınırları (yönetişim sistemi içeriğinde bulunan ve içerisine dahil olmayan unsurlar) çizer."[32]

En İyi Uygulama / İyi Pratik (Best Practices): Yine ISACA'nın tanımına göre en iyi uygulama veya iyi pratik; "Birden fazla kuruluş tarafından başarılı bir şekilde kullanılan, kanıtlanmış bir faaliyet veya süreç." olarak ifade edilir.

[32] ISACA® Glossary of Terms English – Turkish First Edition, 2018, https://www.isaca.org/resources/glossary (Erişim tarihi: 05.01.2021)

2.3.2. Bilgi için Kontrol Hedefleri ve İlgili Teknolojiler (COBIT)

Eskiden Bilgi için Kontrol Hedefleri ve İlgili Teknolojiler (Control Objectives for Information and related Technology-COBIT) olarak bilinen, günümüzdeyse beşinci yinelemesi için kullanılan ISACA kaynağıdır. Kuruluş veri ile bilgi teknolojilerinin yönetişimi ve yönetimi için uluslararası biçimde tanınan, bütün bir çerçevedir. BT yönetişimi ile yönetiminde yöneticileri destekler; iş hedefleri ve bağıntılı BT hedeflerinin tanımlanmasını ve başarılmasını sağlar.[33] BT yönetişimi konusunda kurumlar genellikle COBIT çerçevesindeki yaklaşımı ve standartları esas alarak çalışmalarını sürdürmekte ve süreç ve organizasyonel yapılarını bu doğrultuda revize etmektedir.

COBIT'in ne olduğundan önce ne olmadığından bahsetmek çerçevenin daha net anlaşılmasına yardımcı olacaktır;

- COBIT, bir kurumun bütün BT ortamının bir tanımı değildir.
- COBIT, iş süreçlerini organize etmek için kullanılacak bir çerçeve değildir.
- COBIT, Bütün teknoloji altyapısını yönetecek teknik bir BT çerçevesi değildir.
- COBIT, BT ile ilgili kararların nasıl alınacağını belirlemez.

Genel anlamda COBIT yönetişim çerçevesi;

- Kurumun bilgisinin ve teknolojilerinin yönetişim ve yönetimi için oluşturulmuştur bir çerçevedir. Belirli bir birime odaklanmaz, kurumun bütünün ele alır.
- Kurumun bilgileri ve teknolojileri, kurumun hedeflerine ulaşmak için kullandığı tüm teknoloji ve işlediği bilgiyi içermektedir. Yani farklı bir şekilde anlatmak gerekirse, kurumun bilgi ve teknolojileri, kurum içerisinde BT iş birimi ile limitli olmamakla birlikte, BT iş birimini de içermektedir.

[33] ISACA® Glossary of Terms English – Turkish First Edition, 2018, https://www.isaca.org/resources/glossary (Erişim tarihi: 05.01.2021)

- Bilgi ve ilgili bilgi teknolojilerine ilişkin riskler ve faydaları anlama ve yönetme konusunda çığır açacak bir BT yönetişim aracı olarak dizayn edilmiştir.
- Sağlıklı bir yönetişim sistemi (süreçler, kurumsal yapılar, politikalar ve prosedürler, bilgi akışları, kültür ve davranışlar, yetenekler ve altyapı) kurmak ve bu sistemin sürdürülebilir olması için bileşenleri tanımlar. Yönetişim ve yönetim kavramları net bir şekilde birbirinden ayrılmaktadır. Daha önceki bölümde değinildiği gibi bu iki disiplin farklı aktiviteler içermekte, farklı kurumsal yapılara gereksinim duymakta ve farklı amaçlara hizmet etmektedir.
- Kurumların en uyum yönetişim sistemini kurabilmek için dizayna etki edecek faktörleri tanımlar ve bunlara tasarım etkenleri demektedir.

2.3.2.1. COBIT'in Tarihçesi

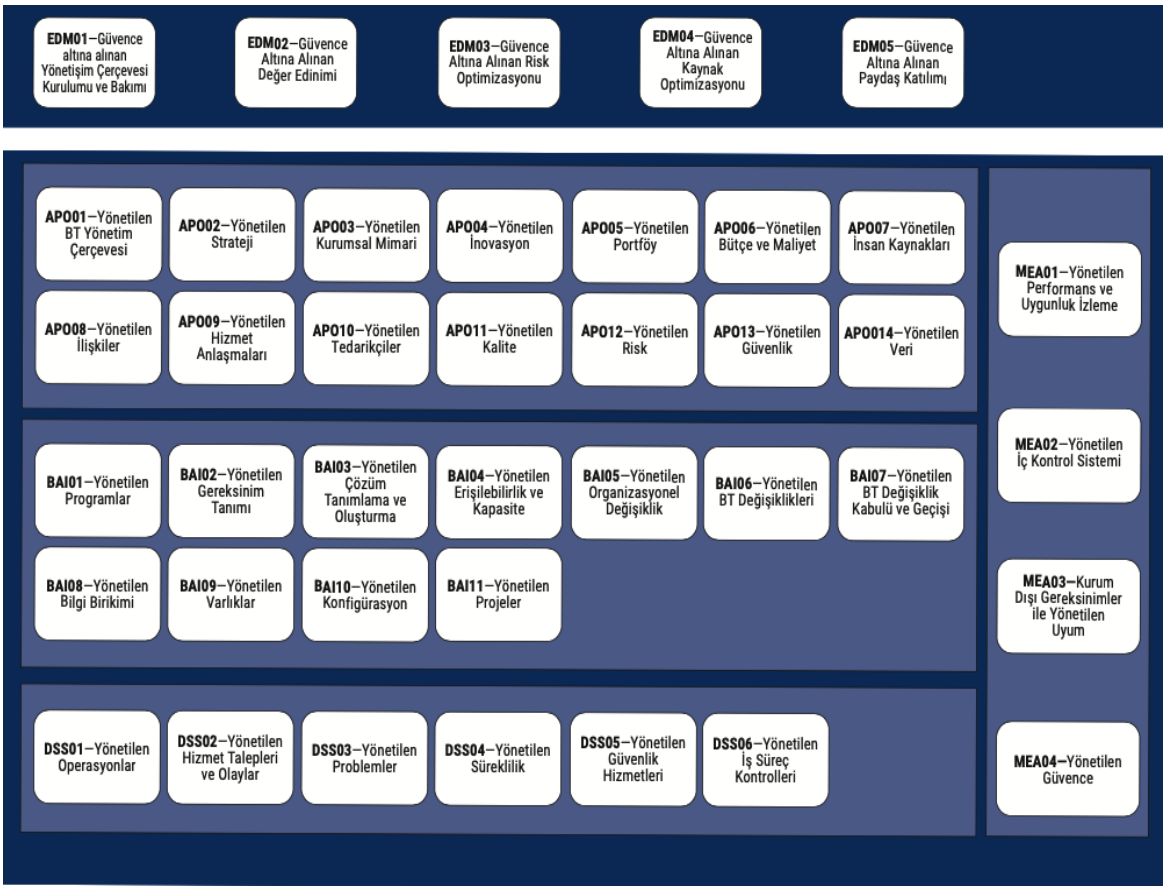
ISACA tarafından 2005 yılında ilk versiyon olan COBIT 4 yayınlanmış olup, 2007 yılında COBIT 4.1 güncellemesi piyasaya sürülmüştür. Bu güncelleme bilgi ve iletişim teknolojileri ile ilgili daha fazla detay içermektedir. COBIT 4.1 yönetişim ve yönetim arasına keskin bir çizgi koymamaktadır. Daha önceki versiyonda böyle bir ayrım olmadığı için bu iki disiplin birlikte ele alınmaktadır. COBIT 4.1, 4 ana etki alanı (domain) ve 34 kontrol hedefinden oluşmaktadır.

2012 yılında COBIT'in yeni versiyonu COBIT 5 piyasaya sürülmüş olup, 2013 yılında ISACA COBIT 5 için bir eklenti yayınlamıştır. Bu ek, risk yönetimi ve yönetişimi açısından daha fazla detay içermektedir. ISACA yönetişim alanı olan EDM (Evaluate, Direct and Manage) alanını COBIT 5 ile ilk defa yayınlamıştır. COBIT 5, 5 ana etki alanı (domain) ve 37 süreçten oluşmaktadır. ISACA'nın diğer çerçeveleri olan "VAL IT" ve "Risk IT" COBIT 5 versiyonunda, bu çerçeve içine entegre edilmiştir.

ISACA 2018 yılında COBIT'in güncel bir versiyonunun çıkacağını duyurmuş ve isim içerisinde rakam kullanmaktan vazgeçmiştir. Bu versiyon en güncel versiyon olmakla birlikte adı COBIT 2019 olarak piyasaya dürülmüştür. Bu versiyon yine 5 ana etki

alanı (domain) içermekle birlikte 40 yönetişim ve yönetim hedefine sahiptir. Bu versiyon ile birlikte ISACA daha sık ve değişken güncellemeler geleceğini, daha kolay adapte olabilen ve gelişen teknolojiye uygun yönetişim stratejileri ortaya koymuştur.

Şekil 2.5 COBIT 2019 Çerçevesi Yönetişim ve Yönetim Hedefleri



Kaynak: COBIT® 2019 Çerçevesi: Yönetişim ve Yönetim Hedefleri, 2019, www.isaca.com[34]

2.3.2.2. COBIT 2019

COBIT 2019 ile gelen yenilikler nelerdir:

[34] COBIT® 2019 Çerçevesi: Yönetişim ve Yönetim Hedefleri, 2019, www.isaca.com (Erişim tarihi: 06.01.2021)

- Kurumlar için bilgi ve teknolojinin önemini daha net bir şekilde ortaya koymaktadır.
- Yeni ve yükselen teknoloji trendlerine değinmektedir.
- Daha güncel bir içerik sunmaktadır.
- Daha iyi adapte olabilme özelliği sunmaktadır.
- Odak alanı konseptini sunmaktadır.
- Veri, proje ve uyuma ilişkin yeni süreçler eklenmiştir.
- Siber güvenlik ve gizlilik konusunda güncellemeler gelmiştir.
- Diğer standart, regülasyon ve en iyi uygulamalara atıfta bulunmaktadır
- Yeni çevrimiçi işbirliği özelliği sunarak, kullanıcıların çerçevenin gelişimine katkı sağlamalarını hedeflemiştir.

Tasarım etkenleri, COBIT 2019 ile ilk defa ortaya çıkmıştır. Tasarım etkenleri kurumun yönetişim sisteminin tasarımını etkileyebilecek ve BT kullanımını başarıya götürebilecek etkenlerdir.

Şekil 2.6 COBIT 2019 Tasarımı

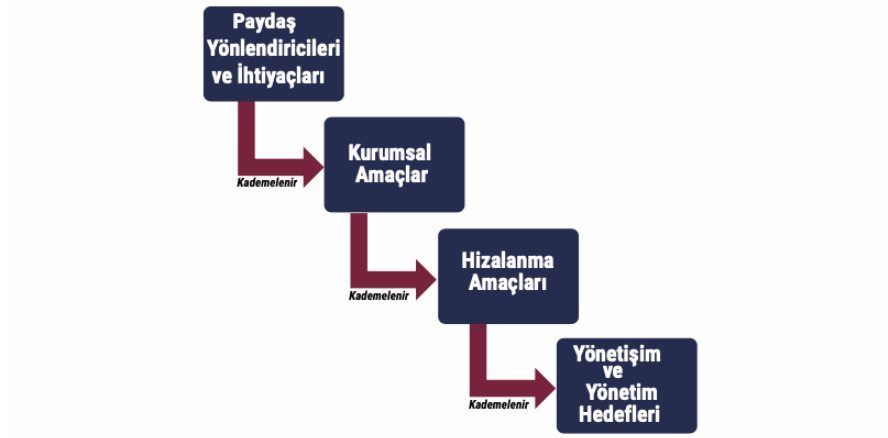
Kaynak: COBIT® 2019 Çerçevesi: Giriş & Metodoloji, 2019, www.isaca.com

Tasarım etkenleri bazı yönetişim ve yönetim hedeflerinin diğerlerinden daha önemli olmasına neden olabilmektedir. Tasarım etkenleri yukarıda sıralanan etkenlerden biridir.[35]

[35] COBIT® 2019 Çerçevesi: Giriş & Metodoloji, 2019, www.isaca.com
(Erişim tarihi:05.01.2021)

COBIT 2019 Amaç Basamakları, kurum hedeflerinin hizalama hedefleri denen BT ve iş birimleri arasında köprü oluşturmak için tasarlanan hedeflerin birbirleri ile etkileşim içinde olmalarını sağlamaktadır.

Şekil 2.7 COBIT Amaç Basamakları



Kaynak: COBIT® 2019 Çerçevesi: Giriş & Metodoloji, 2019, www.isaca.com

Kurum içi paydaşların gereksinimleri, kurumların stratejilerine dönüştürülmüş olmalıdır. Yukarıda görülen amaçların basamaklandırılması yönetişim sisteminin en önemli tasarım etkenlerinden biri olan kurumsal amaçları destekler. Kurumsal amaçlar risk tabanlı yaklaşımda bütünleşik bir yapıyla ifade edilebilir. Bu sayede kurumsal ifadesindeki kurumu oluşturan her fonksiyon, bir organ niteliğinde bütün vücudun fonksiyonlarını temsil eder. COBIT çerçevesi, yönetişim modelinde belirlenen iş stratejisi doğrultusunda kaynakların, insan kaynaklarının, süreçlerin ve uygulamaların efektif olarak kullanılmasını hedefler.

2.3.2.3. COBIT Yönetişim Kavramı

COBIT 2019 birbirine yardımcı fakat iki farklı ilkeler grubu üzerinde oluşturulmuştur. Bunlar yönetişim modelini ve yönetişim sistemini oluşturmak için izlenen ilkelerdir. Yönetişim kavramı yenilenen yapıda yönetim modelinin eksikliğini gidermeyi

hedeflemektedir. Yönetişim modeli ile kurumsal iş birliğinin sağlanması, yönetim ve iletişim kavramlarının birlikte geliştirilmesi yaklaşımında, BT birimleri ile iş birimlerinin uzlaşması hedeflenmektedir. Bu sayede bütüncül bir iş model yaklaşımı ve kurumsal ihtiyaçlara cevap veren bir süreç yapısı sağlanabilir.

COBIT 2019 yaklaşımında dinamik yönetim sistemi ile uçtan uca yönetişim yani her bir iş biriminin dahil olduğu bir çerçeveyi amaçlar ve çerçeve kapsamında modelleme bu doğrultuda oluşturulmuştur.

Şekil 2.8 COBIT Yönetişim Modeli

Kaynak: COBIT® 2019 Çerçevesi: Giriş & Metodoloji, 2019, www.isaca.com

Şekil 2.9 COBIT Yönetişim Sistemi Kurmak için Gereken Yönetişim Çerçevesine Dair Üç İlke

Kaynak: COBIT® 2019 Çerçevesi: Giriş & Metodoloji, 2019, www.isaca.com

2.3.2.4. COBIT İçerisindeki Yönetişim ve Yönetim Hedefleri

BT'nin kurum hedeflerine katkı sağlayabilmesi için birçok yönetişim ve yönetim hedefine ulaşılmalıdır. Yönetişim ve yönetim hedeflerine ilişkin en basit kavramlar aşağıdaki gibidir:

- Bir yönetişim veya yönetim hedefi, belirlenen hedefin gerçekleşmesine yardımcı olmak için her zaman bir süreçle ilişkilendirilir.
- Şekil 2.4'te görüldüğü gibi bir yönetişim hedefi yine bir yönetişim süreci ile, bir yönetim hedefi ise bir yönetim süreci ile ilişkilidir.

COBIT içerisinde daha önce de belirtildiği gibi 5 etki alanı (domain)bulunmaktadır:

İlk etki alanı (domain) yönetişim hedeflerini içermektedir.

- Değerlendir, Yönet ve İzle (Evaluate, Direct and Manage-EDM) etki alanı (domain) yönetişim yaklaşımını içermektedir. Yönetişimden sorumlu bölüm stratejik seçenekleri değerlendirir, üst yönetimi seçilen stratejik yolda yönlendirir ve stratejinin uygulanmasını izler.

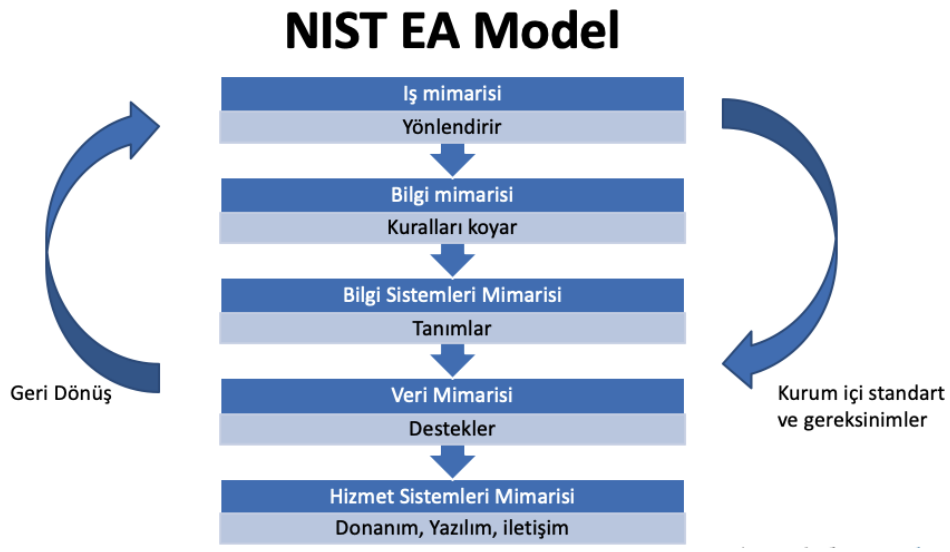
Geri kalan dört etki alanı yönetim hedeflerini içermektedir.

- Hizala, Planla ve Düzenle (Align, Plan and Organize-APO), BT organizasyonel, stratejik ve destekleyici faaliyetleri ele alır.
- Kur, Edin ve Uygula (Build, Acquire and Implement-BAI), BT çözümlerinin oluşturulması, satın alınması ve uygulanması ile bunların kurum içerisine entegrasyonunu ele alır.
- Sağla, Hizmet Sun ve Destek Ver (Deliver, Service and Support-DSS), BT hizmetlerinin operasyon tarafı ve desteğini, BT güvenliği konusuyla birlikte ele alır.
- İzle, Tespit Et ve Değerlendir (Monitor, Evaluate and Assess-MEA), BT performansını izleme ve bunun iç hedefleri iç kontrol hedefleri ve dış gereksinimlere uygunluğunu ele alır.

2.3.3. Ulusal Standartlar ve Teknoloji Enstitüsü (NIST)

Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology-NIST) federal kurumlar ve bu kurumlar ile iş yapan kurumların izleyeceği standartları oluşturan Amerika Birleşik Devleri kökenli bir kamu kurumudur.
Bilgi teknolojilerinin ilerlemesini ve verimli bir şekilde kullanılmasını sağlamak amacı ile testler, kontroller geliştirir ve teknik analiz çalışmaları yapar.
NIST Kurum Mimari Modeli (NIST Enterprise Architecture Model) 80'li yılların sonunda geliştirilen bir referans modeldir. Bu model kurum mimarisini, iş birimleri, bilgi ve teknoloji yatırımları arasındaki ilişkiyi göz önünde alarak tanımlar.

Şekil 2.10 NIST EA Modeli



Kaynak: NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations[36]

Bu modele göre, iş mimarisi bilgi mimarisini yönlendirir, bilgi mimarisi bilgi sistemleri mimarisine ilişkin kuralları koyar, bilgi sistemleri mimarisi veri mimarisinin nasıl olacağını tanımlar, veri mimarisi hizmet sistemleri/son kullanıcının kullandığı sistemleri destekler.

[36] NIST Special Publication 800-53 Revision 5, Security and Privacy Controlsfor Information Systems and Organizations.

NIST zaman içinde birçok standart ve kurallar yayınlamış, sürdürülebilir bir şirket yönetişim sistemi kurulması ve veri güvenliğinin sağlanması açısından çeşitli dokümanlar oluşturmuştur.

Bu dokümanlardan en yaygın olarak kullanılan, NIST Siber Güvenlik Çerçevesi (Cyber Security Framework)'dir. Bu çerçeve ilk olarak 2014'de yayınlanmış olup, 2017 ve 2018 revize edilmiştir. NIST Siber Güvenlik Çerçevesinin en önemli özelliklerinden biri herkesin katılımına açık 8 seminer ile dünyanın her yerinden farklı sektörlerden paydaşların yaptığı yorumlar ve verdiği geri dönüşler çerçevenin şekillenmesini ve bugünkü haline ulaşmasını sağlamış olmasıdır.

Çerçeve, siber güvenlik konusunda kurumlara, genel olarak kullanabilecekleri bir organizasyon yapısı sağlamaktadır. NIST, COBIT ve ISO gibi diğer kaynaklara atıfta bulunduğu için farklı sektörlerde ve her yerde kullanılabilecek bir model olarak değerlendirilmektedir.

NIST siber güvenlik konusunda, özellikle fiziksel, siber ve insan konularındaki güvenlik unsurlarını ele alması açısından kolay adapte olunabilir ve farklı tip kurumlara uygulanabilir bir yapıya sahiptir. Teknolojiyi kullanan kurumların tamamına uygulanabilecek bir çerçevedir. Bu çerçeve, kurumların müşterilerine, çalışanlarına ve diğer partilere ait gizli verileri siber güvenlik riskleri açısından değerlendirme fırsatı sunmaktadır.

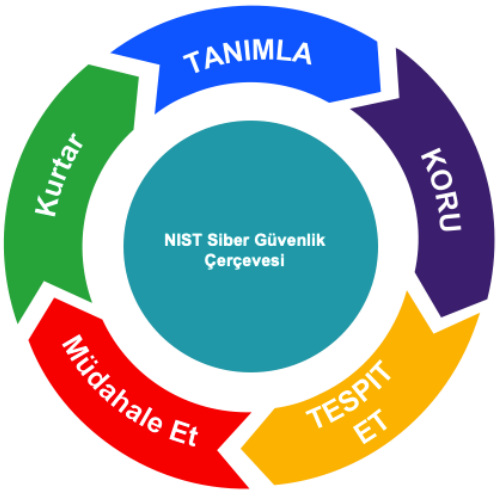
NIST Siber Güvenlik Çerçevesine ek olarak NIST 800-53 özel yayınını çıkarmış olup bu yayınla birlikte, tüm Amerikan ulusal kurumların bilgi güvenliği sistemlerini kurmaları ve yönetmeleri için standartlar ve kılavuzlar oluşturmuştur. Bu ek ve ana çerçeve sayesinde kurumların ve dolayısıyla vatandaşların gizli verilerinin korunması amaçlanmıştır.

2.3.3.1. NIST Siber Güvenlik Çerçevesinin Çekirdek Yapısı

Çekirdek yapı, siber güvenlik hedeflerine ulaşmak adına dikkat edilmesi gereken aktivite adımlarını içerir. Bununla birlikte, hedeflere ulaşmak için yapılması gereken

örneklere referans göstermektedir. Bu çekirdek yapının bir kontrol listesi olmadığı unutulmamalıdır, burada paydaşlar tarafından önemli olarak belirlenmiş anahtar siber güvenlik çıktıları ele alınmaktadır. Bu sebeple NIST Siber Güvenlik Çerçevesi tef seferlik bir denetim olarak değil sürekli takibi ve uygulaması devamedecek biryönetim modeli olarak algılanmalıdır.

Şekil 2.11 NIST Fonksiyonları



Çekirdek çerçevenin içinde beş ana fonksiyon bulunmaktadır:

Tanımla: Kurumun kullanmakta olduğu sistemler, insan faktörü olarak çalışanlar ve ilgili taraflar, varlıklar, veriler ve iş modeline ilişkin siber güvenlik risklerinin nasıl yönetileceğini belirleyen fonksiyondur.
Tanımla fonksiyonundaki aktiviteler çerçevenin doğru bir şekilde kullanımı için büyük önem taşımaktadır. İşin içeriğini, kritik birimleri destekleyen kaynakları ve ilgili siber güvenlik risklerini anlamak kurumların daha odaklı ve doğru önceliklendirilmiş şekilde hareket etmelerini ve ortaya koydukları çabanın risk yönetimi stratejisi ve iş gereksinimleri ile uyumlu olmasını sağlamaktadır. Bu bölümdeki kategoriler Tablo 2.4 üzerinde gösterilmiştir.
Koru: Kritik servislerin işlevinin devam edebilmesi için uygun önlemler geliştirilmeli ve uygulanmalıdır.

Koru fonksiyonu potansiyel bir siber olayın etkisinin sınırlandırılması veya kontrol altına alınmasını sağlamaktadır. Bu bölümdeki kategoriler Tablo 2.4 üzerinde gösterilmiştir.

Tespit Et: Siber güvenlik olaylarının oluşma frekansını belirlemek için uygun aktiviteleri geliştirilir ve uygulanır.
Tespit et fonksiyonu siber güvenlik olaylarının zamanında tespitinin sağlanmasını hedeflemektedir. Bu bölümdeki kategoriler Tablo 2.4 üzerinde gösterilmiştir.

Müdahale Et: Tespit edilmiş bir siber güvenlik vakasına ilişkin aksiyon almak için kullanılacak aktivitelerin geliştirilir ve uygulanır.
Müdahale Et fonksiyonu potansiyel bir siber güvenlik vakasının yaratacağı etkiyi kontrol altına almayı hedeflemektedir. Bu bölümdeki kategoriler Tablo 2.4 üzerinde gösterilmiştir.

Kurtar: Siber güvenlik vakası nedeni ile bozulmuş veya duraksamış servisler eski konumuna getirilmesi ve direncinin artırılması için aktiviteler geliştirir ve uygular.
Kurtar fonksiyonu siber güvenlik vakasının etkisini azaltmak için normale en hızlı şekilde dönülmesini desteklemektedir. Bu bölümdeki kategoriler Tablo 2.4 üzerinde gösterilmiştir.

NIST fonksiyonlarının denetiminin sağlanması için gerçekleşecek kontrollerde örneklem seçimi detaylı değildir. Denetim perspektifini pekiştirmek için COBIT örneklem seçiminde detaylı bir yol gösterici olacaktır.

NIST oluşumu açısından sektörel bir pazar araştırmasını açıkça gerçekleştirdiği için özellikle kurumsal nitelikte şirketler için çok kıymetli bir kaynak niteliğindedir. Gerçekleştirilen pazar araştırması sayesinde sektörel ihtiyaçların ve değişkenlerin göz önünde bulundurulduğu, yasal uyum gereksinimlerini karşılayacak kontroller NIST kapsamına eklenmiştir.

Tablo 2.4 NIST Siber Güvenlik Çerçevesi Kategorileri

Fonksiyon	Kod	Fonksiyon Kategori Kodu	Kategori Adı (EN)	Kategori Adı (TR)
Identify Tanımla	ID	ID.AM	Asset Management	Varlık Yönetimi
		ID.BE	Business Environment	İş Çevresi
		ID.GV	Governance	Yönetişim
		ID.RA	Risk Assessment	Risk Değerlendirme
		ID.RM	Risk Management Strategy	Risk Yönetim Stratejisi
		ID.SC	Supply Chain Risk Management	Tedarik Zinciri Risk Yönetimi
Protect Koru	PR	PR.AC	Identity Management and Access Control	Kimlik Yönetimi ve Erişim Kontrolü
		PR.AT	Awareness and Training	Farkındalık ve Eğitim
		PR.DS	Data Security	Veri Güvenliği
		PR.IP	Information Protection Processes and Procedures	Bilgi Koruma Süreçleri ve Prosedürleri
		PR.MA	Maintenance	Bakım
		PR.PT	Protective Technolgy	Koruyucu Teknolojiler
Detect Tespit Et	DE	DE.AE	Anomalies and Events	Gariplikler ve Olaylar
		DE.CM	Security Continuous Monitoring	Sürekli Güvenlik İzleme
		DE.DP	Detection Processes	Tespit Süreçleri
Respond Müdahale Et	RS	RS.RP	Response Planning	Müdahale Planlama
		RS.CO	Communications	Haberleşme
		RS.AN	Analysis	Analiz
		RS.MI	Mitigation	Azaltma
		RS.IM	Improvements	İyileştirme
Recover Kurtar	RC	RC.RP	Recovery Planning	Kurtarma Planlama
		RC.IM	Improvements	İyileştirme
		RC.CO	Communications	İletişim

[37]Kaynak: https://mturan.net/blog/nist-cybersecurity-framework-surecsel-yapilandirma

2.3.4. Bilgi Teknolojileri Altyapı Kütüphanesi (ITIL)

Bilgi Teknolojileri Altyapı Kütüphanesi (The Information Technology Infrastructure Library-ITIL) detaylı en iyi uygulamalar ve kılavuzlar bütünüdür.

[37] https://mturan.net/blog/nist-cybersecurity-framework-surecsel-yapilandirma/ (Erişim tarihi: 05.01.2021)

ITIL'ın ilk versiyonu 1980'lerin ilk yarısında oluşturulmuştur ve kitaplar serisinden oluşmaktadır. Daha sonra ITIL V2 2001 yılında yayınlanmıştır. 10 ana süreç ve servis masası konusuna ağırlık vermektedir.

Bir sonraki versiyonu 2007 yılında yayınlanmış olup birçok kaynak tarafından ITIL V3 olarak adlandırılsa da resmi olarak ITIL 2007 adını almıştır. Bu versiyonu servis yönetimi sürecini beşe bölmüştür. Bunlar:

- Servis stratejisi
- Servis tasarımı
- Servis geçişi
- Servis operasyonları
- Servisin sürekli geliştirilmesidir.

ITIL V3 2011 yılında yayınlanmış ve ikinci versiyonun güncellemesi olarak kullanılmaya başlanmıştır. ITIL V3 aynı beş bölümden oluşmaktadır.

Son olarak, en güncel versiyon olan ITIL V4 Şubat 2019'da yayınlanmıştır. Uzun bir aradan sonra güncelleme gelmesiyle ITIL, güncel teknolojileri ve trendleri içermeyi ve dijital dönüşüm yaşayan ve iş süreçlerine dijital teknolojileri entegre eden kurumları desteklemeye hedeflemektedir. ITIL, uygulandığı kurum ile BT arasında gerekli olan etkileşimi ve uyumu hızlı ve belirli kurallar çerçevesinde sağlar ve büyük veya küçük tüm BT organizasyonlarına göre ölçeklenebilen süreç merkezli bir yaklaşımı destekler. ITIL V3 ile gelen servis yönetim süreci bu yeni versiyonda servis değer sürecine dönüştürülmüştür (Tablo 2.4) ve 26 ITIL süreci ITIL V4 ile yönetim uygulamalarına dönüştürülmüştür.

ITIL V4 34 adet yönetim uygulaması içermektedir. (Tablo 2.4) Bunlardan 14 tanesi genel yönetim uygulamaları. 17 tanesi servis yönetim uygulamaları ve 3 tanesi teknik yönetim uygulamalarıdır.

- Genel Yönetim Uygulamaları
- Servis Yönetimi Uygulamaları
- Teknik Yönetim Uygulamaları

Tablo 2.5 ITIL Kategoriler ve Uygulamaları

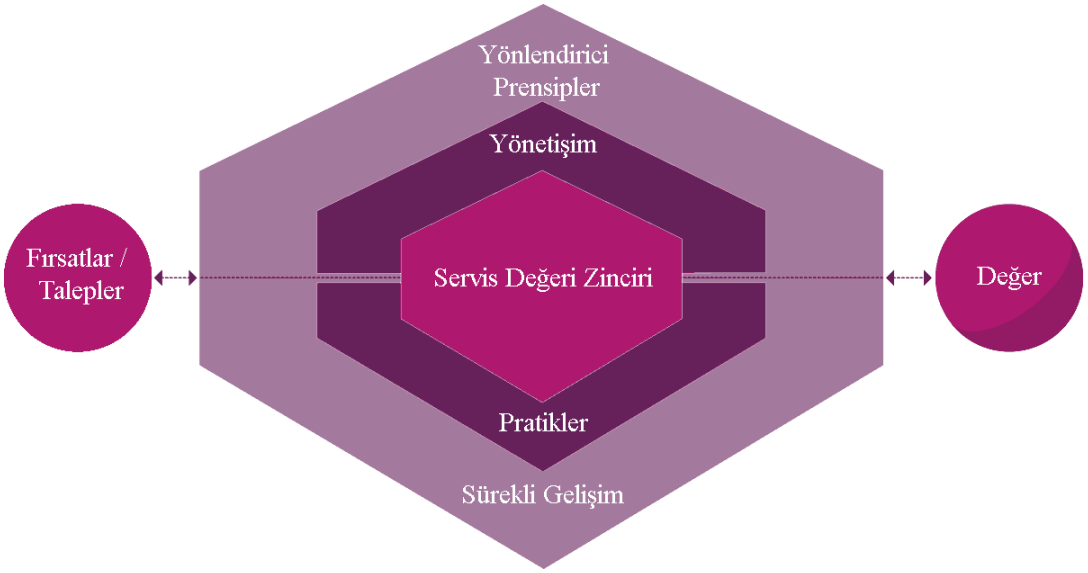
Genel Yönetim Uygulamaları	Servis Yönetimi Uygulamaları	Teknik Yönetim Uygulamaları
Mimarı yönetimi	Erişilebilirlik yönetimi	Dağıtım yönetimi
Sürekli iyileştirme	İş analizi	Altyapı ve platform yönetimi
Bilgi güvenliği yönetimi	Kapasite ve performans yönetimi	Yazılım geliştirme ve yönetimi
Bilgi birikimi yönetimi	Değişiklik kontrol süreci	
Ölçüm ve raporlama	Vaka/olay yönetimi	
Kurumsal değişiklik yönetimi	BT varlık yönetimi	
Portföy yönetimi	İzleme ve olay yönetimi	
Proje yönetimi	Problem yönetimi	
İlişki Yönetimi	Versiyon yönetimi	
Risk Yönetimi	Servis kataloğu yönetimi	
Servis finans yönetimi	Servis konfigürasyon yönetimi	
Strateji yönetimi	Servis sürekliliği yönetimi	
Tedarikçi yönetimi	Servis tasarımı	
İş gücü ve yetenek yönetimi	Servis masası	
	Hizmet seviyesi yönetimi	
	Hizmet isteği yönetimi	

[38]Kaynak: ITIL V4 Management Practices, 2020, https://www.knowledgeapple.com/itil-v4-practices/

ITIL daha çok servis yönetimi alanına odaklanmıştır. Diğer standartlar ve çerçeveler, ITIL'ı tamamlayıcı özelliktedir.

[38] ITIL V4 Management Practices, 2020
https://www.knowledgeapple.com/itil-v4-practices/
(Erişim tarihi: 05.01.2020)

Şekil 2.12 ITIL Servis Değer Süreci



Kaynak : Sophie Danby, The ITIL 4 Service Value System Explained, https://itsm.tools/the-itil-4-service-value-system-explained/[39]

ITIL, operasyonel odağı olan kurumların kullanımı için daha uygundur. ITIL'ın bütün olarak uygulanmaması gerekir ve kuruma göre şekillendirilmelidir.

2.3.4.1. ITIL'ın Genel Özellikleri

- "Kamuya Açık" olarak sınıflandırılmıştır. Bu yüzden ticari bir sahibi yoktur ve herkes tarafından kullanılabilir. Birleşik Krallık Hükümeti (UK)'ne aittir.
- İş süreci odaklıdır.
- Kalite ve bütünsel bir yaklaşımı vardır. Bu yüzden kurumun bütünüyle ne tip bir iş yaptığını anlayıp iş süreçlerine değer katmayı hedefler.
- Uluslarası olarak kullanılır ve kabul edilmiştir.

[39] Sophie Danby, The ITIL 4 Service Value System Explained, https://itsm.tools/the-itil-4-service-value-system-explained/ (Erişim tarihi:06.01.2021)

- Satıcıya göre taraflı değildir; ITIL servis yönetimi uygulamaları, herhangi bir teknoloji platformu veya endüstri tipine göre oluşturulmadığı için, bütün kurumlara uygulanabilir.
- Kural dayatmaz; ITIL adapte edilebilen, olgun ve test edilmiş iyi uygulamaları barındırır ve bu uygulamalar her türlü kuruma uygulanabilir. Bu özelliği sayesinde kamu, özel sektör, iç ve dış servis sağlayıcılar, küçük, orta, büyük ölçekli kurumlar ve her türlü teknolojik süreçleri barındıran ortamda hala kullanışlı ve kabul görmüş durumdadır.
- Kabul edilmiş en iyi uygulamalar bütünüdür.

2.3.5. ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Standardı

ISO 27001 Bilgi Güvenliği Yönetim Standardı, İngiliz Standartlar Enstitüsü (British Standards Institute) tarafından yayınlanmış bir standarttır. İlk olarak BS 7799 (Security Management Standard) adı ile 1995 yılında BSI tarafından yayınlanmıştır. Daha sonra 2000 yılında ISO (Uluslararası Standartlar Organizasyonu) tarafından bünyesine alınarak ISO / IEC17799 adını almıştır. Son olarak 2005 yılında revize edilerek kurumların bilgi varlıklarının güvenliğine odaklanan ISO 27000 ailesine katılarak ISO 27001 adını almıştır. ISO 27001'in en güncel versiyonu ISO / IEC 27001:2013 adlı, 2013 yılında yayınlanmış, ardından 2017 yılında güncellenmiş versiyonudur.

ISO 27001, kurumların bilgi güvenliği yönetimi süreçlerinin oluşturulması, kurumların veri güvenliğine ilişkin risklerin en aza indirgenmesi faaliyetlerinin tayin edilmesi ve kurumun bilgi güvenliğini ciddiye aldığının bir ifadesi olması sebepleri ile düzenleyici makamlar tarafından kabul görmüştür.

Bilgi güvenliği yönetim sistemi (BGYS) kurumlarda bir proje değil bir program olarak yapılandırılmıştır. BGYS programı, bilgi güvenliğine ilişkin risklerin belirlenmesi, iletilmesi ve çözülmesi için kullanılan aktiviteler bütünüdür. BGYS programı kontroller, uygulamalar ve süreçler içermektedir. Bu sayede BT fonksiyonlarının

tehditlere ve değişsen koşullara karşı adaptasyonunu artırır ve risklerin ortaya çıkarılıp etkili bir biçimde yönetilmesini sağlar.

Bilgi güvenliği programları, bahsedilen çerçevelerde olduğu gibi hem BT stratejisini hem de kurumun genel stratejisini desteklemeyi hedeflemektedir. ISO 27001, bilgi güvenliği yönetim sistemi oluşturulması için gerekenleri ve adımları belirler. ISO 27001 bir çerçeve veya en iyi uygulama değildir. ISO 27001 bir standarttır ve kurumlar ISO 27001 uyumlarını kanıtlayarak sertifikasyon sahibi olabilmektedirler. Bu anlamda özellikle ülkemizde kurumlar etkin bir bilgi güvenliği yapısı oluşturmak ve müşteri, iş ortağı, çalışan ve devlet nazarında yetkinliğini kanıtlamak için bu sertifikalandırma sürecini gerçekleştirirler. ISO 27001 BGYS kurmak ve ISO 27001 belgesinin alınması zorunluluğu kamu ve özel sektör olarak incelenebilir.

ISO 27001 belgesinin alınması zorunlu olan özel sektör kuruluşları kısaca aşağıdaki kuruluşlardır.

- Bilişim sektöründe faaliyet gösteren ve kamu ihalelerine giren yazılım, donanım ve entegratör firmalar,
- Elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten firmalar,
- Petrol, elektrik, doğalgaz piyasasındaki lisans gerektiren enerji sektöründeki firmalar,
- E-fatura özel entegratör yetkisi almak isteyen firmalar,
- Gümrük işleri kolaylaştırma yetkisi almak isteyen ihracatçı firmalar
- Görev sözleşmesi imzalayan firmalar şirketler,
- İmtiyaz sözleşmesi imzalayan firmalar şirketler,
- İnternet servis sağlayıcıları,
- Sabit telefon hizmeti firmalar şirketler,
- Altyapı işletmeciliği hizmeti veren firmalar şirketler,
- GMPCS mobil telefon hizmeti veren firmalar şirketler,
- Uydu haberleşme hizmeti veren firmalar şirketler,
- Sanal mobil şebeke hizmeti firmalar şirketler,
- Hava taşıtlarında GSM 1800 mobil telefon hizmeti veren firmalar şirketler,

ISO 27001 bütün dünyada bilgi güvenliği ve risk yönetimi alanında kabul görmüş uluslararası bir standarttır. İki bölüme ayrılmıştır, bu bölümler 10 maddeden oluşan Genel gereklilikler ve A5'ten A18'e farklı kontrol noktalarını içeren EK-A'dır. Genel gereklilikler bölümü kuruma ilişkin yönetişimsel yaklaşımların ele alındığı ve yönetsel kontrollerin kapsamda olduğu bölümlerdir. ISO 27001 standardının EK-A bölümünde bulunan 14 ana maddesi ISO/IEC 27002:2013 (Code of practice for information security controls) standardında detaylandırılmıştır. ISO 27002, bilgi güvenliği kontrolleri için uygulama kodu başlıklı bir bilgi güvenliği standardıdır. Kurumlar ISO 27001 kurulum süreçlerinde standardın daha iyi anlaşılması ve uygulanması için teknik detayların mevcut olduğu ISO 27002 standardını kaynak olarak kullanırlar. ISO 27000 ailesi standartları bilgi güvenliği konseptini farklı başlıklarda ele alarak bir bütünü oluştururlar.

ISO 27001 Genel Gereklilikler bölümünde kurumların yönetişim yaklaşımlarını şekillendirmeyi hedeflemektedir.

Genel Gereklilikler:

- Kuruluşun Bağlamı; kurumun altyapısı ve süreçleri hakkında bilgi edinme ve kapsamın belirlenmesi,
- Liderlik; üst yönetim tarafından bilgi güvenliği yönetim programının desteklenmesi,
- Planlama; bilgi güvenliği sisteminin etkili bir biçimde uygulanabilmesi için gereken planın yapılması, yol haritası oluşturulması
- Destek; bilgi güvenliği sisteminin etkili bir biçimde uygulanabilmesi için kurum içi farkındalık yaratma, kurum içi yönetişime destek verme,
- İşletim; risk analizi ile kurumun maruz kaldığı risklerin belirlenmesi, risklerin iyileştirilmesi,
- Performans Yönetimi; ISO 27001 bilgi güvenliği yönetim sisteminin izlenmesi, analizi ve değerlendirilmesi,
- Yönetim Gözden Geçirme; bilgi güvenliği yönetim sisteminin etkili bir biçimde uygulanması ve işletilmesi için planlanmış gözden geçirme değerlendirmelerinin üst yönetim ile gerçekleştirilmesi, başlıklarını içerir.

Tablo 2.6 ISO 27001 Genel Gereklilikler

ISO 27001 GENEL GEREKLİLİKLER			
4	**Kuruluşun bağlamı**	**5**	**Liderlik**
4.1	Kuruluşun ve bağlamının anlaşılması	5.1	Liderlik ve bağlılık
4.2	İlgili tarafların ihtiyaç ve beklentilerinin anlaşılması	5.2	Politika
4.3	Bilgi güvenliği yönetim sisteminin kapsamının belirlenmesi	5.3	Kurumsal roller, sorumluluklar ve yetkiler
4.4	Bilgi güvenliği yönetim sistemi		
6	**Planlama**	**8**	**İşletim**
6.1	Risk ve fırsatları ele alan faaliyetler	8.1	İşletimsel planlama ve kontrol
		8.2	Bilgi güvenliği risk değerlendirme
6.2	Bilgi güvenliği amaçları ve bu amaçları başarmak için planlama	8.3	Bilgi güvenliği risk işleme
7	**Destek**	**9**	**Performans değerlendirme**
7.1	Kaynaklar	9.1	İzleme, ölçme, analiz ve değerlendirme
7.2	Yeterlilik	9.2	İç tetkik
7.3	Farkındalık	9.3	Yönetimin gözden geçirmesi
7.4	İletişim	**10**	**İyileştirme**
7.5	Yazılı bilgiler	10.1	Uygunsuzluk ve düzeltici faaliyet
		10.2	Sürekli iyileştirme

Kaynak: https://www.iso.org/standard/54534.html[40]

[40] ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements.
https://www.iso.org/standard/54534.html
(Erişim tarihi: 05.01.2021)

EK-A:[41]

ISO 27001 EK-A içerisinde toplam 14 kontrol seti bulunmaktadır. Bunlar genel özellikleriyle aşağıdaki gibidir:

- A.5 Bilgi Güvenliği Politikaları

  Toplam 2 kontrol içermektedir. Politikaların, kurumun bilgi güvenliği uygulamaları ile uyumlu olarak hazırlandığını ve gözden geçirildiğini kontrol eder.

- A.6 Bilgi Güvenliği Organizasyonu

  Toplam 7 kontrol içermektedir. A. 6.1 ve A.6.2 olmak üzere iki bölümden oluşmaktadır. İlk bölümde bilgi güvenliği uygulamalarının oluşturulabileceği ve yönetilebileceği bir çerçeve olup olmadığını kontrol eder. İkinci bölümde mobil cihazlar ve uzaktan çalışma kavramlarını kontrol eder.

- A.7 Personel Güvenliği

  Toplam 6 kontrol içermektedir. Çalışanlar ve sözleşmeli personelin sorumluluklarını anlamasını kontrol eder. A.7.1, A.7.2 ve A.7.3 olmak üzere üç bölümden oluşmaktadır. Kurumlarda genellikle insan kaynakları işbilimleri ile yürütülen çalışmalardır. Çalışan ve sözleşmeli personelin kişisel veri güvenliğinin sağlanması anlamında oldukça önemli kontrollerdir.

- A.8 Varlık Yönetimi

  Toplam 10 kontrolden oluşmaktadır. Kurumun bilgi varlıklarını nasıl belirlediğini ve bunları korumak için uygun önlemler alınıp alınmadığını kontrol eder. A.8.1, A.8.2 ve A.8.3 olarak üç bölümden oluşmaktadır. Veri

[41] ISO 27001: The 14 control sets of Annex A explained, 2020. https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained (Erişim tarihi: 06.01.2021)

envanterlerinin oluşturulması, süreç haritalarının oluşturulması ve veri yaşam döngüsünün yönetilmesi gibi ana faaliyetlere kaynaklık eden oldukça önemli kontrollerdir.

- A.9 Erişim Kontrolü

  Toplam 14 kontrolden oluşmaktadır. Çalışanların sadece kendi görev ve sorumlulukları ile ilgili bilgiye erişebilirliğini kontrol eder. A.9.1, A.9.2, A.9.3 ve A.9.4 olarak dört bölümden oluşmaktadır.

- A.10 Kriptografi

  Toplam 2 kontrolden oluşmaktadır. Veri şifreleme ve hassas verinin yönetimini kontrol eder. Veri güvenliği, ağ yönetimi ve internet güvenliği, bulut bilişim güvenliği, mobil cihaz güvenliği, sunucu güvenliği gibi birçok kontrol başlığını kapsar.

- A.11 Fiziksel ve Çevresel Güvenlik

  Toplam 15 kontrolden oluşmaktadır. A.11.1 ve A.11.2 olarak iki bölümden oluşur. İlk bölüm hassas verinin saklandığı alanlara fiziksel erişim, ikici bölüm ise kurum içinde kullanılan ekipmanı kontrol eder. ISO 27001'in ana ve değişmez kontrol hedefleri arasındadır.

- A.12 Operasyon Güvenliği

  Toplam 14 kontrolden oluşmaktadır. Bilginin işlendiği ortamların güvenliğini kontrol eder. A.12.1, A.12.2, A.12.3, A.12.4, A.12.5, A.12.6 ve A.12.7 olarak yedi bölümden oluşur. ISO 27001'in geniş kontrol maddesidir. Dijitalleşme sürecinin kurumsal bilişim ortamlarında gereken tüm güvenlik gereksinimini kontrol eder. Değişiklik yönetimi, yedekleme yönetimi, teknik zafiyetlerin değerlendirilmesi gibi önemli kontrolleri kapsar.

- A.13 İletişim Güvenliği

  Toplam 7 kontrolden oluşmaktadır. Kurumun ağ yapısı üzerinde veriyi nasıl koruduğunu kontrol eder. A.13.1 ve A.13.2 olarak iki bölümden oluşur. Verinin transferi sürecinde gereken güvenlik kontrollerini ve gizlilik anlaşmalarını kontrol eder.

- A.14 Sistem Edinimi Geliştirilmesi ve Bakımı

  Toplam 13 kontrolden oluşmaktadır. Yazılım geliştirme ve uygulama adımlarında güvenliğin kontrol edilmesi başlıklarını kapsar. A.14.1, A.14.2 ve A.14.3 olarak üç bölümden oluşur.

- A.15 Tedarikçi İlişkileri

  Toplam 5 kontrolden oluşmaktadır. Üçüncü taraflar ile kurum arasındaki sözleşmelerinin kontrolü ve gerekli bilgi güvenliği performans değerlendirmelerinin gerçekleştirilmesi başlıklarını kapsar. A.15.1 ve A.15.2 olarak iki bölümden oluşur.

- A.16 Bilgi Güvenliği Olay Yönetimi

  Toplam 7 kontrolden oluşmaktadır. Güvenlik ihlal olaylarının nasıl yönetildiği ve raporlandığını kontrol eder. Yapısı ve yaklaşımı itibari ile KVK Kanunu ihlal bildirimleri gereksinimlerinin kurum içi boyutta sağlanmasına benzemektedir.

- A.17 İş Sürekliliği Yönetiminde Bilgi Güvenliği Hususları

  Toplam 4 kontrolden oluşmaktadır. İş sürekliliğinin sağlanmasına ilişkin alınan önlemleri ve yapılan planlamayı kontrol eder. A17.1 ve A.17.2 olarak iki bölümden oluşur.

- A.18 Uyum

  Toplam 8 kontrolden oluşmaktadır. Kurumun tabi olduğu kanun ve regülasyonları ve bu regülasyonlar ile uyumu kontrol eder. Özellikle 18.1.4 kontrol maddesi 'Kişisel Bilginin Mahremiyeti ve Korunması' KVK Kanunu kapsamını en yakından destekleyen standart ifadesidir.

Kontrol setlerinin içeriği Tablo 2.7'de incelenecektir.

Tablo 2.7 ISO 27001 Ek-A Kontrolleri

ISO 27001:2013 Ek-A Kontroller		
Ek-A Referans No		**Kontrol Hedefi**
5. Bilgi Güvenliği Politikaları	**5.1**	**Bilgi Güvenliği için Yönetim Yönlendirmesi**
	5.1.1	Bilgi Güvenliği Politikası
	5.1.2	Bilgi Güvenliği Politikasının Gözden Geçirilmesi
6. Bilgi Güvenliği Organizasyonu	**6.1**	**Kurum İçi Organizasyon**
	6.1.1	Bilgi Güvenliği Rol ve Sorumlulukları
	6.1.2	Görevler Ayrılığı
	6.1.3	Yetkili Taraflarla İletişim
	6.1.4	Uzmanlık Grupları ile İletişim
	6.1.5	Proje Yönetiminde Bilgi Güvenliği
	6.2	**Taşınabilir Cihazlar ve Uzaktan Çalışma**
	6.2.1	Taşınabilir Cihaz Politikası
	6.2.2	Uzaktan Çalışma
7. Personel Güvenliği	**7.1**	**İşe Almadan Önce**
	7.1.1	İnceleme
	7.1.2	İşe Alma Şart ve Koşulları
	7.2	**Çalışma Boyunca**
	7.2.1	Yönetimin Sorumlulukları
	7.2.2	Bilgi Güvenliği Farkındalığı ve Eğitim

	7.2.3	Disiplin Süreci
	7.3	**Görev Değişikliği ve İşten Ayrılma**
	7.3.1	Görev Değişikliğinde veya İşten Ayrılmada Sorumluluklar
8. Varlık Yönetimi	**8.1**	**Varlıklarla İlgili Sorumluluklar**
	8.1.1	Varlık Envanteri
	8.1.2	Varlıkların Sahipleri
	8.1.3	Varlıkların Kabul Edilebilir Kullanımı
	8.1.4	Varlıkların İadesi
	8.2	**Bilgi Sınıflandırması**
	8.2.1	Bilginin Sınıflandırılması
	8.2.2	Bilginin İsimlendirilmesi
	8.2.3	Bilginin İşlenmesi
	8.3	**Medya Kullanımı**
	8.3.1	Çıkartılabilir Medyanın Yönetimi
	8.3.2	Medyanın İmhası
	8.3.3	Fiziksel Medya Transferi
9. Erişim Kontrolü	**9.1**	**Erişim Kontrolü için İş Gereksinimleri**
	9.1.1	Erişim Kontrol Politikası
	9.1.2	Ağlara ve Ağ Hizmetlerine Erişim
	9.2	**Kullanıcı Erişim Yönetimi**
	9.2.1	Kullanıcının Kaydedilmesi ve Silinmesi
	9.2.2	Kullanıcı Erişim Konfigürasyonu
	9.2.3	Ayrıcalıklı Erişim Haklarının Yönetimi
	9.2.4	Kullanıcıların Gizli Kimlik Doğrulama Bilgilerinin Yönetimi
	9.2.5	Kullanıcı Erişim Haklarının Gözden Geçirilmesi
	9.2.6	Erişim Haklarının Kaldırılması ya da Değiştirilmesi
	9.3	**Kullanıcının Sorumlulukları**
	9.3.1	Gizli Kimlik Doğrulama Bilgisinin Kullanımı
	9.4	**Sistem ve Uygulama Erişim Kontrolü**
	9.4.1	Bilgiye Erişimin Sınırlandırılması
	9.4.2	Güvenli Oturum Açma Prosedürleri

	9.4.3	Şifre Yönetim Sistemi
	9.4.4	Ayrıcalıklı Destek Programlarının Kullanımı
	9.4.5	Program Kaynak Kodlarına Erişimin Kontrolü
10. Kriptografi	**10.1**	**Kriptografik Kontroller**
	10.1.1	Kriptografik Kontrollerin Kullanımına Yönelik Politika
	10.1.2	Anahtar Yönetimi
11. Fiziksel ve Çevresel Güvenlik	**11.1**	**Güvenli Alanlar**
	11.1.1	Fiziksel Güvenlik Parametreleri
	11.1.2	Fiziksel Erişim Kontrolleri
	11.1.3	Ofislerin, Odaların ve Tesislerin Güvenliğinin Sağlanması
	11.1.4	Dışarıdan ve Çevresel Tehditlere Karşın Koruma
	11.1.5	Güvenli Alanlarda Çalışma
	11.1.6	Dağıtım ve Yükleme Alanları
	11.2	**Ekipman**
	11.2.1	Ekipmanların Yerleştirilmesi ve Korunması
	11.2.2	Destek Ekipmanları
	11.2.3	Kablolama Güvenliği
	11.2.4	Ekipmanların Bakımı
	11.2.5	Varlıkların Kaldırılması
	11.2.6	Bina Dışındaki Ekipmanların ve Varlıkların Güvenliği
	11.2.7	Ekipmanların Güvenli İmhası ya da Tekrar Kullanımı
	11.2.8	Gözetimsiz Kullanıcı Ekipmanı
	11.2.9	Temiz Masa, Temiz Ekran Politikası
12.Operasyon Güvenliği	**12.1**	**Operasyonel Prosedürler ve Sorumluluklar**
	12.1.1	Dokümante Edilmiş Operasyonel Prosedürler
	12.1.2	Değişiklik Yönetimi
	12.1.3	Kapasite Yönetimi

	12.1.4	Geliştirme, Test ve Operasyonel Ortamların Ayrıştırılması
	12.2	**Zararlı Yazılımlardan Korunma**
	12.2.1	Zararlı Yazılımlara Karşı Kontroller
	12.3	**Yedekleme**
	12.3.1	Bilginin Yedeklenmesi
	12.4	**Kayıtların Tutulması ve İzleme**
	12.4.1	Olay Kayıtlarının Tutulması
	12.4.2	Kayıt Bilgilerinin Korunması
	12.4.3	Yönetici ve Operatörlerin Yaptıkları İşlemlerin Kayıtları
	12.4.4	Sistem Saati Senkronizasyonu
	12.5	**Operasyonel Yazılımların Kontrolü**
	12.5.1	İşletim Sistemlerine Yazılımların Yüklenmesi
	12.6	**Teknik Zafiyetlerin Yönetimi**
	12.6.1	Teknik Zafiyetlerin Yönetilmesi
	12.6.2	Yazılım Yükleme Konusunda Kısıtlamalar
	12.7	**Bilgi Sistemleri Denetimi Hususları**
	12.7.1	Bilgi Sistemleri Denetim Kontrolleri
13. İletişim Güvenliği	**13.1**	**Ağ Güvenlik Yönetimi**
	13.1.1	Ağ Kontrolleri
	13.1.2	Ağ Hizmetlerinin Güvenliği
	13.1.3	Ağların Ayrıştırılması
	13.2	**Bilgi Transferi**
	13.2.1	Bilgi Transferi Politika ve Prosedürleri
	13.2.2	Bilgi Transferine Yönelik Anlaşmalar
	13.2.3	Elektronik Mesajlaşma
	13.2.4	Gizlilik Anlaşmaları
14. Sistem Edinimi, Geliştirilmesi ve Bakımı	**14.1**	**Bilgi Sistemleri Güvenlik Gereksinimleri**
	14.1.1	Bilgi Güvenliği Gereksinimleri Analizi ve Spesifikasyonu
	14.1.2	Açık Ağlarda Uygulama Servislerinin Güvenliğinin Sağlanması

	14.1.3	Uygulama Servislerindeki İşlemlerin Korunması
	14.2	**Geliştirme ve Destek Süreçlerinde Güvenlik**
	14.2.1	Güvenli Yazılım Geliştirme Politikası
	14.2.2	Sistem Değişiklik Kontrol Prosedürleri
	14.2.3	İşletim Sistemi değişiklerinin ardından uygulamaların teknik olarak gözden geçirilmesi
	14.2.4	Yazılım Paketlerinde Yapılacak Değişikliklerin Kısıtlanması
	14.2.5	Güvenli Sistem Mühendisliği Prensipleri
	14.2.6	Güvenli Yazılım Geliştirme Ortamı
	14.2.7	Dış Kaynaklı Yazılım Geliştirme
	14.2.8	Sistem Güvenlik Testleri
	14.2.9	Sistem Kabul Testleri
	14.3	**Test Verisi**
	14.3.1	Test Verisinin Korunması
15. Tedarikçi İlişkileri	**15.1**	**Tedarikçi İlişkilerinde Bilgi Güvenliği**
	15.1.1	Tedarikçi İlişkileri için Bilgi Güvenliği Politikası
	15.1.2	Tedarikçi Sözleşmelerinde Güvenlikle Konuları
	15.1.3	Bilgi ve İletişim Teknolojisi Tedarik Zinciri
	15.2	**Tedarikçi Hizmet Sunumu Yönetimi**
	15.2.1	Tedarikçi Hizmetlerinin İzlenmesi ve Gözden Geçirilmesi
	15.2.2	Tedarikçi Hizmetlerindeki Değişikliklerin Yönetimi
16. Bilgi Güvenliği Olay Yönetimi	**16.1**	**Bilgi Güvenliği Olaylarının Yönetimi ve İyileştirmeler**
	16.1.1	Sorumluluklar ve Prosedürler

	16.1.2	Bilgi Güvenliği Olaylarının Raporlanması
	16.1.3	Bilgi Güvenliği Zayıflıklarının Raporlanması
	16.1.4	Bilgi Güvenliği Olaylarının Değerlendirilmesi ve Kararı
	16.1.5	Bilgi Güvenliği Olaylarının Cevaplanması
	16.1.6	Bilgi Güvenliği Olaylarından Öğrenilenler
	16.1.7	Kanıtların Toplanması
17. İş Sürekliliği Yönetiminde Bilgi Güvenliği Hususları	**17.1**	**Bilgi Güvenliği Sürekliliği**
	17.1.1	Bilgi Güvenliği Sürekliliğinin Planlanması
	17.1.2	Bilgi Güvenliği Sürekliliğinin Uygulanması
	17.1.3	Bilgi Güvenliği Sürekliliğinin Doğrulanması, Gözden Geçirilmesi ve Değerlendirilmesi
	17.2	**Yedeklilik**
	17.2.1	Bilgi İşleme Altyapısının Erişilebilirliği
18. Uyum	**18.1**	**Yasal ve Sözleşmelerden Kaynaklanan Gereksinimlere Uyum**
	18.1.1	Uygulanabilir Yasal ve Sözleşmelerden Kaynaklanan Gereksinimlerin Tanımlanması
	18.1.2	Fikri Mülkiyet Hakları
	18.1.3	Kayıtların Korunması
	18.1.4	Kişisel Bilginin Mahremiyeti ve Korunması
	18.1.5	Kriptografik Kontrol Mevzuatı
	18.2	**Bilgi Güvenliği Gözden Geçirmeleri**
	18.2.1	Bilgi Güvenliğinin Bağımsız Gözden Geçirmesi
	18.2.2	Güvenlik Politikalarına ve Standartlara Uyum
	18.2.3	Teknik Uyum Gözden Geçirmeleri

2.3.6. Küresel Standart, Çerçeve ve En İyi Uygulamaların Farkları

Çalışmada bahsedilen küresel standart, çerçeve ve en iyi uygulama tanımlarına destekle, standartlar akredite kurumlar tarafından onaylanmalıdır. Kurumlar ISO 27001 gibi bir standarda göre denetlenebilir ve standarda uyumları tasdiklenebilir/ sertifika alabilirler. Fakat En iyi uygulamalar yine tanımından da anlaşılacağı gibi daha önce başarısı test edilmiş faaliyet ve süreçlerdir. ITIL gibi en iyi uygulamalara uyumluluk çalışmaları sonucunda sertifika sahibi olunmayacaktır, uyumluluk kurum içerisindeki süreçlerin ve servislerinin daha iyi hale gelmesini amaçlar. En iyi uygulamalar kurum geneline odaklanmaktan çok spesifik faaliyet ve süreçlere odaklanırlar. Ve son olarak COBIT gibi yönetişim çerçeveleri ise en iyi uygulamaya daha yakın olup, daha genel ve kurumunun bütününü ele alır. Yönetişim çerçevesinin amacı neyin yapılması gerektiğini ortaya koymak ve bir yol haritası oluşturmaktır. Kısaca Yönetişim çerçevesi yol haritasını çizerken en iyi uygulamalar, bunlara nasıl ulaşılacağını detaylandırır.

Dünya da birçok standart, çerçeve ve en iyi uygulamalar bulunmaktadır ve bunlar farklı sektörler içerisinde kullanılmaktadır. Bu çalışmada BT yönetişim alanında ülkemizde en yaygın olarak kullanılan ISO 27001, COBIT, NIST ve ITIL incelenmiştir.

2.3.7. Küresel Standart, Çerçeve ve En İyi Uygulamaların Veri Güvenliği ile İlişkisi

BT denetimi, bilgi teknolojileri altyapı ve süreçlerinin kendilerinden beklenen faydaları sağlayıp sağlayamayacaklarına dair güvence sağlamayı hedefler. Bu faydalar; etkililik, yani iş ihtiyaçlarını karşılama gücü; etkinlik, yani kaynakların verimli kullanımı; güvenlik, yani bilgi varlıklarının gizlilik, bütünlük ve sürekliliğinin korunması ve bu faydaların türevleri olan güvenilirlik ve yasalara uyumdur. Dünya'da BT denetimine yönelik yasalar, yönetmelikler, rehber niteliğinde standartlar ve geniş kapsamlı çerçeveler incelendiğinde Bilgi Sistemleri Denetimi kavramı için çeşitli tanımlamalar ve uygulamalar görülmekle birlikte, bilgi sistemleri denetiminin ağırlıklı

olarak özerk bir süreçten ziyade, bütünleşik denetim süreci dâhilinde değerlendirildiği görülmektedir.

Risk yönetimi çalışmada bahsedildiği gibi riskin belirlenme, değerlendirme ve aksiyon alınması sürecini tanımlamaktadır. Riski yönetebilir kılmak için, kurumlar riskin gerçekleşme olasılığı ve potansiyel etkisini iyi bir şekilde anlamalıdırlar. Bu bilgi ile kurumlar hedeflerine ulaşma yolunda kabul edebilecekleri risk miktarını belirleyebilir ve bunu risk iştahı olarak adlandırabilirler. Risk iştahının ve risk toleransının anlaşılması, kurumların siber güvenlik aktivitelerini önceliklendirmelerini, siber güvenlik yatırımları konusunda daha net kararlar alabilmelerini sağlayabilecektir. Risk yönetim programlarının oluşturulması kurumların siber güvenlik programlarında iyileştirme yapmalarını da desteklemektedir.

Kurumlar riskleri farklı şekillerde yönetebilirler. Bahsedilen standart, çerçeve ve en iyi uygulamalar kurumların risk yönetimi süreçleri ile ortak hareket ederek veri güvenliği ve siber güvenlik konularında doğru kararlar alabilmeleri ve bu kararları doğru bir şekilde önceliklendirmelerini sağlamaktadır. Standart, çerçeve ve en iyi uygulamalar tekrarlanan risk değerlendirmeleri ve iş süreçleri açısından itici etkenlerin tanımlanması ve doğrulanmasını destekler. Bu nedenle kurumlara veri güvenliğini sağlama konusunda büyük bir destek oluştururlar. Kurumlara veriye ilişkin riskleri saptamaları, değerlendirmeleri ve kontrol altına almaları için yardım ederler. Bahsedilen standart, çerçeve ve en iyi uygulamalar kurumlara adapte edilebilen risk bazlı uygulamalara sahip oldukları için çok geniş yelpazede ve değişik tip sektörlerde kullanılabilir haldedirler. Bugüne yüzümüzü çevirdiğimizde, veri güvenliğini direkt ve dolaylı ilgilendiren tüm mevzuatların bu standart, çerçeve ve en iyi uygulamalardan alıntılar ile desteklendiği ve yakınsandığı görülmektedir.

ÜÇÜNCÜ BÖLÜM

RİSK TABANLI KÜRESEL STANDART, ÇERÇEVE VE EN İYİ UYGULAMA YAKLAŞIMLARININ VERİ GÜVENLİĞİ BAKIMINDAN HUKUKA UYUM VE MEVZUAT İLİŞKİSİ

3.1 VERİ GÜVENLİĞİ AÇISINDAN TEKNOLOJİ, HUKUK VE UYUM İLİŞKİSİ

3.1.1. Uyum Yaklaşımları

3.1.1.1. Yönetişim Kavramı ve BT Yönetişimi İlişkisi

Son yıllarda yaşanan uluslararası teknolojik travmalar, büyük kurumlarda görülen veri kayıpları, bulut bilişim ve büyük veri gibi büyük hacimde değerli verinin bir arada bulundurulması, kurumların uluslararası platformlarda rekabet gücünü ve itibarını attırmak istemesi, daha güvenilir ve sağlam kurumlar haline gelebilmesi kurumsal yönetişim anlayışını hayatımıza kazandırmıştır. Yönetişim kavramı, yönetim kavramının tek başına yeterli verimliliği artık sağlamadığı görüşü ile hayatımıza girmiştir. Yönetişim, yönetim ve iletişim kelimelerinden türetilmiş olup, etkileşimin olduğu bir süreci temsil eder. Bu sayede kurumlar yönetim modeli anlayışını hiyerarşik olarak sürdürseler bile, paydaşlık çerçevesinde iş yapış modelini paralel bir yapılandırma ile her katmana yaymayı amaçlamaktadırlar. Yönetişim (governance) ile yenilikçi, hesap verebilir, cevap verebilir, şeffaf bir yapı hayal edilmiştir. Profesyonel hayatta yönetim kadrolarının görünmez odalarının camdan kapılara, operasyon ekiplerinin açık ofislere geçişi ile de bu görüşle desteklenen fikri günlük yaşama adapte edilmiştir. BT yönetişimi, BT'nin ve veri güvenliğinin yönetimini iyileştirmeyi ve bilgi teknolojilerine ayrılan finansal yatırımdan daha yüksek değer elde etmeyi amaçlayan bir kurumsal yönetişim unsurudur. BT fonksiyonunun etkin, kontrollü ve sürekli iyileştirme hedefli ile çalışmasını tanımlayan ve sağlayan bir kurallar, düzenlemeler ve politikalar bütünüdür. Bir BT yönetişim çerçevesi, kuruluşların BT

risklerini etkin bir şekilde yönetmelerini sağlar. Küresel standart, çerçeve ve en iyi uygulama örnekleri BT yönetişimin modelini destekler ve risk tabanlı bir denetim ve iyileştirme fırsatı oluşturur. BT yönetişim modeli sayesinde organizasyonel yapı içerisinde BT ve diğer iş kollarının koordine olması ve yeknesak bir risk değerlendirme çalışması yapılması mümkündür. Genel yönetişimin bir parçası olan BT yönetişimi, veri güvenliğini sağlamayı amaçlar ve bu amacı destekler nitelikte, veriye dokunan tüm kullanıcılar risk ve denetim fonksiyonunun bir parçasıdır. ISO 27001, COBIT, NIST, ITIL gibi küresel standart, çerçeve ve en iyi uygulama örnekleri veri güvenliği iyileştirme çabasında risk tabanlı yaklaşımı benimserken, BT yönetişimi kurumsal modelde bu yaklaşımın temsilcisi olmalıdır. BT yönetişiminin kurumlara sağladığı katma değerler;

- Daha geniş iş stratejileri ve hedeflerine karşı ölçülebilir sonuçlar göstermesi,
- Kurumsal olarak ilgili yasal ve düzenleyici yükümlülüklerin yerine getirilmesi,
- Kurumların iş ortaklarına veri güvenliği güvencesi verebilmesi,
- Mevcut teknolojilerin yürürlükteki kanunlarla ilişkisinde kurumsal uyum sağlanması.

Hem kamu hem özel sektör kuruluşlarının başarılı bir veri güvenliği politikası oluşturabilmesi için, kurumsal stratejileri ve hedefleri ile BT fonksiyonlarının aynı doğrultuda buluşması gerekmektedir. Teknoloji sistemlerinin kullanılmadığı bir kurumsal operasyon düşünülemeyeceği ve verinin güvenliğinin ulusal ve uluslararası bir mesele olduğu günümüzde BT yönetişim modelini benimseyerek, uyum süreçlerinin sağlanması en doğru çözüm olacaktır.

3.1.1.2. BT Yönetişimi ve Kurum Yapısı ve Kültürü İlişkisi

Bilişim disiplinin temel kavramları olan veri, enformasyon ve bilgi piramidinde[42]girdi olarak verinin toplanması, depolanması,[43] işlenmesi ve nihayetinde nitelikli bilgiye

[42] Frické, M., The Knowledge Pyramid: A Critique of the DIKW Hierarchy, Journal of Information Science, 35 (2), 2009,131-142.

dönüşümünde iş zekâsı (business intelligence) tekniklerinden de faydalanan enformasyon sistemleri, günümüzde özellikle karar verici yöneticiler açısından doğrudan etkilidir. Bu açıdan bakıldığında bu sistemler, kurum yönetiminde ve dolayısıyla kurum kültüründe önemli rol oynamaktadır.

Bir kurumda kültür kavramı, iş süreçleri ve BT'ye bağlı değişimin başarılı olabilmesi için sıklıkla kritik bir öğe olarak tanımlanmaktadır.[44]

Bireyler, onların değerlerini etkileyen pek çok kültürel gruplara ait olup, çeşitli kimliklere sahiptirler. Dolayısıyla, kültürel bir grupta; tüm grup üyelerinin benzer düşünüp hareket etmelerinin homojen olması mümkün değildir. Söz konusu farklılıklara rağmen, kültürel bir gruptaki üyeler arasındaki ortak özellikler; paylaşılan değerlere dayanmaktadır.

Günümüzde teknoloji birçok iş/süreç probleminin çözümü olarak görülmektedir. Ancak insan faktörünün iş/süreçlerin çözümüm hususunda göz ardı edilmesi kurumların başarısız sonuçlar elde etmesine sebep olmaktadır. Benzer şekilde konulara sadece süreç ve insan faktörü açısından bakılması, olası teknolojilerin göz ardı edilmesi de çözümsüzlüklere yol açmaktadır. İnsan, süreç ve teknolojinin birbiri ile bütünlüğünün sağlanması dünya genelinde uyum çerçevesinde başarıyı getirmektedir.

Kurumların oturmuş yapıları ve kültürlerine uygun olarak birbirinden farklı BT yönetişim modelleri bulunmaktadır. Bu modeller BT birimleri ve ilgili tüm kararların kurumun tepe yönetimi tarafından alındığı iş monarşisi modeli, BT ile ilgili tüm kararların BT'nin yöneticileri tarafından alındığı BT monarşisi modeli, BT ve iş birimlerinin uzlaşmasına dayanan federal model, kurum içi birey ve küçük grupların kendi kararlarını aldıkları anarşi modeli bunların arasında yer alan modellerdir.

Ülkemizde 90'lı yılların ilk yarısına kadar kurumlarda genellikle BT monarşisi modeli uygulanmakta olduğu görülmektedir. Bunun sebebi bu yıllara kadar BT fonksiyonlarının henüz kullanılmaya başlanması ve konu uzmanı olmayan kişiler

[43] Vercellis, C., Business Intelligence: Data Mining and Optimization for Decision Making, John Wiley & Sons Ltd., UK., 2009.
[44] Cooper, R., B., The Inertial Impact of Culture on IT Implementation, Information & Management, 1994, S.27, 17-31.

tarafından anlaşılamamasıdır. Ancak günümüze geldiğimizde BT fonksiyonları kurum genelinde uçtan uca her çalışanın dahil olduğu bir bütün yapı ile sağlanmaktadır. Bu sebeple federal model olarak ifade edilen iş birimleri ile BT birimlerinin uzlaşması yaklaşımı başarılı bir bilgi güvenliği ve teknoloji çatısı kurmanın ana kuralıdır.

BT yönetişimi kurum içinde ve dışında kurum faaliyetlerinden etkilenen tüm tarafları ilgilendiren bir kurumsal olgudur. Bilgi teknolojileri sorumlularının diğer iş birimlerinden bağımsız karar vermesini ve bu bağımsız kararlar sonucu yaşanan başarısızlıkların sorumluğunun tek başına BT yüklenmesi eğiliminden uzaklaşmayı hedefler. Gelişmiş organizasyonlarda bilgi teknolojileri kararlarını üst yönetim ve bilgi teknolojisi birimlerinin ortak almasını sağlayan bir ortam sunar.

BT yönetişiminin temel amacı BT yatırımlarının kurum için değer yaratmasını güvence altına almak ve BT den kaynaklanabilecek riskleri azaltmaktır. Bunu yapmanın en uygun yolu organizasyondaki rollerin veri, iş süreçleri, uygulama ve altyapılarla olan ilişkilerini net bir şekilde tanımlayabilmektir. Böylelikle yatırım öncelikleri kurum hedefleri ile paralellik gösterirken bu hedeflerin bireylere yaygınlaştırılması da kolaylaşır.

Kurumsal bir yönetişim modelini uçtan uca uygulayamayan kurumlar reaktif bir yaklaşım sergileyerek bir uygunsuzluk yaşanması durumunda veya gereksinim acil hale geldiğinde tüm kaynaklarını o yönde seferber ederek plansız ve düzensiz bir ortamda çalışmak durumunda kalır. Bu yöntem ile çalışılması sürekli iyileştirme ve risk analizi yaklaşımından tamamen uzak olup bununla birlikte rekabetçiliğin azalması ve iş kayıpları, artan proje maliyetleri ve uzayan süreler, temel süreçlerin ve kurumsal verimliliğin olumsuz etkilenmesi gibi sonuçlar doğurur. Hâlbuki kurumsal BT yönetişim modeli üst yönetimin desteği ile tüm ilgili taraflara uçtan uca benimsetilir ve kaynakların verimli paylaşıldığı bir ortam sağlanırsa, kurumsal yapı genelinde uyum çerçevesi sağlanacaktır.

BT yönetişiminin tüm kurum genelinde şeffaf bir şekilde izlenebilmesi ve iletişiminin en verimli şekilde sağlanmasında süreç modelleme ve kurumsal mimari araçları ile veri güvenliği teknoloji çözümleri bu konuda en çok yararlanılan teknolojilerin başında gelmektedir.

Kurumların BT yönetişim modelleri, teknoloji bütçeleri, sektörel gereksinimleri, lokasyon bazlı öncelikleri vb. özellikleri farklılık gösterebilmektedir. Tüm bahsedilen kurumsal değişkenler ihtiyaçlar ve güncel şartlara uygun olarak şekillenmektedir. Her değişimde olduğu gibi mevcut yapıya adapte olan çalışanlar tarafından direnç de kaçınılmaz olmaktadır. BT yönetişim modellerinin başarılı olması kurum üst yönetimlerinin bu ihtiyaçların farkına varması ve değişimin başarılı ile tamamlanması için gerekli kararlılık olması ve gereken desteği sağlaması ile mümkündür. Yönetişim kültürünün kurum içinde oluşturulması öncelikle BT birimleri ve iş birimleri arasındaki iletişimin ve fayda ilişkisinin sağlanması ile temellenir. Bu sebeple denetim ve mevzuatlara uyum gibi stratejik kurum faaliyetleri, ancak tüm çalışanları katılımı ve sürekli yönetişim stratejisi algısının benimsetilmesi ile en doğru şekilde sağlanabilir.

3.1.1.3. Yönetişim, Risk ve Uyum (GRC)

Son dönemde yönetişim, risk yönetimi ve uyum fonksiyonlarının bir arada düşünülmesini savunan model, GRC (Yönetişim Risk ve Uyum-Governance Risk Compliance) kısaltmasıyla ifade edilen yeni bir yönetim yaklaşımı olarak ortaya çıkmıştır. "GRC modeli, kurumların farklı fonksiyonlarının faaliyetleriyle ilgili çeşitli faydalar sağlamasına ek olarak, gerekli risk değişkenlerinin belirlenmesini sağlayarak stratejik kararların alınmasında kuruma yol gösterir. GRC yaklaşımının getirdiği bütüncül bakış açısı, ortak paylaşılan güvence evreninden faydalanılması sayesinde iç denetimin diğer güvence çalışanlarının faaliyetleriyle bütünleşmesine ve denetimin daha kolay, planlı, anlaşılabilir ve düşük maliyetle yapılmasına katkı sağlar."[45]

Mevcut regülasyonlar, ortaya çıkan yeni risk faktörleri, değişen kanuni uyum beklentileri söz konusu faaliyetlerin Microsoft Excel veya Access gibi basit ofis programlarıyla takip edilmesini ve ölçülmesini imkânsızlaştırmıştır. Benzer durum KVK Kanunu uyum sürecinde kurumların oluşturması beklenen kişisel veri işleme

[45] Erdoğan, M.,Yönetişim-Risk-Uygunluk Yaklaşımı ve İç Denetim Fonksiyonu İlişkisi: İç Denetim Sorumluluklarının Yaklaşımına Etkisi Üzerine Yapısal Eşitlik Modeli Araştirması, S.2, 2019, S. 149-198

envanteri ya da süreç haritalanması çalışmalarında da görülmüştür. GRC modelinin yazılım çözümleri ile kurumlar, kurumsal tüm faaliyetlere ilişkin veri envanteri, risk analizleri, iç denetim ve performans raporları, ilgili yasal düzenlemeleri veya faaliyet gösterilen sektöre özgü ölçümlemeleri izleyebilmektedir. Riskler, denetim kontrolleri, kanunlar, yönetmelikler, politikalar ve denetim sonuçlarının, risk ve uyum yöneticileri ve çalışanları, iç denetçiler ve işletme üst yönetimi arasındaki işbirliğini kolaylaştıran ortak bir çerçevede ele alınmasını sağlar. Bu sayede kolay raporlanabilir çözümlerin geliştirilmesi ve uygulanmasını kolaylaştırır.

"CRM yazılımları, ortak bir çerçeveye bağlı kalınarak, geleneksel kontrol taksonomisinin ötesinde daha proaktif bir anlayışla geliştirilen kontrollerin, BT ortamında uygulanmasını sağlayan teknolojilerin kullanılabilmesini sağlamaktadır. CRM yazılımlarının sağladığı temel faydalar şunlardır: "[46]

- Görevlerin ayrılığı ilkesine uyumun sağlanması eş zamanlı olarak izlenebilir ve denetimi sağlanır.
- Erişim yönetimi riskleri, şeffaf bir şekilde izlenebilir ve gerekli önleyici kontrol mekanizmaları devreye alınır.
- Merkezileştirilmiş denetim belgelendirmesi yürütülebilir.
- Manuel gerçekleştirilen kontroller otomatikleştirilir.
- Kontrollerin kurumsal yönetişim yapısına yönelik iyileştirilmesini sağlar.
- Kontrol ilkelerine uyumun güvence denetçileri tarafından değerlendirilmesine yardımcı olur.
- Kontrol testleri ve belgelendirmeye yönelik merkezi raporlama altyapısını sunar.
- Birçok iç ve dış faktörden etkilenen uygunluk çerçevesini işletme süreçleriyle bütünleştirir.
- Risklerin anahtar risk göstergeleriyle (key risk indicator-KRI) proaktif olarak izlenmesini sağlar.
- İç denetim, iç kontrol, risk yönetimi, uygunluk, BT ve hukuk fonksiyonları tarafından bilginin değerlendirilmesi süreçlerini bütünleştirir.

[46] Pehlivanlı, D., Yönetişim, Risk ve Uyum. İstanbul: Beta Basım Yayım Dağıtım, 2015.

- Sürekli izleme altyapısı sağlar, geriye dönük ve eş zamanlı kayıt mekanizması sağlar.
- Kontrol testlerinin otomatik ve sürekli yürütülmesini sağlar.
- Kontrol ve iç denetim maliyetlerini, sağladığı bütünleşmeyle azaltır.

Başlıca YRU teknoloji sağlayıcıları ve yazılımları şunlardır: SAP-GRC, RSA Archer-eGRC, Oracle-GRC Manager, MetricStream- MetricStream IT GRC, ProcessGene-GRC, Continuity Partner-TrackMyRisks, ACL-GRC, Parapet-Integrated Risk Management, SAI Global-Compliance 360, IRM Security- SYNERGi GRC Platform, GBTEC, BWise-BWise GRC Platform, Compass IT ComplianceCompass IT GRC, Symmetry-ControlPanelGRC, Software-BIC Cloud GRC, Dion Global Solutions-GRC Enterprise, Risma Systems- GRC Software, SAS Institute-SAS Governance and Compliance Manager, DDi-Tula Oversight, Nasdaq BWise- GRC.

3.2 VERİ GÜVENLİĞİNE İLİŞKİN GÜNCEL DÜZENLEMELER

3.2.1. Veri Güvenliği ve Mevzuat İlişkisi

Verilerin elektronik ortamlarda işlenmesi ve kolayca paylaşılabilmesi, günlük her türlü faaliyetin artık elektronik olarak çözümlenmesi, matbu kağıt devrinden dijital kayıtlara dönüşüm, verinin büyüyerek paradan daha kıymetli hale gelmesi vb. birçok sebeple teknoloji hayatımızın en mahrem noktalarına dahi dokunur hale gelmiştir.

İnternet kullanımının yaygınlaşması, teknolojinin ırk, dil, cinsiyet, etnik köken yaş grubu vb. ayrımcılığa sebep olan her türlü niteliği umursamadan dünyayı saran kolları güncel yasal düzenlemelerle kontrol altına alınmaktadır.

Tüm dünyada olduğu gibi ülkemizde de veri güvenliğinin sağlanması farklı alanları kapsayan mevzuatlar ile düzenlenmektedir. Bu mevzuatlar sektörel ya da tüm sektörleri ortak şekilde ilgilendirir niteliktedir. Veri güvenliği konusu geçmişten günümüze evrilerek artık ulusal ve uluslararası boyutlarda ortak bir noktada buluşma olgunluğundadır. Bu sebeple kanun koyucuların vurguladığı veri güvenliğinin

sağlanması bakımından risk değerlendirme yaklaşımları bütünleşik ve belirli bir nizamda karşımıza çıkmaktadır.

3.2.1.1 Kişisel Verilerin Korunması Kanunu (KVKK) - Teknik ve İdari Tedbirler

Kişisel verilerin korunması hakkı ülkemizde 2010 yılında anayasal teminata bağlanmıştır. Bu tarihe kadar, kişisel veriler daha çok genel hukuki düzenlemelerde yer alan hükümler ile korunmaktaydı. Türk Medeni Kanunu ve Türk Ceza Kanununda kişilik hakkı ile kişisel verilerin korunmasına yönelik hükümler ve yaptırımlar bu düzenlemelere örnek gösterilebilir. 7 Nisan 2016 tarihinde 29677 sayılı karar ile 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) yürürlüğe girmiştir. KVK Kanun ile Türkiye'de kişisel veri olarak değerlendirilen verilerin kullanılması, işlenmesi, paylaşılması, saklanması gibi her türlü veri ilişkili faaliyetin sınırları belirlenmiş ölçüde ve uluslararası standartlara tabi olacak şekilde düzenlenmesi ve güvence altına alınmasını amaçlar. Anayasal bir hak olarak kişisel verilerin korunmasını isteme hakkı bugün sıklıkla hayatımızda karşılaştığımız KVK Kanunu önemini vurgular niteliktedir.

Kişisel veriler kamu kurumları ve özel kuruluşlar tarafından işlenmekte ve KVKK Kanunu uygulamaya girinceye kadar bu konuda herhangi bir kısıtlama olmamıştır. Anayasal bir hak olarak kişisel verilerin korunması farklı gerekliliklerin sonucunda yürürlüğe girmiştir.

- Teknolojik Sebepler
- Hukuki Sebepler
- Siyasi Sebeple
- Ekonomik Sebepler

Kişisel veriler yalnızca KVK Kanunu yürürlüğe girdikten sonra değil, günümüze gelinceye dek farklı yöntemlerle işlenmeye devam edilmiştir. Bu sebeple KVK Kanunun yürürlüğe girmesinden sonra ülkemizde genel adaptasyonu ilk aşamada çok kolay olmamıştır. Bugüne geldiğimizde teknolojinin ulaşmış olduğu nokta, internet

kullanımının yaygınlaşması ve dijitalleşme akımı kişisel verilerin bilişim ortamlarında hareket edebilirliğini kolaylaştırmış, bu da verileri tehditlere açık hale getirmiştir. Kanunun yürürlüğe girmesindeki etmenlerden belki de önemlisi olan teknolojik sebepler, kişisel verinin yaşam döngüsünü kolaylaştırdığı gibi, güvenliğine ilişkin risklerin de artmasına sebep olmuştur.

Kişisel verilerin korunmasına ilişkin düzenlemelerde, verilerle ilgili yapılan işlemlerin kişisel verinin bir insan hakkı olması kaydıyla uyulması gereken ortak ilkeler belirlenmiştir.

- "Hukuka ve dürüstlük kuralına uygun olma,
- Doğru ve gerekli ise güncel olma,
- Belirli, açık ve meşru amaçlar için işlenme,
- Kişisel verilerin, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması,
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme, "

KVK Kanunu ilkeleri, kişisel verilerin belirli bir amaç dâhilinde, gerekli bilgilendirmeler ilgili taraflara yapılarak, gerekli ise açık rıza alınarak, ihtiyaç olan bilgi ile sınırlandırılmış kadar verinin belirlenen sürede güvenli bir şekilde muhafaza edilmesi esasına dayalıdır.

KVK Kanunu ile belirlenen bazı tanımlar:

Kişisel veri: Kimliği belirli ya da belirlenebilir nitelikteki gerçek kişiye ilişkin her türlü bilgidir.

Özel Nitelikli Kişisel Veri (Hassas Veri): Özel nitelikli kişisel veriler, işlenmeleri halinde ilgili kişilerin mağdur olmasına veya ayrımcılığa maruz kalmasına neden olma riski taşıyan verilerdir. Kanunun 6. maddesi gereğince özel nitelikli kişisel veriler; "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı,

ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileridir.

"Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder. Bu kişiler, gerçek kişiler olabileceği gibi, kamu kurumları, şirketler, dernekler veya vakıflar gibi tüzel kişiler de olabilecektir.

Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak, onun adına kişisel verileri işleyen gerçek veya tüzel kişilerdir. Bu kişiler veri sorumlusunun kişisel veri işlemek üzere yetkilendirdiği ayrı bir gerçek veya tüzel kişi de olabilir.

Açık rıza: Belirli bir konuya ilişkin bilgilendirilmeye dayanan ve özgür irade ile açıklanan rızadır. Başka bir ifade ile ilgili kişinin verilerinin işlenmesine özgürce, konu hakkında yeterli bilgi sahibi olarak ve sadece o işlemle sınırlı kalmak kaydıyla verdiği onay beyanıdır.

Veri Sicil Kayıt Sistemi (VERBİS): Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade etmektedir. Bir dosyalama sistemi olarak nitelenebilecek ver kayıt sistemi elektronik ya da fiziki ortamda oluşturulabilir."[47]

KVK Kanunu 12. maddesi hükmünde veri sorumlusu;

- Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- Kişisel verilerin muhafazasını sağlamak,

amacıyla, gerekli teknik ve idari tedbirleri almak zorundadır. Bu anlamda kurumların kanuna uyum süreçlerini tamamlayabilmeleri için Kişisel Verileri Koruma Kurulu tarafından Kişisel Veri Güvenliği Rehberi yayımlanmıştır. Rehberde veri güvenliğine

[47] Kişisel Verilerin Korunması Konunu, https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf (Erişim tarihi:06.01.2021)

ilişkin teknik ve idari tedbirler yer almaktadır. Teknik ve idari tedbirler uluslararası standart, çerçeve ve en iyi uygulamalar göz önünde bulunarak hazırlanmıştır. "[48]

Veri ihlal bildirimlerinin hem Kişisel Verileri Koruma Kuruluna hem de ihlalden etkilenmiş kişilere bildirim yapılmasındaki amaç, ihlal nedeniyle bu kişiler hakkında ortaya çıkabilecek olumsuz sonuçların azami sürede önüne geçilmesi veya en aza indirilmesine imkan verecek önlemler alınmasını sağlamaktır. 6698 sayılı Kişisel Verilerin Korunması Kanununa kaynak teşkil eden Avrupa Genel Veri Koruma Tüzüğünde de veri ihlal bildirimlerine ilişkin olarak Direktifin aksine detaylı düzenlemelere yer verildiği dikkate alındığında Kurul tarafından bu konuda alınacak kararlar arasında herhangi bir uyumsuzluğa sebep olmaması ve uygulamada bir standartlaşma sağlanabilmesini teminen; Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararı ile;

- Kanunun 12 nci maddesinin (5) numaralı fıkrasının "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi 2019/10 - Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Karar hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir…." hükmünde yer alan "en kısa sürede" ifadesinin 72 saat olarak yorumlanmasına ve bu kapsamda veri sorumlusunun bu durumu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesine, veri sorumlusunca söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmasına,
- Veri sorumlusu tarafından Kurula haklı bir gerekçe ile 72 saat içinde bildirim yapılamaması halinde, yapılacak bildirimle birlikte gecikmenin nedenlerinin de Kurula açıklanmasına,

[48] Kişisel veri güvenliği rehberi (Teknik ve İdari Tedbirler) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf (Erişim tarihi:06.01.2021)

- Kurula yapılacak bildirimde aşağıda yer verilen "Kişisel Veri İhlal Bildirim Form"unun kullanılmasına,[49]
- Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgilerin gecikmeye mahal verilmeksizin aşamalı olarak sağlanmasına,
- Veri sorumlusu tarafından veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurulmasına,
- Veri işleyen nezdinde bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri işleyenin bu konuda herhangi bir gecikmeye yer vermeksizin veri sorumlusuna bildirimde bulunmasına,
- Veri ihlalinin yurtdışında yerleşik veri sorumlusu nezdinde yaşanması halinde, bu ihlalin sonuçlarının Türkiye'de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye'de 2019/10 - Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Karar faydalanmaları durumunda, bu veri sorumlusu tarafından da aynı esaslar çerçevesinde Kurula bildirimde bulunulmasına,
- Veri ihlali gerçekleşmesi halinde veri sorumlusu tarafından kendi nezdinde kimlere raporlama yapılacağı, KVK Kanunu kapsamında yapılacak bildirimler ile veri ihlalinin olası sonuçlarının değerlendirilmesi hususunda, kendi nezdindeki sorumluluğun kimde olduğunun belirlenmesi gibi konuları içeren bir veri ihlali müdahale planı hazırlanarak belirli aralıklarla bu planın gözden geçirilmesine karar verilmiştir.[50]

Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararı sonrası farklı sektörden farklı şirketlerin yaşamış olduğu veri ihlalleri Kurul tarafından kamuoyuna sunulmaktadır. Kurulun resmi internet sitesinde Veri Bildirim Formu ve

[49] https://kvkk.gov.tr/Icerik/5362/VeriIhlali-Bildirimi
Erişim Tarihi: 04.01.2021
[50] Kaya, M.,B., Taştan, F.,G., Kişisel Veri Koruma Hukuku, Mevzuat, İçtihat, Bibliyografya, 2. Baskı, Oniki Levha Yayıncılık, 2019, s.221-223.

Veri Bildirim Formu Kılavuzu karara ilişkin bildiride erişime sunulmuştur.[51] Kişisel Verileri Koruma Kurulunun resmi internet sitesi olan 'https://www.kvkk.gov.tr/veri-ihlali-bildirimi/' üzerinden kamuoyuna sunduğu bazı örnek kişisel veri ihlal bildirim örnekleri ve Kurul kararları şöyledir.

Kişisel Verileri Koruma Kurulu'nun 11.04.2019 tarihli ve 2019/104 sayılı kararı ile Kamuoyuna yansıyan ve "Fotoğraf API" olarak adlandırılan Facebook veri ihlali, Facebook Mühendislik Direktörü Tomer Bar tarafından 14.12.2018 tarihinde https://developers.facebook.com/blog/post/2018/12/14/notifying-our-developer-ecosystem-about-a-photo-api-bug/ adresinden "Geliştirici ekosistemimizin bir fotoğraf API'si hatası hakkında bilgilendirme" başlığıyla duyurulmuştur. Duyuruda;

- Facebook kullanıcı fotoğraflarına erişmek için üçüncü taraf uygulamalara izin veren bir fotoğraf API hatası keşfedildiği,
- Sorunun çözüldüğü, ancak bu kusur nedeniyle 13 Eylül - 25 Eylül 2018 tarihleri arasında bazı üçüncü taraf uygulamaların 12 gün boyunca yetkisini aşan düzeyde fotoğraflara erişmiş olabileceği,
- Üçüncü parti bir uygulamaya Facebook platformu üzerinden Facebook kullanıcısı tarafından fotoğraflarına erişim izni verildiğinde sadece zaman çizelgesinde paylaştığı fotoğraflara erişim sağlaması gerekirken, açıklanan kusurdan kaynaklı Marketplace veya Facebook Stories'de paylaşılan diğer fotoğraflara da üçüncü parti uygulamaların erişim sağladığı,
- Ayrıca söz konusu kusurun Facebook kullanıcılarının Facebook'a taslak olarak yüklediği ve henüz paylaşıma açmadığı fotoğrafları da etkilediği,
- Açıklanan kusurun 6,8 milyon kullanıcıyı ve 876 geliştirici tarafından oluşturulan 1.500 uygulamayı etkilemiş olabileceği,
- Açıklanan kusurun, Facebook'un fotoğraf API'sına erişmek için izin alan ve kişilerin fotoğraflarına erişebilen uygulamaları etkilediği,
- Facebook uygulama geliştiricilerinin, uygulamalarını kullanan ve bu kusurdan etkilenen kişileri belirlemelerine imkân sağlayacak araçların geliştirileceği,

[51] https://kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi
(Erişim tarihi:04.01.2021)

ifadelerine yer verilmiştir. İfade edilen durumun "veri gizliliğine/mahremiyetine" aykırı bir husus olması sebebiyle veri ihlali olduğu ve bu ihlalin 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (5) numaralı fıkrasında yer alan "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir…." hükmü uyarınca Facebook tarafından Kurul'a bildirilmesi gerektiği ancak herhangi bir bildirimin yapılmadığı tespit edilmiştir. Bunun üzerine, Kanun'un 15 nci maddesinin (1) numaralı fıkrasında yer alan "Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapar." hükmü kapsamında resen inceleme yapma kararı almıştır.

Yapılan inceleme neticesinde,

- Facebook kullanıcı fotoğraflarına erişmek için üçüncü taraf uygulamalara izin veren bir fotoğraf API hatası keşfedildiği, Facebook tarafından yapılan inceleme sonrası bu durumu potansiyel bir yazılım bozukluğu olarak rapor ettiği,
- API hatasının 13 Eylül - 25 Eylül 2018 tarihleri arasında 12 gün boyunca gerçekleştiği, bahse konu API hatasına Facebook tarafından zamanında müdahale edilmemesi bu konuda teknik ve idari tedbirlerin alınmasında eksikliklerin göstergesi olduğu,
- Üçüncü taraf bir uygulamaya Facebook platformu üzerinden Facebook kullanıcısı tarafından fotoğraflarına erişim izni verildiğinde sadece zaman çizelgesinde paylaştığı fotoğraflara erişim sağlaması gerekirken, açıklanan ihlalden kaynaklı Marketplace veya Facebook Stories'de paylaşılan diğer fotoğraflara da üçüncü taraf uygulamaların erişim sağladığı, ayrıca Facebook kullanıcılarının Facebook'a taslak olarak yüklediği ve henüz paylaşıma açmadığı fotoğraflara da söz konusu üçüncü taraf uygulamaların erişim sağladığı dikkate alındığında, Facebook kullanıcılarının genel olarak izin vermiş olduğu kapasiteden çok daha fazla sayıda fotoğraflara erişim sağlanmasının, Kanunun 12 nci maddesinin (1) numaralı fıkrasına ve 4 üncü maddesinin (2) numaralı fıkrasının (a) bendinde belirtilen "Hukuka ve

dürüstlük kurallarına uygun olma" ve (ç) bendinde belirtilen "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine aykırılık teşkil ettiği,

- Facebook'un bahsi geçen üçüncü taraf uygulamaların normalde erişime izin verilmiş olan sayıdan daha fazla spesifik fotoğrafa gerçekten erişip erişemediklerini belirleyemediği dikkate alındığında, bu durumun Facebook'un kendi platformundaki veri akışını kontrol etme noktasında sıkıntılar yaşadığı ve bu kapsamdaki hususun Kanunun 12 nci maddesinin (1) numaralı fıkrasında öngörülen veri güvenliğine ilişkin yükümlülüklere aykırılık teşkil ettiği,
- Facebook platformu uygulamaları daha ilk aşamada "Arkadaşların, bağlantıların ve birlikte oyun oynadığın diğer kişiler senin oyun hareketlerini görebilecek. Oyunun senin herkese açık profiline ve bu oyunu oynayan tanıdığın kişilere erişimi vardır" ifadesini kullanarak, kullanıcının arkadaş bilgilerine veya diğer bilgilere kişi istemese bile ulaşabilecek şekilde çalışması hususunda izin almaktadır. İlgili kişilerin uygulamada paylaşmaya izin verecekleri kişisel verilerinin neler olması gerektiği ve yükleme aşamasında gizlilik ayarlarıyla ilgili seçimlere imkân sağlamayarak, kişisel verilerin bu şekilde işlenmesini açık rızaya dayandırmaktadır. Açık rızanın özgür irade ile açıklanması gerektiğinden, ilgili kişinin açık rızasının alınması, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmemelidir. Bu durumun Kanunun 4 üncü maddesinin (2) numaralı fıkrasının (a) bendine belirtilen "Hukuka ve dürüstlük kurallarına uygun olma" ilkesine aykırılık teşkil ettiği,
- Açıklanan ihlalin 6,8 milyon kullanıcıyı ve 876 geliştirici tarafından oluşturulan 1.500 uygulamayı etkilemiş olabileceği,
- Türkiye'de bulunan yaklaşık 300 bin kullanıcının veri ihlalinden etkilenmiş olabileceği,
- Kamuoyuna yansıyan ve "Fotoğraf API" olarak adlandırılan Facebook veri ihlali, Facebook Mühendislik Direktörü tarafından 14.12.2018 tarihinde https://developers.facebook.com/blog/post/2018/12/14/notifyingour-developer-ecosystem-about-a-photo-api-bug/ adresinde söz konusu Facebook uygulamasından kaynaklanan ihlalin "Geliştirici ekosistemimizi bir fotoğraf

API'si hatası hakkında bilgilendirme" başlığıyla duyurmasının böyle bir ihlalin varlığı ve Facebook tarafından kabulü anlamına geleceği hususları dikkate alınarak

1) Yukarıda gerekçeleriyle ortaya konulan durumun bir veri ihlali olduğu ve ihlalin oluşmaması için Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde gerekli teknik ve idari tedbirleri almadığı anlaşılan Facebook hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 1.100.000 TL oy birliğiyle,

2) Söz konusu veri ihlalinin 19.09.2018 tarihinde tespit edilmesine rağmen Kuruma bildirim yapılmadığının ve 13.09.2018 - 25.09.2018 tarihleri arasında gerçekleşen veri ihlalinin ilgili kişilere 17.12.2018 tarihinde bildirilmeye başlandığının tespit edildiği, bu çerçevede Kanunun 12 inci maddesinin (5) numaralı fıkrasında yer alan en kısa sürede bildirim yapılması gerektiği hükmüne aykırı hareket eden Şirket hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 550.000 TL oy birliğiyle idari para cezası uygulanmasına, karar verilmiştir.[52]

Kişisel Verileri Koruma Kurulu'nun 16/05/2019 tarihli ve 2019/143 sayılı kararı ile, bildiriminde Marriott International Inc'in (Marriott) 04.12.2018 ve 28.03.2019 tarihlerinde Kurumumuza intikal eden yazılarında özetle;

- 2016 yılı Eylül ayında Marriott'un önceden halka açık ve ayrı bir konaklama şirketi olan Starwood Hotels & Resorts Worldwide Inc'i (Starwood) devralma işlemi gerçekleştirdiği,
- Starwood otel markaları arasında St. Regis, Sheraton Hotel Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels'in bulunduğu,
- Starwood misafir veritabanının tutulduğu ağa Temmuz 2014'ten beri yetkisiz erişim olduğu,

[52] https://www.kvkk.gov.tr/Icerik/5450/2019-104
(Erişim tarihi:04.01.2021)

- Starwood misafir veritabanına yetkisiz erişimin 08.09.2018'de tespit edildiği,
- Starwood müşteri rezervasyon veri tabanının Marriott otelleri için değil sadece Starwood otellerindeki rezervasyonlar için kullanıldığı,
- Marriott'un yaklaşık 383 milyon müşteri kaydı arasında ülke/bölge adresi Türkiye olan yaklaşık 1.24 milyon müşteri kaydının bulunduğu,
- Saldırganın web sunucusuna bir komut istemi yüklediği ve Starwood ağına girdiğinin Marriot tarafından tespit edildiği,
- Web sunucusuna erişimin sağlanmasının ardından, saldırgan tarafından web sunucusuna uzaktan erişim sağlayan bir truva atı (RAT) yüklendiği,
- İhlal hakkında otel müşterilerini aydınlatmak için, özel bir web sitesinin (info.starwoodhotels.com) kurulduğu

ifadelerine yer verilmiştir. Söz konusu bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 16.05.2019 tarih ve 2019/143 sayılı Kararı ile;

- Starwood otel markaları arasında Türkiye'de faaliyet gösteren, St. Regis, Sheraton Hotel & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels'in bulunduğu,
- İhlalden etkilenen veri tabanının tutulduğu Starwood Hotels ağına 2014'ten beri yetkisiz erişim olduğu, 2016 yılı Eylül ayında Marriott'un önceden halka açık ve ayrı bir konaklama şirketi olan Starwood'u devralma işlemi gerçekleştirdikten sonra da ihlalin 19.11.2018 tarihine kadar yaklaşık 4 yıl sürmesinin çok ciddi bir güvenlik açığı olduğu ve Şirket tarafından gerekli denetimlerin ve kontrollerin yapılmadığının göstergesi olduğu,
- İhlalden etkilenen veriler arasında müşterilere ait ad, soyad, posta adresi, telefon numarası, doğum tarihi, cinsiyet, pasaport numarası, Starwood Preferred Guest ("SPG") hesap bilgileri, otel ödül bilgileri, otele giriş ve çıkış bilgileri, ödeme kartı numaraları ve ödeme kartı son kullanma tarihleri, rezervasyon tarihi ve iletişim tercihlerini içeren bilgilerin olduğu,

- Sistemde şifrelenmiş ödeme kartı bilgilerinin yanında çok sayıda şifrelenmemiş ödeme kartı numaralarının da bulunmasının sistemin tasarım aşamasından itibaren doğru bir şekilde planlanmadığı ve gerekli kontrollerin yapılmadığının göstergesi olduğu, bu durumun ilgili kişiler açısından olumsuz etki oluşturabilecek bir güvenlik açığı olduğu,
- İhlalden etkilenen müşterilere ait bilgiler arasında ülke/bölge adresi Türkiye olan yaklaşık 1.24 milyon müşteri kaydının bulunduğu, ancak 2019/143 - Marriot International Inc.'nin Veri İhlal Bildirimi Hakkında Bilgilendirme aynı müşteri için birden fazla kayıt bulunduğu için ihlalden etkilenen Türk müşterilerin sayısının tam olarak tespit edilemediği,
- Saldırganın web sunucusuna bir komut istemi yükleyerek Starwood ağına girdiğinin tespit edildiği ve web sunucusuna erişimin sağlanmasının ardından, saldırgan tarafından web sunucusuna uzaktan erişim sağlayan bir truva atı (RAT) yüklendiği, saldırganın daha sonra kimlik bilgilerini toplayan ilave araçlar yüklediği ve sonrasında Starwood ağındaki diğer cihazlara erişim sağlayabilmek için kimlik bilgilerini ve iç ağ bağlanabilirliğini kullandığının tespit edilememesinin alınan teknik ve idari tedbirlerin yetersizliğinin göstergesi olduğu,
- 2014 yılından itibaren mevcut olan yetkisiz erişim ve komut sisteminin kurulumunu gösteren web olay günlüklerinin (log kayıtları) olmasına rağmen, olayın tespit edilememesinin Şirket tarafından alınması gereken teknik ve idari tedbirlerin alınmadığının somut bir göstergesi olduğu

hususları dikkate alınarak;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12. maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari ve tedbirleri almayan Şirket hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 1.100.000 TL,
- Şirket tarafından 08.09.2018 tarihinde tespit edilen ihlale ilişkin Kuruma 03.12.2018 tarihinde bildirim yapılmasının, ihlalden etkilenen kişilere ise 30.11.2018 tarihinden sonra bildirimde bulunulmaya başlanmasının, Kanunun

12 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi nedeniyle, Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca Şirket hakkında 350.000 TL, olmak üzere toplam 1.450.000 TL idari para cezası uygulanmasına, karar verilmiştir.[53]

Kişisel Verileri Koruma Kurulunun 10.05.2019 tarih ve 2019/130 sayılı Kararı ile, Veri sorumlusu sıfatını haiz olan Microsoft Corporation tarafından Kurumumuza gönderilen 08.05.2019 tarihli yazıda özetle;

- Microsoft'un bir hizmet sağlayıcısının bünyesinde çalışan çağrı destek yöneticisine ait kimlik bilgilerinin ele geçirildiği,
- Bu sayede Microsoft ile bağı olmayan kişilerin Microsoft kullanıcılarının e-posta hesaplarındaki bilgilere erişebildiği,
- İlgili yöneticinin Microsoft Politikası'na aykırı olarak, hesap login bilgilerini kendisine bağlı 13 destek temsilcisiyle paylaştığının tespit edildiği,
- İhlalin yöneticiye bağlı bu kişilerden birinin, e-dolandırıcılık saldırısına maruz kalması sonucu olabileceği gibi; doğrudan bu kişilerden birisinin fiili sonucunda gerçekleşmiş olabileceği,
- İhlal tespitinin ardından, hesap login bilgilerinin derhal sonlandırıldığı,
- İhlalden etkilenen Türkiye'de yerleşik kişi sayısının tahmini 1.820 olduğu,
- Bu yetkilendirilmemiş erişim neticesinde 01.01.2019 ve 28.03.2019 tarihleri arasında e-postaların veya eklerin içeriği hariç e-posta adresi, klasör adları, e-postaların konu satırları, iletişim kurulan diğer e-posta adreslerinin adına erişilmiş veya bu bilgilerin görüntülenmiş olabileceği,
- Türkiye'de etkilenen kişilerden sayıca çok az kısmının yukarıda sayılan bilgilere ek olarak, e-posta hesaplarının ekler de dahil içeriklerine yetkisiz kişiler tarafından erişilmiş olabileceği,
- İhlalin e-posta adreslerini içeriyor olması sebebiyle kullanıcıların e-dolandırıcılık (phishing) saldırılarına maruz kalma ihtimallerinin bulunduğu,

[53] https://www.kvkk.gov.tr/Icerik/5322/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-(Erişim tarihi:04.01.2021)

bilgilerine yer verilmiştir. 6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir. Konuya ilişkin inceleme devam etmektedir.[54]

Kişisel Verileri Koruma Kurulunun 04.02.2020 tarih ve 2020/82 sayılı Kararı ile, veri sorumlusu sıfatını haiz olan Microsoft Corporation tarafından Kurumumuza gönderilen 29.01.2020 tarihli yazılarında özetle;

- İhlalin 05.12.2019 ile 31.12.2019 tarihleri arasında gerçekleştiği ve 26.01.2020 tarihinde tespit edildiği,
- İhlalin güvenlik kurallarının yanlış yapılandırılması nedeniyle Microsoft destek hizmetleri temsilcilerinin müşteriler ile gerçekleştirdikleri etkileşimlere ilişkin bilgileri içeren bir veri tabanının internet vasıtasıyla erişilebilir olması dolayısıyla gerçekleştiği,
- İhlalden etkilenen kişisel veri kategorilerinin iletişim, müşteri işlem, işlem güvenliği, finans verileri olduğu,
- İhlalden etkilenen tahmini kişi sayısının Türkiye'den 158 kullanıcı olduğu,
- İlgili kişilerin veri ihlaliyle ilgili olarak https://msrc-blog.microsoft.com/2020/01/22/access-misconfiguration-for-customer-support-database/ adresinden bilgi alabilecekleri,

bilgilerine yer verilmiştir. 6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul,

[54] https://www.kvkk.gov.tr/Icerik/5451/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Microsoft-Corporation (Erişim tarihi:04.01.2021)

gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir. Konuya ilişkin inceleme devam etmektir.[55]

Kişisel Verileri Koruma Kurulunun 18.08.2020 tarih ve 2020/634 sayılı Kararı ile, Veri sorumlusu sıfatını haiz olan Kariyer.net Elektronik Yayıncılık ve İletişim Hiz. AŞ tarafından Kurumumuza gönderilen yazıda özetle;

- İhlalin Kariyer.Net'e tedarikçi olarak hizmet veren bir danışman tarafından 12 Ağustos 2020 tarihinde Kariyer.net'in bir çalışanına, adı geçen sitede üyeliği bulunan 50.000 kişiye ait olduğu iddia edilen bir dosyanın aynı gün internette bir siteye yüklendiği bilgisinin aktarılmasıyla tespit edildiği,
- İhlalin 10.08.2020 tarihinde gerçekleştiği, Kariyer.net tarafından 12.08.2020 tarihinde tespit edildiği,
- İhlalden etkilenen verilerin, "email adresi", "kullanıcı şifresi", "isim soyad", "doğum tarihi", "telefon numarası", "profil fotoğrafı" URL link bilgisi, "yaşadığı il", "yaşadığı ilçe" bilgileri olduğu,
- İhlalden etkilenen kişi sayısının 40.955, kayıt sayısının 53.149 olduğu,
- İlgili kişilerin veri ihlaliyle ilgili olarak adaydestek@kariyer.net adresinden ve 0 216 468 76 00 numarasından bilgi alabilecekleri,

ifade edilmiştir. 6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir. Konuya ilişkin inceleme devam etmektedir.[56]

[55] https://www.kvkk.gov.tr/Icerik/6670/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Microsoft-Corporation
[56] https://www.kvkk.gov.tr/Icerik/6786/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Kariyer-net-Elektronik-Yayincilik-ve-Iletisim-Hiz-A-S-
(Erişim tarihi:04.01.2021)

Kişisel Verileri Koruma Kurulunun 29.12.2020 tarih ve 2020/1011 sayılı Kararı ile, Veri sorumlusu sıfatını haiz olan Ficosa International Otomotiv San. ve Tic. AŞ tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri sorumlusunun sunucularına 16.12.2020 tarihinde fidye saldırısının gerçekleştirildiği ve dosyaların şifrelendiği,
- İhlalin log kayıtlarında bir problem olduğunun fark edilmesiyle tespit edildiği,
- İhlalden etkilenen kişisel verilerin; ad, soyadı, e-posta ve/veya telefon numarası olduğu ancak bilişim incelemesinin devam ettiği,
- İhlalden çalışanların, müşterilerin, tedarikçiler ve hizmet sağlayıcıların etkilendiği
- İhlalden tahmini 1084 kişinin etkilendiği, incelemenin devam ettiği dolayısıyla kişi ve kayıt sayısının tam olarak bilinmediği,

ifade edilmiştir. 6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir. Konuya ilişkin inceleme devam etmektedir.[57]

Bankacılık ve elektronik haberleşme sektöründe yaşanan kişisel veri ihlal vaka örneklerine ilişkin detaylı bigilere çalışmanın ilerleyen bölümünde değinilmiştir.

Veri güvenliğinin sağlanması ve kişisel veri ihlallerinin önlenmesi veya en aza indirgenmesi ancak veri güvenliği risklerinin ortadan kaldırılması ile mümkündür. Teknik ve idari tedbirler; yetki matrisi, yetki kontrol, erişim logları, kullanıcı hesap yönetimi, ağ güvenliği, uygulama güvenliği, şifreleme, sızma testi, saldırı tespit ve önleme sistemleri, log kayıtları, veri maskeleme, veri kaybı önleme yazılımları, yedekleme güvenlik duvarları, güncel anti-virüs sistemleri silme, yok etme veya

[57] https://www.kvkk.gov.tr/Icerik/6851/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Ficosa-International-Otomotiv-San-ve-Tic-AS
(Erişim tarihi:04.01.2021)

anonim hale getirme anahtar yönetimi olarak verilmiştir. Bahsedilen kontroller ilgili teknik tedbirlerin detaylandırılmasında standart, çerçeve ve en iyi uygulama kontrollerine paralel şekilde hazırlanmıştır. Standart, çerçeve ve en iyi uygulama kaynakları risk değerlendirme ve gereken önlemleri denetim mantığı ile sağlamayı hedeflemektedir. Bu anlamda BT yönetişimlerine yol göstermesi için standart, çerçeve ve en iyi uygulama kaynaklarından birini takip etmekte olan kurumlar Kişisel Verileri Koruma Kurulu tarafından Kişisel Veri Güvenliği Rehberine kolaylıkla uyum sağlayabilirler, mevcut ve oluşabilecek riskleri önleyebilirler.

Tablo 3.1 Teknik tedbirler

Teknik Tedbirler
Yetki Matrisi
Yetki Kontrol
Erişim Logları
Kullanıcı Hesap Yönetimi
Ağ Güvenliği
Uygulama Güvenliği
Şifreleme
Sızma Testi
Saldırı Tespit ve Önleme Sistemleri
Log Kayıtları
Veri Maskeleme
Veri Kaybı Önleme Yazılımları
Yedekleme
Güvenlik Duvarları
Güncel Anti-Virüs Sistemleri
Silme, Yok Etme veya Anonim Hale Getirme
Anahtar Yönetimi

Kaynak: Kişisel veri güvenliği rehberi (Teknik ve İdari Tedbirler)

Tablo 3.2 İdari Tedbirler

İdari Tedbirler
Kişisel Veri İşleme Envanteri Hazırlanması
Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.)
Sözleşmeler (Veri Sorumlusu - Veri Sorumlusu, Veri Sorumlusu - Veri İşleyen Arasında)
Gizlilik Taahhütnameleri
Kurum İçi Periyodik ve/veya Rastgele Denetimler
Risk Analizleri
İş Sözleşmesi, Disiplin Yönetmeliği (Kanuna Uygun Hükümler İlave Edilmesi)
Kurumsal İletişim (Kriz Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimi vb.)
Eğitim ve Farkındalık Faaliyetleri (Bilgi Güvenliği ve Kanun)
Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim

Kaynak: Kişisel veri güvenliği rehberi (Teknik ve İdari Tedbirler)

“213 sayılı Vergi Usul Kanunu'nun mükerrer 298. maddesi uyarınca belirlenen yeniden değerleme oranı 2020 yılı için %9,11 olarak açıklanmıştır. 28.11.2020 tarihli ve 31318 sayılı Resmî Gazete'de yayımlanan orana göre 6698 sayılı Kişisel Verileri Koruma Kanunu'nun18. maddesinde yer alan idari para cezaları, 2021 için yeniden belirlenmiştir.

- Kanun’un 10. maddesinde düzenlenen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,
- Veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar,
- Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar,
- Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar para cezası verilebilecektir.”[58]

Kişisel Veri Güvenliğine İlişkin Teknik ve İdari Tedbirlerin ISO 27001, COBIT, NIST ve ITIL ile ilişkilendirilmesi;

Kişisel Veri Güvenliğine İlişkin İdari Tedbirler:

- Mevcut Risk ve Tehditlerin Belirlenmesi:

  ISO 27001 Genel Gereksinimler 6. madde ve 8. madde-Risk Analizi ve Risk İyileştirme, COBIT APO12- Yönetilen risk, NIST ID.RA-Risk değerlendirme, ID.RM-Risk yönetim stratejisi, ITIL Genel Yönetim Uygulamaları-Risk yönetimi

- Çalışanların Eğitilmesi ve Farkındalık Çalışmaları:

[58] https://www.gsghukuk.com/tr/bultenler-yayinlar/duyurular/2021-yili-kvkk-idari-para-cezalari.html (Erişim tarihi: 06.01.2021)

ISO 27001 Genel Gereksinimler 7. madde-Farkındalık, COBIT APO12-Yönetilen insan kaynakları, NIST PR.AT-Farkındalık ve Eğitim

- Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi

  ISO 27001 Genel Gereksinimler 5. madde-Politika, COBIT APO13-Yönetilen güvenlik, NIST PR.IP-Bilgi koruma süreçleri ve prosedürleri, ITIL Genel Yönetim Uygulamaları-Bilgi güvenliği yönetimi,

- Kişisel Verilerin Mümkün Olduğunca Azaltılması

  ISO 27001 EK-A-Varlık yönetimi, COBIT BAI09-Yönetilen varlıklar, NIST PR.DS-Veri güvenliği, ITIL Servis Yönetimi-BT varlık yönetimi

- Veri İşleyenler ile İlişkilerin Yönetimi

Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler:

- Siber Güvenliğin Sağlanması

  ISO 27001 EK-A-12-Operasyon güvenliği, COBITNIST PR.IP-Bilgi koruma süreçleri, NIST PR.PT-Koruyucu teknolojiler, NIST DE.CE-Sürekli güvenlik izleme, DSS05-Yönetilen güvenlik hizmetleri, ITIL Servis yönetimi uygulamaları-İzleme ve Olay yönetimi

- Kişisel Veri Güvenliğinin Takibi

  ISO 27001 EK-A-8-Varlık yönetimi, COBIT APO01-Yönetilen BT yönetim çerçevesi, COBIT BAI02-Yönetilen gereksinimlerin tanımı, COBIT DSS.06-Yönetilen iş süreç kontrolleri, NIST PR.DS-Veri güvenliği, ITIL-Genel yönetim uygulamaları-Bilgi güvenliği yönetimi

- Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması

ISO 27001 EK-A-8-Varlık yönetimi, COBIT APO01-Yönetilen BT yönetim çerçevesi, COBIT BAI02-Yönetilen gereksinimlerin tanımı, COBIT DSS.06-Yönetilen iş süreç kontrolleri, NIST PR.DS-Veri güvenliği, ITIL-Genel yönetim uygulamaları-Bilgi güvenliği yönetimi

- Kişisel Verilerin Bulutta Depolanması

  ISO 27001 EK-A-8-Varlık yönetimi, COBIT APO01-Yönetilen BT yönetim çerçevesi, COBIT BAI02-Yönetilen gereksinimlerin tanımı, COBIT DSS.06-Yönetilen iş süreç kontrolleri, NIST PR.DS-Veri güvenliği, ITIL-Genel yönetim uygulamaları-Bilgi güvenliği yönetimi

- Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı

  ISO 27001 EK-A-14- Sistem Edinimi, Geliştirilmesi ve Bakımı, COBIT BAI09-Yönetilen varlıklar, COBIT DSS05-Yönetilen güvenlik hizmetleri, NIST PR.MA-Bakım, NIST PR.PT-Koruyucu teknolojiler COBIT BAI03-Yönetilen çözümleri belirleme ve oluşturma, ITIL-Servis yönetimi uygulamaları-Servis konfigürasyon yönetimi, ITIL-Teknik yönetim uygulamaları-Yazılım geliştirme ve yönetimi

- Kişisel Verilerin Yedeklenmesi

  ISO 27001 EK-A-12- Operasyon yönetimi, COBIT APO14-Yönetilen veri, COBIT DSS04-Yönetilen süreklilik, NIST PR.IP-Bilgi koruma süreçleri ve prosedürleri, NIST RC.RP-Kurtarma planlama, ITIL-Servis yönetimi uygulamaları-Servis sürekliliğinin yönetimi

Kişisel verilerin korunması kapsamında uygulanacak teknik ve idari tedbirler uluslararası bilgi güvenliği ve BT yönetişimi standart, çerçeve ve en iyi uygulamaları kontrolleri ile düzenli olarak kontrol edilip gerekli güvenlik izlenebilirliği sağlanabilir.

3.2.1.2. Genel Veri Koruma Yönetmeliği (GDPR) - Veri Koruma Etki Değerlendirmeleri (VKED/DPIA)

AB 1950 yılında kabul ettiği ve 1953 yılında yürürlüğe giren İnsan Haklarının Korunmasına ve Temel Özgürlüklere İlişkin Avrupa Konvansiyonu, AB'de kişisel verilere ilişkin çalışmaların temellerini oluşturmuştur. Sonrasında ise 1981 tarihli Bireylerin Korunması Konvansiyonu, 1995 tarihli Verilerin Korunması Direktifi, 2002 tarihli Gizlilik ve Elektronik İletişime İlişkin Direktif ile mevzuat çerçevesini iyileştirmeye çalıştırmıştır. Son olarak AB Komisyonu tarafından 2016 Mayıs'ta kabul edilen Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR) 25 Mayıs 2018'den itibaren yürürlüğe girmiştir. GDPR bir yönerge değil, doğrudan bağlayıcı ve uygulanabilir bir yönetmeliktir. GDPR'nin yürürlüğe girmesi ile veri işlenmesi sırasında göz önünde tutulacak hesap verilebilirlik, privacy by design, one-stop shop mekanizması, veri koruma sorumlusu atanması ve risk tabanlı yaklaşım gibi yeni ilkeler getirilmiştir.[59]

Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR) 5. maddesi, genel veri koruma rejiminin merkezinde yatan temel ilkeleri ortaya koymaktadır. Bu temel ilkeler, GDPR'nin hemen başında belirtilmiştir ve mevzuatta bulunan diğer kuralları ve yükümlülükleri hem doğrudan hem de dolaylı olarak etkiler. Bu nedenle, bu temel veri koruma ilkelerine uyum, denetçilerin GDPR kapsamındaki yükümlülüklerini yerine getirmelerini sağlamanın ilk adımıdır. GDPR'nin 5. maddesinde bulunan Veri Koruma İlkeleri:

Yasallık, adalet ve şeffaflık: Kişisel verilerin herhangi bir şekilde işlenmesi yasal ve adil olmalıdır. Kendileriyle ilgili kişisel verilerin toplandığı, kullanıldığı, bunlara danışıldığı veya başka şekilde işlendiği ve kişisel verilerin ne ölçüde işlendiği veya işleneceği bireyler için şeffaf olmalıdır. Şeffaflık ilkesi, bu kişisel verilerin

[59] ICO, Information Commissioner's Office / Bilgi Komisyonu Ofisi, Data protection impact assessments https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ (Erişim tarihi:04.01.2021)

işlenmesiyle ilgili her türlü bilgi ve iletişimin kolayca erişilebilir ve anlaşılır olmasını ve bu açık ve yalın dilin kullanılmasını gerektirir.

Amaç Sınırlaması: Kişisel veriler yalnızca belirli, açık ve meşru amaçlar için toplanmalı ve bu amaçlarla uyumlu olmayan bir şekilde daha fazla işlenmemelidir. Özellikle, kişisel verilerin işlendiği belirli amaçların açık ve meşru olması ve kişisel verilerin toplandığı tarihte belirlenmiş olması gerekir. Bununla birlikte, kamu yararına, bilimsel veya tarihsel araştırma amaçlarına veya istatistiksel amaçlara (GDPR'nin 89(1). maddesi uyarınca) arşivleme amaçlarına yönelik daha fazla işlem, başlangıçtaki amaçlarla uyumsuz olarak değerlendirilmez.[60]

Veri Minimizasyonu: Kişisel verilerin işlenmesi yeterli, ilgili ve işlendikleri amaçlarla ilgili olarak gerekli olanlarla sınırlı olmalıdır. Kişisel veriler, ancak işlemenin amacı başka yollarla makul bir şekilde yerine getirilemiyorsa işlenmelidir. Bu, özellikle, kişisel verilerin saklandığı sürenin katı bir minimum ile sınırlı olmasını gerektirir.

Doğruluk: Kontrolörler kişisel verilerin doğru olmasını ve gerektiğinde güncel tutulmasını sağlamalıdır; İşlendikleri amaçlarla ilgili olarak yanlış olan kişisel verilerin gecikmeden silinmesini veya düzeltilmesini sağlamak için her makul adımı atmalıdır. Özellikle, kontrolörler topladıkları veya aldıkları bilgileri ve bu bilgilerin kaynağını doğru bir şekilde kaydetmelidir.

Saklama Sınırlaması (Verilerin amaç için gereken süre kadar muhafaza edilmesi): Kişisel veriler, yalnızca kişisel verilerin işlendiği amaçlar için gerekli olduğu sürece veri sahiplerinin tanımlanmasına izin veren bir biçimde tutulmalıdır. Kişisel verilerin gerekenden daha uzun süre saklanmamasını sağlamak için, kontrolör tarafından silinme veya periyodik gözden geçirme için zaman sınırları belirlenmelidir.

Bütünlük ve Gizlilik: Kişisel veriler, kişisel verilere ve işleme için kullanılan ekipmana yetkisiz veya hukuka aykırı erişime veya kullanımına karşı koruma ve

[60] Determann, Lothar ,Determann's Field Guide To Data Privacy Law International Corporate Compliance, Fourth Edition, Elgar Compliance Guides, 2020, S.170-171.

kazara kayıp, imha veya kaza eseri kayıp, imha veya uygun teknik veya organizasyonel önlemleri kullanarak hasar.

Hesap Verebilirlik: Son olarak, veri sorumlusu yukarıda adı geçen Veri Koruma İlkelerinin tümüne uyumluluğundan sorumludur ve bu ilkelere uygunluğunu gösterebilmelidir. Veri sorumlusu, kişisel verilerin işlenmesi ve GDPR'ye nasıl uydukları konusunda sorumluluk almalı ve özellikle Data Protection Commission (DPC)'ye uygunluklarını (uygun kayıtlar ve önlemlerle) gösterebilmelidir.[61]

Tablo 3.3 Kişisel Verileri Koruma İlkeleri Bakımından 6698 sayılı Kanun ile GDPR Karşılaştırması

6698 sayılı Kişisel Verilerin Korunması Kanunu'nda Yer Alan Temel İlkeler	**GDPR'de Yer Alan Temel İlkeler**
1-Hukuka ve dürüstlük kurallarına uygun olma	1- Hukuka, dürüstlük kurallarına uygun olma ve veri öznesine karşı şeffaf işleme
2-Doğru ve gerektiğinde güncel olma	2-Doğru, gerekli hallerde işleme ve güncel olma
3- Belirli, açık ve meşru amaçlar için islenme	3-Kişisel verilerin belirli, açık ve meşru amaçlarla işlenmesi
4- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma	4- Veri işleme için gerekli olduğu kadar, ilgili ve ölçülü biçimde işleme
5- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme	5- Kişisel verinin işleme amacı için gerekli olandan daha uzun süre tutulmaması
	6- Veri kontrolörünün sayılan tüm temel prensiplerden sorumlu süje olması (hesap verebilirlik prensibi)

Kaynak: Akıncı, A.,N., Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuk Bakımından Değerlendirilmesi, 2017, S.36[62]

[61] https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection (Erişim tarihi:04.01.2021)

[62] Akıncı, A.,N., Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuk Bakımından Değerlendirilmesi, T.C. Kalkınma Bakanlığı, İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü, 2017, S.36.

GDPR kapsamında söz konusu ilkelerin uygulanmasından sorumlu olan süje açıkça belirlenerek veri sorumlusunun hesap verebilirliği artırılmıştır. GDPR'nin temel yaklaşımında yer alan artırılmış kişisel veri koruması eğilimine paralel olarak ilkelerin uygulanmasından sorumlu olan veri kontrolörü doğrudan temel ilkeler başlıklı 5. maddede düzenlenmiştir.

Hesap verebilirlik kavramı, GDPR kurallarının merkezinde yer almaktadır: Bu, AB sakinlerini hedef alan AB içindeki veya AB dışındaki kuruluşların, GDPR'ye uygun olarak kişisel bilgilerin ele alınmasında şeffaflığı ve adaleti arttırması gerektiği anlamına gelir. Buradaki kişisel bilgiler, tanımlanabilir bir şahıs ile her türlü bilgiyi ifade eder (yasada bir veri konusu olarak atfedilir).

Hesap verebilirlik ilkesine göre veri işlemenin yasal dayanağını belirlemek veri işleme faaliyetleri için temel taşlardan biridir. Veri toplama amacı ve yöntemi belirlenerek her türlü işleme faaliyeti bu dayanağa binaen yapılır. Bu yasal dayanaklar, açık onay, sözleşme, hayati çıkarlar, yasal zorunluluk, kamu görevi ve meşru çıkarlar olarak sınıflandırılmıştır. Veri işlemeye başlamadan önce yasal dayanağın belirlenmesi gerekir. Kişilerin onayının açık, şeffaf, opt-in bir şekilde alınması GDPR'nin üzerinde önemle durduğu en önemli noktalardan biridir. Birleşik Krallık Parlamentosuna rapor vermekle görevli ulusal veri koruma otoritesi Bilgi Komisyonu Ofisi (ICO) resmi internet sitesinde kurumların öz değerlendirmelerini yapabilmeleri için hesap verebilirlik takibi kontrol listesini (accountability tracker) erişime sunmuştur.[63]

GDPR uyarınca, belirli kuruluşların belirlenmiş bir Veri Koruma Görevlisi (DPO) ataması gerekir. Kuruluşların ayrıca DPO'larının ayrıntılarını yayınlamaları ve bu ayrıntıları ulusal denetim otoritelerine sağlamaları gerekir.

Bir kurumun aşağıdaki durumlarda belirlenmiş bir veri koruma görevlisi ataması gerekir:

- İşlemin bir kamu makamı veya organı tarafından yürütülmesi,

[63] https://ico.org.uk/for-organisations/accountability-framework-self-assessment/ (Erişim tarihi:04.01.2021)

- Veri sorumlusu veya veri işleyen temel faaliyetleri, veri konularının büyük ölçekte düzenli ve sistematik olarak izlenmesini gerektiren işleme operasyonlarından oluşması,
- Veri sorumlusu veya veri işleyen temel faaliyetleri, ceza mahkûmiyetleri ve suçlarıyla ilgili büyük ölçekli özel veri kategorileri veya kişisel verilerin işlenmesinden oluşması.

Veri Koruma Görevlisi (DPO) hesap verebilirlik için önemli bir unsur olup, bir DPO atanması uygunluk sağlamayı kolaylaştıracağı gibi işletmeler için bir rekabet avantajı da sağlayabilir. Bununla birlikte, DPO görevlerini bağımsız olarak yerine getirebilmelidir. AB kurumlarında ve organlarında, bu bağımsızlığı garanti eden bir dizi güvence vardır. AB kurumları ve organları için geçerli kurallar, DPO'nun görevlerinin yerine getirilmesine ilişkin herhangi bir talimat almayacağını açıkça belirtir. Bireyin DPO olarak görevleri ile varsa diğer görevleri arasında bir çıkar çatışması olmamalıdır. Çatışmayı önlemek için aşağıdakilerin yapılması önerilir:

- DPO kişisel veri işleme faaliyetlerinin bir denetleyicisi olmamalıdır.
- Veri sorumlusu ve veri işleyen, DPO'yu kişisel verilerin korunması ile ilgili her sürece zamanında ve uygun bir şekilde dahil etmek zorundadır.
- Veri sorumlusu ve veri işleyen, DPO'nun kendisine yüklenen görevlerini yaparken, görevlerin yerine getirilebilmesi için gerekli kaynakları, kişisel verilere ve işlemlere erişebilmesini, uzmanlığını sürdürebilmesini sağlamakla yükümlüdür.
- Veri sorumlusu ve veri işleyen, DPO'nun görevleriyle ilgili herhangi bir talimat almamasını sağlamalıdır. Görevlerini yerine getirmesinden dolayı veri sorumlusu veya veri işleyen tarafından görevinden alınamaz ve cezalandırılamaz. DPO, veri sorumlusu ve veri işleyenin en üst yönetim seviyesine doğrudan bağlı çalışmalıdır.
- İlgili kişiler, kişisel verilerinin işlenmesi ile ilgili konularda ve haklarının kullanılmasında DPO ile irtibata geçebilmeliler.

- DPO'ya başka görevler ve sorumluluklar verilebilir. Veri sorumlusu ve veri işleyen verilen diğer görevlerle görevlinin asli görevlerinin çatışmamasını sağlamalıdır.
- DPO, soruşturma yetkisine sahip olmalıdır. Örneğin AB kurum ve kuruluşlarında, DPO'lar tüm kişisel verilere ve veri işleme işlemlerine anında erişebilir, sorumluların da sorularına cevap olarak bilgi vermeleri gerekmektedir.
- Bir DPO görevi için kuruluş tarafından asgari bir atama süresi ve işten çıkarılma için katı koşullar belirlenmelidir. AB kurum ve organlarında, DPO üç ila beş yıllık bir süre için atanır, yeniden atanabilir ve yalnızca European Data Protection Supervisor (EDPS)'nin onayı ile görevden alınabilir.

DPO, veri koruma otoritesi ile işbirliği içinde veri koruma kurallarına uyulmasını sağlamalıdır (AB kurumları ve organları için bu, Data Protection Supervisor (EDPS)'dir). AB kurum ve organlarında DPO şunları yapmalıdır:

- Denetçilerin ve veri konularının veri koruma hakları, yükümlülükleri ve sorumlulukları hakkında bilgilendirilmelerini sağlamak ve onlar hakkında farkındalık yaratmak,
- Veri koruma kurallarının yorumlanması veya uygulanması hakkında kuruma tavsiye ve önerilerde bulunmak,
- Kurum içindeki işleme operasyonlarının bir kaydını oluşturun ve belirli riskler sergileyenleri EDPS'ye bildirmek,
- Kurum içinde veri koruma uyumluluğunu sağlamak,
- Kurum, veri sorumlusu, ilgili taraflar tarafından talep üzerine veya kendi inisiyatifiyle soruları veya şikâyetleri ele almak,
- EDPS ile işbirliği yapmak (soruşturmalar, şikâyetlerin ele alınması, EDPS tarafından yürütülen incelemeler vb. taleplerine yanıt vermek),
- Geçerli veri koruma kurallarına uyulmaması durumunda kurumun dikkatini çekmek.

Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR) 35. maddesi kapsamında öngörülen veri koruma etki değerlendirmesi; kişisel verilerin gizliliğini etkileme ve ihlal etme potansiyeline sahip olan fiziksel etmenler ve bilişim sistemlerinin uygulama esnasında ve uygulamadan sonraki süreçte; verinin gizliliği açısından kontrol edilmesine yönelik denetim mekanizması vazifesi görmektedir.

GDPR'de 35. ve 36. maddelere göre, özellikle yeni teknolojilerin kullanıldığı veri işleme çalışmalarının gerçek kişilerin temel hak ve özgürlükleri için yüksek riskler doğurması olasılığına yönelik Veri Koruma Etki Değerlendirmeleri (VKED/DPIA) gerçekleştirilmesi esası ifade edilmiştir. Bu kapsamda risk değerlendirme çalışmalarına öncülük eden ülke konumunda olan Kanada; kamu kurumlarının kişisel veri işledikleri bilişim sistemlerinde, gizlilik etki değerlendirmesini zorunlu kılmıştır. Gelişmiş ülkeler, bireylerin verilerini koruma altına almak amacıyla; bilişim sistemlerinin geliştirilmesi, güncellenmesi ve bu kapsamda politika ve prosedür belirlenme sürecini, gizlilik risklerini saptamak ve ihtiyaç duyulan önlemleri almak adına yönetmelikte ifade edilmiştir.[64]

GDPR'nin 24. maddesi kapsamında risk, iki unsura dayalı olarak ölçümlenmektedir:

- Riskin gerçekleşme ihtimali (Likelihood)
- Riskin gerçekleşmesi durumunda kişilerin hak ve özgürlükleri üzerinde doğuracağı etkinin ağırlığı (Severity of the impact)

GDPR'nin 32. maddesi verilerin işlenmesi sürecinde güvenliğin sağlanması hususunda, veri sorumlularına veri işleme eyleminin doğuracağı risklerle doğru orantılı olarak gerekli teknik ve idari tedbirleri alma yükümlülüğü getirilmektedir. Alınacak aksiyon ve operasyonun eş zamanlı öz denetimini sağlamasını beklediği bu yöntem risk tabanlı yaklaşımdır. Risk tabanlı yaklaşımda değerlendirme yapılırken beklenen azami kontroller:

- Kişisel verilerin psödoanonimizasyon ve kriptolama yöntemleriyle korunması,

[64] https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf
(Erişim tarihi:04.01.2021)

- Veri işleme sistemlerinin ve hizmetlerinin gizliliğinin, güvenliğinin, ulaşılabilirliğinin ve dirençliliğinin sağlanması,
- Teknik veya fiziksel bir kazanın meydana gelmesi durumunda sistemlerin eski haline döndürülmesi için gereken önlemlerin alınması.
- Sistemlerin güvenilirliğinin sağlanması için alınan önlemlerin düzenli olarak kontrol edilmesi.[65]

Kurumların işlediği kişisel verilerin risk profili, gerçekleştirilen kişisel veri işleme faaliyetlerine, veri işlemenin karmaşıklığına ve boyutuna, işlenen verilerin hassasiyetine ve işlenmekte olan veriler için gerekli korumaya göre belirlenmelidir. Örneğin, bir veri işleme faaliyetinin özellikle karmaşık olduğu veya büyük hacimli veya hassas verilerin söz konusu olduğu durumlarda (örneğin bir internet, sağlık, finans veya sigorta şirketi), daha yüksek bir risk derecesi taşıyan çalışan veya müşteri verilerini bulundurabilir.

Kurumların işlediği kişisel verilerin risk profiline bakarken, kurumların koruması gereken kişilere yönelik somut zararlara bakmak yararlıdır. Bunlar, GDPR'nin 75. maddesinde ayrıntılı olarak açıklanmıştır ve aşağıdakilere yol açabilecek işlemleri içerir: ayrımcılık, kimlik hırsızlığı veya dolandırıcılık, mali kayıp, itibarın zedelenmesi, mesleki gizlilikle korunan kişisel verilerin gizliliğinin kaybı, psödoanonimizasyonun yetkisiz olarak iptali veya diğer önemli ekonomik veya sosyal dezavantajlar.[66]

Bir risk değerlendirmesi yürütmek, bir projeyle ilişkili gelecekteki potansiyel veri koruma sorunları konusunda kurumların farkındalığını artıracaktır. Bu da, veri işleme tasarımını iyileştirmeye ve ilgili paydaşlarla veri gizliliği riskleri hakkında iletişimin geliştirilmesine yardımcı olacaktır.

GDPR, gelecekteki veri işleme faaliyetlerinin planlaması için iki önemli kavram tanımlamaktadır. Bunlar, Data Protection By Design (Tasarım Yoluyla Veri Koruma)

[65] Room, Stewart, LLM, Chairman, National Association of Data Protection and Freedom of Information Officers Proprietor, Data Protection and Compliance in Context, British Cataloguing in Publication Data, s. 57, 63,112, 2007.
[66] Kuner, Christopher, European Data Protection Law Corporate Regulation and Compliance, Second Edition, Oxford University Press, 2007, S.61-64.

ve Varsayılan Olarak Veri Korumadır (Data Protection By Default). Bu ilkelerin her ikisi de GDPR'nin 25. maddesi kapsamında yönetmelikte yer almaktadır.
Data Protection By Design, veri gizliliği özelliklerinin ve veri gizliliğini artıran teknolojilerin doğrudan erken bir aşamada projelerin tasarımına yerleştirilmesi anlamına gelmektedir. Böylelikle, bireysel veri gizliliği için daha iyi ve daha uygun maliyetli koruma sağlanması amaçlanmaktadır.

Data Protection By Default, kullanıcı hizmeti ayarlarının otomatik olarak veri koruma dostu olması gerektiği ve yalnızca işlemenin her bir özel amacı için gerekli olan verilerin toplanması gerektiği anlamına gelir.

GDPR kapsamında, Veri Koruma Etki Değerlendirmesi (Data Protection Impact Assessment-DPIA), gerçek kişilerin hakları ve özgürlükleri açısından büyük bir risk oluşturması muhtemel öngörülen projenin, girişimin veya hizmetin, veri işlemeyi içerdiği zorunlu bir ön işleme gerekliliğidir. Veri koruma etki değerlendirmesi gerçekleştirmek kurumlar için sürekli değerlendirme şansı sağlar ve veri güvenliği denetleyicilerinin veri koruma hususunda yasal uyumu sağlamalarına yardımcı olur.
Veri koruma risk kaydı tutmak, veri koruma risklerini tanımlanmasını, bunlara karşı önlem alınmasını ve denetim durumunda yasal uyum gereksinimlerinin sağlandığına dair kanıt gösterilmesine olanak tanır.[67]

3.2.1.3. Bankacılık Sektöründe Veri Güvenliğine İlişkin Güncel Düzenlemeler

Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından 15 Mart 2020 tarihli 31069 sayılı Resmî Gazete'de, 2011 yılından beri yürürlükte olan "Bankaların Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliği" yerine "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik" kademeli olarak yürürlüğe girmiştir. Türkiye'nin veri güvenliği ve teknoloji yatırımı en büyük olan sektörü olan Türk bankacılığında yeni yönetmelik, daha gelişmiş bir bankacılık sisteminin modellenmesine adımı niteliğindedir. Bankacılık sektöründe bilgi sistemleri dinamiklerinin daha oldun bir seviyede

[67] https://www.dataprotection.ie/en/organisations/know-your-obligations/risk-based-approach (Erişim tarihi:04.01.2021)

yürütülmesi planlanmaktadır. Yönetmelik, yürürlükte olan ve veri güvenliğini yakından ilgilendiren kanun ve mevzuatların gereksinimleri ile paralel içerikte olup, özellikle KVK Kanunu ile gelen uyum esaslarıyla bütünleşik bir yaklaşımda olduğu gözlemlenebilir.[68]

Diğer yönetmelik ve kanun yaklaşımlarında olduğu gibi bankaların öngörülen süre zarfında gerekli aksiyonları alıp uyumun sağlanması beklenmektedir. Mevcut düzende her yıl COBIT uyumluluk denetimi gerçekleştiren bankalar yeni yönetmelik ile uluslararası standart ve çerçevelere daha da yakınlaştırılmıştır.

Yönetmelik incelendiğinde yapılan değişikliklerle her ne kadar resmi olarak ISO 27001 Bilgi Güvenliği Yönetim Sistemi beklentisi ifade edilmese dahi, standardın kapsamına paralel gereksinimlerin bulunduğu gözlemlenebilir. Bankalar COBIT ve ITIL çerçeve yaklaşımlarını gerek uyum gerek denetim fonksiyonlarında kanunun da çizdiği şekilde takip etmektedirler. Yeni yönetmelik ile bu çerçeve yaklaşımlara ek olarak Türkiye'de birçok sektörün yine çeşitli kanunlar yaptırımı ile aşina olduğu ISO 27001 standardına yaklaşılmıştır.

Yeni yönetmeliğin veri güvenliğinin sağlanması konularına ağırlık vermesi özellikle dikkat çekicidir.[69]

Yönetmeliğin 4. maddesi ve 8. maddesinde bilgi sistemleri (BS) yönetişim rol ve sorumluluklarına getirilen yeni esasları ve doğrudan yazılı tanımlamaları ile yeni rol ve sorumlulukların tahsis edilmesi, ayrıca görevlerin ayrılığı prensibine dikkat çekerek bilgi güvenliği fonksiyonunun doğrudan Yönetim Kurulu'na ya da genel müdüre bağlı olması esas olarak belirtilmiştir. Bu değişikliklerin yönetmeliğe yansımasında, bankaların son yıllarda yaşadığı bilgi güvenliği ihlallerinin büyük etkisinin olduğu görülmektedir. Bu yaklaşım ISO 27001 standardının genel gereksinimler bölümü 5. maddesi rol ve sorumluklar ilkesi ile kesişmektedir.

Yönetmeliğin 5. maddesinde dokümanların gizlilik derecelerine atıfta bulunulmuş, 6. maddesinde banka bünyesinde varlık envanteri hazırlanması ve oluşturulacak

[68] https://assets.kpmg/content/dam/kpmg/tr/pdf/2020/11/Gundem-37.pdf, 2020 (Erişim tarihi:06.01.2021)
[69] https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm (Erişim tarihi:06.01.2021)

envanterler ile sınıflandırma kılavuzlarının da oluşturulması beklenmiştir. Varlık yönetimi ISO 27001 standardının ekler bölümünde bulunan 8. maddesi ile kesişmektedir. Yönetmelikte ayrıca kişisel veriye de ayrıca değinilerek sınıflandırma kılavuzu için yönlendirme yapılmıştır.

Yönetmeliğin 7. maddesinde bilgi sistemleri risk sürecine değinilmiştir. Risklerin gerçekleşmesi halinde ilişkili bilgi varlığının gizliliği, bütünlüğü, erişilebilirliği gibi ana bilgi güvenliği kriterlerine olan etkilerin belirlenerek bilgi varlığına yönelik etki hesaplaması yapılması beklenmiştir. Bu yaklaşım risk analizi ve varlık yönetimini birbirine bağlayan ISO 27001 standardının eski versiyonuna paralel bir yaklaşım olmuştur. Risk analizinde gerçekleştirilen çalışmaların bütününü özet risk değerlendirme raporu olarak üst yönetime sunulmalıdır. Bu yaklaşım ISO 27001 standardının genel gereksinimler bölümü 6. maddesi ve 8. maddesi ile kesişmektedir. Risk yönetimi yaklaşımı denetim fonksiyonunun temel taşı olup bütün standart, çerçeve ve en iyi uygulama örnekleri için en önemli ana başlıklardandır.

Yönetmeliğin 8. maddesinde nihai sorumluluğu Yönetim Kurulu'na ait olmak üzere bir bilgi güvenliği yönetim sistemi tesis edilmesi ve bu yönetim sistemi kapsamında dikkate alınacak esaslar düzenlenmesini belirtmiştir. Yönetim kurulu, bilgi varlıklarının sınıflandırılması sürecinde uygun güvenlik önlemlerinin alınması, risk değerlendirmeleri, veri ihlali bildirimleri, farkındalığın arttırılması gibi konulardan birinci derecede sorumludur. Bu yaklaşım ISO 27001 standardının genel gereksinimler bölümü 5. maddesi ile kesişmektedir. Böylelikle yönetişim yaklaşımında yönetimin rolü daha net belirlenmiştir.

Yönetmeliğin 10. maddesinde KVK Kanunu'na paralel olacak şekilde "Müşterinin, bilgilerini paylaşmaya dair açık rıza göstermesi verilecek hizmet için bir ön şart haline getirilemez." hususu belirtilmiş ve ilgili verilerin paylaşımına yönelik net ifadelerle sınırlandırılma yapılmıştır. Bankacılık kanununda yer alan istisnalar dışında, müşteri sırrı niteliğindeki verilerin yurt içindeki veya yurt dışındaki üçüncü kişilerle paylaşabilmesi için müşterilerinin, ispat edilebilir izninin alınması gerekmektedir. Yönetmelikte direk atıflarla ifade edilen kişisel veri tanımlaması ve tekrarlanması

KVK Kanunu'nun etkinliğini ve kanun koyucu mertebesindeki etkisini yadsınamaz şekilde göstermektedir.

Yönetmeliğin 9. maddesi veri gizliliği 10. maddesi veri paylaşımı başlıklarına değinilmiştir. Kişisel veriye, hassas veri yaklaşımı ile gizlilikte üst limit uygulaması getirilmesi ve anahtar yönetimi, şifreleme anahtarlarının yaşam döngüsü boyunca güvenliğinin sağlanması vurgulanmıştır. ISO 27001 standardı EK-A bölümünde bulunan 10. madde anahtar yönetimi ile kesişmektedir.

Yönetmeliğin 11. maddesi kimlik ve erişim yönetimi ile ilgili olarak doğrulama mekanizmaları veri gizliliği esas alınarak düzenlenmiş ve bunlara ilişkin kontroller somutlaştırılmıştır. Kimlik ve erişim yönetimi ISO 27001 standardı ve bankacılık sektörünün denetim çerçevesi olan COBIT kapsamında önemli kontrol başlıklarındandır. ISO 27001 standardı EK-A bölümünde bulunan 9. madde erişim kontrolü ile kesişmektedir.

Yönetmeliğin 18. maddesinde siber olayların ele alınmasına yönelik olay yönetim süreç yapısının oluşturulması ve kurumsal siber olaylara müdahale ekipleri (SOME) kurulması kararı bildirilmiştir. SOME raporlama kriterleri belirtilmiş ve Kurumsal SOME'ye ilişkin iletişim bilgilerinin BDDK'ya iletilmesi vurgulanmıştır. Bankaların kendi bünyelerinde siber olayların yaşanması halinde müdahale edebilecek bir ekibin bulundurulması ve gerekli ihlal bildirim kanalının oluşturulması ISO EK-A bölümünde bulunan 16. madde bilgi güvenliği olay yönetimi kontrolü ile kesişmektedir.

Yönetmeliğin 25. maddesinde üzerinde çokça değerlendirme yapılan bulut bilişim konusunda değilmiş, birincil ve ikincil sistemler için bulut bilişim veya dış hizmet sağlayıcının kullanımına izin verilmekle beraber ön koşul olarak yurt içinde barındırma zorunluluğu getirilmiştir. Birincil ve ikincil sistemler süreklilik konusunda geçtiğimiz yıllarda çok defa değerlendirilmiş bir konudur. Bankalara ait birincil sistemlerin kaç tane yedeği olduğuna bakılmaksızın, birincil sistemler dışında her türlü yedek sistem, ikincil sistemler olarak kabul edileceği vurgusu oldukça önemlidir. Buna ek olarak soruşturma yürüten adli merciler tarafından kanıt niteliğinde veri

taleplerinde, bankalar tarafından talep edilen verileri ilgili mercilere iletilmesi, yedeklerinin alınması ve saklanması hakkında vurgu yapılmıştır.
Türkiye'de çokça tartışılan konulardan biri olan bulut bilişim konusuna, BDDK yaklaşımı ile bankaların kullanamadığı bir teknoloji konumundan farklılaşan bir perspektifle yeni yürürlükte değinilmiştir. Yürüklükte, bankaların bulut bilişim hizmet modelinin yararlanmalarına ilişkin, özel ve topluluk bulut hizmeti kullanımına ilişkin düzenlemeye yer verilmiştir.

Yönetmeliğin 34. maddesi, 38. maddesi, 39. maddesi, 40. maddesi, 41. maddesi, 42. maddesi 43. maddesi, elektronik bankacılık, internet bankacılığı, mobil bankacılık, telefon bankacılığı, açık bankacılık hizmetleri ve ATM bankacılığına ilişkin kimlik doğrulama ve işlem güvenliği kriterleri belirlenmiş ve vurgulanmıştır. Yönetmelik, ATM bankacılığında, cihazların ve kameraların yönetimine ilişkin usul ve esasları belirlemektedir. ATM'ler kameralar ile uzaktan izlenebilecek ve müdahale edilebilecek şekilde konumlandırılacak, kameralar eskiye göre daha uzun süreli ve kaliteli kayıtlar tutacaktır. Böylece dolandırıcılık vakalarının kimlik tespiti kolaylıkla yapılabilecektir. Elektronik bankacılık işlemlerinde, bankaların müşterilerinden edineceği hassas veri ya da sır niteliğinde veri içeren dekont, hesap özeti vb. bilgilerin elektronik bankacılık hizmeti sunulan kanallar üzerinden müşterilere gönderilmesi gereksinimidir. Orijinal dokümanın müşteriye iletilmesine nazaran elektronik ortamda bu tür verilerin paylaşılması güvenlik gereksinimlerinin belirli bir standardı sağlaması anlamda veri güvenliği bakımından daha az riskli olacaktır.

Bankacılık sektörü ülkemizde lokomotif sektörlerin başında gelmektedir. Yapılan düzenleme ve denetlemeler ile, uluslararası örneklerine göre özellikle teknoloji kullandırım olanakları göz önünde bulundurulduğunda çok daha gelişmiş seviyededir. Müşteri, paydaş, çalışan gibi ilgili tarafların veri güvenliğinin sağlanması bankacılık sektöründe sürekli önem arz eden konuların başında gelmektedir. Ülkemizde KVK Kanunu'nun yürürlüğe girmesi öncesi bankacılık sektöründe yaşanan en bilinen veri ihlali örneklerinden biri 2014 yılında HSBC bankasının 2.7 milyon müşterisinin banka kartı ve kredi kartı bilgilerinin çalınması vakasıdır. KVK Kanunu yürürlüğe girmesi ardından gerçekleşen veri ihlali vakaları KVKK kurumu resmi web sayfasından kamuoyuna duyurulmuştur. Bu duyurulara göre: Kişisel Verileri Koruma Kurulunun

31.07.2019 tarih ve 2019/230 sayılı kararı ile DenizBank A.Ş. Teftiş Kurulu Başkanlığı tarafından yıllık olarak gerçekleştirilen denetimler kapsamında, bir banka çalışanı tarafından işin gerekliliğini aşacak sayıda bireysel nitelikli kredi bilgilerini içeren sorgulama yapılması tespit edilmiştir ve banka için inceleme gerçekleştirilmiştir.[70]

Kişisel Verileri Koruma Kurulunun 17.07.2019 tarih ve 2019/219 sayılı kararı ile Türk Ekonomi Bankası A.Ş. (TEB) Teftiş Kurulu soruşturması sonucunda; banka çalışanlarının, kendilerine tanımlanan KKB sorgulama yetkilerini bankanın erişim ve bilgi güvenliği politikalarına aykırı şekilde amacı dışında kullandığı tespit edilmiştir ve banka için inceleme gerçekleştirilmiştir. Gerçekleşen ihlalden tahmini olarak 17.582 banka müşterisinin ve 7.706 banka müşterisi olmayan kişinin etkilendiği kamuoyuna duyurulmuştur.[71]

Kişisel Verileri Koruma Kurulunun 01.03.2019 tarih ve 2019/43 sayılı kararı ile ING Bank A.Ş.'nin bir çalışanının, bir banka uygulaması üzerinde tanımlı yetkileri uyarınca Ticari Nitelikli Kredi Bildirimi ve Paylaşımı (KRM) sorgusu yapamadığı halde, yetkilendirme sistemini devre dışı bırakacak bir yöntem ile yetki aşımı yaparak TBB Risk Merkezi web sitesine eriştiği ve 19.055 adet gerçek kişinin kişisel bilgilerinin banka dışına aktarıldığı tespit edilmiştir ve banka için inceleme gerçekleştirilmiştir.[72]

Bahsedilen ihlal vakaları bankaların yıllık COBIT denetimleri esnasında, banka tarafında 5651 sayılı kanun gereği tutulan verilerin SIEM yöntemiyle analiz edilmesi sonucu ortaya çıkarılmıştır. Denetimlerde ihlale sebebiyet veren aktiviteler log kayıtlarında SIEM yardımı ile ilişkilendirilmiştir. Benzer şekilde bahsedilen ihlal vakalarında, bankalar tarafından hazırlanan yetki matrisine göre yetkisi olmayan kişilerin, bankada kayıtlı müşterilerin verilerini banka dışına çıkarması durumu tespit edilmiştir. Bu kontroller ISO 27001, NIST ve ITIL kaynaklarında da kayıtların kontrol

[70] https://www.kvkk.gov.tr/Icerik/5516/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-DenizBank-A-S-
(Erişim tarihi: 04.01.2021)
[71] https://www.kvkk.gov.tr/Icerik/5492/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Turk-Ekonomi-Bankasi-A-S-
(Erişim tarihi: 04.01.2021)
[72] https://www.kvkk.gov.tr/Icerik/5375/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-ING-Bank-A-S-
(Erişim tarihi: 04.01.2021)

edilmesi ve erişim yönetimi başlığı ile bulunmaktadır. Yaşanan veri ihlalleri veya veri sızıntıları ulusal ve ulusal açılardan benzer sebeplerle yaşanan farklı örneklerdir. Örnek olarak verilen veri güvenliği ihlal olaylarında KVKK Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası ile gerekli bildirim resmi kanallara sağlanmıştır.

3.2.1.4 Elektronik Haberleşme Sektöründe Veri Güvenliğine İlişkin Güncel Düzenlemeler

Bilgi Teknolojileri ve İletişim Kurumu (BTK) 4 Aralık 2020 tarihli 31324 sayılı Resmî Gazete'de "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik" yayımlamıştır. Yönetmelik'in yürürlüğe girmesi ile birlikte 24 Temmuz 2012 tarihli ve 28363 sayılı Resmî Gazete'de yayımlanan "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik" yürürlükten kalkmış olacaktır.[73] Yönetmelik, elektronik haberleşme sektöründe faaliyet gösteren kurumların ve işletmelerin müşteri veya abonelerine ait verilerin güvenliği bakımından uymaları gereken usul ve esasları içermektedir. Yönetmeliğin uygulanmasının BTK tarafından gerçekleştirileceği yönetmelikte belirtilmiştir.

Yönetmeliğin 5. maddesinde elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin kişisel veri işleme faaliyetini gerçekleştirirken uyması gereken genel ilkeler belirlenmiştir. Bu ilkeler şöyledir:

- "Hukuka ve dürüstlük kurallarına uygun olarak işlenmesi,
- Doğru ve gerektiğinde güncel olması,
- Belirli, açık ve meşru amaçlar için işlenmesi,
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması,

[73] https://www.resmigazete.gov.tr/eskiler/2020/12/20201204-13.htm
(Erişim tarihi: 04.01.2021)

- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi,"[74]

İşletmeler tarafından abonelerinin kişisel verilerinin işlenmesinde hukuka ve dürüstlük kurallarına uygun olarak hareket edilmesi, verilerin doğru ve gerektiğinde güncel olması yürürlük kapsamında özellikle vurgulanmıştır. Yürütmelikteki bu vurgulanan bölümde ISO 27001 standardı temel ilkelerinden olan gizlilik, bütünlük, erişilebilirlik, inkâr edilemezlik ve güvenilirlik yaklaşımları ile kesişmektedir. Yürütmelikte belirtilen bu ilkeler KVK Kanunu kapsamında veri güvenliği ve veri işleme ilkeleri ile de paralellik göstermektedir.

Yürütmelik 5. maddesinde milli güvenlik gerekçesi ile trafik ve konum verilerinin yurtdışına çıkartılmaması esası bildirilmiştir. Ülkemiz siber güvenlik ve bilişim teknolojileri tabanında son yıllarda yerli ve milli perspektifi kabul gördüğünden konum verilerinin yurtdışına çıkartılmaması esası büyük veri çalışmaları yapan algoritmik yapıların dışında kalmayı hedefleyebilmektedir. Ancak mülga yönetmelikte ulusal içerikli kişisel verilerin uluslararası paylaşımı hususunda genel anlamda çıkartılmama esası benimsenmişken, yeni yönetmelik yurtdışına çıkmaması gereken verileri trafik ve konum verileri ile sınırlandırmıştır. BTK'nın yaklaşımı KVK Kanunu tutumuna benzer olacak şekilde, nasıl ki KVK Kanunu kişisel verilerin yurtdışına aktarımını kısıtlarken, belirtilen özel şartlar dahilinde ilgili veriler kişilerin açık rızaları alınarak veya Kişisel Verileri Koruma Kurulu'ndan temin edilen bir izinle mümkün ise, yürütmelik de trafik ve konum bilgisinin uluslararası paylaşımı için özel şartlar getirmiştir.

Yönetmelik'in 6. maddesi veri güvenliği kapsamında düzenleme getirmiştir. Elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin, abonelerine veya kullanıcılarına ait kişisel verilerin güvenliğini ve sağladıkları hizmetlerin güvenilirliğini KVKK'ya ve ulusal ve uluslararası standartlara uygun olarak yerine getirmeleri vurgulanmıştır. Yönetmelikte belirtilen teknik ve idari tedbirler ile KVK Kanunu Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) kastedilmektedir.

[74] https://www.resmigazete.gov.tr/eskiler/2020/12/20201204-13.htm
(Erişme tarihi: 06.01.2021)

Teknik ve idari tedbirlerin uluslararası standartlara uygunluğu ifadesi ile sektörel yaklaşımla bakılırsa ülkemizde sıkça veri güvenliği uyumluluğu kapsamında kullanılan ISO 27001, COBIT, NIST, ITIL gibi çerçeve ve en iyi uygulama örnekleri akla gelmektedir. İşletmeler tarafından alınması gereken teknik idari tedbirler için mevcut riskin belirlenmesi vurgusu ile de risk değerlendirme ya da risk tabanlı yaklaşım karşımıza çıkmaktadır.

KVK Kanunu uyumluluğunda teknik ve idari tedbirler bir kontrol listesi ya da maddelendirilmiş açıklıkta değildir. KVK Kanunu Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) dikkate alınarak gerekli kontrol mekanizmaları yorumlanarak sağlanmaktadır. Yönetmeliğin 6/2 maddesinde teknik ve idari tedbirlerin asgari olarak neleri içermesi gerektiği belirtilmiştir. Bu asgari tedbirler, standart ve çerçeve kontrol maddeleri arasında bulunan veri güvenliğinin ihlal edileceği, yetkisiz erişim, kişisel verilerin bütünlüğünün bozulması, sadece veriyi değil verinin bulundurulduğu sistemin de aynı güvenlik şartlarında korunması gereksinimlerini vurgulamaktadır.

Yönetmelik'in 6. maddesi kapsamında, işletmeciler, kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtlarını iki yıl saklamakla yükümlüdür. Yürürlük bu yaklaşımı ile 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu yükümlülüklerini hatırlatmaktadır.

Yönetmeliğin 7. maddesi elektronik haberleşme sektöründe faaliyet gösteren işletmeciler, kendilerine bağlı şebekelerin ve sağladıkları hizmetlerin güvenliğini tehdit eden bir risk olması halinde eğer yönetmelikte belirtilen teknik ve idari tedbirler yeterli olmazsa KVK Kanunu ihlal durumu bildirim kurallarına uygun olarak abonelerine gerekli bilgilendirmeyi sağlamalıdırlar. Bu bilgilendirme hem riskin ne olduğu hem de riskin nasıl ortadan kaldırıldığı içeriğini ilgili kişilere sağlamalıdır. Bu noktada elektronik haberleşme sektöründe faaliyet gösteren işletmeciler risk tabanlı bir veri güvenliği yaklaşımını ne yöntemle sağlamalıdır sorusunun bir yanıtı veya yöntemin standartlaşması yönünde bir düzenleme yoktur. Bahsedilen risk analiz ve yönetimi; ISO 27001 standardı genel gereksinimler bölümü 6.madde ve 8. maddesinde

risk analizi ve riskin iyileştirilmesi veya COBIT 2019 çerçevesi kapsamında yönetişim hedeflerinden EDM03-güvence altına alınan risk operasyonu, yönetim hedeflerinden APO12-yönetilen risk, ITIL en iyi uygulaması kapsamında genel yönetim uygulamaları altında risk yönetimi gibi veri güvenliği kaynakları izlenerek sağlanmalıdır.

Kişisel veri ihlali olması durumunun tespiti sağlanması halinde işletmelerin, aboneler dışında KVKK'ya uygun yöntemlerle BTK'ya, Kişisel Verileri Koruma Kurumu'nu da bilgilendirmeleri gerekmektedir. Bu bildirim süreci KVK Kanununu takiple yine 72 saat ile sınırlandırılmıştır.

Yönetmeliğin 8. maddesinde işletmecilerin, abonelerinden veya kullanıcıdan açık rıza alınmasını gerektiren durumlarda KVK Kanunu ilkelerine uyarak izlemesi gereken yöntem ve esaslar bildirilmiştir.

Kişilerden açık rıza alınması konusu KVK Kanununun yürürlüğe girmesinin ardından veri güvenliği içeriğinde ve ilişkili düzenlemelerde tanım olarak karşımıza çıkmaktadır. Açık rıza, kişi tarafından özgür iradeyle belirli bir amaca ilişkin olarak işlem öncesi verilen beyandır ve eğer belirli bir konu veya amaç ile sınırlanmazsa geçerliliği kabul edilmemektedir. KVK Kanunu açık rıza alınması yöntemini hizmetler için bir ön şart olarak tayin etmese dahi uygulamadaki yaklaşımlar bu yönde olmuştur. Aynı durum Ticari Elektronik İleti Mevzuatı kapsamında ticari elektronik iletilerin alınma yönteminde de geçerlidir.

Yönetmelik açık rızaların alınması hususunda KVK Kanunu aydınlatma yükümlülüklerinde olduğu gibi abonelerin veya kullanıcıların, işlenecek olan kişisel verilerinin genel bilgilendirmesinin işletmeciler tarafından yapılması esası bildirilmiştir.

İşletmeciler, abone ve kullanıcılarından almış oldukları açık rızaları mevzuat hükümlerinde yer aldığı gibi asgari abonelik süresi olacak şekilde saklamakla yükümlüdür.

Elektronik haberleşme sektörü gereksinimleri itibari ile değerli veri hacmi en yoğun sektörlerin arasındadır. Uluslararası rekabette hukuki imkân ve ticari şartlar en önemli

faktörlerdendir. Bu sebeple veri lokalizasyonu gibi ülkemizin de hassas kararlar almakta olduğu teknolojik hususlar mevzuatlarla netleştirilmekte ve gerekli düzenlemeler yapılmaktadır.

KVK Kanunu yürürlüğe girmesi ardından elektronik haberleşme sektörü gerçekleşen veri ihlali vakaları KVKK kurumu resmi web sayfasından kamuoyuna duyurulmuştur.

Bu duyurulara göre: Kişisel Verileri Koruma Kurulunun 18.06.2019 tarih ve 2019/178 sayılı kararı ile Vodafone Telekomünikasyon A.Ş. ile yarı münhasır bayilik ilişkisi bulunan bir bayinin (Lotus Telekom) çalışanı tarafından MERNİS (Merkezi Nüfus ve İdare Sistemi) kullanıcı adı ve şifresinin üçüncü bir şahısla paylaşıldığı ihbarı gerçekleştirilmiş olup, bu ihbar üzerine şirket tarafından suç durusunda bulunulmuştur. İhlale sebebiyet veren çalışanı tarafından, GSM hattı abonesi olmak isteyen kişilerin verdiği kimlik fotoğraflarına ait ekran görüntülerinin kopyalandığı ve söz konusu kimlik bilgilerinin bayi çalışanı tarafından yasa dışı bahis oynatan siteler için bazı kişilere satıldığı bildirilmiştir. Veri güvenliğinin hukuka aykırı olarak ihlali neticesinde yaşanan vakada ilgili kişilere herhangi bir bildirim yapılmadığı ve elde edilen bilgilere göre ihlalden etkilenen kişi sayısının yaklaşık 5-6 bin civarında olduğuna dair açıklama yapılmıştır.[75]

Kişisel Verileri Koruma Kurulunun 12.11.2020 tarih ve 2020/863 sayılı Kararı ile veri sorumlusu sıfatını haiz olan Çizgi Telekomünikasyon A.Ş. tarafından bildirilen kişisel veri ihlali bildiriminde 7 Kasım 2020 tarihli hafta sonu vardiyası için şirkete gelen görevli çalışanın, rutin kontrolleri yapmak için sunucuya uzaktan bağlandığında sunucu masaüstünde bir mesaj bulduğu, bunun üzerine yapılan inceleme neticesinde, müşteri bilgilerinin bulunduğu şirket sunucularında bazı kötü amaçlı yazılımların bulunduğunun aynı gün tespit edildiği, ihlalden, T.C. kimlik numarası, ad ve soyadı, e-posta ve ev adresi, müşteri işlem detayları (kredi kartı bilgileri gibi), müşterinin satın aldığı hizmetler ve bu hizmetlere ilişkin işlemlere konu tarih-saat bilgileri gibi müşteri bilgilerinin etkilenmiş olabileceği, ihlalden etkilenen kişilerin şirketten hizmet alan

[75]https://www.kvkk.gov.tr/Icerik/5473/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Vodafone-Telekonikasyon-A-S-
(Erişim tarihi:04.01.2021)

müşteriler olduğu, ihlalden etkilenen kişi ve kayıt sayısının henüz bilinmediği ve ihlal hakkında incelemenin devam ettiği kamuoyuna duyurulmuştur.[76]

Örnek olarak verilen veri güvenliği ihlal olaylarında 6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir.

3.3. VERİ GÜVENLİĞİ AÇISINDAN RİSK TABANLI YAKLAŞIMLA KÜRESEL STANDART, ÇERÇEVE VE EN İYİ UYGULAMALARIN HUKUKİ UYUMA DESTEĞİ

Veri güvenliğinin sağlanabilmesi yaklaşımında dünyada kullanılan birçok küresel kabul görmüş standart, detaylı ve kimi sektörlerce kılavuz olarak kabul edilmiş çerçeve (framework), ya da en iyi uygulamalar (best practices) bulunmaktadır. Bu standart, çerçeve ve en iyi uygulama örnekleri, mevzuatlara (yasa, tüzük, yönetmelik, kararname vb.) konu olmuş teknik ve idari tedbirler niteliğinde her türlü içeriğin kaynağı olarak gösterilebilir. Bugün veri güvenliğine ilişkin her türlü bilişim yönetimi unsuru ve bilişim yönetimine yön verecek yasal düzenleme esasları bahsedilen standart, çerçeve ve en iyi uygulama örnekleri ile birebir paralellik göstermektedir.

Hazırlanan çalışmada Türkiye'de en yaygın şekilde kullanılmakta olan standart, çerçeve ve en iyi uygulama yaklaşımlarına örnek olarak ISO 27001, COBIT, NIST ve ITIL incelenmiştir. Sektörel zorunluluk ya da kurumların kendi kararları doğrultusunda takip ettiği ve uyum gösterdiği kaynaklar farklılık gösterebilmektedir. Ancak teknolojinin ortak bir bilişim dili ve dünyanın her yerinde bu dilin etkisinin aynı olduğu düşünülürse, bu kaynakların da ortak özellikleri ortaya çıkacaktır.

[76]https://www.kvkk.gov.tr/Icerik/6836/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Cizgi-Telekomunikasyon-A-S-
(Erişim tarihi:04.01.2021)

Veri güvenliğini, risk tabanlı yaklaşımda standart, çerçeve, en iyi uygulama kaynaklarını takip ederek gerçekleştirmek kurumları eş zamanlı olarak ilgili mevzuatların ilişkili maddeleri için de uyumlu hale getirecektir. Risk tabanlı yaklaşım, düzenli denetimler esnasında ilişkili kontrol gereksinimlerinin sağlanamaması halinde, mevcut risklerin neler olduğunun anlaşılması ya da değişen çevresel, ekonomik, teknolojik şartlarda karşılaşılabilecek yeni risk ve tehditlerin belirlenmesini sağlamaktadır. Kurumların risk tabanlı yaklaşımı benimseyebilmelerinde en önemli kıstas sahip oldukları verilerin türünü ve büyüklüğünü anlamaları ve bu verilerin kurumsal ağ yapısındaki trafiği yani nerede olduklarını anlamalarıdır. Verilerin tanımlanması ve iş süreçlerinde konumlandırılması ile sınıflandırılması ardından, mevcut riskler ortaya çıkacak ve gerekli veri güvenliği iyileştirme faaliyetleri gerçekleştirilebilecektir. Veri güvenliği olgunluk seviyeleri, güvenlik risklerinin kabul edilebilir seviyeye indirilmesi ile paraleldir. Kurumların en doğru risk değerlendirmelerini yapabilmeleri için; standart, çerçeve ve en iyi uygulama yaklaşımlarından en az birini kaynak kabul ederek, yönetişim modeli olarak entegre etmeleri kaçınılmazdır.

Önceki bölümde detaylıca incelenen standart, çerçeve ve en iyi uygulama yaklaşımlarına örnek olarak ISO 27001, COBIT, NIST ve ITIL kontrol bölümleri ve maddeleri aşağıda eşlenmiştir. Bu çalışma kullanılarak, güncel yasal düzenlemelere ve mevzuatlara uyumun sağlanabilmesi ve veri güvenliği risklerinin tayin edilebilmesi için etkili bir denetim fonksiyonu oluşturulabilecektir.

Dünya genelinde çoklanan şekilde standart, çerçeve ve en iyi uygulama yaklaşımlarının oluşturulmasının sebebi, sektörel ihtiyaçlara ve mevcut güvenlik sorunlarına bir denetim fonksiyonu çözümü olarak hazırlanmalarıdır. Bu sebeple yönetişim modelleri sektörel ihtiyaç, organizasyon yapıları, BT yönetselliği göz önünde bulundurularak hazırlanmıştır. Belirtildiği üzere teknoloji dili dünyaca kabul gören tekil bir dil olduğundan, kontrol ve ana bölümler birbirinden farklı ifadelerde ancak benzer veri güvenliği yaklaşımları ile karşımıza çıkmaktadır.

Bu anlamda sektörel olarak kurumların pozisyonlarını doğru tayin ederek, çevresel değişkenler ve iş modellerine bağlı olarak veri güvenliği risklerini en iyi analiz

edebilecekleri yönetişimler yaklaşımları benimsemeleri mevzuatlara uyum için de birincil adım olacaktır.

ISO 27001, COBIT, NIST, ITIL standart, çerçeve ve en iyi uygulama örnekleri olup, her bir kaynak bir diğeri ile ilişkisel bir modellemeye sahiptir. Bu ilişkisel yapı her bir kaynağın ortak amacı olan bilgi güvenliği ve yönetişim stratejisi yaklaşımlarını ortaya koymaktadır.

Tablo 3.4 ISO 27001 - COBIT - NIST- ITIL Kontrol Listeleri Eşleşme Tablosu

COBIT 2019	NIST Siber Güvenlik Çerçevesi	ISO/IEC 27001	ITIL V4
EDM01- Garanti Edilmiş Yönetişim Çerçeve Kurulumu ve Sürdürülmesi	ID.GV-1	ISO/IEC 27001:2013 A.5.1.1	
EDM02- Garanti Edilmiş Fayda Temini		ISO/IEC 27001:2013 Genel Gereksinimler 7.1	
EDM03- Garanti Edilmiş Risk Optimizasyon	RC.CO-1	ISO/IEC 27001:2013 Genel Gereksinimler 6.1, 6.2, 8.2, 8.3	
EDM04- Garanti Edilmiş Kaynak Optimizasyon		ISO/IEC 27001:2013 Genel Gereksinimler 7.1, 7.2	
EDM05- Garanti Edilmiş Paydaş Katılımı		ISO/IEC 27001:2013 Genel Gereksinimler 7.1, 7.2, 7.3	
APO01-Yönetilen BT Yönetim Çerçevesi	ID.AM-6 ID.GV-1 PR.DS-1 PR.DS-2 PR.DS-5	ISO/IEC 27001:2013 Genel Gereksinimler 4.3, 4.4 ISO/IEC 27001:2013 A.6.1.1 A.5.1.1, A.8.2.3, A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3,	

		A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.4, A.14.1.2, A.14.1.3	
APO02-Yönetilen Strateji	ID.AM-4 ID.BE-2 ID.BE-3	ISO/IEC 27001:2013 Genel Gereksinimler 4.3, 4.4 ISO/IEC 27001:2013 A.11.2.6	Strateji Yönetimi
APO03-Yönetilen Kurumsal Mimari	ID.AM-5 ID.BE-2 ID.BE-3	ISO/IEC 27001:2013 Genel Gereksinimler 5.1, 5.3 ISO/IEC 27001:2013 A.8.2.1	Mimari Yönetimi
APO04-Yönetilen İnovasyon		ISO/IEC 27001:2013 Genel Gereksinimler 4.2, 4.3, 4.4	
APO05-Yönetilen Portföy			Portföy Yönetimi
APO06-Yönetilen Bütçe ve Maliyetler			Servis Finans Yönetimi
APO07-Yönetilen İnsan Kaynakları	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5 PR.IP-11 DE.CM-6	ISO/IEC 27001:2013 A.7.2.2, A.6.1.1, A.7.2.2, A.7.1.1, A.7.3.1, A.8.1.4, A.14.2.7, A.15.2.1	
APO08-Yönetilen İlişkiler	ID.BE-1	ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2	İlişki Yönetimi
APO09-Yönetilen Hizmet Anlaşmaları		ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2	Hizmet Seviyesi Yönetimi

APO10-Yönetilen Tedarikçiler	ID.BE-1 ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4 PR.AT-3	ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2, A.15.1.1, A.15.1.2, A.6.1.1, A.7.2.2	Tedarikçi Yönetimi
APO11-Yönetilen Kalite	PR.IP-7 PR.PT-1 DE.DP-5	ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, A.16.1.6	
APO12-Yönetilen Risk	ID.RA-1 ID.RA-3 ID.RA-5 ID.RA-6 ID.RM-1 ID.RM-2 ID.SC-1 ID.SC-2 DE.AE-4 DE.AE-5 DE.DP-4	ISO/IEC 27001:2013 Genel Gereksinimler 6.1, 6.2, 8.2, 8.3 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3, A.12.6.1, A.15.2.1, A.15.2.2, A.16.1.2	Risk Yönetimi
APO13-Yönetilen Güvenlik	ID.GV-2 ID.RA-6 ID.RM-1 ID.SC-1 ID.SC-2 PR.AC-3 PR.DS-4 PR.IP-2 PR.IP-4 PR.PT-2 PR.PT-4 DE.DP-3	ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.6.2.2, A.13.1.1, A.13.2.1, A.12.3.1, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5, A.14.2.8, A.17.1.2A.17.1.3, A.18.1.3, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9	Bilgi Güvenliği Yönetimi
APO14-Yönetilen Veri		ISO/IEC 27001:2013 A.18.1.3, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3,	

BAI01-Yönetilen Programlar	ID.SC-1 PR.IP-3 RS.RP-1 RS.IM-1	ISO/IEC 27001:2013: A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, A.16.1.5, A.16.1.6	
BAI02-Yönetilen Gereksinimlerin Tanımı	ID.RM-1 ID.SC-1 ID.SC-2 PR.DS-1	ISO/IEC 27001:2013: A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.8.2.3	
BAI03-Yönetilen Çözümleri Belirleme ve Oluşturma	PR.DS-8 DE.CM-8	ISO/IEC 27001:2013: A.11.2.4, A.12.6.1	Yazılım Geliştirme Yönetimi
BAI04-Yönetilen Erişebilirlik ve Kapasite	ID.RM-1 ID.SC-1 PR.PT-5	ISO/IEC 27001:2013: A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.17.1.2, A.17.2.1	Erişilebilirlik Yönetimi Kapasite ve Performans Yönetimi
BAI05-Yönetilen Kurumsal Değişim	PR.AT-1 RC.IM-1	ISO/IEC 27001:2013 A.7.2.2	Kurumsal Değişiklik Yönetimi
BAI06-Yönetilen BT Değişiklikleri	PR.DS-1 PR.IP-3	ISO/IEC 27001:2013 A.8.2.3, A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	Değişiklik Kontrol Süreci
BAI07-Yönetilen BT Değişim Kabul ve Geçişi	PR.DS-7 RC.IM-2	ISO/IEC 27001:2013 A.12.1.4	Versiyon Yönetimi
BAI08-Yönetilen Bilgi Birikimi	PR.AC-6	ISO/IEC 27001:2013: A.6.1.2, A.7.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4	Bilgi Birikimi Yönetimi

BAI09-Yönetilen Varlıklar	ID.AM-1 ID.AM-2 ID.AM-5 PR.DS-3 PR.IP-6 PR.MA-1	ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.8.1.1, A.8.2.1, A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7, A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.11.1.2, A.11.2.4, A.11.2.5	BT Varlık Yönetimi
BAI10-Yönetilen Konfigürasyon	PR.IP-1	ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	Servis Konfigürasyon Yönetimi
BAI11-Yönetilen Projeler		ISO/IEC 27001:2013 A.6.1.5	Proje Yönetimi
DSS01-Yönetilen Operasyonlar	PR.AC-2 PR.AC-3 PR.IP-5 PR.PT-5	ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.6.2.2, A.13.1.1, A.13.2.1, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.17.1.2, A.17.2.1	
DSS02-Yönetilen Hizmet Talepleri ve Olayları	RS.AN-1 RC-RP-1	ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5	Vaka/Olay Yönetimi Hizmet İsteği Yönetimi
DSS03-Yönetilen Problemler	DE.AE-1 RC.RP-1	ISO/IEC 27001:2013 A.16.1.5	Problem Yönetimi
DSS04-Yönetilen Süreklilik	DE.DP-5 ID.BE-5 ID.GV-4 ID.RA-4 ID.SC-5 PR.IP-7 PR.IP-9	ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1, A.17.1.3, A.16.1.1, A.17.1.1, A.17.1.2, A.16.1.6	Servis Sürekliliği Yönetimi

DSS05-Yönetilen Güvenlik Hizmetleri	ID.AM-3 PR.AC-1 PR.AC-2 PR.AC-3 PR.AC-6 PR.IP-5 PR.MA-2 PR.PT-2 PR.PT-3 PR.PT-4 DE.CM-1 DE.CM-4 DE.DP-1	ISO/IEC 27001:2013 A.13.2.1, A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.6.2.2, A.13.1.1, A.13.2.1, A.6.1.1, A.6.1.2, A.7.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.4, A.15.1.1, A.15.2.1, A.12.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9	
DSS06-Yönetilen İş Süreç Kontrolleri	ID.AM-6 PR.AC-1 PR.AC-6 PR.AT-2 PR.DS-1 PR.DS-2	ISO/IEC 27001:2013 A.11.2.6, A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.6.1.2, A.7.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4, A.6.1.1, A.7.2.2, A.8.2.3, A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	Ölçüm ve Raporlama
MEA01-Yönetilen Performans ve Uyum İzlemesi	ID.SC-4	ISO/IEC 27001:2013: A.15.2.1, A.15.2.2	Ölçüm ve Raporlama
MEA02-Yönetilen İç Kontrol Sistemi		ISO/IEC 27001:2013 Genel Gereklilikler 9.1, 9.2, 9.3, 10.1,10.2	Ölçüm ve Raporlama
MEA03-Yönetilen Dış Gereksinimlerle Uyum	ID.GV-3 RC.CO-2	ISO/IEC 27001:2013 A.18.1	Ölçüm ve Raporlama

MEA04-Yönetilen Güvence		ISO/IEC 27001:2013 Genel Gereklilikler 9.1, 9.2, 9.3, 10.1,10.2 ISO/IEC 27001:2013 A.18	Ölçüm ve Raporlama

SONUÇ

Dünya genelinde nereye kadar gelişeceğini şimdiden tahmin edemediğimiz, hızla koşan, büyüyen ve değişen teknoloji kapasitesinin her geçen gün artması, internet kullanımı ve sosyal mecraların dünyayı düz, verileri kolay erişilebilir kılması ve dijital dönüşümün hem günlük hayatı hem de iş dünyasını hızla uçtan uca sarması beraberinde birçok avantajın yanı sıra kurumları veri güvenliği ve siber güvenlik riskleriyle de karşı karşıya bırakmaktadır.

Pandemi ile hatırlanacak bir seneyi geride bıraktığımız günlerde dijital platform ve bilişim araçlarının kullanımında, Dünya Sağlık Örgütü (World Health Organization-WHO)'nün yaşanan krizin mevcut koşulları doğrultusunda bir pandemi olduğunu resmi olarak ilan etmesi ile öngörülmeyen bir artış olduğu görülmektedir. Bu öngörülmeyen büyüme ve kontrolsüzce yayılan her türlü veriye erişebilirlik kabiliyeti, hem kişileri hem de kurumları mevzuatlara uyum çerçevesinde önemli bir sınava tabi tutmaktadır. Mevzuata uyum, risk yönetimi perspektifinden yapılmazsa, dünyanın sürüklendiği kriz döneminde karşılaşılan dinamik tehdit alanlarına yenik düşülmesi kaçınılmazdır.

Veri güvenliğinin günümüzde çok ciddi tehditlerle karşı karşıya olduğunu henüz tamamladığımız 2020 yılında, gerçekleştirilen uluslararası siber saldırıda zararlı yazılım içeren Covid-19 içerikli e-postalar çeşitli kullanıcılara paylaşılarak yalnızca 5 saat içinde 2500 bilgisayarı ve bilgisayarlarda bulunan kişisel verilerin ele geçirilmesi, Dünya Sağlık Örgütü, Dünya Bankası, IMF'yi hedef alan siber saldırılar 5 kat artması üzerine Interpol WashYourCyberHands (SiberEllerinizi Yıkayın) sloganıyla kurum ve bireyleri veri güvenliğine ilişkin farkındalığa çağırdı. Pandemi öncesi süreçte önemli giderek artan veri güvenliği, tüm çalışma fonksiyonlarının uzaktan çalışma yöntemine geçişi ve bireylerin sokağa çıkmama kuralları neticesinde neredeyse tüm hayati, sosyal, finansal vb. faaliyetlerini evlerinden gerçekleştirmek zorunluluğu gibi majör etkenler sayesinde bugün yaşanan zamanın en büyük sorunu haline gelmiştir. İnsan sağlığına Covid-19'un virüs etkisi ne ise, krizi fırsata çeviren veri güvenliği tehditleri de siber alanda farklı bir virüs etkisi göstermiştir. Bugünün dünyasında, kurumların üretken ve rekabetçi iş modellerini sürdürebilmeleri ancak uzaktan çalışan

personellerinin verimli çalışma aksiyonları ile sağlanabilmektedir. Kriz yönetimi ve iş sürekliliği gibi önceden hazırlanılması gereken adımları atmayan kurumlar, çalışanlarının yönetmediği veya güvenmediği makineler, bilişim ortamları ve ağlardan kritik iş sistemlerine ve verilere erişmesine izin vermek durumunda kalarak, veri güvenliği riskinin katlanarak büyüdüğünü göstermektedir. Bugün pek çok kurumun hâlihazırda resmi bir uzaktan çalışma politikası bulunmadığı görülmektedir. Eğer çalışanları yönlendirecek bir rehber oluşturulmaz ise uzaktan çalışma onayları yetkisiz olarak kullanılabilir ve suistimal riski doğurur.

Günümüzde siber güvenlik tehditleri, veri güvenliğinin ne kadar önemli olduğunu göstermektedir. Nitekim gerçekleşen siber atakların neredeyse tümü kişisel veriyi hedefler hale gelmiştir. Bu nedenle veri güvenliği hem bireyler hem de kurumlar için büyük öneme sahiptir. Veri güvenliğinin ve özellikle kişisel veri gizliliğinin yeterli seviyede sağlanamaması kurumların finansal kayıplar yaşamasına, iş operasyonu aksamalarına, itibar hasarlarına, mevzuat uyumsuzluğuna ve ticari sırların ifşa edilmesine neden olmaktadır.

Yeni dönemde bilinen siber güvenlik ve veri hırsızlığı ataklarına artık sosyal medya platformlarında yaşanan veri güvenliği ihlalleri eklenmiştir. Web 2.0'ın kullanıcı hizmetine sunulmasıyla birlikte sosyal medya hayatımıza girmiş ve 2000'li yıllar tek yönlü bilgi paylaşımından, çift taraflı ve eş zamanlı bilgi paylaşımına ulaşılmasını sağlayan medya sistemlerinde gün geçtikçe veri güvenliği tehditlerini beraberinde getirmiştir. Günümüz popüler veri güvenliği ihlal haberlerinden çokça ilgi toplayan örneği, Mart 2018 tarihinde kendisi de Cambridge Analytica çalışanı olan Christopher Wylie'nin ihbarı ile ortaya çıkan haberlerde, firmanın 2015-2016 yıllarını kapsayan süreçte siyasi danışmanlık verdiği seçim kampanyasında, 87 milyon Facebook kullanıcısı profilleri üzerinden yasal olmayan şekilde kişisel verilerinin kullanılarak psikografik modelleme teknikleri uyguladığı ortaya çıkmasıdır. Tüm dünyada yankı bulan olayda görülmüş oldu ki kişisel verilerimiz düşündüğümüzden çok daha etkili bir silah haline gelebilmektedir. Büyük veri analiz yöntemleri ile artık yalnızca psikolojik profil değil, sosyolojik, ekonomik, hatta biyolojik profiller oluşturulabilmektedir. Facebook ortaya çıkan büyük veri ihlali sonucunda hukuken birçok süreç yaşamış ve hisseleri yüzde 24 değer kaybetmiştir. Mayıs 2019 tarihinde

Facebook'un sahibi olduğu WhatsApp uygulamasını hedef alan bir saldırıda, kullanıcıların mesajlarına, e-postalarına, mikrofonlarına ve kameralarına yetkisiz ve yasal olmayan şekilde erişim sağlanmıştır. 2020 yılına gelindiğinde günümüzün en çok kullanılan haberleşme uygulaması haline gelen WhatsApp, kişilerin uygulama üzerinden paylaştığı verileri işleme metodu ile veri güvenliği hususunda hukuki uygulama konusunda farklı ülkelere tehdit oluşturmayı sürdürmektedir. Haziran 2019 tarihinde, yaklaşık 100 bin kişinin biyometrik görüntülerini ve araç plakalarını da içeren ABD Gümrük ve Sınır Muhafaza verileri çalınmıştır. Yani, son yıllarda yaşanan her türlü siber saldırının amacı değerli veriye sahip olmaktır. Bu örnekler gün geçtikçe artmakta, vahim olarak ise artık alışılagelmiş olmaktadır.

Türkiye'de veri güvenliğine ilişkin güncel mevzuat yaklaşımlarına bakıldığında dünyadan çok da farklı olmadığı kolaylıkla görülebilir. Dijital ortamda verinin güvenliğinin sağlanması tüm iş modeli ve mevzuat uyumlarının kökenindedir. Veri güvenliğinin sağlanması konusunda birbirinden farklı yaklaşımlar aynı amaçla denetim ve kontrol fonksiyonlarını sağlamaktadır. Veri güvenliği ancak, veri güvenliğinin bozulmasına sebep olan ya da olabilecek risk ve tehditlerin tayin edilmesi ve yönetilmesi ile mümkündür. Risk tabanlı veri güvenliği uygulamaları özellikle Genel Veri Koruma Yönetmeliği (GDPR) yaklaşımı ile daha bilinir ve uygulanabilir olmuştur. Her riskin verileri üzerinde bir etkisi olacağı yaklaşımı, veri güvenliği çerçevesinde risk etki analizi kavramını hukuki olarak ortaya çıkmıştır. Çalışmada anlatılan GDPR ilkeleri arasında bulunan hesap verebilirlik ile gelen "sorumluluk ilkesi" KVK Kanunu kapsamında açıkça ifade edilmesi bile hukuka aykırı işleme ve davranışların müeyyidelere bağlanan hükümlerinden aynı sonuca varmak mümkündür. Bu anlamda kişisel veriler, işlenmesi gerekli ise sınırlı ve ölçülü bir şekilde işlenmelidir. İşlenmeyi gerektirmeyecek veriler işleme alınmamalıdır. Gerçekleşen her türlü kişisel veri faaliyetinin kayıt altına alınarak, amaca bağlı sebeplendirilmesi veri güvenliğinin sağlanması hususunda da çok kritik rol oynamaktadır. GDPR'nin 37. maddesi gereği işin doğası gereğince büyük ölçüde ya da hassas veri işleyen kurumlara atanması zorunlu olan DPO özellikle hesap verebilirlik ilkesinin sağlanmasını sağlamakla görevlidir. DPO rolü bu yaklaşımla otoriteye karşı bir sorumluluk taşırken ilişkili kurumun şeffaflığını da temsil eder. Veri güvenliği

ihlallerinin ve yasal uygunsuzluğa sebep olacak her türlü oluşumun önlenmesi için hesap verilebilirlik ilkesinin kurumların yönetim modellerinde sürekliliğinin sağlanması şarttır. Veri güvenliğinin sağlanması yaklaşımında hesap verebilirlik ilkesi bir seferlik bir çalışma (box ticking exercise) değildir. Hesap verilebilirlik ilkesinin uygulanabilmesi için kurum stratejisi, veri güvenlik modeli, risk değerlendirmeleri, çalışan farkındalığı ve güvenlik politikaları bu ilkeyi kavramalı ve benimsemeli, iş modellerinde sürekli bir şekilde uygulanmalıdır.

Risk analizi ve yönetimi konusunda kurumsal organizasyonların küresel standart, çerçeve ve en iyi uygulama yaklaşımlarını yönetişim yapılarına entegre etmeleri şarttır. Sürekli izlenebilir ve ölçümlenebilir bir veri güvenliği olgunluk seviyesi farkındalığı, ancak belirlenmiş risklerin yönetimi ve yeni tehditlerin öngörümlenebilmesi ile mümkündür.

İş modellerini şekillendiren veri güvenliğine ilişkin mevzuatlar belirli sektörlere yönelik ya da sektör bağımsız şekilde uygulama alanına sahiptir. Özellikle farklı büyüklükte ve farklı sektörlerde de faaliyet gösteren şirketlerin aynı hukuki düzenleme esaslarına ve yaptırımlarına uyum sağlamaları noktasında sıklet farkı kaçınılmazdır. Kurumsal, finansal ve yapısal olarak birbirinden farklı olan bu şirketler, kurumlar ya da organizasyonlar kanuna uyum şartlarını aynı olgunluk seviyesinde karşılayamamaktadır. Bilgi Güvenliği Yönetim Sistemi (BGYS) faaliyetleri açısından her kurumun birbirinden farklıdır. Büyük ölçekli firmalar veri güvenliği alanında büyük yatırımlar yapabilirken, orta ve küçük ölçekli birçok firma aynı bütçelere sahip değildir. Veri güvenliğinin sağlanması anlamında çok çalışanlı ve değerli veri üreten kurumların teknolojik çözüm ürünlerinden faydalanmaları bir ihtiyaçtır. Özellikle DLP, SIEM, veri envanteri uygulamaları vb. teknoloji çözüm ürünleri mevzuat gereksinimlerine göre değiştirilip geliştirilmektedir. Bu teknolojik çözümler merkezileştirilmiş ve yeknesak bir veri güvenliği yönetim modeli kurulmasında belirleyici unsurlardır. Ancak kurumlar veri güvenliğinin sağlanması noktasında öncelikle veri güvenliği önemini ve uygulama yöntemini tüm çalışanlarına, hizmet aldıkları ve sağladıkları ilişkili taraflara açık, net ve anlaşılır şekilde duyurmalıdır. Büyük, orta ve küçük ölçekli kurumlar bilgi sistemleri yönetimini kurumsal yönetim uygulamalarının bir parçası olarak ele almalıdır. Bilgi sistemlerinin etkin yönetimi için

gerekli finansman ve insan kaynağını sağlamalı, bilgi varlıklarının, elektronik ve fiziksel bilişim ortamlarının güvenliği, gizliliği, bütünlüğü ve erişilebilirliğini sağlamak amacıyla bilgi sistemleri üzerinde etkin kontrollerin tesis edilmesini amaçlamalıdır. Veri güvenliğinin sağlanabilmesi bilgi sistemlerinin kullanımından kaynaklanan risklerin yönetilmesi ile mümkündür.

Yapılan çalışmada Türkiye'de en bilinen küresel standart, çerçeve ve en iyi uygulama yaklaşımları örneklerinden olan ISO 27001, COBIT, NIST, ITIL detaylı bir şekilde incelenmiş ve veri güvenliği açısından mevzuatlara paralel kontrol başlıklarını nasıl sağlayabileceği tartışılmıştır. Veri güvenliği risk analizi denetimi sağlayacak bir kaynak olarak ISO 27001, COBIT, NIST, ITIL ilişkisel olarak değerlendirilmiş ve bu değerlendirmeler tablolaştırılarak kontrol listelerine yol gösterebilecek hale getirilmiştir. Geçmişten günümüze ulaşan deneyimlerin harmanlanarak, sektörel tecrübe ve yönetişim algısı ile hazırlanılmış bu kaynaklar, kurumların veri güvenliği yaklaşımlarında en büyük yol göstericileri olmalıdır.

Ulusal ve uluslararası bakış açısıyla veri güvenliği çağımızın gelişen ve değişen dünyasında daha nice tehdit ve riskle karşılaşacaktır. Büyük veri, bulut bilişim, IoT gibi büyük teknolojik adımlar, bugün yaşantımızda dakikalar içerisinde milyonlarca kez kullanılmakta ve artık günlük yaşamın büyük bir parçası haline gelmiş durumdadır. Bireylerin ve kurumların kişisel veri güvenliğini sağlayabilmeleri için risklere karşı farkında olmaları ve dirençli güvenlik önlemleri almaları gereksinimi kaçınılmazdır. Türkiye'de son dönemde gerçekleşen siber güvenlik hareketinin global dünyada daha güçlü bir hale gelmesi, ulusal girişimlerle olduğu gibi uluslararası platformlarda da varlığını gösterebilmesi ile mümkündür. Bu anlamda ülkemizde teknolojik alanda atılan her veri güvenliği adımı, çeşitli hukuki dayanaklar ile güçlendirilmiştir. Normatif bir bilim olan hukukun matematiğinde; birey, kurum ve devlet olmak üzere ana etkenlerin ortak menfaati gözetilecek şekilde hak ve özgürlüklerin korunması, ancak küresel dünya ile kucaklaşmış bir ulusal teknoloji zenginliği ile sağlanabilir. Bu sayede ülkeler küresel hukuk sahnesinde kanun koyucu lokomotif niteliğini teknoloji güçleri ile vurgulayabilirler. Ulusal ve uluslararası veri güvenliğinin etkin bir şekilde sağlanabilmesi; verileri paylaşmamak değil, paylaşılan veriyi koruyabilmek demektir.

Kurumlar dijital dönüşümün bir parçası olarak yönetişim kavramında BT yönetişimine gereken değeri verip, yönetim kurulu seviyesinde veri güvenliğini tartışıp aksiyon alabilecek ortak dili sağlamalıdırlar. Bu sayede teknoloji ve hukuk ilişkisi, yalnızca cezalardan kaçınmayı sağlayacak bir kontrol listesi niteliğinde değil, kurumsal iyileştirme adımlarını kararlılık ile atabilecek bir güç olacaktır. Yeni iş modelleri, yeni teknoloji çağında yeni nesiller ile artan risklere ve tehditler karşı veri güvenliğini etkin şekilde sağlayabilecek güç ve yetkinlikte olmalıdır.

KAYNAKÇA

Akıncı : Ayşe Nur Akıncı, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuk Bakımından Değerlendirilmesi, T.C. Kalkınma Bakanlığı, İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü, 2017, S.36.

Canberk : Canberk Gürol, Şeref, Sağıroğlu, Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme Politeknik Dergisi, C.9, S.3, 2006 s. 165-174.

Cisco : Cisco Annual Internet Report (2018–2023) White Paper, 2020.
Erişim adresi:
https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
(Erişim tarihi: 05.01.2021)

CNN : How Obama's data crunchers helped him win, 2016.
Erişim adresi:
http://edition.cnn.com/2012/11/07/tech/web/obama-campaign-tech-team/
(Erişim tarihi: 05.01.2021)

Cooper : R. B. Cooper, The Inertial Impact of Culture on IT Implementation, Information & Management, 1994, S.27, 17-31.

COSO :COSO, Enterprise Risk Management Integrated Framework: Executive Summary, 2004.

Dalto : Jeffrey Dalto, The Three Phases of Risk Assessment: Risk Management Basics, 2019.
Erişim tarihi:
https://www.convergencetraining.com/blog/three-phases-risk-assessment-risk-management-basics
(Erişim tarihi: 06.01.2021)

Danby : Sophie Danby, The ITIL 4 Service Value System Explained.
Erişim adresi:
https://itsm.tools/the-itil-4-service-value-system-explained/
(Erişim tarihi:06.01.2021)

Demirci : M. Demirci, Bilgi Güvenliği. Ankara : Kamu Hastaneleri Kurumu, 2015, S.30.

Determann : Lothar Determann, Determann's Field Guide To Data Privacy Law International Corporate Compliance, Fourth Edition, Elgar Compliance Guides, 2020, S.170-171

DDI : DDI, 2018, Why use DDI (Data Documentation Initiative).
Erişim adresi:
https://www.ddialliance.org/training/why-use-ddi
(Erişim tarihi: 05.01.2021)

Erdoğan : M. Erdoğan, Yönetişim-Risk-Uygunluk Yaklaşımı ve İç Denetim Fonksiyonu İlişkisi: İç Denetim Sorumluluklarının Yaklaşımına Etkisi Üzerine Yapısal Eşitlik Modeli Araştırması, S. 2, 2019, s. 149-198.

Eskiyörük : D. Eskiyörük, BGYS Risk Yönetim Süreci Kılavuzu, Kocaeli: Tübitak, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, 2007.

Frické : M. Frické, The Knowledge Pyramid: A Critique of the DIKW Hierarchy, Journal of Information Science, 35 (2), 2009,131-142.

Friedman : Thomas L. Friedman, Dünya Düzdür: Yirmi Birinci Yüzyılın Kısa Tarihi, Çevirmen: Levent Cinemre, Boyner Yayınları,2006.

GSG Hukuk Bülten : 2021 Yılı KVKK İdari Para Cezaları.
Erişim adresi:
https://www.gsghukuk.com/tr/bultenler-yayinlar/duyurular/2021-yili-kvkk-idari-para-cezalari.html
(Erişim tarihi: 06.01.2021)

ICO : ICO, Information Commissioner's Office / Bilgi Komisyonu Ofisi, Data protection impact assessments
Erişim adresi:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
(Erişim tarihi: 06.01.2021)

ISACA : ISACA® Glossary of Terms English – Turkish First Edition, 2018.
Erişim adresi:
https://www.isaca.org/resources/glossary
(Erişim tarihi: 04.01.2021)

ISACA : COBIT® 2019 Framework: Introductıon & Methodology.

ISACA : COBIT® 2019 Framework: Governance And Management Objectives.

iso.org : ISO/IEC 27001:2013Information technology - Security techniques - Information security management systems – Requirements.
Erişim adresi:
https://www.iso.org/standard/54534.html
(Erişim tarihi: 05.01.2021)

Itgovernance.co.uk : ISO 27001: The 14 control sets of Annex A explained, 2020.
Erişim adresi:
https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained
(Erişim tarihi: 06.01.2021)

ISMS.online : ISO 27001 Will Help Reduce Information Security And Data Protection Risks To Your Organisation, 2019.
Erişim adresi:
https://www.isms.online/iso-27001/#:~:text=ISO%2027001%20can%20be%20traced,organistions%20keep%20information%20assets%20secure.
(Erişim tarihi: 07.01.2020)

Jenik : Claire Jenik, A Minute on the Internet in 2020, Statista, Visual Capitalist, 2020.
Erişim adresi:
https://www.statista.com/chart/17518/data-created-in-an-internet-minute/
(Erişim tarihi:05.01.2021)

Kalman : S. Kalman, Web Security Field Guide. Indianapolis, 2003.

Kaya - Taştan : Mehmet Bedii Kaya, Furkan Güven Taştan, Kişisel Veri Koruma Hukuku, Mevzuat, İçtihat, Bibliyografya, 2. Baskı, Oniki Levha Yayıncılık, 2019, s.221-223.

kvkk.gov.tr : Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi, Teknik ve İdari Tedbirler.
Erişim adresi:
https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf
(Erişim tarihi: 04.01.2020)

Knowledgeapple : ITIL V4 Management Practices, 2020.
Erişim adresi:
https://www.knowledgeapple.com/itil-v4-practices/
(Erişim tarihi: 05.01.2020)

KPMG : KPMG Gündem 2020 Dergisi.
Erişim adresi:
https://assets.kpmg/content/dam/kpmg/tr/pdf/2020/11/Gundem-37.pdf, 2020
(Erişim tarihi:05.01.2021)

Kuner : Christopher Kuner, European Data Protection Law Corporate Regulation and Compliance, Second Edition, Oxford University Press, 2007, S.61-64.

NIST : NIST Special Publication 800-53 Revision 5, Security and Privacy Controlsfor Information Systems and Organizations

NIST : NIST Special Publication 800-30 Revision 1, Managin Information Security Risk

NIST : NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.

Öztürk : Günce Öztürk, Tübitak, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE), Bilgi Güvenliği Politikası Oluşturma Kılavuzu, Doküman Kodu: BGYS-0005, S.1, 2008.

Pehlivanlı : D. Pehlivanlı, Yönetişim, Risk ve Uyum. İstanbul: Beta Basım Yayım Dağıtım, 2015.

Pfleeger : C.P. Pfleeger, The fundamentals ofinformation security, Software, IEEE, C.14, 1997, s.14.

Room,LLM : Stewart Room,LLM, Chairman, National Association of Data Protection and Freedom of Information Officers Proprietor, Data Protection and Compliance in Context, British Cataloguing in Publication Data, s. 57,63,112, 2007.

Ross-Hellauer : T. Jones Ross-Hellauer, Research Data Management: An Introductory webinar, 2016. Erişim adresi: https://webinars.eifl.net/2016-05-26_ResearchDataManagementAnintroductoryWebi1/default.html (Erişim tarihi: 05.01.2021)

Shephard : B. Shephard, Information security-who cares?. Power System Management and Control, Fifth International Conference, Conf. Publ. No. 48, 2002, 126s.

Stewart : Thomas A. Stewart, Entelektüel Sermaye Kuruluşların Yeni Zenginliği, Çev: Nurettin, Elhüseyni, BZD Yayıncılık, 1997, 339s.

Symeonides : Markos Symeonides, A Brief History of ITIL, 2020. Erişim adresi: https://info.axiossystems.com/blog/itil4-the-evolution-of-processes (Erişim tarihi:06.01.2021)

Tekerek : Mehmet Tekerek, Bilgi Güvenliği Yönetim Bilişim Güvenliği Kitapçığı. Prog Bilişim Güvenliği ve Araştırma, s.7, 2007.
Erişim adresi:
http://www.prog.com.tr/whitepapers/bilisim guvenligi-v1.pdf
(Erişim tarihi:05.01.2021)

Turan : Mustafa Turan, NIST Cybersecurity Framework Süreçsel Yapılandırma, 2020.
Erşim adresi:
https://mturan.net/blog/nist-cybersecurity-framework-surecsel-yapilandirma/
(Erişim tarihi:05.01.2021)

Vercellis : C. Vercellis, Business Intelligence: Data Mining and Optimization for Decision Making, John Wiley & Sons Ltd., UK., 2009.

Youtube :The Power of Big Data and Psychographics, 2016.
Erişim adresi:
https://www.youtube.com/watch?v=n8Dd5aVXLCc
(Erişim tarihi: 05.01.2021)

EKLER

Ek A.1 COBIT 2019 - ITIL Haritalanması