TÜBİTAK
BİLGEM
YTE

DİJİTAL KABİLİYET
REHBERLERİ

BİLGİ GÜVENLİĞİ YÖNETİMİ REHBERİ
İŞLETİM VE BAKIM

Ocak 2021

DEĞİŞİKLİK TARİHÇESİ

Rev. No	Yayın Tarihi	Yayın Nedeni	Hazırlayan(lar)
Sürüm 1	Ocak 2021	İlk sürüm	TÜBİTAK BİLGEM YTE

İÇİNDEKİLER

TABLOLAR

ŞEKİLLER

YÖNETİCİ ÖZETİ

Dijital Devlet (d-Devlet) alanında ülkemiz koşulları ile kamu kurumlarının ihtiyaçlarını göz önünde bulunduran ve uluslararası çalışmaları dikkate alan, kurumsal dijital kabiliyetlerini bütüncül bir yapı üzerinden değerlendirmeyi sağlayan **Dijital Olgunluk Değerlendirme Modeli'**nin geliştirilmesi ve bu **Model** ile uyumlu **Rehberlerin** hazırlanması ile dijital kurumsal kapasitenin artırılmasına ihtiyaç bulunmaktadır. Bu ihtiyaç doğrultusunda TÜBİTAK-BİLGEM-YTE tarafından iç destekli olarak **Dijital Olgunluk Değerlendirme Modeli ve Rehberlik** (DİJİTAL-OMR) Projesi 2016 yılında başlatılmıştır. Proje kapsamında d-Devlet çalışmalarında sistemli ve bütüncül bakış açısı getirilerek kamu kurumlarının dijital yetkinliklerinin geliştirilmesi ve yürüttükleri proje ve faaliyetlerinin etkililik, etkinlik ve bilgi güvenliği niteliklerinin artırılması ile dijital kamu hizmetlerinin kalite ve performansının iyileştirilmesi sağlanacaktır.

Modeli ve **Rehberlerin** hazırlanmasına yönelik ulusal politika hedefleri, ülkemizde geliştirilen ve uygulamaya alınan Bilgi Teknolojileri (BT) rehber ve olgunluk modelleri ile 5 uluslararası kuruluş, 12 danışmanlık firması, 6 ülke tarafından geliştirilen standart, rehber ve çerçeve modelleri, uygulama örnekleri ve ilgili akademik çalışma örnekleri incelenmiştir. Farklı dijital kabiliyet alanlarında 34 bilişim uzmanından tecrübe aktarımı sağlanmıştır. Merkezi Yönetim ile yapılan anket üzerinden ilgili kapsama giren konular özelinde anket sonuçları analiz edilmiştir. Elde edilen tespitler doğrultusunda, **Dijital Olgunluk Değerlendirme Modeli**'nin taslağı oluşturulmuş ve seçilen kamu kurumlarında pilot uygulama yapılmıştır. Pilot uygulama sırasında alınan geri bildirimler doğrultusunda **Model** nihai hale getirilmiştir. **Model** ile Stratejik Yönetim, Organizasyon, Yazılım Hizmetleri, Yazılım Yaşam Döngüsü, BT Hizmetleri, İşletim ve Bakım, d-Hizmetler başlıklarında yedi yetkinlik belirlenmiştir. Bu yetkinlikler altında gruplandırılmış dijital kabiliyetler bazında seviyelendirilmiş 2834soru belirlenmiştir.

Model'in 8 kurumda uygulaması yapılarak Dijital Olgunluk Seviyeleri belirlenmiş ve dijital kabiliyetler bazında tespit değerlendirmeleri gerekçelendirilerek Dijital Olgunluk Seviyesini geliştirmeye yönelik kısa, orta ve uzun vadede çözüm önerileri sunulmuştur.

Dijital Olgunluk Değerlendirme Modeli kapsamında yer alan yetkinlikler ve söz konusu yetkinlikler kapsamında yer alan dijital kabiliyetler dikkate alınarak yol gösterici olarak kullanılmak üzere **Rehberler** hazırlanmaktadır. Kurumsal kaynakların büyük bir kısmının işletim ve bakım proje ve faaliyetlerine ayrılmış olduğu tespitinden hareketle, ilk olarak **İşletim ve Bakım Rehberi** hazırlanmış ve 2017 yılında yayımlanmıştır. **Rehber**'de, işletim ve bakım yetkinliği altında toplanan kabiliyetler bazında tespit edilen seviyelendirilmiş

sorular ile kurumların mevcut olgunluğuna yönelik referans, rol, işleyiş, iş akışı ve çıktılar ile ilgili bilgiler sunulmaktadır. Aynı yıl **Model** ile belirlenen tüm dijital kabiliyetler için, yatırım planlanırken dikkate alınması gereken unsurlar ve alternatifleri ile ilgili bilgi ve yönlendirmeleri içeren 32 adet **Dijital Kabiliyet Rehberi** hazırlanmıştır. Söz konusu rehberlerin yetkinlikler altında ve tüm yaşam döngüsü dikkate alınarak genişletilmesine yönelik rehber hazırlama çalışmaları devam etmekte olup bu kapsamda 2018 yılında **BT Hizmetleri** yetkinliği altında yer alan **Veri Merkezi Rehberi**, 2019 yılında aynı yetkinlik altında **Kablosuz Ağların İşletimi Rehberi**, **Kablosuz Ağların Yönetimi Rehberi**, **Aktif Dizin Yönetimi Rehberi**, **Sunucu Yönetimi Rehberi ve İstemci Yönetimi Rehberi** yayımlanmıştır. 2020 yılı içerisinde bunlara ek olarak **Uzaktan Çalışma Rehberi**, **VOIP Rehberi, Alan Adı Sistem Yönetimi Rehberi ve Bilgi Güvenliği Yönetimi Rehberi** yayınlanmıştır.

Bilgi Güvenliği Yönetimi Rehberi, On Birinci Kalkınma Planı'nda da yer alan, kuruluşların " BGYS oluşturmasına, uygulamasına, çalıştırmasına, izlemesine, gözden geçirmesine, sürdürmesine ve sürekli iyileştirmesine" yardımcı olmayı amaçlamaktadır. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayınlanan Bilgi ve İletişim Güvenliği Rehberi'nin temel amacı ise; bilgi güvenliği risklerinin azaltılması ortadan kaldırılması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik bilgi/verinin güvenliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve belirlenen tedbirlerin uygulanması için yürütülecek faaliyetlerin tanımlanmasıdır. Bilgi Güvenliği Yönetimi Rehberi'nin, bilgi işlem birimi barındıran veya bilgi işlem hizmetlerini sözleşmeler çerçevesinde üçüncü taraflardan alan, devlet teşkilatı içerisinde yer alan kurum ve kuruluşlar ile kritik altyapı hizmeti veren işletmelerin bilgi güvenliği yönetim sistemi oluşturmalarına yönelik katkı sağlaması hedeflenmektedir.

Dijital Devlet ekosistemi paydaşlarının değerlendirmesine yönelik tüm **Rehberlerin** https://www.dijitalakademi.gov.tr/ platformu ile açık erişimi sağlanmakta ve **Rehberlerin** kullanımının yaygınlaşması amacıyla eğitim programları, toplantılar ve çalıştaylar düzenlenmesi ile **Rehberlik Mekanizmaları** hayata geçirilmektedir. Bu sayede d-Devlet ekosisteminde görev alan bilişim uzmanlarının yetkinliklerinin artırılması hedeflenmektedir. Yanı sıra **Dijital Olgunluk Değerlendirme Modeli** ile uyumlu olarak 2017 yılında Türkiye'ye özgü **Dijital Yetkinlik Değerlendirme Modeli** geliştirilmiş ve **Model** ile kamu kurumlarında çalışan bilişim uzmanlarının yetkinlik değerlendirmesi yapılarak güçlü ve zayıf yönlerinin belirlenmesi ve eğitim ve mesleki gelişim açısından iyileştirmeye açık alanların tanımlanması amaçlanmıştır. 38 bilişim profesyonel rolü ile bu

rollerdeki çalışanların sahip olması hedeflenen 56 yetkinlik ve yetkinlik için 5 kademeli seviye tanımlanmış olup, roller, yetkinlik alanları ve yetkinlik seviyeleri arasındaki ilişkiler belirlenmiştir. 6 kurumda yaklaşık 550 uzman için yetkinlik değerlendirmeleri yapılmış ve kurumların dijital kapasitelerinin geliştirilmesi için öneriler geliştirilmiştir.

On Birinci Kalkınma Planı'nda ve 2020 Yılı Yıllık Programı'nda belirlenen kurumsal olgunluk ve insan kaynağı yetkinlik modelleri geliştirilmesi ihtiyacının karşılanmasında Dijital Devlet ekosistemine katkı sağlayacağını öngördüğümüz Türkiye'ye özgü geliştirilen ilk **Dijital Olgunluk ve Yetkinlik Değerlendirme Modelleri** ile **Dijital Kabiliyet Rehberleri'nin** içeriğine yönelik olarak epid.yte@tubitak.gov.tr ve https://www.dijitalakademi.gov.tr/ adresleri aracılığıyla ileteceğiniz değerlendirmelerinizle ilgili çalışmaların tüm ekosistemin bilgi ve tecrübesiyle iyileştirilmesini temenni ederiz.

1 GİRİŞ

Bilgi Güvenliği Yönetimi Rehberi 5 bölümden oluşmaktadır:

1. Bölüm'de, dokümanın kapsamı, kullanılan terimler ve yararlanılan kaynaklar,
2. Bölüm'de, Proje'nin amacı ve kapsamı,
3. Bölüm'de, Dijital Olgunluk ve Yetkinlik Değerlendirme Modelleri ile ilgili bilgiler,
4. Bölüm'de, Bilgi Güvenliği Yönetimi Rehberi'nin gerekçesi, yapısı, kapsamı ve ilgili çalışmalar,
5. Bölüm'de, Bilgi Güvenliği Yönetimi Rehberi kapsamında tanımlanan kabiliyetlere ilişkin yönlendirici bilgiler

sunulmaktadır.

1.1 TERİMLER VE KISALTMALAR

Terim / Kısaltma	Tanım
Açıklık	Tehditlere karşı savunmaz bulunan alan
Akıllı Kart	Temaslı veya temassız olarak kart okuyucu cihazlardan okunabilen, içerisinde kendine özel işlemcisi olan, özel şifreleme tekniğiyle izinsiz kopyalanma ve içeriğini okumaya izin vermeyen plastik kartlardır.
Altyapı	Sunucular, istemciler ve diğer BT ekipmanları ve bu ekipmanların birbirleri arasındaki iletişimi sağlayan araçların tümü
BGYÖK	Bilgi Güvenliği Yönetim Komitesi
BGYS	Bilgi Güvenliği Yönetim Sistemi
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

Terim / Kısaltma	Tanım
Bilgi Güvenliği	Bilginin gizlilik, bütünlük ve erişilebilirlik niteliklerinin korunmasıdır.
Bilgi Varlığı	Bulunduğu biçim ve yapıdan bağımsız kurumsal bilgilerdir.
BT	Bilişim Teknolojileri
d-Devlet	Dijital Devlet
Destek Birimler	İhtiyaç durumunda işin gerçekleşmesinde faydanılan birimlerdir
Entegre	Birbirleri ile tümleşik halde bulunma durumu
Erişilebilirlik	Hizmetin veya hizmeti oluşturan bileşenin ihtiyaç duyulduğunda istenilen fonksiyonu gerçekleştirebilme durumudur.
Erişilebilirlik	Herhangi bir verinin yetkili kişiler tarafından ulaşılabilir halde olması
Etken	Etki yapan, tesir eden etmen
Farkındalık	Bilgi güvenliği ile ilgili gelişen olayların algılama ve duyumsama becerisidir.
Hizmet	Kullanıcını ihtiyaçlarını karşılayarak bir fayda yaratma biçimidir. (ör. Kullanıcıların iletişim ihtiyaçları için sunulan e-posta hizmeti, kurum içi yazışmaların oluşturulması ve yönetilmesi için sunulan doküman yönetim hizmeti, vb.)

Terim / Kısaltma	Tanım
Kabiliyet	Bir işin kalite, bilgi güvenliği, performans vb. gereksinimlerinin karşılanabilmesi yetisidir.
Kullanıcı	Hizmeti kullanan kişilerdir. Kurum içi BT hizmeti kullanıcıları olabileceği gibi, kurumun elektronik ortamda sunduğu kamu hizmetlerinin son kullanıcıları (vatandaş, özel sektör, diğer kurumlar vb.) da olabilir.
LOG	Sistemde meydana gelen işlem ve olayların kaydedildiği dosyalara verilen addır.
Olgunluk	Önceden tanımlanmış bir durumu sağlama halidir.
Olgunluk Değerlendirme Modeli	Başlangıç durumundan, önceden tanımlanmış yetkinlik alanlarındaki olgunluk durumuna kadar, öngörülen, arzu edilen ya da tercih edilen yol doğrultusunda, sıralı düzeyler ya da aşamalar içeren modeldir. İlgili alanda referans modele göre mevcut durumun değerlendirilmesi ve referans modele göre iyileştirme alanlarının belirlenmesi için kullanılır.
Problem	Bir veya birden fazla arızaya/kesintiye neden olan ve çözülmesi istenen sorundur.
Risk	Hedeflenen kazanç veya çıktıya, gelecekte olumlu veya olumsuz etkisi olabilecek belirsizliklerdir.
STK	Sivil Toplum Kuruluşu
Süreç Sahipleri	Bir sürecin yönetiminden sorumlu olan kişi veya kişiler

Terim / Kısaltma	Tanım
Şifreleme	Bir veriyi matematiksel işlemler kullanarak şifreli duruma getirme
Tehdit	Bilgiye zarar verme olasılığına sahip herhangi bir şey
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
Yetkinlik	Kabiliyet ya da kabiliyet gruplarının bir yaşam döngüsü ve amaç bazında gruplanmış şeklidir.
YTE	Yazılım Teknolojileri Araştırma Enstitüsü
Yüklenici	Bir işi başkası adına yapmayı üstlenen kimse

1.2 REFERANSLAR

Ref 1. An Introduction to Information Security (2017), Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), Amerika Birleşik Devletleri

Ref 2. IT Grundschutz (2020), Bilgi Teknolojileri Güvenliği Enstitüsü (BSI), Almanya.

Ref 3. BIS Standard 200-1: Information Security Management Systems (2017), Bilgi Teknolojileri Güvenliği Enstitüsü (BSI), Almanya.

Ref 4. ISO (2013). ISO/IEC 27001 - Information security management.

Ref 5. ISO (2013). ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security controls

Ref 6. ISO (2017). ISO/IEC 27003 - Information technology - Security techniques – Information Security Management Systems – Guidance

Ref 7. ISO (2011). ISO/IEC 27005 - Information technology - Security techniques – Information Security Risk Management

2 DİJİTAL OLGUNLUK DEĞERLENDİRME MODELİ VE REHBERLİĞİ PROJESİ

Dijital Olgunluk Değerlendirme Modeli ve Rehberlik (DİJİTAL-OMR) Projesi, 2016 yılında TÜBİTAK-BİLGEM-YTE tarafından yürütülen iç destekli bir projedir. Projenin amacı, Dijital Devlet (d-Devlet) alanında gelinen düzeyde ülkemiz koşulları ile kamu kurumlarının ihtiyaçlarını göz önünde bulunduran ve uluslararası çalışmaları dikkate alan kurumsal **Dijital Olgunluk Değerlendirme Modeli'nin** geliştirilmesi ve bu yönde kurumsal kapasitenin artırılması için **Model** ile **Rehberlerin** hazırlanmasıdır.

Bu proje, On Birinci Kalkınma Planı'nda "Kamu Hizmetlerinde e-Devlet Uygulamaları" başlığı altında yer alan aşağıdaki politika ve tedbirler ile desteklenmektedir:

- "811.2. Kamu kurumlarının bilişim projeleri hazırlama ve yönetme kapasitelerinin artırılmasına yönelik eğitimler verilecek ve rehberler hazırlanacaktır."
- "814.2. Kamu kurumlarında bilgi güvenliği yönetim sistemi kurulması ve denetlenmesine yönelik usul ve esaslar belirlenecek, hazırlanacak rehberlerle bu konuda kamu kurumlarına yol gösterilecektir."
- "811.3. Kurumsal olgunluk ve insan kaynağı yetkinlik modelleri geliştirilerek kamu kurumlarında yaygınlaştırılacaktır."

2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'nda doğrudan rehberlik mekanizmalarına yönelik tanımlanan aşağıdaki eylemlere de bu proje ile katkı sağlanacaktır:

- "*E1.1.4-e-Devlet Ekosistemi Rehberlerinin Hazırlanması ve Güncellenmesi*" eylemi, e-Devlet ekosisteminin etkin bir şekilde çalışabilmesi ve sürdürülebilirliği için birlikte çalışabilirlik, kamu kurum / kuruluşlarının internet siteleri ve mobil uygulamaları ile kamu kurum / kuruluşlarının resmi sosyal medya hesaplarının kullanımı ve yönetimine dair rehberler başta olmak üzere mevcut rehberlerin güncellenmesi ve ihtiyaç duyulan yeni rehberlerin hazırlanmasına yönelik bir eylemdir.
- *"E1.1.6-Ulusal e-Devlet Olgunluk Seviyesi Ölçümleme Mekanizmasının Oluşturulması"* eylemi, yaşamsal olaylar bütünlüğünde kamu hizmetlerinin e-Devlet olgunluk düzeyi, Kurum seviyesinde e-Devlet olgunluk düzeyi ve Ulusal e-Devlet olgunluk düzeyi kapsamında e-Devlet olgunluk ve olgunluk ölçümleme modellerinin tanımlanması, tanımlanan bu modeller kullanılarak ulusal düzeyde e-Devlet olgunluk düzeyi ölçümleme çalışmaları ile birlikte, seçilen e-Devlet

hizmetleri ve kamu kurumları için e-Devlet olgunluk düzeyi ölçümleme çalışmalarının yürütülmesine yönelik bir eylemdir.

Proje kapsamında yapılacak faaliyetler, kurumsal düzeydeki dijital dönüşümü ve 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'ndaki eylemler ile hayata geçirilmesi öngörülen ulusal düzeydeki olgunluk değerlendirme modelini destekleyecektir. Bir başka ifadeyle, Proje kapsamında üretilecek **Model** ve **Rehberler** ile kurumların teknoloji odaklı güncel dönüşüm ihtiyaçlarına cevap verebilmek adına kurumsal düzeyden başlayan ve ulusal düzeye çıkan ölçümleme çalışmalarına katkı sağlanacaktır. Dolayısıyla mikro seviyede kurum düzeyindeki kurumsal etkinliği artırma odağı ile şekillendirilen proje çıktıları, makro seviyede ulusal olgunluk düzeyine çekilebilecek bir alt yapı oluşturacaktır. Bu alt yapı sayesinde 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'nda yer alan eylemlerin uygulanabilirliği artırılacaktır.

Dijital Olgunluk Değerlendirme Modeli ile;

- Kamu kurumlarının bilişim proje ve faaliyetlerine sistemli ve bütüncül bakış açısının geliştirilmesi desteklenecektir.
- Kamu kurumları ve sundukları hizmetlerin dijital olgunlukları hakkında bir değerlendirme yapabilmek ve seviye tespit edebilmek mümkün olacaktır.
- Kurumların içinde bulunduğu dijitalleşme sürecinde değişimlere ve yeniliklere uyumu desteklenecektir.

Model kapsamında hazırlanacak **Rehberler** ve **Rehberlik** mekanizması ile;

- Bilişim projeleri ve faaliyetlerinin daha verimli, etkin ve güvenli planlanması, yürütülmesi ve tamamlanması sağlanarak başarı oranının artırılmasına katkı sağlanacaktır.
- Bilişim proje ve faaliyetlerinin verimliliği artırılarak ilgili hizmetlerin kalite ve performansı iyileştirilecektir.
- Bilişim uzmanlarının dijital kabiliyetleri artırılacaktır.
- TÜBİTAK tarafından yürütülen Kamu BT projeleri ile edinilen bilgi ve tecrübenin, özel sektör ve STK ile açık paylaşımı sağlanacak ve ilgili paydaşlar ile karşılıklı bilgi ve tecrübe alışverişi gerçekleştirilecektir.

3 DİJİTAL OLGUNLUK VE YETKİNLİK DEĞERLENDİRME MODELLERİ

Dijital Olgunluk Değerlendirme Modeli, bir organizasyonun önceden tanımlanmış yetkinlik alanlarındaki yetkinlik durumundan hedeflenen ya da gerekli görülen seviyeye kadar, dijital dönüşüm ve/veya dijital hizmet kabiliyetlerindeki seviyelerin değerlendirilmesini ve iyileştirilmesini sağlayan kademeli referans modeldir.

Dijital teknolojilerin yenilikçi fırsatlarıyla iş süreçlerine uyarlanması ve dijital teknolojiler doğrultusunda yeni katma değerli hizmet ve süreçler oluşturulması kurumsal düzeyde dijital dönüşümün en öncelikli amacı olmaktadır. Dünyada özellikle son 10 yıldır dijitalleşmenin ve ülkelerin farklılaşan koşullarına göre geliştirilen birçok dijital olgunluk değerlendirme modeli olmasına karşın, Türkiye'de kamu kurumlarında "e-Kurum" "e-Devlet" ve "dijital" gibi kavramların hiçbirine yönelik olgunluk referans modelinin olmadığı görülmüştür.

Günümüz koşulları değerlendirildiğinde "dijital" kavramı doğrultusunda hazırlanacak ve kurumların dijital dönüşümlerini analiz edip referanslar doğrultusunda yönlendirecek bir modelin ve model uygulama yaşam döngüsünün olması önemli bir ihtiyaçtır. Ancak bilişim ya da bilgi güvenliği standart ve rehberlerine benzer şekilde uluslararası kabul gören bir kurumsal dönüşüm standardı mevcut değildir.

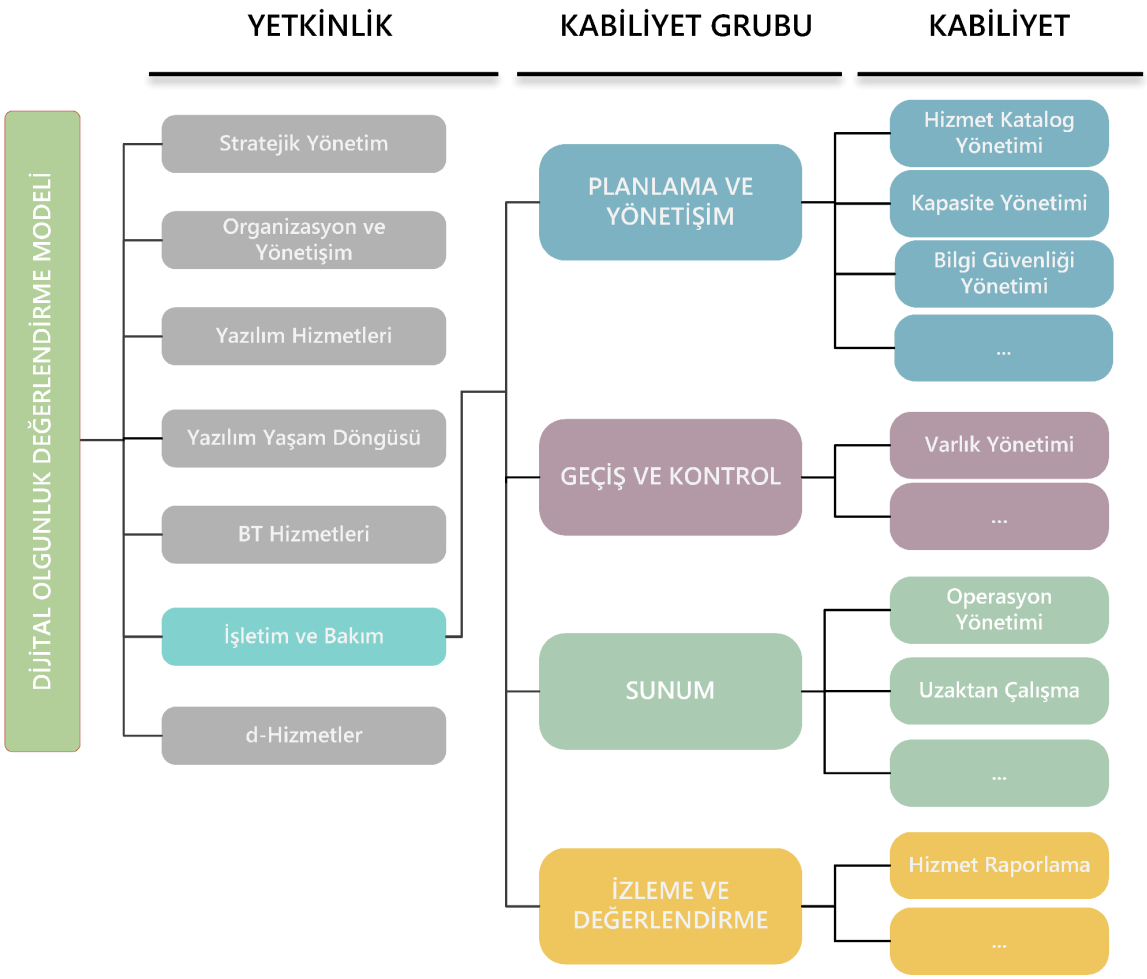
Bununla birlikte, kurumların teknoloji odaklı güncel dönüşüm ihtiyaçlarına cevap verebilmek üzere danışmanlık firmaları ve teknoloji firmaları tarafından oluşturulmuş birçok ticari dijital dönüşüm modeli söz konudur. Bu modellerin çoğunluğu özel sektöre yönelik olarak özel sektör bakış açısıyla hazırlanmaktadır. Ancak ortak alanlar olmakla birlikte kamu kurumlarının ihtiyaçları özel sektör ihtiyaçlarından ayrışmaktadır. Üstelik kamu yönetim anlayışı ve birikimi göz önüne alındığında, ülkemiz diğer ülkeler ile de ayrışmaktadır. Teknoloji odaklı dönüşüm çabası içerisinde olan tüm organizasyonlar için ortak gereksinimler söz konusu iken mevcut koşulları doğrultusunda her organizasyon tipinin kendi içerisinde özelleşmiş ihtiyaçları da olabilmektedir. Bu doğrultuda, kamu kurumlarında dijital dönüşüme yön verilmesi ve uygulamanın başarı ile hayata geçirilebilmesi için öncelikli olarak, kamu kurumlarına yönelik **Dijital Olgunluk Değerlendirme Modeli** oluşturulmuş ve **Model'in** ülke koşullarına uygun yapıya sahip olması sağlanmıştır. Oluşturulan **Model**, aynı zamanda ülkenin mevcut dijital dönüşüm politikalarıyla uyumludur ve uluslararası tecrübeleri dikkate almaktadır.

Model ile bir organizasyonun dijital kabiliyetlerini değerlendirerek, tespit edilen mevcut kabiliyet seviyelerinin iyileşmesi için yol haritası sağlanmaktadır. Böylece, kurumların dijital

dönüşümlerinin yapısal, standart, tutarlı, etkin ve verimli bir şekilde yapılmasına katkı sağlanmaktadır.

Dijital Olgunluk Değerlendirme Modeli gereksinim ağacı 3 basamak olarak oluşturulmuştur:

- Yetkinlik
- Kabiliyet Grubu
- Kabiliyet
    - Alt Kabiliyet



Şekil 1. Dijital Olgunluk Değerlendirme Modeli Gereksinim Seviyeleri

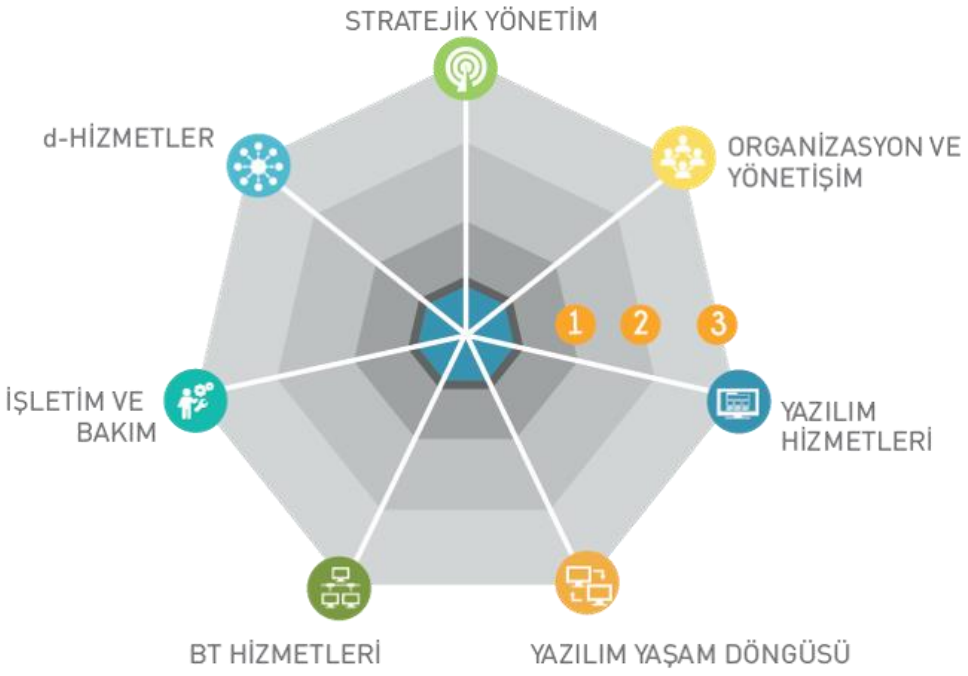
Dijital Olgunluk Değerlendirme Modeli 7 yetkinlik altında tanımlanmış 35 kabiliyet grubu ve bu kabiliyet grupları altında gruplandırılmış çeşitli kabiliyetlerden oluşmaktadır:

- **Yetkinlik**, kendi aralarında ilişki söz konusu olan kabiliyet gruplarından oluşmaktadır. Her bir yetkinlik kendi içerisinde bir bütündür ve organizasyonlarda dijital dönüşüm için müstakil olarak ele alınabilir. Belirlenecek tespitler ve

değerlendirmeler doğrultusunda organizasyonun her bir yetkinlik için yetkinlik seviyesi ortaya konmaktadır.

- Birbirlerine yakın olan kabiliyetler **kabiliyet grupları** altında toplanmıştır. Her bir yetkinlik altında tanımlanmış kabiliyet grupları arasında ilişki mevcuttur. Bu ilişki genel olarak bir döngü ya da pratikler üzerinden tarif edilmektedir.
- **Kabiliyetler**, organizasyonun iş ve işlemlerini gerçekleştirebilmek için gerek duyduğu/duyacağı en küçük bileşenlerdir. Kabiliyetler uluslararası normlara ve ulusal gereksinimlere uygun olarak belirlenmiştir.
- **Alt Kabiliyetler,** kabiliyetlerin; amaç, hedef kitle ve operasyonel sorumluluk alanlarına göre özelleşmiş alt bileşenleridir.
- **Seviye**, kurumun varlıklarının, uygulamalarının ve süreçlerinin gerekli çıktıları güvenilir ve sürdürülebilir bir şekilde üreterek olgun bir yapıya ulaşması amacıyla yapılandırılmış düzeylerdir.

Dijital dönüşümü hedefleyen kurumların ihtiyaç duyacağı yetkinlik alanları **Dijital Olgunluk Değerlendirme Modeli** kapsamında aşağıdaki gibi tanımlanmıştır:



Şekil 2. Dijital Olgunluk Değerlendirme Modeli - Genel Görünüm

1. Yetkinlik: STRATEJİK YÖNETİM

Dijital dönüşüm ve dijital hizmet yönetimi kapsamında orta ve uzun vadeli amaçları, temel ilke ve politikaları, hedef ve öncelikleri ve bunlara ulaşmak için izlenecek yol ve yöntemleri içeren strateji belgelerinin; kapsamına ilişkin faaliyetleri amaç, yöntem ve içerik olarak

düzenleyen ve gerçekleştirme esaslarının bütününü içeren politika belgelerinin hazırlanmasını, izlenmesini ve güncellenmesini kapsar. Bu strateji ve politikalar doğrultusunda, kurumsal mimari yapısının kurulması, ihtiyaçların tanımlanması, çözümlerin planlanması ve bütçenin yönetilmesi amaçlanmaktadır. Bu yetkinlik, dijital strateji yönetimi, politika yönetimi, kurumsal mimari yönetimi, dijital dönüşüm yönetimi ve bütçe yönetimi kabiliyet gruplarını içermektedir.

2. Yetkinlik: ORGANİZASYON VE YÖNETİŞİM

Dijital dönüşüm çalışmalarının (portföy, program vb.) yönetişim mekanizmasından sorumlusu ekip / kişilerin mevcudiyeti, yönetişim mekanizmasının işlerliği, rol, yetenek ve yetkinliklerinin yönetilmesini kapsar. Bu yetkinlik, organizasyon, dijital kültür, dijital kapasite geliştirme ve dijital yönetişim kabiliyet gruplarını içermektedir.

3. Yetkinlik: YAZILIM HİZMETLERİ

Kurum ihtiyaçlarına göre bir yazılımın yaşam döngüsü için yapılan yazılım fizibilitesi, geliştirilmesi, bakımı ve modernizasyonu, hazır paket yazılımların tedariki ile veri üretimi ve sayısallaştırma hizmetlerini kapsar. Bu yetkinlik, yazılım fizibilite, yazılım geliştirme, yazılım modernizasyonu, yazılım tedarik, yazılım bakımı, veri üretimi ve sayısallaştırma kabiliyet gruplarını içermektedir.

4. Yetkinlik: YAZILIM YAŞAM DÖNGÜSÜ

Yazılım projesinin planlamasından başlayarak teslimatına kadar geçirmiş olduğu bütün aşamaları ve bu aşamalardan oluşan döngüyü kapsar. Bu yetkinlik, gereksinim mühendisliği, teknik çözüm, doğrulama ve geçerleme, konfigürasyon yönetimi ve kalite güvence kabiliyet gruplarını içermektedir.

5. Yetkinlik: BT HİZMETLERİ

Kurumun sahip olduğu teknolojiler ile mevcut donanım ve altyapıların yönetilmesini kapsar. Bu yetkinlik, ağ ve iletişim, veri merkezi, uygulamalar ve BT sistemleri kabiliyet gruplarını içermektedir.

6. Yetkinlik: İŞLETİM VE BAKIM

Kurumsal BT hizmetlerinin planlanması ve yönetişimi, yeni planlanan / değişen BT hizmetlerinin devreye alınması ve kontrolü, BT hizmetlerinin yönetimi, sunulması ve desteği ile BT Hizmet kalitesinin sürekli iyileştirilmesi için gerekli kabiliyetleri kapsar. Bu

yetkinlik, planlama, geçiş ve kontrol, sunum ile izleme ve değerlendirme kabiliyet gruplarını içerir.

7. Yetkinlik: D-HİZMETLER

Kurumun sahip olduğu idari uygulamaların yönetimini, kurum dijital tanıtım kanalları (internet sitesi, sosyal medya hesapları vb.) ve dijital olarak sunulan kamu hizmetlerinin tasarımını ve iyileştirilmesini içeren tüm adımları kapsar. Bu yetkinlik, kurumsal uygulamaların kullanımı, kurumsal bilgi yönetimi, d-hizmet yönetişimi, d-hizmet tasarımı, d-hizmet sunumu, d-hizmet iyileştirme, d-hizmet inovasyonu kabiliyet gruplarını içerir.

Kabiliyet grubu altındaki hangi kabiliyetlerin organizasyon için gerekli olduğu ve mevcut durumu dijital olgunluk değerlendirmesi kapsamında belirlenebilmektedir. Bu sayede, bazı kabiliyetler ya da kabiliyet grupları değerlendirme dışında bırakılabilmektedir. Benzer şekilde, kurumsal faaliyetlerin çeşitliliğine göre bazı kabiliyet ya da kabiliyet grupları diğerlerinden daha öncelikli olabilmektedir. Nihai kurumsal dijital olgunluk değerlendirmesi, kurumun faaliyet alanı, iş ve işlemlerini dikkate alarak kuruma uygun olarak özelleştirilebilmektedir. Bu sayede, dijital dönüşüm çalışmaları özelleşmiş ihtiyaçlara göre yönlendirilebilmektedir.

Kurumsal Dijital Olgunluk Seviyesi 4 ana gruba ayrılmıştır:

- Seviye 0 (Eksik): kabiliyet yoktur.
- Seviye 1 (Uygulanan): kabiliyetin temel pratikleri uygulanmaktadır.
- Seviye 2 (Kurumsallaşmış): kabiliyetler tanımlı, olup pratikleri, standart ve tutarlı bir şekilde uygulanmaktadır.
- Seviye 3 (Optimize Edilen): kabiliyet seviyeleri ölçülmekte olup, gerçek ve potansiyel problemlerin kaynağı analiz edilerek sürekli iyileşen kabiliyetler vardır.

Her kabiliyet seviyesinin altında tanımlanan sorular, doküman inceleme, ilgili personelle görüşmeler, yerinde gözlemleme, katılımcı gözlemi, fiziksel bulgular gibi çeşitli veri toplama yöntemleri kullanılarak yanıtlanmaktadır. Elde edilen yanıtların konu uzmanlarının değerlendirmeleri ile kabiliyetin seviyesi tespit edilmektedir.

Dijital Olgunluk değerlendirmesi kapsamında kurumun büyüklüğüne göre değişen ortalama 16 haftalık bir süreçte, ilgili alan uzmanlarından oluşan 10-15 kişilik **Değerlendirme Ekibi** tarafından değerlendirme yapılmaktadır. Kurum çalışanlarıyla **Dijital Olgunluk Öz Değerlendirme Anketi** yolu ile bilgi toplanmakta, kurum uzmanları ile 3-4 tam gün değerlendirme mülakatları yapılmakta, bilgi, belge ve dokümanlar

incelenmekte ve değerlendirme sonrası kurumun mevcut **Dijital Olgunluk Seviyesi** belirlenmektedir. Dijital Olgunluk Seviyesinin bir üst seviyeye çıkması amacı ile değerlendirme sonucu elde edilen tespitler gerçekleşme etkisi ve gerçekleşme süresi üzerinden sınıflandırılarak kısa, orta ve uzun vadeli öneriler ilgili uzman görüşleri dijital kabiliyet rehberleri ile desteklenecek şekilde raporlanmaktadır.

Dijital Olgunluk Değerlendirme Modeli ile;

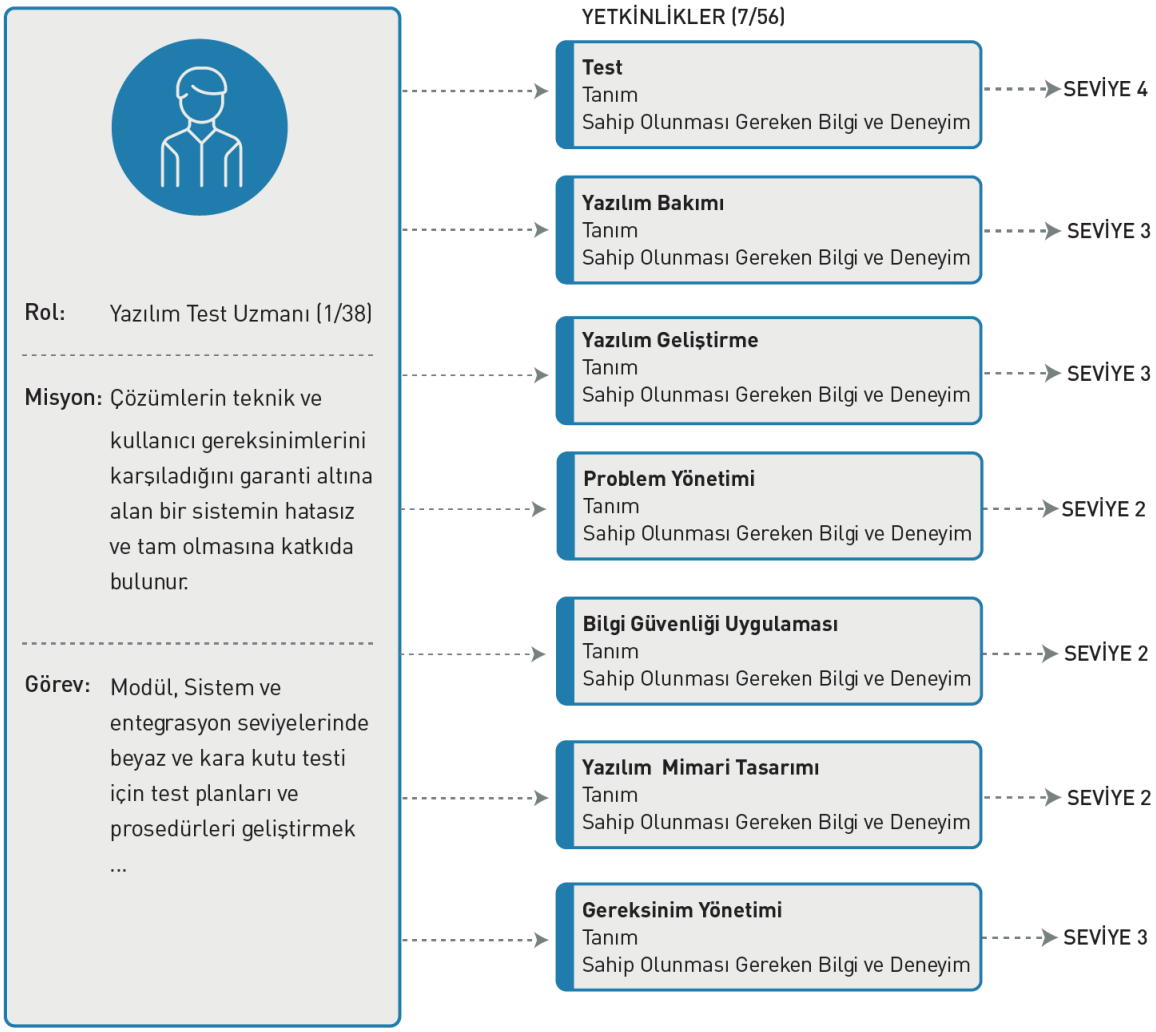
- Dijital Devlet çalışmalarında sistemli ve bütüncül bakış açısının geliştirilmesi,
- Kamu kurumların dijital kapasitelerinin yapısal, standart ve tutarlı bir şekilde değerlendirilmesi,
- Kamu kurumların dijital kapasitelerinin etkin ve verimli bir şekilde arttırılması için rehberlik edecek yol haritasının belirlenmesi,
- Dijital kamu hizmetlerinin kalite ve performansının iyileştirilmesi, çalışan ve vatandaş memnuniyetinin arttırılması

sağlanmaktadır.

Kurum dijital olgunluğunun yetkin insan kaynağı ile iyileştirilmesine yönelik **Dijital Olgunluk Değerlendirme Modeli'nde** yer alan kabiliyetler baz alınarak TÜBİTAK-BİLGEM-YTE tarafından **Dijital Yetkinlik Değerlendirme Modeli** geliştirilmiştir. Model ile kamu kurumlarında çalışan bilişim uzmanlarının yetkinlik değerlendirmesi yapılarak güçlü ve zayıf yönleri belirlenmekte, eğitim ve mesleki gelişim açısından iyileştirmeye açık alanların tanımlanması amaçlanmaktadır. "SFIA - Skills Framework for the Information Age" ve "European e-Competence Framework" modelleri analiz edilerek Türkiye'ye özgü ihtiyaçlar dikkate alınarak **Dijital Yetkinlik Değerlendirme Modeli** geliştirilmiştir. Dijital Yetkinlik Değerlendirme Modeli'nde;

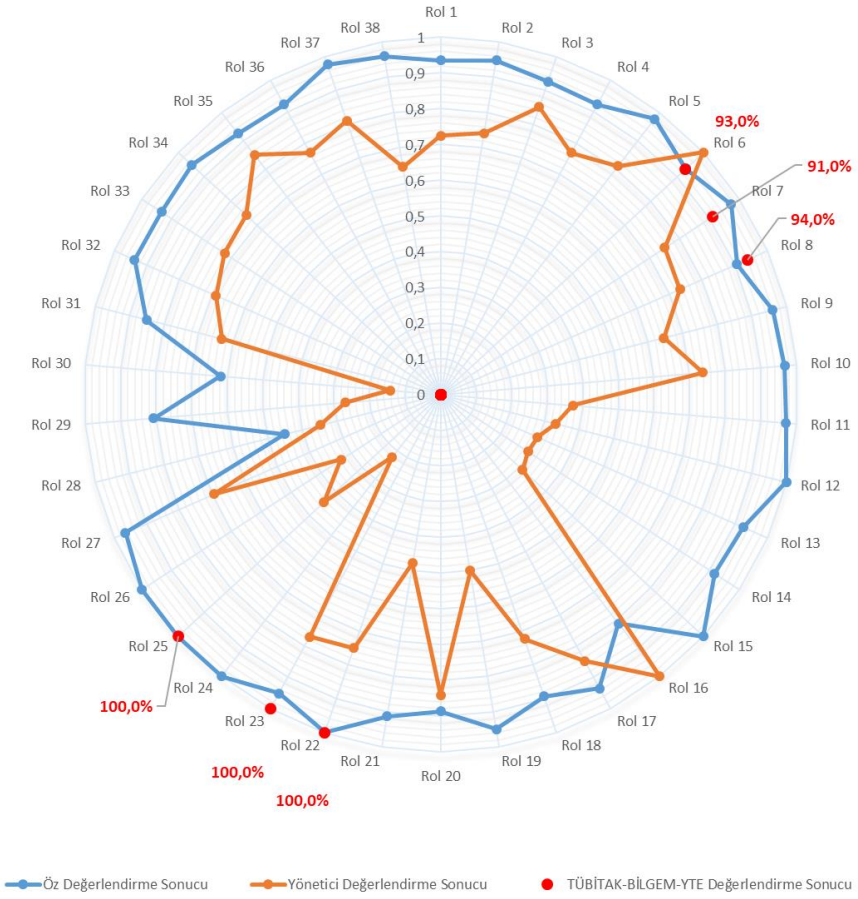
- BT Yönetimi,
- İhtiyaç Tanımlama ve Çözüm Planlama,
- Bilişim Sistemleri Yönetimi,
- Yazılım Teknolojileri Yönetimi

alanlarında Türkiye'deki organizasyon yapılarına özgü 38 bilişim profesyonel rolü tanımlanmıştır: Ayrıca, bu rollerdeki çalışanların sahip olması hedeflenen 56 yetkinlik ve yetkinlik için 5 kademeli seviye tanımlanmış olup, roller; yetkinlik alanları ve yetkinlik seviyeleri arasındaki ilişkiler belirlenmiştir. Bunun için bir örnek aşağıdaki gibidir:



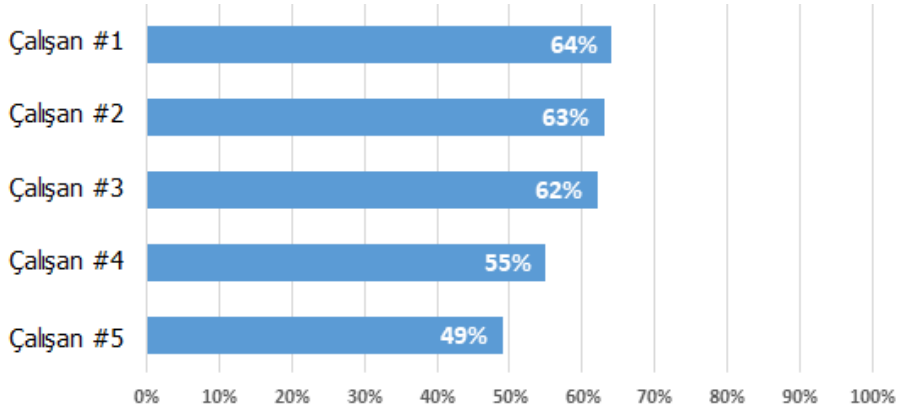
Şekil 3. Örnek Rol-Yetkinlik-Yetkinlik Seviyesi Eşlemesi

Dijital yetkinlik değerlendirmesi kapsamında kurumdaki bilişim uzmanı sayısına bağlı olarak değişen bir sürede, ilgili alan uzmanlarından oluşan 10-15 kişilik **Değerlendirme Ekibi** tarafından değerlendirme yapılmaktadır. Kurum çalışanlarının **Dijital Yetkinlik Öz Değerlendirme Anketi** yolu ile kendilerini değerlendirmesinin yanında, çalışanın bağlı olduğu bir üst yöneticisi tarafından **Yönetici Çalışan Değerlendirme Anketi** yoluyla yöneticisinin çalışanı değerlendirmesi sağlanmaktadır. Çalışan sayısına bağlı olarak değişen sürede çalışanlar ile değerlendirme mülakatları gerçekleştirilmektedir. Çalışan öz değerlendirme ve yönetici değerlendirmesi ile YTE değerlendirme sonucu üzerinden 38 rol bazında uygunluğu raporlanmaktadır:



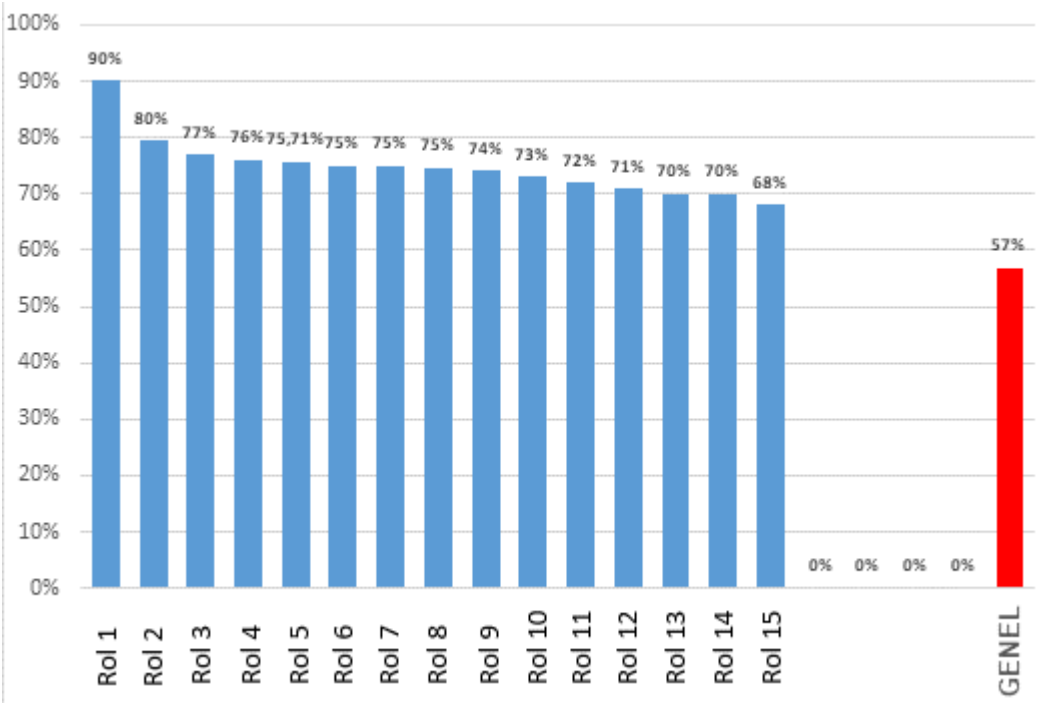
Şekil 4. Çalışan Dijital Yetkinlik Değerlendirmesi

Rol bazlı çalışan karşılaştırması yapılarak insan kaynağı kapasitesi değerlendirilmektedir



Şekil 5. Rol Bazında Dijital Yetkinlik Değerlendirmesi

Bunun yanı sıra kurumdaki roller bazında değerlendirme raporlanmaktadır ve **Kurum Dijital Yetkinlik Haritası** çıkarılmaktadır:



Şekil 6. Kurum Dijital Yetkinlik Haritası

Kurumun büyüklüğü ve bağlı olduğu sektöre göre benzer kategoriye giren dünyadaki en iyi örnekler ile bilişim istihdam dağılımının karşılaştırması yapılarak kurumun istihdam planına rehberlik sağlanmaktadır.

Dijital Yetkinlik Değerlendirme Modeli ile;

- Yetkin bilişim insan kaynağı kapasitesinin arttırılması,
- Bilişim insan kaynağı yetkinliğinin ve kapasitesinin yapısal, standart ve tutarlı bir şekilde değerlendirilmesi,
- Bilişim uzmanlarının kariyer planı için gerekli yetkinlikleri ve gereken yetkinlik seviyelerini içeren yol haritasının belirlenmesi,
- Bilişim insan kaynağının etkin bir şekilde yönetilmesi

sağlanmaktadır.

4 İŞLETİM VE BAKIM YETKİNLİĞİ

İşletim ve Bakım Yetkinliği altında toplanan rehberler ile kamu kurumlarına işletim ve bakım alanında yol göstermesi amacıyla işletim ve bakım yetkinliği altında toplanan kabiliyetler bazında tespit edilen seviyelendirilmiş sorular ile kurumların mevcut olgunluğuna yönelik referans, rol, işleyiş, iş akışı ve çıktılar ile ilgili bilgiler sunulması amaçlanmıştır. Böylece, bu kabiliyet için öncelikli yapılması veya kontrol edilmesi gereken noktalar ve bundan sonra uygulanması gereken faaliyetler sıralı bir şekilde verilmektedir. Bu sayede, bir yol haritası da sunulmaktadır. Bu anlamda bu rehber, kurumun olgunluk seviyesi artıkça sürekli kullanılabilecek bir rehber olma özelliği taşımaktadır.

Rehberin hedef kitlesi öncelikli olarak kamu kurumlarında, işletim ve bakım proje ve faaliyetlerini yürütmekle sorumlu birimlerdir. Bu birimler kurumlarda genel olarak Bilgi İşlem Daire Başkanlığı olmaktadır. Bir diğer **Rehber** kullanıcısı olan özel sektör ve STK gibi d-Devlet ekosistemi paydaşları ile **Rehberler** üzerinden ortak bir dil oluşturulması ve bilgi alışverişi yapılması hedeflenmektedir.

"**İşletim ve Bakım**" altında geçen;

- "**İşletim**", her türlü uygulama, donanım, ağ, veritabanı, arşiv vb. BT ile ilgili varlığın sağlıklı bir şekilde işletilmesi ve BT hizmetlerini kullanan diğer iş alanlarına ve müşterilere sorunsuz sunum sağlamak amacıyla gerçekleştirilen operasyon ve destek çalışmalarını kapsamaktadır. Örn: Sunucu yönetimi, ağ yönetimi, veritabanı yönetimi, kimlik yönetimi, arıza yönetimi, uygulama destek.
- "**Bakım**" ise, BT varlıklarının devamlı olarak sağlıklı ve güvenli çalışmasını garanti etmek üzere düzenli / dönemsel olarak gerçekleştirilen çalışmalardır. Örn: Veri merkezi bakımı, sistem odası bakımı.

İşletim ve Bakım Yetkinliği altından hazırlanan rehberler kapsamında, BT hizmet yönetim standartları konusunda kamu kurumlarında ciddi bir açık olduğu, bu nedenle planlanan bu rehberin kamu kurumlarına önemli bir katkı sağlayacağı öngörülmüştür. BT yaşam döngüsü içerisinde işletim ve bakım proje ve faaliyet tiplerine odaklanılarak özel bir rehber üretilmesi ile ekosisteme büyük katkı sağlaması hedeflenmiştir

4.1 YÖNTEM

Bu rehber çalışmaları sırasında, uluslararası boyutta hazırlanmış ve bu alanda kabul görmüş çeşitli standartlar, çerçeveler ve makalelerden faydalanılmıştır.

Faydalanılan kaynaklar şunlardır:

- Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) [Ref 1], Amerika Birleşik Devletleri.
- Bilgi Teknolojileri Güvenliği Enstitüsü (BSI) [Ref 2, Ref 3], Almanya.
- ISO 27001 [Ref 4]: Bilgi Güvenliği Yönetimi Sistemi gereksinimlerini tanımlayan uluslararası denetlenebilir standarttır.
- ISO 27002 [Ref 5]: Bilgi Güvenliği Yönetim Sistemine ait iyi uygulama örneklerini içeren dokümandır.
- ISO 27003 [Ref 6]: ISO 27001 standardında tanımlanan, Bilgi Güvenliği Yönetimi Sistemi gereksinimler için yönlendirmeler ve öneriler içeren dokümandır.
- ISO 27005 [Ref 7]: ISO 27001 standardında tanımlanan bilgi güvenliği riskler yönetiminin uygun bir şekilde yürütülebilmesi için yönlendirmeler içeren dokümandır.

Özellikle **Rehber'de** detaylandırılacak alt kabiliyetlerin belirlenmesi için NIST An Introduction to Information Security, IT-Grundschutz BSI, ISO 27003 ve ISO 27005 temel alınmıştır. Türkiye'nin yapısına uygun uluslararası model ve standartlar örnek alınarak ilgili temel başlıklar oluşturulmuş ve kabiliyetler üzerinden **Rehber'in** yapısı belirlenmiştir.

4.2 REHBER YAPISI

Rehber, kurum ve kuruluşların **Bilgi Güvenliği Yönetimi** kabiliyetini geliştirmeye yönelik bilgiler sunmaktadır. Bu rehberde, bir bilgi güvenliği yönetimi sisteminin kurulumu ve idamesi sırasında yapılması veya kontrol edilmesi gereken noktalar ve uygulanması gereken faaliyetler sıralı bir şekilde verilmektedir. Bu sayede, bir yol haritası da sunulmaktadır. Bu anlamda rehber, kurum ve kuruluşların Bilgi Güvenliği Yönetimi kabiliyeti olgunluk seviyesini artırmaya yönelik sürekli kullanabilecekleri bir kaynak olma özelliği taşımaktadır.

Bu rehber, bilgi güvenliği yönetimi gereksinimlerini basit ve verimli bir şekilde yerine getirebilmeyi mümkün kılmaktadır. Rehber içerisindeki standartlaştırılmış bilgi güvenliği yönetimi gereksinimleri, BGY çalışanları tarafından kendi kurumsal koşullarına uyan süreçlere kolay bir şekilde dönüştürülebilir.

Rehberde belirtilen başlıklar, bilgi güvenliği yönetimi için asgari düzeyde uygulanması gereken gereksinimleri ve gereksinimlere ait açıklamaları içermektedir. Bunun yanı sıra, gereksinimlere ait en iyi uygulamalar ve yönlendirici örneklere de rehberde yer verilmiştir.

Rehber, araç ve teknoloji bağımsız olarak geliştirilmiştir. Kabiliyetlerin kurumlarda uygulanması sırasında kullanılabilecek araçlar için farklı alternatifler olabilmektedir. Bu alternatifler kabiliyetin ne olduğundan bağımsız olarak 3 farklı tipte toplanabilir:

- Kurum kendi ihtiyaçlarına uygun olarak bir sistem oluşturabilir.
- Dışarıdan hazır bir uygulama satın alabilir.
- Daha kapsamlı bir hizmet yönetim aracı içerisinde yer alan ilgili modülden yararlanabilir.

4.3 KABİLİYET GRUPLARI

İşletim ve bakım yetkinliğinde ele alınan kabiliyet gruplarının açıklaması ve altlarındaki kabiliyetler şu şekildedir (Şekil 7).

Şekil 7. İşletim ve Bakım Yetkinliği Kabiliyet Grupları

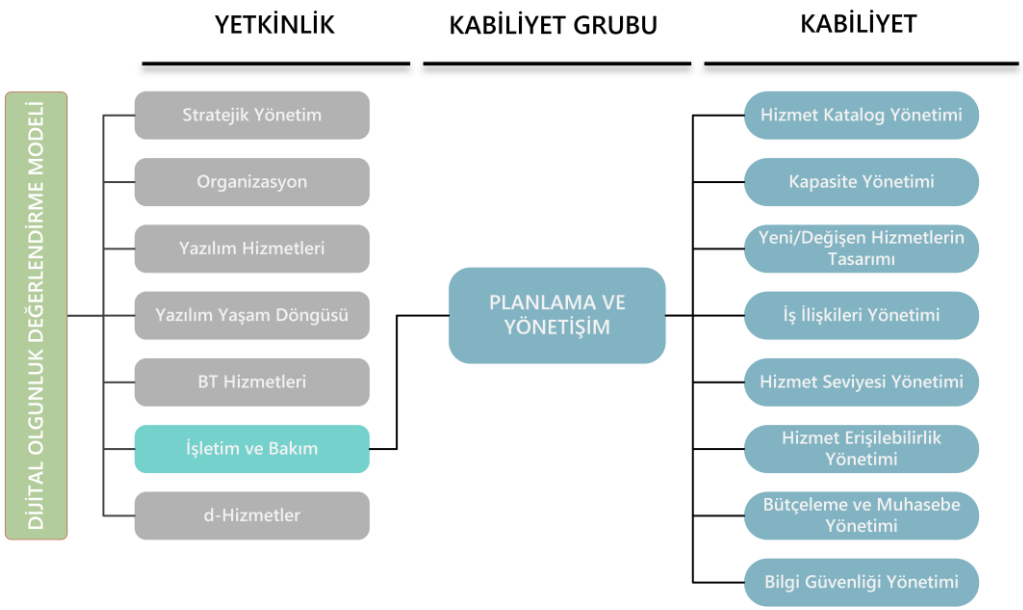
- **Planlama ve Yönetişim**; BT hizmetlerinin planlanması ve yönetişiminin sağlanması için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:

- Hizmet Katalog Yönetimi
- Kapasite Yönetimi
- Tedarikçi Yönetimi
- Bilgi Güvenliği Yönetimi
- Yeni / Değişen Hizmetlerin Tasarımı
- İş İlişkileri Yönetimi
- Bütçeleme ve Muhasebe Yönetimi
- Hizmet Seviyesi Yönetimi
- Hizmet Erişilebilirlik Yönetimi

- **Geçiş ve Kontrol**; Yeni planlanan / değişen BT hizmetlerinin devreye alınması ve kontrolünün sağlanması için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
  - Varlık Yönetimi
  - Değişiklik Yönetimi
  - Konfigürasyon Yönetimi
  - Sürüm ve Yaygınlaştırma Yönetimi
- **Sunum**; BT hizmetlerinin yönetimi, sunulması ve desteğinin sağlanması için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
  - Operasyon Yönetimi
  - Çağrı (Arıza / Kesinti Ve İstek) Yönetimi
  - Hizmet Sürekliliği Yönetimi
  - Altyapı Yönetimi
  - Problem Yönetimi
  - Kimlik ve Erişim Yönetimi
  - Uzaktan Çalışma
- **İzleme ve Değerlendirme**; BT Hizmet kalitesinin sürekli iyileştirilmesinin sağlanması için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
  - Hizmet Raporlama
  - Hizmet İyileştirme

Rehber'de yer alan sorular EK-A'da yer almaktadır.

5 KABİLİYETLER



Şekil 8. Kabiliyetler

PVY: PLANLAMA VE YÖNETİŞİM

PVY.8 BİLGİ GÜVENLİĞİ YÖNETİMİ REHBERİ

PVY.8 BİLGİ GÜVENLİĞİ YÖNETİMİ

1 AÇIKLAMA

1.1 TANIM

Bilgi Güvenliği Yönetim Sistemi (BGYS)'nin tam ve doğru bir şekilde anlaşılabilmesi için öncelikle bazı terimlerin bilinmesi gereklidir. Bu terimler "Bilgi", "Bilgi Sistemi", "Bilgi Güvenliği" ve "Yönetim Sistemi" olarak listelenebilir.

"Bilgi"; çok çeşitli formlarda yer alabilen veridir. Bilgi kağıt üzerinde, sistem varlıklarında, hatta çalışanların zihninde olabilir. “Bilgi Sistemi (Information System)” ise; bilginin toplanması, işlenmesi, sürdürülmesi, kullanılması, paylaşılması, dağıtılması veya imhası için düzenlenmiş bilgi kaynakları kümesidir. Bu noktada, "Bilgi Güvenliği", gizlilik, bütünlük ve erişilebilirlik sağlamak için bilgi ve bilgi sistemlerinin yetkisiz erişim, değişiklik ve kullanım, ifşa, kesinti veya imhadan korunmasıdır.

Bilgi güvenliği, tüm ortamlardaki her türlü bilgiyi korumak amacına sahiptir. Bilgi güvenliğinin bir alt kümesi olarak "Bilgi Sistemleri Güvenliği", elektronik olarak depolanan bilgilerin korunmasına ve işlenmesine odaklanır. Her ne kadar, bilgi güvenliğinin temel değerleri gizliliği, bütünlüğü ve erişilebilirliği içerse de; bilgi güvenliği aynı zamanda özgünlük, güvenilirlik, dayanıklılık ve inkâr edememeyi de sağlamayı amaçlar.

Bilgi güvenliği sadece kasıtlı davranışlar nedeniyle (örn. kötü amaçlı yazılım, iletişimin kesilmesi, bilgisayar hırsızlığı) tehdit altında değildir. Aşağıdaki örnekler; kontrollerin yetersizliği, farkındalık eksikliği, en iyi uygulamaların var olmayışı gibi birçok kasıtsız nedenin de bilgi güvenliğini olumsuz etkileyebileceğini göstermektedir:

- Afetler (örn. yangın, sel, fırtına, yıldırım, deprem) sonucunda veri depolama ortamına ve bilgi sistemlerine erişimin kaybedilmesi. Belgelerin, bilgi sistemlerinin veya hizmetlerin artık gerektiği gibi kullanılamaması,
- Başarısız bir yazılım güncellemesinden sonra, uygulamaların çalışmasının durması veya verilerin fark edilmeden değişime uğraması,
- Kullanılan programların uzmanı olan ve yedeği olmayan çalışanların hasta olması durumunda önemli bir iş sürecinin ertelenmesi,
- Uygun gizlilik derecesi ile işaretlenmediği için gizli bilgilerin yanlışlıkla bir çalışan tarafından yetkisiz kişilere aktarılması.

BGYS'nin anlaşılabilmesi için gerekli son tanım yönetim sistemine aittir. Bir yönetim sistemi, kurumun amaçlarına ulaşmak için denetim ve yönetime ilişkin tüm politikaları kapsayan yapıdır. Yönetim sisteminin bilgi güvenliği ile ilgili kısmına Bilgi Güvenliği Yönetim Sistemi (BGYS) denir. BGYS, bilgi güvenliğini sağlamaya yönelik görev ve

faaliyetleri açıkça yönetmek (planlamak, benimsemek, uygulamak, denetlemek ve geliştirmek) için yönetim seviyesinin kullanması gereken araç ve yöntemleri belirtir.

1.2 HEDEF

Bu rehberin amacı; bilgi güvenliği kapsamlı hizmet gereksinimlerinin, yasal ve düzenleyici gereksinimlerin ve sözleşme gereksinimlerinin gerçekleştirilmesi, kurum için bilgi varlıklarının ve bu varlıklara yönelik bilgi güvenliği risklerinin belirlenmesi için bir sistematik oluşturulması, kurumda gerekli bilgi güvenliği kontrollerinin uygulanması ve kurum için bilgi güvenliğinin farkındalığının oluşturulması hususlarında bilgileri sağlamaktır.

1.3 KAPSAM DIŞI

Bu rehber Bilgi Güvenliği Yönetimi Sistemi kurulumu, sürdürülebilirliği ve Sistemin bileşenleri hakkında bilgiler içermektedir. Ancak Sistemde kullanılacak uygulamalar ve bu uygulamaların güvenli işletimiyle ilgili konular için farklı kaynaklar kullanılmalıdır.

2 KABİLİYET UYGULAMALARI

2.1 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ'NİN TEMELLERİ

BGYS'nin doğru bir şekilde uygulanması; bir kurumun bilgi varlıklarının yanı sıra itibarını, yasal zorunluluklarını, çalışanlarını ve diğer somut ve soyut varlıklarını koruyabilmesi için büyük önem taşımaktadır. Bir kurumun BGYS'yi yeterli bir şekilde kuramamış olması, uygun bilgi güvenliği kontrollerini seçememesi, kurumun amaç ve hedefleri üzerinde muhtemel olumsuz etkiler doğuracaktır. BGYS'nin uygun ve doğru bir şekilde kurulabilmesi için kendi başına bir amaç olarak görülmemesi gerekmektedir. BGYS, kurumun amaç ve hedeflerine ulaşabilmesi ve iş süreçlerini ve ana faaliyetlerini güvenilir bir şekilde yürütebilmesi için katkıda bulunacak bir araç olarak düşünülmelidir. Bu nedenle, kurulumun ilk aşamalarından itibaren BGYS ile kurumun amaç ve hedefleri arasındaki ilişki güçlü bir şekilde kurulmalı ve her adımda bu ilişki göz önünde bulundurulmalıdır.

BGYS kurulumu öncesinde, kurum BGYS'ye neden ihtiyaç duyduğunu kavramsal olarak analiz etmelidir. BGYS'nin kurumun amaç ve hedeflerine ulaşmak için nasıl katkı sağlayacağının belirlenmesi BGYS'nin doğru şekilde kurulmasında büyük ölçüde rol oynayacaktır. Bu aşamalarda, Üst Yönetim'in liderliği ve yol göstericiliği BGYS'nin çerçevesinin belirlenmesinde yüksek derecede önem taşımaktadır. BGYS kurulacak olan kurumu en üst seviyede yöneten ve kontrol eden kişi veya kişiler Üst Yönetim olarak adlandırılmaktadır. Kurumun iş hedeflerini ve stratejisini en iyi bilen Üst Yönetim, BGYS'nin kurulumunda aktif rol almadığı durumlarda BGYS yanlış hedefleri destekleyecek şekilde kurulabilir ve etkinliğini kısa sürede kaybedebilir. Bu nedenle, kurulumun ilk adımlarından itibaren Üst Yönetim karar verme aşamalarında yol gösterici olarak kendini konumlandırmalıdır.

Üst Yönetim'in, diğer faaliyetler gibi BGYS faaliyetlerini de en üst seviyede yönetmesi gerekmektedir. Üst Yönetim'in desteği ve bağlılığı, çalışanların BGYS süreçlerini daha olumlu bir şekilde algılamasını sağlayacaktır. Çalışanlar, BGYS sürecinde gösterdikleri efor ve çabanın daha üst kademeler tarafından dikkate alınacağını bilerek; bu konuda kendilerini daha motive hissedeceklerdir.

Üst Yönetim'in desteği ayrıca, BGYS'nin ihtiyaç duyduğu kaynakların temin edilmesi hususunda da önem taşımaktadır. Üst Yönetim, BGYS ile ilgili faaliyetleri yürütmesi için gerekli kaynakları sağlayarak yetkilerini kurumdaki başka kişilere de devredebilir. Ancak, nihai olarak BGYS ile ilgili bütün sorumluluk Üst Yönetim'indir. Bunlara ek olarak, BGYS'nin etkin bir şekilde uygulanabilmesi için gereken çalışma alışkanlıklarında, süreçlerde ve prosedürlerdeki değişikliklerin çalışanlar tarafından kabul görebilmesi Üst Yönetim'in desteğine bağlıdır. Çalışanların BGYS süreçlerini sahiplenmesi kendi

yöneticilerinin gösterdikleri destek ve bağlılık kadar olacaktır. Üst Yönetim'in görev ve sorumlulukları Rehber'de 2.6 maddesinde detaylandırılmıştır.

2.2 KURUMUN VE İÇİNDE BULUNDUĞU ORTAMIN ANLAŞILMASI

BGYS ile kurum amaç ve hedefleri arasındaki ilişkinin uygun bir şekilde kurulabilmesi için öncelikle, kurum kendini ve içinde bulunduğu ortamı analiz etmelidir. Bu analizin amacı, kurumun bilgi güvenliğinin hedeflenen çıktılarına ulaşmasını etkileyebilecek faktörleri tespit etmektir. Bu faktörler, kurumun kendi iç yapısıyla alakalı olabileceği gibi dış etkenler de olabilir. Ayrıca bu analizin sonucunda, kurumun BGYS'yi nasıl idame edeceği ve BGYS'nin kurumun amaç ve hedefleri ile nasıl paralel hale getirileceği tespit edilecektir.

Kurumun kendini ve çevresini analiz etmesi, BGYS'nin bütün süreçleri için temel bir dayanaktır. Çünkü, BGYS'yi doğru bir şekilde değerlendirebilmek için kurumla ilişkili bütün bilgilerin eksiksiz olarak tespit edilmesi gerekmektedir. Bunlara ek olarak; kurumun öz değerlendirmesi, gelecekte BGYS ile kurumun diğer iş süreçleri arasında yaşanabilecek uyuşmazlıkların önüne geçilmesini sağlar. Bu adımın düzenli olarak uygulanması ise BGYS'nin değişen iç ve dış faktörlere göre tekrar adapte olabilmesine imkan tanıyacaktır.

İç Etkenler

İç etkenler kurumun kontrolünde olan etkenler olarak tanımlanmaktadır. İç etkenler belirlenirken aşağıdaki başlıklardan faydalanılabilir:

Kurumun;

- Faaliyet alanı
- İş stratejisi
- Vizyon, misyon ve değerleri
- Organizasyon yapısı
- Amaç ve hedefleri
- Kültürü
- Çalışan profili
- Mevcut durumda kurulu olan diğer yönetim sistemleri, modelleri vb.
- İç ve dış hizmetleri
- Mevcut politikaları ve prosedürleri
- Süreçlerindeki roller, sorumluluklar ve görevler
- İş süreçleri
- Mali ve insan kaynağı
- Bilgi birikimi
- Teknoloji kaynağı ve bilgi sistemleri altyapısı

- Bilgi akışı ve karar verme süreçleri
- Denetim ve risk analizi sonuçları

Dış Etkenler

Dış etkenler kurumun kontrolünde olmayan etkenler olarak tanımlanmaktadır. Dış etkenler çoğunlukla kurumun içinde bulunduğu ortamı ifade eder. Kurum, içinde bulunduğu ortamı analiz ederken aşağıdaki başlıklardan faydalanabilir:

Kurumun;

- İçinde bulunduğu sosyal ve kültürel çevre
- Uymakla zorunlu olduğu yasal düzenlemeler
- Bağlı olduğu üst kuruluşlar
- Teknolojik ve finansal etkenleri
- İçinde bulunduğu fiziksel çevre ve doğal felaket doğurabilecek fiziksel etkenler
- Birlikte çalıştığı müşteri veya tedarikçi firmalar

İç ve dış etkenler belirlenirken kurum mutlaka bu etkenlerin BGYS'yi ve kurumun bilgi güvenliği hedeflerine ulaşmasındaki performansını nasıl etkileyeceğini göz önünde bulundurmalıdır.

Bu analiz sonucu tespit edilen ve BGYS'ye olumlu veya olumsuz etkisi olabileceği düşünülen etkenlerin yazılı olarak kayıt altına alınması önerilmektedir. Bu kayıtta aşağıdaki başlıkların yer alması tavsiye edilir:

- Etken kategorisi (İç veya Dış),
- Etkenin adı (İncelenecek olan etkenin kısa bir şekilde adlandırılması),
- Etkenin özeti (İncelenecek olan etkenin açıklaması ve kurumdaki mevcut durumu),
- Bilgi güvenliği üzerine olan olumlu ve/veya olumsuz etkileri (İncelenecek olan etkenin kurumun BGYS'sine olumlu ve olumsuz etkileri bu başlık altında detaylandırılmalıdır.)

Kurum; BGYS kapsamını (2.4) bu adımın sonuçlarına dayandırmalıdır. Buna ek olarak, bu adımın sonuçları bilgi güvenliği risk yönetimine (2.7) girdi olarak kullanılmalıdır. Ayrıca bu adım düzenli olarak (senede en az 1 kez) tekrar edilmeli, değişen iç ve dış etkenlere göre bütün BGYS'nin çatısı tekrar gözden geçirilmeli ve güncellenmelidir. Bu analiz, yönetimin gözden geçirmesi sırasında ele alınmalıdır. Analiz, mutlaka Üst Yönetim ile yapılmalı veya sonuçları Üst Yönetim ile gözden geçirilerek onaylatılmalıdır.

2.3 İLGİLİ TARAFLARIN TESPİT EDİLMESİ

İlgili taraflar, kurumun aldığı kararlar veya eylemler sonucunda etkilenen ve kurumun aldığı kararları veya eylemleri etkileyen kişi veya kuruluşlardır. İlgili taraflar hem iç kaynaklı hem de dış kaynaklı olabilirler.

İlgili İç Taraflar

- Üst Yönetim
- Orta ve alt seviye yöneticiler
- Süreç sahipleri
- Varlık sahipleri
- Destek birimler
- Çalışanlar

İlgili Dış Taraflar

- Hükümet
- Yasa ve kural koyucu kurumlar
- Üst kuruluşlar veya hissedarlar
- Tedarikçiler ve altyükleniciler
- Kurumun faaliyet alanındaki diğer kuruluşlar
- Müşteriler
- Proje ortakları
- Kolluk kuvvetleri
- Adli kurumlar
- Belediyeler

İlgili tarafların bilgi güvenliği açısından kurumdan beklentileri ve karşılanması gereken ihtiyaçları olabilir. Bu adımda tespit edilen ilgili tarafların ihtiyaç ve beklentilerinin mutlaka analiz edilmesi gerekmektedir. Bu analiz sonucu tespit edilen ve BGYS'ye olumlu veya olumsuz etkisi olabileceği düşünülen etkenlerin yazılı olarak kayıt altına alınması tavsiye edilmektedir. Bu kayıtta aşağıdaki başlıkların yer alması önerilir:

- İlgili taraf
- Paylaşılan bilgiler / varlıklar
- İhtiyaçları
- Beklentileri
- İlgili iş birimleri (İlgili tarafla bilgi paylaşmakla veya ihtiyaç ve beklentilerini karşılamakla sorumlu iş birimi)

Kurum; BGYS kapsamını (2.4) ve bilgi güvenliği risk yönetimi (2.7) çalışmalarını bu adımda yapılan analiz sonucuna dayandırmalıdır.

2.4 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ'NİN KAPSAMININ BELİRLENMESİ

BGYS kapsamı, BGYS süreçlerinin kurumun hangi alanları için uygulanmasının zorunlu olduğunu ve hangi alanlar için zorunlu olmadığını tanımlar.

Kapsamın belirlenmesi BGYS için yapılacak diğer faaliyetlerin belirlenmesinde büyük önem taşıyan temel bir adımdır. Örneğin; uygulanacak risklerin değerlendirilmesi çalışması ve uygulanacak kontrollerin belirlenmesi adımları, BGYS kapsamı net olarak belirlenmediği veya anlaşılmadığı durumlarda doğru ve yeterli sonuçlar üretmeyecektir. BGYS'nin uygulanabilirliği ve sınırları, BGYS'nin diğer kurum süreçleriyle bağlantıları ve bağımlılıklarının kesin ve net bir şekilde anlaşılması ve belirlenmesi de büyük önem taşımaktadır. BGYS kapsamında yapılacak en ufak değişiklikler bile uygulamada büyük iş yükleri doğurabilir. Bu nedenle, BGYS kapsamı kurulum çalışmalarının en başında doğru bir şekilde belirlenmelidir.

BGYS kapsamı belirlenirken aşağıda belirtilen maddeler göz önünde bulundurulmalıdır:

- 2.2 numaralı uygulamada belirlenen kurumun içinde bulunduğu ortam
- 2.3 numaralı uygulamada belirlenen ilgili taraflar ve ilgili tarafların ihtiyaç ve beklentileri
- Mevcut iş süreçleri ve bu iş süreçlerinin BGYS'ye uyum durumu
- Tesis Yönetimi ve İnsan Kaynakları gibi destek birimleri
- Dış taraflardan edinilen bütün hizmetler

BGYS kapsamı her kurumda farklılık gösterebilir. İlk kurulumda kapsam bütün kurum olarak belirlenebileceği gibi, kapsam aşamalı olarak da büyütülebilir. Kapsamın bütün kurumu içerecek şekilde belirlenmesi en az risk barındıran yöntem olarak görülebilir. Ancak, kurumun büyüklüğüne göre bütün iş süreçlerinde BGYS'nin uygulanması detaylı bir planlama ve büyük bir iş yükü getirebilir. Bu nedenle; kurumun amaç ve hedeflerine, en değerli süreçlerine, ilgili taraflarına, insan ve mali kaynaklarına bağlı olarak kendisi için en verimli BGYS kapsamını belirlemesi önerilmektedir. BGYS kapsamı aşağıda sıralanan başlıklara göre belirlenebilir:

- Fiziksel lokasyon
- Tesisler
- İş birimleri
- İş süreçleri
- Sunulan hizmetler

- Projeler

Aşağıda, yol gösterici olarak kullanılabilecek kısa ve genel BGYS kapsam cümlesi örnekleri verilmiştir. BGYS kapsam cümlesi tek bir cümleden oluşabileceği gibi birkaç paragraftan da oluşabilir.

- BGYS, kurumumuzun Ankara'da bulunan tesislerindeki üretim süreçleri için kullanılan bütün bilgi varlıklarını ve sistemleri kapsar.
- BGYS, kurumumuza ait alan adı (.kurum) altında hizmet veren bütün sunucuları, servisleri ve ağ altyapısını kapsar.
- BGYS, kurumumuz tarafından kullanılan ve hizmet olarak verilen elektronik ödeme süreçleri ile ilgili tüm sistemleri ve bilgi varlıklarını ve bu sistem ve bilgi varlıklarına erişen tüm çalışanları kapsar.
- BGYS, kurumun iç süreçlerinde kullanılan (e-posta, belge yönetim sistemi ve personel bilgi sistemi) bütün bilgi sistemleri altyapısını kapsar.
- BGYS, kurumumuz tarafından üretilen yazılımların bütün proje süreçlerini ve yazılımların hizmet olarak sunulmasını sağlayan bütün bilgi sistemleri altyapısını kapsar.

BGYS kapsamı mutlaka yazılı bilgili olarak kayıt altına alınmalıdır.

2.5 BİLGİ GÜVENLİĞİ POLİTİKALARININ OLUŞTURULMASI

Kurum içi gerçekleştirilen bilgi güvenliği çalışmalarına yön verecek ilke, prensip vb. unsuları tanımlamak, ilgili iç ve dış taraflara duyurmak, Üst Yönetim desteğini sağlamak ve bilgi güvenliği ile ilgili görev ve sorumlulukları tanımlamak amacıyla bilgi güvenliği politikaları hazırlanmalıdır. Bilgi güvenliği politikaları, bir kurumun bilgiyi nasıl yönettiğini, koruduğunu ve dağıttığını belirleyen yönergeler, düzenlemeler, kurallar ve uygulamalar olarak tanımlanabilir.

BGYS kapsamında hazırlanan bütün bilgi güvenliği politikalarına altyapı oluşturan temel bir bilgi güvenliği politikası oluşturulmalıdır. Diğer bütün politikalar temel bilgi güvenliği politikasına uyumlu olmalı ve ondan beslenmelidir.

Temel bilgi güvenliği politikası;

- BGYS'nin çatısını oluşturmak için kullanılmalı,
- Bilgi güvenliği faaliyetlerini yönlendirmek amacıyla, BGYS'nin stratejik önemini tarif edecek şekilde Üst Yönetim tarafından hazırlanmalı,
- Kurumun bilgi güvenliği ile alakalı stratejik yönünü belirlemeli ve bilgi güvenliğinin uygulanması için gerekli kaynakları atamalı,

- BGYS'nin stratejik yönünü, amacını, kapsamını, uyum yükümlülüklerini ve bilgi güvenliği ile ilgili sorumlulukları kısa ve üst seviye ifadeler ile belirtmeli,
- Bilgi Güvenliği Yöneticisi tarafından BGYS organizasyon yapısını kurulmasında ve yönetilmesinde kullanılmalıdır.

Temel bilgi güvenliği politikası oluştururken aşağıdaki başlıklar göz önünde bulundurulmalıdır:

- BGYS'nin amacını içermelidir. Kurumun; gizlilik, bütünlük, erişilebilirlik gibi bilgi güvenliği gereksinimleri politikanın temellerini oluşturabilir. Örneğin; hizmet sürekliliği ön planda olan bir kurum için erişilebilirlik gereksinimleri politikada belirtilirken, bilgi gizliliği ön planda olan bir kurum için gizlilik gereksinimleri politikada daha çok yer alabilir.
- BGYS kapsamında yapılacak faaliyetler ile ilgili sorumluluklar çalışan ve iş birimi bazında üst seviye bir şekilde belirtilmelidir.
- BGYS'nin hangi kaynakları korumakla sorumlu olduğu belirtilmelidir (örn. tesis, donanım, yazılım, bilgi veya çalışan).
- Bilgi güvenliği ile ilişkili diğer bütün politikalar, prosedürler, faaliyetler ve hedefler bu politika ile aynı doğrultuda olmalı veya bu politika kullanılarak türetilmelidir.
- Kurumun iş planını, amacını, kültürünü ve bilgi güvenliği ile ilgili konuları yansıtmalıdır.
- Politika, hem kolay okunabilir hem de içerik olarak gereken her şeyi yansıtacak şekilde hazırlanmalıdır. Bu politikaya tabi olan çalışanların, kendilerini politikanın stratejik yönü ile özdeşleştirebilmeleri önemlidir.
- Kurum için bilgi güvenliği hedeflerini içerebilir veya bilgi güvenliği hedeflerinin nasıl belirlendiğine ilişkin çerçeveyi tanımlayabilir (örn. bilgi güvenliği hedeflerini kim belirler ve BGYS kapsamında bu hedefler nasıl uygulanır). Kurumun büyüklüğüne göre, Üst Yönetim tarafından üst düzey hedefler belirlenmeli, daha sonra bilgi güvenliği politikasında oluşturulan çerçeveye göre, hedefler ilgili çalışanları yönlendirecek şekilde detaylandırılmalıdır.
- Üst Yönetim, temel bilgi güvenliği politikasında bilgi güvenliği ile ilgili gereksinimlerini karşılamayı kabul ettiğini ve BGYS'nin sürekli iyileşmesini/gelişmesini desteklediğini açık bir şekilde taahhüt etmelidir. Bu taahhüt, bütün çalışanların Üst Yönetim'in BGYS'yi desteklediğini bilmesi ve farkında olması için önem taşımaktadır.
- Politika kapsam dahilindeki bütün çalışanlar ile paylaşılmalıdır. Buna ek olarak, politika ilgili dış taraflarla da paylaşılmalıdır. Bu nedenle, politikanın yazım dilinin herkes tarafından anlaşılabilir ve uygun olması, ayrıca politikanın gizli bilgi

barındırmaması gerekmektedir. Dış taraflara örnek olarak müşteriler, tedarikçiler, alt yükleniciler ve denetleyici kuruluşlar verilebilir.

- Temel bilgi güvenliği politikası, ayrı bir politika olarak hazırlanabileceği gibi, mevcut durumda hazırlanmış kapsamlı bir politika dokümanına da eklenebilir. Temel bilgi güvenliği politikası mutlaka yazılı bilgi olarak kayıt altına alınmalıdır.
- BGYS'nin belirtilen gereksinimlere kıyasla uygunluğunun kimin tarafından ve ne şekilde denetleneceği politikada belirtilmelidir. Buna ek olarak, çalışanların politikaya uymaması durumunda karşılaşacakları disiplin cezaları politikada tanımlanmalıdır.

Temel bilgi güvenliği politikası belirli konulara özgü oluşturulmuş alt bilgi güvenliği politikaları ile desteklenmelidir (Tablo 1).

Tablo 1. Kullanılabilecek Politikalar ve Açıklamaları

Politika	Tanımı
BT varlıklarının kullanımı	Kurum içerisinde kullanılmakta olan BT varlıklarının kullanımına ilişkin dikkat edilmesi gereken unsurları içerir.
Erişim kontrol politikası	Kurum içerisinde kullanılan hizmetlere, uygulamalara, sistemlere ve (Hizmet bileşenlerinin bulunduğu) ortamlara erişime ilişkin temel kuralları içerir
Parola kontrol politikası	Parola kullanımına ilişkin kuralları (parola uzunluğu, parola değiştirme süresi, parola içerisinde kullanılması gereken karakterler, vb.) içerir.
Fiziksel güvenlik ve ortam güvenliği politikası	Veri merkezi/sistem odası gibi fiziksel ortamların güvenliğini sağlamak için gerekli kuralları içerir.
e-Posta politikası	Kurum çalışanlarının, e-posta kullanımında dikkat etmeleri gereken unsurlar bu politika içerisinde belirlenir.
İnternet politikası	Kurum çalışanlarının, İnternet kullanımına ilişkin uymaları gereken kurallar (girilebilecek siteler, kullanım saatleri, vb.) bu politika içerisinde tanımlanır.
Son kullanıcı ile ilgili politikalar	Kurum içerisinde BT hizmetlerinden yararlanan çalışanların, bu hizmetlerden yararlanırken dikkat

	etmeleri gereken temel unsurlar bu politikalarda tanımlanır. Bu politika içerisinde: Varlıkların kullanımı, Temiz masa, temiz ekran, Mobil cihazların kullanımı, Bilgi transferi, Yazılım kurulum ve kullanım kısıtlamaları gibi alt başlıklar yer alabilir.
Anti-virüs ve zararlı yazılımdan korunum politikası	Zararlı yazılımlardan (virüs, solucan, vb.) korunma ile ilgili kuralları içerir.
Bilgi transferi politikası	Bilginin taşınması/iletilmesi sırasında göz önünde bulundurulması gereken temel güvenlik kuralları bu politika içerisinde belirlenir.
Bilgi sınıflandırma politikası	Kurum içerisinde kullanılmakta olan bilgiyi sınıflandırmak için kullanılacak kategorilerin belirlendiği, bilgi sınıflandırma yöntemlerinin tanımlandığı bir politikadır.
Uzaktan erişim politikası	Sunulan hizmetlere ve BT varlıklarına uzaktan erişim ile ilgili kurallar bu politika içerisinde yer alır.
Tedarikçi erişimi politikası	Tedarikçilerin kurum içerisinde BT hizmetleri ve varlıklarından yararlanırken uymaları gereken kuralları içeren bir politikadır.
BT varlıklarının imhası politikası	Kullanım ömrünü dolduran, bundan sonra kullanılmayacağı bilinen BT varlıklarının imhası sırasında dikkat edilecek unsurlar bu politika içerisinde yer alır.
Kayıtların saklanması politikası	Hizmetler kapsamında oluşturulan kayıtların saklanmasına ilişkin unsurlar (saklama süresi, saklama alanı, vb.) bu politika ile tanımlanır.

Bu politikalar farklı rollerin değişen ihtiyaçları dikkate alınarak hazırlanır, kurum içi gerekli bilgi güvenliği önlemlerinin uygulanmasını destekler. Oluşturulan temel bilgi güvenliği politikası ve ilgili diğer bilgi güvenliği politikaları tüm kurum ve ilgili tedarikçi çalışanlarına

duyurulur. Oluşturulan bilgi güvenliği politikaları belirli aralıklarla gözden geçirilir, gerekli durumlarda güncellenir.

2.6 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ ORGANİZASYONUNUN KURULMASI

Kurumun tüm faaliyetleri için, açıkça tanımlanmış rol ve sorumlulukların olması büyük önem taşımaktadır. BGYS'nin kurulması ve bilgi güvenliği gereksinimlerinin belirlenmeye başlamasından önce, rol ve sorumlulukların resmi bir şekilde tanımlanması gerekmektedir. Bu nedenle; Üst Yönetim, BGYS ile ilişkili bütün rollerin tanımlanmasını ve bu rollere ait yetki ve sorumluluklarının atanarak kurum içerisinde duyurulmasını sağlamalıdır. Üst Yönetim, BGYS ile ilişkili bütün görevlerin atamasını yapamayabilir. Bu gibi durumlarda ilgili görevlerin atanabilmesi için Üst Yönetim bu konudaki yetkisini ilgili kişilere devredebilir. Ancak, BGYS ile ilgili kritik rol ve sorumlulukların onayı Üst Yönetim'den alınmalıdır.

Aşağıda bilgi güvenliği ile ilgili bazı roller ve sorumlulukları belirtilmiştir. Açıkça tanımlanmış rol ve sorumluluklar, kurumun ve çalışanlarının daha verimli ve etkin bir şekilde çalışmasına yardımcı olacaktır. Aşağıda belirtilen liste BGYS ile ilişkili her kuruma bire bir uygulanabilecek kapsamlı bir liste olarak düşünülmemelidir. Kurumlar kendi rol isimlendirmesini ve sorumluluk tanımlamasını yapabilir.

Üst Yönetim

BGYS'nin kurulması, yönetilmesi ve sürekli iyileştirilmesinden nihai sorumluluk sahibi, kurumdaki en üst seviye yönetici veya yöneticilerdir. Üst Yönetim'in kurumdaki her bir varlıktan haberdar olması beklenmez. Ancak, Üst Yönetim'in kritik varlıklar ve bu varlıkların iş süreçleri için önemi hakkında genel bir bilgiye sahip olması gerekmektedir. Üst Yönetim; genellikle kurumun yapısına bağlı olarak, Kurum Müdürü, Kurum Müdür Yardımcıları, Yönetim Kurulu Üyeleri gibi kişilerden oluşur.

Üst Yönetim'in sorumlulukları aşağıdaki başlıkları kapsamaktadır:

- BGYS'ye ait politika ve hedeflerin tanımlandığından ve bunların kurumun stratejik yönü ile aynı doğrultuda olduğundan emin olmak.
- BGYS gereksinim ve kontrollerinin organizasyonel süreçlere entegre edildiğinden emin olmak. Bu sürecin nasıl yönetileceği kurumun yapısına göre farklılar gösterebilir. Örneğin; süreç sahibi tanımı olan bir kurum, sorumlulukları süreç sahiplerine atarken; başka bir kurum sorumlulukları orta ve alt seviye yöneticilere atayabilir.
- BGYS'nin çalışanlar tarafından gösterilen kurumsal dirence karşı zarar görmemesi için destek vermek.

- Etkili bir BGYS için, BGYS'nin ihtiyaç duyduğu kaynakları (mali, insan, tesis veya teknik altyapı) sağlamak.
- Çalışanların bilgi güvenliği politikalarına, kılavuzlarına ve yönlendirmelerine uygun davrandığını doğrulamak. Bu sürecin yönetilebilmesi için Üst Yönetim BGYS'nin gereksinimleri konusunda hassasiyetini mümkün olan durumlarda göstermeli ve BGYS sürecinde aktif rol oynayarak somut örnekler sergilemelidir.
- BGYS'nin etkinliği konusunda raporlar talep ederek ve bu raporları gözden geçirerek, BGYS'nin hedeflenen sonuçlarına ulaştığından emin olmak. Bu raporlar performans ölçümlerinden, yönetimin gözden geçirmesi faaliyetlerinden veya denetimlerden türetilebilir.
- BGYS sürecinde aktif rol alan çalışanları yönlendirmek, desteklemek ve bu çalışanlar için performans hedefleri koymak. Çalışanların üstlendiği BGYS görevleri konusunda desteklenmesi, çalışanların bu konuda daha istekli olmasına ve alanlarındaki bilgi güvenliği süreçlerini daha verimli ve etkin bir şekilde yürütmesine olanak sağlayacaktır.
- Kurumsal süreçleri desteklemek için kullanılan bilgi ve bilgi sistemlerinin uygun bilgi güvenliği önlemlerine sahip olduğundan emin olmak.
- Yönetimin gözden geçirmesi faaliyetlerinde aktif rol almak.
- BGYS'nin sürekli gelişmesine destek olmak ve bu konuda kurumun stratejik yönü ile paralel bilgi güvenliği hedefleri belirlemek.

Bilgi Güvenliği Yönetim Komitesi

Bazı durumlarda, BGYS'nin yönetilmesi için kurumdaki bütün paydaşlardan temsilci barındıran bir Bilgi Güvenliği Yönetim Komitesi (BGYÖK) oluşturulması gerekebilir. Bu komitenin oluşturulmasına, kurumun büyüklüğü ve organizasyonel yapısını göz önünde bulundurarak Üst Yönetim karar verecektir. Komitenin karar verici görevini daha iyi yerine getirebilmesi için, komitenin görevlerini, sorumluluklarını ve yetkilerini tanımlayan bir tüzük hazırlanması tavsiye edilmektedir. Komitenin içerisinde Üst Yönetim'den bir kişinin veya Üst Yönetim'e doğrudan raporlama yapabilme yetkisine sahip bir çalışanın bulundurulması faydalı olacaktır. Komite düzenli aralıklarla veya ihtiyaç durumunda toplantılar düzenlemelidir. BGYÖK'ün görevleri kurum yapısına göre değişiklik gösterebilir. Komitenin temel görevleri aşağıdaki başlıkları kapsamaktadır:

- Bilgi güvenliği kuralları ve prosedürlerinin gözden geçirilmesi ve onaylanması,
- Risk analizlerinin ve tedavi planlarının gözden geçirilmesi,
- Denetim sonuçlarının ve bunlarla ilişkili faaliyet planlarının gözden geçirilmesi,
- Planlanan faaliyetlerin izlenmesi,

- Bilgi güvenliği amaç, hedef ve performans göstergelerinin gözden geçirilmesi,
- Bilgi güvenliği ile ilişkili çalışan farkındalık seviyesinin gözden geçirilmesi,
- Bilgi güvenliği ile ilişkili eğitim planlamalarının yapılması.

BGYÖK yapısının kurulmasının faydaları aşağıdaki şekilde sıralanabilir:

- Farklı iş birimleri arasında daha güçlü bir koordinasyonun sağlanması,
- Farklı iş birimlerinde bilgi güvenliği kültürünün daha etkin bir şekilde yayılması,
- Karar süreçlerinin daha geniş bir bakış açısıyla yürütülmesi,
- Bilgi güvenliği seviyesinin ve gelişiminin rutin olarak gözden geçirilmesi ve kontrol edilmesi.

BGYÖK yapısı kurulurken aşağıdaki başlıklara dikkat edilmelidir:

- Her iş birimi aynı seviye yöneticiler veya çalışanlar tarafından temsil edilmelidir. Temsilciler arasında yetki ve sorumluluk farkı olması komitede karar verme süreçlerinde dengesizliklere sebep olacaktır.
- Toplantılar öncesinde planlama yapılmalı ve toplantı içerikleri temsilciler ile paylaşılmalıdır.
- Toplantılar düzenli aralıklarla veya ihtiyaç halinde gerçekleştirilmelidir.
- Toplantıyı kimin yöneteceği ve anlaşmazlıkların ne şekilde çözüleceği gibi konular belirlenerek yazılı hale getirilmelidir.

Bilgi Güvenliği Yöneticisi

Bilgi güvenliği, kurumdaki bütün iş birimlerini ilgilendiriyor olsa bile, kurum içerisinde bilgi güvenliği ile ilişkili faaliyetleri koordine etmekten sorumlu bir Bilgi Güvenliği Yöneticisi ataması yapılmalıdır. Bu rolün, gerekli koordinasyonu sağlayabilmesi için bilgi akışı süreçlerine dahil edilen bir yönetici pozisyonundaki çalışana atanması tavsiye edilmektedir. BGYS'nin kurum içerisindeki diğer iş birimlerini denetlemek ve düzenlemekle sorumluğu olduğu düşünüldüğünde, rolün çıkar çatışmasına sebebiyet vermeyecek bir çalışana atanması gerekmektedir. Bilgi güvenliği bütün iş birimlerini kapsamasına rağmen, günümüz dünyasında kurumlardaki bilgi akışı daha çok bilgi sistemleri birimi üzerinden geçmektedir. Bu nedenle, BGYS büyük oranda bilgi sistemleri birimini etkileyecektir. Bilgi sistemleri biriminden sorumlu bir çalışana Bilgi Güvenliği Yöneticisi rolü atamak, o kişinin hem kendi birimi ile alakalı kuralları koyan hem de o kuralları denetleyen bir pozisyonda görev yapmasına sebebiyet verecektir. BGYS ile ilişkili süreçlerin ve kuralların daha verimli ve etkin bir şekilde yürütülebilmesi için, Bilgi Güvenliği Yöneticisi unvanının, diğer iş birimlerini bağımsız bir şekilde denetleyebilecek bir çalışana atanması doğru olacaktır.

Bilgi Güvenliği Yöneticisi, BGYS kurgusunun en önemli unsurlarından biridir. Bu nedenle, Bilgi Güvenliği Yöneticisi bu alandaki yeterlilik ve deneyimleri doğrultusunda belirlenmelidir. Bilgi Güvenliği Yöneticisi'nin sorumlulukları aşağıdaki başlıkları kapsayacak şekilde tanımlanmalıdır:

- BGYS'nin kurulmasını, uygulanmasını, sürdürülmesini, performansının raporlanmasını ve sürekli geliştirilmesini koordine etmek,
- Bilgi güvenliği risk değerlendirmesi ve müdahelesi aşamalarını yönetmek,
- Bilgi güvenliği süreçlerini tasarlamak,
- Bilgi güvenliği önlemlerine ilişkin kurallar, düzenlemeler, prosedürler ve politikalar belirlemek,
- Bilgi güvenliği ihlal olaylarını yönetmek,
- BGYS'yi gözden geçirmek ve denetlemek.

Risk Yöneticisi

Risk yöneticisi; kurumdaki risk ile alakalı kararların geniş bir perspektiften bakılarak kurumsal hedef ve amaçlarla aynı doğrultuda olmasını sağlamak ve risklerin kurum çapında tutarlı bir şekilde yönetildiğini kontrol etmekle sorumlu çalışandır. Risk Yöneticisi'nin görevleri aşağıdaki başlıkları kapsayacak şekilde tanımlanmalıdır:

- Kurum çapında, risklere yönelik bütüncül bir yaklaşım tanımlamak.
- Kurumsal risk yönetim stratejisini belirlemek.
- Kurumdaki yöneticiler arasında risk ile alakalı bilgi akışını sağlamak.
- Kurumdaki risk ile ilgili faaliyetleri denetlemek.

Varlık Sahibi

Varlık; kurum için değeri olan bilgi, yazılım, donanım, fiziksel lokasyon, hizmet, çalışan, itibar ve imaj gibi soyut ve somut etkenlerin hepsini kapsar. Varlık Sahibi, kendilerine ait varlıklar için erişim yetkisi tanımlama, değişiklik yapma, güncelleme, taşıma ve kopyalama gibi faaliyetler noktasında onay yetkisi bulunan çalışandır. Varlık Sahipleri, varlığın uygun şekilde kullanılması ve korunması için gereken kuralları tanımlamakla sorumludur. Varlık Sahibi aldığı kararlarda, bilgi güvenliği ile ilişkili riskleri ve etkileri her zaman göz önünde bulundurmalıdır. BGYS sürecinin etkin bir şekilde yürütülebilmesi için, ilgili varlıkların ve sahiplerinin açık ve net bir şekilde tespit edilmesi ve Varlık Sahipleri ile sorumluluklarının duyurulması gerekmektedir.

Çalışanlar

BGYS'nin başarısı büyük oranda, kurum çalışanlarının bilgi güvenliği ile ilgili farkındalık ve eğitimlerine bağlıdır. Kurum çalışanlarının kendi faaliyet alanlarındaki bilgi güvenliği

süreçlerini ve önlemlerini benimseyebilmeleri ve etkili bir şekilde uygulayabilmeleri için, BGYS'nin ve bilgi güvenliği önlemlerinin arkasında yatan sebepleri açık bir şekilde görebilmeleri gerekmektedir. Bilgi güvenliğine zarar vermeye yönelik saldırılara hedef oldukları durumlarda, çalışanlar olağandışı durumları tespit edebilmeli ve Bilgi Güvenliği Yöneticisi'ne durumu bildirmelidirler. Bu doğrultuda, çalışanların farkındalık seviyesini güçlendirmek için gerekli eğitimleri almaları sağlanmalıdır. Çalışanların, bilgi güvenliği farkındalığının artırılması, bilgi güvenliğinin bir kurum kültürü haline gelmesine de olanak sağlayacaktır. Çalışanlar, kurumsal varlıkları kabul edilebilir kullanım kurallarına göre kullanmak ve tespit ettikleri olağandışı veya şüpheli durumları Bilgi Güvenliği Yöneticisi'ne bildirmekten sorumludur.

2.7 BİLGİ GÜVENLİĞİ RİSK YÖNETİMİ

Risk, belirsizliğin söz konusu olduğu ve gerçekleşmesi durumunda hedefleri olumlu ya da olumsuz etkileyebilecek bir olay ya da durumdur. Bu belirsizliğin etkisi olumsuz olabileceği gibi olumlu da olabilir. Rehberde, risk: belirsizlik etkisinin olumsuz olduğu durumlar olarak ele alınmıştır. Bireysel olarak farkında olmasak da günlük işlerimiz içerisinde sürekli risk yönetimi yaparız. Arabaya bindiğimizde emniyet kemerimizi takmamız, havanın bulutlu olduğunu gördüğümüzde yanımıza şemsiye almamız tehditlerle başa çıkma yöntemlerimiz olarak gösterebilir. Günlük hayatımızda birey olarak birçok risk tespit edip, etkilerini azaltmak için aksiyon uygularız.

Kurumlar, normal iş faaliyetleri sırasında birçok riski yönetmek için farklı süreçler yürütürler. Örneğin; yatırım gelirlerini artırmak için agresif ancak yüksek risk barındıran stratejiler ile pasif ancak düşük risk barındıran stratejiler arasında seçim yapmak gibi. Bu seçimleri doğru ve etkin bir şekilde yapabilmek için; kurumun riskleri ve potansiyel faydaları analiz etmesi, alternatif yöntemleri değerlendirmesi ve son olarak karar verilen stratejiyi uygulamaya geçirerek izlemesi gerekir.

Risk yönetimi sürecinin adımları aşağıda şekilde sıralanabilir:

- Risklerin Değerlendirilmesi
  - Risklerin Belirlenmesi
  - Risklerin Analiz Edilmesi
  - Risklerin Değerlenmesi
- Risk Müdahalesi
- Risklerin İzlenmesi ve Gözden Geçirilmesi
- Risk Yönetim Sürecinin İzlenmesi, Gözden Geçirilmesi ve Geliştirilmesi

Bilgi güvenliği risk yönetim sürecinde uyulması gereken temel gereksinimler aşağıda şekilde sıralanabilir:

- Mevcut durumda kalite yönetim sistemi gibi risk yönetim süreçleri oluşturulmuş yönetim sistemleri olan kurumların, bu yönetim sistemleriyle uyumlu ve entegre bir bilgi güvenliği risk yönetim süreci oluşturması,
- Kurumun bilgi güvenliği risk yönetimi için detaylı, kapsamlı ve eksiksiz bir süreç tanımlayıp uygulaması,
- Bilgi güvenliği risk yönetim sürecinin BGYS'nin temeli olduğu unutulmadan hazırlanması.

BGYS sürecinde riskler iki farklı kategoride incelenebilir. Kurum iki kategori için farklı risk yönetimi teknikleri kullanabileceği gibi risklerini aynı teknikleri kullanarak da yönetebilir.

BGYS'nin hedeflenen çıktıları ile ilişkili riskler

Bu kategorideki riskler BGYS'nin kendi süreçlerini, BGYS'nin kapsam tanımını, Üst Yönetimin bağlılığını, BGYS'nin ihtiyaç duyduğu kaynakları doğrudan etkileyen risklerdir.

Kurum bu risklerini 2.2 ve 2.3 numaralı başlıklardaki uygulamaları temel alarak ve aşağıdaki adımları göz önünde bulundurarak belirlemelidir:

- BGYS'nin hedeflenen çıktılarına ulaşabilmesinin sağlanması (örn. açık ve net olmayan süreç ve sorumluluklar, çalışanların düşük farkındalığı, Üst Yönetimin desteğinin yetersizliği gibi riskler),
- BGYS'nin hedeflenen çıktılarına etki edebilecek risklerin önlenmesi veya olasılığının azaltılması (örn. yanlış kurgulanmış risk yönetim süreci veya risk farkındalığının azlığı gibi riskler),
- Sürekli iyileştirmenin sağlanması (örn. BGYS süreç ve dokümanlarının yanlış ve eksik yönetilmesi gibi riskler).

BGYS kapsamındaki bilginin gizliliği, bütünlüğü ve erişilebilirliği ile ilişkili riskler

Bu kategorideki riskler doğrudan doğruya bilginin veya bilgi varlığının gizliliğini, bütünlüğünü ve erişilebilirliğini etkileyen risklerdir. Bilgi veya bilgi varlığının üzerindeki riskler dolaylı olarak kurumun veya BGYS'nin hedeflerine ulaşması üzerinde olumsuz etkileri olabilir. Bunlara ek olarak, finansal kayıp, yasal zorunluluklara uyumsuzluk veya kurum imajında kayıp yaşanması gibi etkilere de sebep olabilir.

Kurum bilgi güvenliği risklerini yönetebilmek için bir süreç oluşturarak yazılı hale getirmelidir. Bu süreç aşağıda belirtilen risk yönetim adımlarını içermelidir.

2.7.1 RİSKLERİN DEĞERLENDİRİLMESİ

Risk, istenmeyen bir olayın yaşanması durumunda ortaya çıkacak sonuçlar ile bu olayın yaşanma olasılığının bir kombinasyonudur. Risk değerlendirme çalışmaları, riskin niceliğini belirtebilir veya riski nitel olarak tanımlayabilir. Bu sayede yöneticilerin kritiklik seviyesine göre riskleri daha etkin bir şekilde önceliklendirebilmesine olanak sağlar.

Risk değerlendirme çalışmalarının amacı;

- Bilgi varlıklarının değerini belirlemek,
- Mevcut tehdit ve açıklıkları tespit etmek,
- Risklerin bilgi varlıkları üzerindeki etkisini belirlemek,
- Tespit edilen risklerin değerini hesaplayarak yöneticilerin riskleri önceliklendirmesini sağlamak.

2.7.1.1 RİSKLERİN BELİRLENMESİ

Kurum, bilgi varlıklarına, bilgi güvenliğinin hedeflenen çıktılarına, 2.2 ve 2.3 adımlarında belirlenen hususlara etki edebilecek riskleri belirlemelidir. Bilgi güvenliği riskleri kurumun birçok farklı seviyesinde ve farklı alanlarında mevcut olabilir. Bu sebeple kurumun farklı alanlarına dokunan ve hiç bir alanı göz ardı etmeyen bir risk belirleme süreci oluşturulmalıdır. Bunun için kurumun, riskleri hangi yöntemleri kullanarak belirleyeceğini tanımlanmalıdır.

Aşağıda örnek olarak verilen yöntemler bu adımda kullanılabilir:

- Çalışan ile mülakatlar,
- Fikir yürütme (Beyin Fırtınası),
- Benzer kurumlarda yaşanan olaylar,
- Önceki uygunsuzluklar,
- İş sürecine ait şemalar, kılavuzlar,
- Varlık envanteri,
- Teknik zafiyet test raporları,
- Sistem uyarı kayıtları (Aşılması halinde sorun oluşturacak eşik değerler),
- Bilgi güvenliği ihlal olayı bildirimleri.

Risk belirleme çalışmaları belirli aralıklarla (asgari yılda bir kez) gerçekleştirilmelidir. Bunlara ek olarak teknik altyapı değişikliği, sistem devreye alma ve devreden çıkarma gibi operasyonel işlemler sırasında ortaya çıkabilecek riskleri tespit edebilmek için BGYS'nin bu süreçlere entegre edilmesi gerekmektedir.

Riskler, Risk Yöneticisi tarafından tespit edilebileceği gibi çalışanlar tarafından da tespit edilebilir. Bu nedenle, çalışanların risk konusunda farkındalıklarının yüksek olması sağlanmalı ve risk önerilerinin Risk Yöneticisi'ne hangi kanallar kullanılarak iletileceği belirlenerek çalışanlara duyurulmalıdır.

Tespit edilen her risk gerçek anlamda bir risk olmayabilir. Risk Yönetimi sürecinin daha verimli ve etkin bir şekilde yürütülebilmesi için Risk Yöneticisinin, tespit edilen risklere bir ön değerlendirme uygulayarak; riske dönüştürülmesi uygun olup olmayan riskleri tespit etmelidir. Risk yöneticisinin, riskleri hangi kriterleri göz önünde bulundurarak değerlendireceği tanımlanmalıdır. Risk Yöneticisi, risklere bir ön değerlendirme uygularken gerekli gördüğü durumlarda çalışanların, üçüncü tarafların, Üst Yönetimin veya alan uzmanlarının görüşlerini alabilir. Bu görüşler ve Risk Yöneticisi'nin yorumları kayıt altına alınmalıdır.

Riskler belirlenirken aşağıdaki faktörler göz önünde bulundurulmalıdır:

- Maliyet,
- Bütçe,
- Proje kapsamındaki görevler,
- Performans,
- İş hedefleri,
- Çevresel etkenler (doğal afet, politik değişimler, vb.),
- Gereksinimler,
- Teknoloji,
- İnsan kaynağı,
- Alt yükleniciler,
- Yasal zorunluluklar.

Risklerin belirlenmesinin amacı, olası bir kayba sebep olabilecek unsurları tespit etmek ve bu kaybın nasıl, nerede ve ne için meydana gelebileceğini öngörmektir. Risk belirlenmesi sırasında kurum risk kaynağı kendi kontrolünde olmasa bile veya risk kaynağı kesin olarak tespit edilememiş olsa bile riskleri ele almalıdır. Risk belirleme çalışmalarında izlenecek ana adımlar aşağıdaki şekilde sıralanabilir:

Varlıkların Tespit Edilmesi

Varlık: kurum için değere sahip olan ve koruma gerektiren herhangi bir şeydir. Varlıkların tespit edilmesi sırasında, varlıkların yalnızca donanım ve yazılımdan oluşmadığı; insanların, süreçlerin ve hizmetlerin de birer varlık olarak ele alınabileceği unutulmamalıdır.

Varlıkların tespiti çalışmaları, risklerin yönetilebilmesi için ihtiyaç duyulan uygun seviyede ve ayrıntıda yürütülmelidir. Varlık tespiti çalışmaları, risk yönetimi sürecinin temelini oluşturacak ve risk yönetimi sürecinin sonuçlarını büyük oranda etkileyecektir. Varlıklar için yetki ve sorumluluğa sahip varlık sahipleri atanmalıdır. Varlık sahibi, varlığın mülkiyet haklarını sahip olmayabilir ancak; varlığın geliştirilmesinden, sürdürülmesinden, kullanılmasından ve güvenliğinin sağlanmasından sorumlu kişidir. Varlık sahibi, varlığın değerini belirlemek için kurumdaki en uygun kişidir.

Varlıkların gizlilik, bütünlük ve erişilebilirliklerine bir zarar gelmesi durumunda ortaya çıkacak sonuçlar belirlenmelidir. Bu adımda, bir senaryo sonucunda kuruma gelebilecek zararlar ve sonuçları tespit edilir. Bahsedilen senaryo: bir tehdidin, bir veya daha fazla açıklığı kullanarak oluşturduğu bilgi güvenliği olaylarıdır. Etkinlik, hizmet ve itibar kayıpları veya olumsuz çalışma koşulları bir tehdidin açıklığı kullanarak ortaya çıkarabileceği sonuçlar olabilir.

Bir bilgi güvenliği ihlal olayı, bir veya daha fazla varlığı etkileyebilir. Bu nedenle varlık değerleri, varlığa bir zarar gelmesi durumunda yaşanacak mali kayıp, hizmet kesintisi ve iş süreçlerine etkisi gibi kriterler ile değerlendirilmelidir.

Kurum, yaşanabilecek bir bilgi güvenliği ihlal olayı sonucunda ortaya çıkabilecek operasyonel sonuçları aşağıda başlıkları kullanarak belirleyebilir:

- Olayın araştırılması ve onarım süresi,
- İş gücü kaybı,
- Fırsat kaybı,
- İş sağlığı ve güvenliği etkileri,
- Hasarın giderilmesi için harcanacak mali kaynak,
- İtibar kaybı.

Varlıkların değerlerinin tutarlı ve tekrarlanabilir bir şekilde belirlenebilmesi için daha önce tanımlanan kriterler üzerinden bir ölçüm tablosu belirlenmelidir. Bu kriterler; bilgi varlığının gizliliğine, bütünlüğüne ve erişilebilirliğine zarar gelmesi durumunda ortaya çıkabilecek sonuçları tanımlamalıdır. Aşağıda, bilgi varlığının değerini belirlemede kullanılabilecek bazı kriterler listelenmiştir:

- Yasal yükümlülüklere uyumsuzluk,
- İtibar kaybı,
- Kişisel verilerin açığa çıkması,
- Mali kayıp,
- İş faaliyetlerinde aksama,

- Hizmet kesintisi,
- Sözleşme ihlali.

Varlık değeri belirleme çalışmalarında kullanılacak kriterler; her kurumun kendi faaliyet alanına ve güvenlik gereksinimlerine göre belirlenmelidir.

Kriterlerin belirlenmesinden sonra kurum, bu kriterler çerçevesinde belirleyeceği ölçüm değerlerini tanımlamalıdır. İlk adım olarak ölçüm değerlerinin kaç seviye olacağı belirlenmelidir. Kurumun gereksinimlerine göre ölçüm değerlerinin seviyesi değişiklik gösterebilir. Ancak, genel olarak 3 seviye ile 10 seviye arasında ölçüm değeri tanımlamak yeterli olacaktır. Aşağıda 3 seviyeli bir varlık değeri tablosu örnek olarak verilmiştir (Tablo 2).

Tablo 2. Varlıkların Erişilebilirlik Değeri Örnek Tablosu

Varlığın Erişilebilirlik Değeri	Açıklama
1	Varlığın 2 gün - 1 hafta erişilemez olması durumunda Kurumun iş süreçlerinde ve hizmetlerinde küçük çaplı kesintiler yaşanır.
2	Varlığın 24 saat erişilemez olması durumunda Kurumun ana iş süreçleri ve hizmetlerinde büyük çaplı kesintiler yaşanır
3	Varlığın 4 saat erişilemez olması durumunda Kurumun ana iş süreçleri ve hizmetleri tamamen kesintiye uğrar

Varlığın değerlendirilmesi için kullanılacak ölçüm değerleri belirlenirken bir veya birden fazla kriter kullanılabilir. Varlığın gizlilik, bütünlük ve erişilebilirlik değerleri ayrı ayrı hesaplanıp varlık değeri bunların bir kombinasyonu olarak belirlenmelidir.

Tehditlerin Tespit Edilmesi

Tehditler bir varlık üzerinde, dolayısıyla kurum üzerinde, olası bir etki yaratma fırsatına sahip unsurlardır. Tehditler doğal veya insan kaynaklı, kasti veya kasıtsız olabilir. Bir tehdit kurum içinden doğabileceği gibi kurum dışından da meydana gelebilir. Tehditler, genel olarak tanımlanmalı ve kategorize edilmelidir. Bu şekilde mevcut durumda var olmayan tehditlerin ileride gözden kaçırılması engellenecek veya bir varlık için mevcut olan tehditlerin diğer varlık için de gözden geçirilmesi sağlanacaktır.

Tehditlerin tespit edilmesi sırasında, daha önce yaşanmış olaylardaki kazanılan deneyimler ve geçmişte yapılmış tehdit değerlemeleri göz önünde bulundurulmalıdır. Tehditler için uzman kuruluşlar, kamu kuruluşları veya yasal otoriteler tarafından

yayımlanan genel tehdit unsurları listelerinden yararlanılabilir. Geçmişte yapılmış tehdit değerlemeleri veya yayımlanmış listelerden yararlanılırken, kurumun içinde bulunduğu iş ortamının, bilgi sistemleri teknolojilerinin ve buna bağlı olarak tehditlerin sürekli bir değişim halinde olduğu unutulmamalı ve güncel gelişmeler doğrultusundan ele alınmalıdır. Aşağıda bazı örnek tehdit kategorileri ve tehdit unsurları verilmiştir (Tablo 3).

Tablo 3. Tehdit Kategorisi ve Tehdit Unsuru Örnek Tablosu - 1

Tehdit Kategorisi	Tehdit Unsuru
Doğal Afet	Yangın
	Sel
	Deprem
Temel Hizmetlerin Kesintiye Uğraması	Elektrik kesintisi
	Ağ bağlantısı kesintisi
	Su kesintisi

Tehdit unsurları doğal kaynaklı olabileceği gibi insan kaynaklı da olabilir (Tablo 4).

Tablo 4. Tehdit Kategorisi ve Tehdit Unsuru Örnek Tablosu - 2

Tehdit Kategorisi	Tehdit Unsuru
Çalışan	Kötü niyetli çalışan
	Çalışan dikkatsizliği
Saldırgan	Terörist
	Siber suçlu

Açıklıkların Tespit Edilmesi

Tehditler, açıklıkları kullanarak varlıklar üzerinde etki yaratırlar. Bu nedenle tehditlerin hangi açıklıkları kullanabileceği tespit edilmeli ve tanımlanmalıdır. Açıklıklar, aşağıda belirtilen alanlarda tespit edilebilir:

- Kurum,
- Süreç ve prosedürler,
- Yönetimsel süreçler,
- Çalışanlar,
- Fiziksel çevre,

- Bilgi sistemleri altyapısı,
- Donanım, yazılım veya iletişim ekipmanları,
- Dış taraflar.

Bir açıklığın varlığı, onu kullanacak bir tehdit olmadığı sürece tek başına risk oluşturmaz. Tehdidi olmayan bir açıklık için önlem alınması ihtiyacı olmayabilir. Ancak bu açıklık, yaşanabileceği değişiklikler için kayıt altına alınmalı ve düzenli olarak izlenmelidir. Yanlış uygulanmış, hata barındıran, doğru kullanılmayan bir önlem de kendi başına bir açıklık oluşturabilir. Önlem, içinde bulunduğu ortama bağlı olarak etkisiz olabilir. Aynı şekilde, açıklığı olmayan bir tehdit bir risk teşkil etmeyebilir.

Aşağıda örnek bazı açıklıklar listelenmiştir (Tablo 5).

Tablo 5. Açıklık Örnek Tablosu

Kaynak	Açıklık
Donanım	Yetersiz bakım
	Nem, toz ve kire duyarlılık
Yazılım	Güvensiz oturum açma mekanizması
	Yanlış konfigürasyon
	Yetersiz log kaydı
Çalışan	Çalışanın işe gelememesi
	Yetersiz işe alım prosedürleri
	İzleme mekanizmalarının eksikliği

2.7.1.2 RİSKLERİN ANALİZ EDİLMESİ

Kurumun tespit ettiği riskleri, risk yönetim süreci kapsamında nasıl analiz edileceği tanımlanmalıdır. Risk analizi çalışmalarının detay seviyesi; varlıkların kritiklikleri, bilinen güvenlik açıklıkları ve kurumda daha önce meydana gelmiş olaylar göz önünde bulundurularak, kurumdan kuruma farklılık gösterebilir. Risk analizi yöntemi tamamen nicel, tamamen nitel veya ikisinin bir karışımı olabilir. Ancak uygulamada, risklerin genel seviyesini tespit etmek ve büyük riskleri daha verimli ve hızlı bir şekilde ortaya çıkarmak için nitel analiz yöntemleri kullanılabilir. Çünkü nitel analiz yöntemleri, nicel analiz yöntemlerine göre daha az maliyetli ve efor gerektiren yöntemlerdir. Sonrasında tespit edilen büyük riskler için daha detaylı ve nicel bir risk analizi yöntemi uygulanması gerekir.

- **Nitel risk analizi:** Riskin meydana gelmesi durumunda ortaya çıkacak etkilerin ve bu riskin meydana gelme olasılığının nitel tanımlar ile belirlenmesidir. Nitel risk analizi yapılırken mümkün olduğu yerlerde hissiyate değil, gerçek verilere ve bilgilere dayandırılmalıdır. Nitel risk analizi, herkes tarafından kolay anlaşılır bir altyapı ve farklı riskler için farklı tanımlar kullanma imkanı sunarken; risk analizi sonuçlarının kişiden kişiye öznel olarak değişmesine yol açabilir. Örneğin; "Riskin meydana gelmesi durumunda uzun süreli hizmet kesintisi yaşanacaktır" tanımında "uzun süreli hizmet kesintisi" farklı iş birimleri için farklı süreler ifade edecektir. Nitel risk analizi aşağıdaki durumlarda kullanılabilir:
  - Daha ayrıntılı analiz gerektiren riskleri tanımlamak için ilk tarama faaliyeti olarak,
  - Bu tür analizlerin karar verme faaliyetleri için daha uygun yerlerde,
  - Sayısal verilerin ve kaynakların nicel risk analizi için yetersiz olduğu durumlarda.
- **Nicel risk analizi:** Çeşitli kaynaklardan gelen verileri kullanarak hem etkinin hem de olasılığın sayısal değerler ile belirlenmesidir. Analizin kalitesi kullanılan bütünlüğü, geçerliliği ve hassasiyetine bağlıdır. Nicel risk analizinde çoğunlukla geçmişte yaşanan olaylardan toplanan veriler kullanılır. Bu sayede risk analizi doğrudan bilgi güvenliği hedefleri ve Kurumun bu konudaki endişeleri ile ilişkilendirilebilir. Yeni ve daha önce yaşanmamış riskler ve açıklıklar için yeterli veri bulunmaması durumu nicel risk analizinin dezavantajı olarak gösterilebilir. Bu durumda, nicel risk analizi öznesel tahminler ile tamamlanacak ve bu tahminler risk analizinin doğru ve kesin yapıldığı yanılgısını yaratarak yanlış bir güven duygusu oluşturacaktır. Risk sonuçlarının etkisi ve olasılıklarının değerleri birleştirilerek riskin derecesi tespit edilir. Etki ve olasılık değerlerinin hangi işlemler ile kullanılarak birleştirileceği Kurumun içeriği ve bilgi güvenliği kriterlerine bağlı olarak değişiklik gösterebilir. Bazı kurumlar risk seviyesini hesaplarken oldukça karmaşık işlemler uygularken; bazı kurumlar için daha basit ve üst seviye işlemler yeterli olabilir. Örn. risk seviyesi: etki değeri ile olasılık değerinin çarpımı olarak hesaplanabilir.

Riskin Etkisinin Değerlendirilmesi

Bütün bilgi güvenliği varlıkları tespit edilip değerlendirildikten sonra, bu varlıklar üzerindeki risklerin etkileri varlık değerleri de hesaba katılarak tespit edilmelidir. Etki değerlendirmesi nitel veya nicel yöntemler kullanılarak gerçekleştirilebilir. Ancak, bu adımda etki değerine daha nicel kriterler belirlemek, karar verme sürecine daha fazla bilgi sağlayacağı için karar verme sürecini daha verimli hale getirecektir.

Varlıkların değerlendirilmesi adımı, etki değerlendirilmesi adımı için temel oluşturmakta ve büyük önem taşımaktadır. Bir bilgi güvenliği riski birden fazla varlığı veya bir varlığın bir parçasını etkileyebilir. Farklı tehditler ve açıklıkların farklı varlıklar üzerinde gizlilik, bütünlük ve erişilebilirlikleri açısından farklı etkileri olacaktır. Etki, bir olayın başarı seviyesiyle alakalıdır. Bu nedenle etki ile varlık değeri arasında büyük bir fark vardır.

Etki değerleri, potansiyel bilgi güvenliği olaylarının geçmişte yarattığı etkiler veya tatbikat sonuçları kullanılarak hesaplanabilir. Örneğin, kurumun internet servis sağlayıcısında yaşanan bir hizmet kesintisi durumunda; kurumun bilişim sistemleri altyapısını yedek internet servis sağlayacısına entegre etme süresinin ölçülmesi.

Etki değeri için kriterler belirlenirken; mali, teknik ve insan etkileri veya kurum için önem taşıyan başka etkenler göz önünde bulundurulmalıdır. Bazı durumlarda bir etkinin değerini belirlemek için birden fazla kriter kullanılabilir. Etki değeri hesaplamaları, risk analizi sırasında kullanılan diğer hesaplamalarla (varlık değeri ve olasılık hesaplama gibi) tutarlı olmalıdır. Nitel veya nicel, hangi yöntem kullanılırsa kullanılsın; analizin tutarlı ve tekrarlanabilir sonuçlar üretebilmesi sağlanmalıdır.

Aşağıda bazı etki değerlendirme kriterleri sıralanmıştır:

- Varlığın etki gören parçasının veya tamamının yeniden satın alınması ve değiştirilmesi için gereken mali kaynak,
- Varlığın yedekten geri döndürülmesi için gereken mali kaynak veya efor,
- Varlığın sağladığı hizmetlerde kesinti yaratması durumunda hizmet kesintisinden dolayı ortaya çıkan mali kayıp,
- Varlığın eski haline geri getirilmesi için harcanan mali kaynak ve eforun sonucunda yaşanan fırsat kaybı (mali kaynağın ve eforun başka bir alanda kullanılması durumunda sağlanacak kazanç),
- İhlal olayı sırasında gizliliği, bütünlüğü veya erişilebilirliğine zarar gelen bilginin değeri,
- Uyulması gereken yönetmelikler karşısında yaşanan kayıp.

Yapılan ilk risk analizi sonucunda, bu adımda elde edilen değerler oldukça yüksek çıkacaktır. Ancak BGYS, zamanla bu risklere karşı kontroller uygulayacağı için daha sonraki risk analizinde mevcut kontroller de göz önünde bulundurulduğunda değer düşecektir.

Riskin Olasılığının Değerlendirilmesi

Varlık değerlerinin, tehditlerin ve etki değerlerinin hesaplanmasından sonra bu riskin gerçekleşme olasılığının nicel veya nitel yöntemler ile hesaplanması gerekir. Bu adımda,

tehdidin oluşabilme sıklığı ve açıklığın kullanılma kolaylığı göz önünde bulundurulmalıdır. Olasılık hesaplanırken aşağıdaki başlıklar göz önünde bulundurulabilir:

- Tehdidin oluşma sıklığı için deneyim veya istatistiki veriler kullanılabilir.
- Kasti tehditler için aşağıda başlıklar hesaba katılabilir:
    - Tehdit unsurunun amacı,
    - Tehdit unsurunun kabiliyeti,
    - Tehdit unsurunun ihtiyaç duyduğu kaynak,
    - Açıklığın ve varlığın tehdit unsuru için çekiciliği.
- Kasti olmayan tehditler için aşağıdaki başlıklar hesaba katılabilir:
    - Coğrafi faktörler (çevrede bulunan ve tehdit oluşturabilecek fabrika, elektriği santrali gibi yerler),
    - Hava koşulları,
    - Mevcut açıklıklar ve bunların kullanılabilme kolaylığı,
    - Mevcut güvenlik önlemleri.

Örneğin, bir varlık üzerinde kimlik doğrulama yöntemlerinin eksikliği sebebiyle bir açıklık bulunabilir. Ancak bu açıklığın olasılığı; varlığın üzerindeki bilgiye erişimin başka yöntemler ile (fiziksel veya ağsal olarak erişebilecek kişilerin kısıtlanması vb.) sebebiyle düşük olabilir.

Olasılık değerlerinin daha doğru ve kesin hesaplanabilmesi için varlıklar sundukları hizmetlere, bulundukları fiziksel konumlara veya kullandıkları teknolojilere göre gruplanabilir.

Risk Değerinin Belirlenmesi

Risk analizi; riskin gerçekleşme olasılığına ve etkisine değer atar. Bu değerler nitel olabileceği gibi nicel de olabilir. Risk analizi, değerlendirilen etki ve olasılığı temel alır. Bunlara ek olarak, fayda-maliyet, paydaşların ihtiyaçları ve beklentileri gibi konular ile kurumun uygun gördüğü diğer başlıklar da risk analizine entegre edilebilir. Entegre edilmesi düşünülen başlıkların etki değeri veya olasılık değeri hesaplamalarına entegre edilmesi; o başlıkların farklı riskler analiz edilirken göz ardı edilmemesini ve risk analizi sonuçlarının tutarlı ve tekrar edilebilir olmasına olanak tanıyacaktır. Risk değeri, temel olarak etki değeri ve olasılık değerinin bir kombinasyonu olarak hesaplanır.

2.7.1.3 RİSK DEĞERLEME

Risk değerleme ve risk değerleme kriterlerine ilişkin verilecek kararların içeriği, kavramsal olarak risk analizi çalışmalarının başlangıcında belirlenmelidir. Bu adımda; tehditlerin, açıklıkların ve olasılıklarının belirlenmesinin ardından bu kararlar tekrar gözden geçirilerek

detaylandırılmalıdır. Riskleri değerlemek için, analiz edilen risklerin tahmini değerleri ile risk değerleme kriterleri karşılaştırılmalıdır.

Karar verme süreçlerinde kullanılacak olan risk değerleme kriterleri, iç ve dış risk yönetimi içeriği ile tutarlı olmalı ve kurumun hedeflerini ve iç ve dış paydaşların görüşleri gibi konuları dikkate almalıdır. Risk değerleme sonucunda alınacak kararlar, temel olarak risk kabul kriterleri ile doğrudan ilişkilidir. Kurum, kurum politikalarını, amaçlarını, hedeflerini ve ilgili iç ve dış tarafları dikkate alarak risk kabul kriterlerini belirlemelidir belirlemelidir. Aşağıda listelenen başlıklar risk kabul kriterleri belirlenirken kullanılabilir:

- Kabul edilebilir risk seviyesi birden fazla eşik değeri içerebilir. Hangi eşik değerleri için riskin nasıl ele alınacağı tanımlanmalıdır. Örn. belirli bir seviyenin altındaki riskler yönetimin onayı olmayan kabul edilebilirken, belirli bir seviyenin üstündeki risklerin mutlaka yönetim onayı sonrasında kabul edilmesi gerekir.
- Farklı risk grupları için farklı kabul kriterleri kullanılabilir. Örn. yasal düzenlemelere uyumsuzluk doğuracak riskler için düşük bir eşik değeri kullanılırken, sözleşmede yer almayan konular ile ilgili riskler için yüksek eşik değerleri kullanılabilir.

Risk kabul kriterleri belirlenirken; riskin etkileri, olasılığı, risk belirleme ve analiz aşamasının ne kadar tutarlı yapıldığı da göz önünde bulundurulmalıdır. Örneğin, birden fazla düşük ve orta seviyeli riskin birleşmesi sonucunda tahmin edilemeyen, yüksek seviyede bir risk doğabilir. Bu nedenle kurum, risk değerleme sürecinde yalnızca risk değerleme kriterlerine bağlı kalmadan o an ki durumu da dikkate almalıdır.

Risk değerleme, risk analizi sonucunda öğrenilen bilgileri bu riskler hakkında nasıl faaliyetler uygulanacağının karar verilmesi sürecinde kullanır. Alınacak kararlar:

- Riskin seviyesini düşürmek için bir faaliyet uygulanıp uygulanmayacağı,
- Risklerin hangi öncelikle işleneceği,
- Risk seviyesinin hangi seviyeye indirileceği olabilir.

2.7.2 RİSK MÜDAHALESİ

Risk müdahalesi için kullanılacak dört temel yanıt stratejisi bulunmaktadır:

- Azaltma,
- Kabul etme,
- Kaçınma,
- Transfer etme.

Risk yanıt stratejisi, risk analizi ve risk değerleme adımlarından çıkan sonuçlara göre belirlenmelidir. Bunun yanı sıra, risk yanıt stratejisinin tahmini maliyeti ve riskin oluşması sonucunda ortaya çıkacak tahmini maliyet de hesaba katılmalıdır. Küçük maliyetler ile uygulanan risk tedavileri sonucunda, risk seviyesinde büyük düşüşler yaşanacaksa, bu tedaviler uygulanmalıdır.

Temel olarak, riskin gerçekleşmesi sonucunda ortaya çıkacak sonuçlar ve risk seviyesi, mümkün olduğunca düşürülmeye çalışılmalıdır. Risk seviyesini düşürmek için etki değeri veya olasılık değeri düşürülebilir.

Olasılığı düşük ancak etkisi büyük riskler ayrıca incelenmelidir. Eğer uygulanacak kontrollerin ekonomik etkisi fayda maliyet analizi sonucunda kabul edilebilir sınırlarda olmadığı düşünülüyorsa, risk kabul edilerek önlem uygulanmayabilir.

Bazı riskler için birden fazla risk yanıt stratejisi uygulanabilir. Örn. bir riskin etki ve olasılık değerini düşürüp, kabul edilebilir seviyenin üzerinde kalan risk kabul edilebilir veya transfer edilebilir.

Bu adımda kurum, risk tedavi alternatiflerini göz önünde bulundurarak bir risk yanıt stratejisi seçmeli ve riskin etki veya olasılık değerini düşürmek için uygulanacak eylem maddelerini belirlemeli ve bu eylem maddelerinin hangi tarihe kadar uygulanacağı planlanmalıdır. Bunun yanı sıra, riskler için ihtiyaç duyulan kaynakların belirlenmesi ve öngörülen maliyetin hesaplanması ve risk tedavi planına eklenmesi, risklerin izlenmesi ve karar verme süreci için girdi sağlayacaktır. Risk eylem maddelerini uygulamaktan veya koordine etmekten sorumlu bir kişi atanmalı ve bu kişiye gerekli kaynaklar sağlanmalıdır. Risk eylem maddeleri uygulandıktan sonra, riskin mevcut durumdaki risk seviyesi (artık risk) tekrar hesaplanmalı ve bu seviyenin risk kabul etme kriterleri ile uyumlu olup olmadığı gözden geçirilmelidir. Eğer artık risk, risk kabul etme kriterlerine uygun değilse; risk yeniden analiz edilmeli ve işlenmelidir. Risk yönetim sürecinin performansını ölçmek ve izlemek amacıyla risk eylem maddelerinin uygulandığı tarih, tedavi planına işlenmelidir.

Risk tedavi planında aşağıdaki başlıklara yer verilebilir:

- Riskin ait olduğu varlık ve varlık değeri,
- Tehdidin açıklaması,
- Açıklığın açıklaması,
- Riskin açıklaması,
- Risk tespit tarihi,
- Risk sahibi,
- Etki değeri,

- Olasılık değeri,
- Risk Seviyesi,
- Risk yanıt stratejisi,
- Riskin azaltılması için uygulanacak eylem maddeleri,
- İhtiyaç duyulan kaynaklar (insan kaynağı, teknoloji ve mali kaynak vb.),
- Öngörülen maliyet (teknoloji alımı, harcanacak efor vb. etkenler sonucu hesaplanmış değer),
- Risk sorumlusu (riskin azaltılması için uygulanacak eylem maddelerini uygulamaktan veya koordine etmekten sorumlu kişi),
- Planlanan bitiş tarihi,
- Gerçekleşen bitiş tarihi,
- Tedavi uygulandıktan sonraki olasılık değeri,
- Tedavi uygulandıktan sonraki etki değeri,
- Artık risk seviyesi (tedavi uygulandıktan sonraki risk seviyesi).

2.7.3 RİSKLERİN İZLENMESİ VE GÖZDEN GEÇİRİLMESİ

Riskler durağan değildir ve herhangi bir emare göstermeden tehditler, açıklıklar, riskin gerçekleşme olasılığı ve etkisi büyük değişiklikler gösterebilir. Bu sebeple, bu değişikliklerin tespit edilebilmesi için riskler sürekli olarak izlenmelidir. Bu adımda, yeni tehditler ve açıklıklar hakkında bilgi sağlayan dış kaynaklardan yararlanılabilir.

Kurum aşağıdaki başlıkların sürekli olarak izlendiğinden emin olmalıdır:

- Risk yönetim sürecine eklenen yeni varlıklar,
- Varlıkların değerlerinde değişiklikler,
- Daha önce değerlendirilmemiş kurum içi ve kurum dışından gelebilecek yeni tehditler,
- Yeni açıklıklar,
- Daha önce tanımlanmış açıklıkların yeni tehditler tarafından kullanılabilme durumu,
- Daha önce tespit edilmiş veya yeni ortaya çıkmış tehdit ve açıklıkların risk oluşturabilme olasılıkları,
- Etki değerlerinde ki değişiklikler,
- Yeni varlık, tehdit ve açıklıkların kombinasyonu sonucu ortaya çıkabilecek risk kabul kriterlerinin dışında kalan etki değerleri,
- Süreç içinde yaşanmış güvenlik ihlal olayları.

Yeni tehditler, açıklıklar, olasılık veya etki değerindeki değişiklikler daha önce düşük seviyeli olarak tespit edilmiş risklerin risk seviyesini artırabilir. Düşük seviyeli riskler bu

adımda, tek tek ve toplu olarak oluşturdukları riski tespit edebilmek için, bir arada tekrar gözden geçirilmelidir. Eğer riskin yeni seviyesi, risk kabul kriterleri içerisinde yer almıyorsa; bu risk için risk analizi çalışmaları tekrar yürütülmelidir.

Riskin gerçekleşme olasılığını ve etkisini belirleyen unsurlar zamanla değişiklik gösterebilir. Aynı şekilde, bir risk tedavisinin sürdürülmesini ve diğer risk tedavi seçeneklerinin maliyetini etkileyen unsurlar da zamanla değişiklik gösterebilir. Bunlara ek olarak, kurumda yaşanan büyük değişiklikler (teknoloji değişikliği, organizasyon yapısındaki değişiklik, lokasyon değişikliği vb.) riski oluşturan faktörlerin tamamen değişmesine sebep olabilir. Bu nedenle, risk izleme çalışmaları belirlenen aralıklarla tekrarlanmalı ve risk tedavisi için seçilen yöntemlerde bu çalışma kapsamında tekrar gözden geçirilmelidir.

Kurum, bütün risklerini düzenli aralıklarla veya büyük değişiklikler sonrasında tekrar gözden geçirmelidir.

2.7.4 RİSK YÖNETİMİ SÜRECİNİN İZLENMESİ, GÖZDEN GEÇİRİLMESİ VE GELİŞTİRİLMESİ

Risk Yönetimi sürecinin bağlamının, risk değerleme ve risk müdahalesi çalışmalarının sonuçlarının hala geçerli ve uygun olup olmadığının tespit edilmesi için risk yönetimi sürecinin izlenmesi ve gözden geçirilmesi gerekir.

Kurum, bilgi güvenliği risk yönetimi sürecinin ve ilgili faaliyetlerinin mevcut durumda hala uygun olduğundan ve planlanan şekilde uygulandığından emin olmalıdır. Süreci geliştirmek ve uyumu artırmak için yapılan her değişiklik yöneticilere zamanında bildirilmelidir. Bu sayede, riskin veya risk unsurlarının gözden kaçırılmasının veya hafife alınmasının önüne geçilecektir.

Ek olarak, kurum risk ve unsurlarını ölçmek için kullandığı kriterlerin hala geçerli olup olmadığını ve kurum hedefleriyle, stratejisiyle, politika ve prosedürleri hala uyumlu olup olmadığını doğrulamalıdır. Kurumun bağlamında (iş hedeflerinde, ilgili taraflarında, iş modelinde vb.) olabilecek bir değişiklik sonrasında risk yönetim süreci yeni bağlam kapsamında tekrar gözden geçirilmeli ve düzenlenmelidir. Bu izleme ve gözden geçirme sürecinde aşağıdaki başlıklar dikkate alınmalıdır:

- Yasal zorunluluklar,
- Kurum içerisinde bulunduğu ortam,
- Risk değerleme yaklaşımı,
- Varlık değerleri ve kategorileri,
- Etki kriterleri,

- Risk değerleme kriterleri,
- Risk kabul kriterleri,
- Gerekli kaynaklar.

Kurum, risk değerleme ve risk müdahale için gerekli olan kaynakların; riskin gözden geçirilmesi, yeni veya değişen tehdit ve açıklıkların tespit edilmesi ve üst yönetimin uygun şekilde bilgilendirilebilmesi için sürekli olarak erişilebilir olduğundan emin olmalıdır.

Risk yönetim sürecinin gözden geçirilmesi; risk yönetimi yaklaşımının, yönteminin veya kullanılan teknolojinin değişmesi ile sonuçlanabilir.

2.8 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNE KAYNAKLARIN SAĞLANMASI

Kurum; BGYS'nin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekli kaynakları belirlemeli ve sağlamalıdır. Her türlü faaliyeti gerçekleştirmek için farklı kaynaklar bulunmaktadır:

- Faaliyetleri yönetecek ve yürütecek kişiler,
- Faaliyetleri gerçekleştirmek için gereken süre,
- Yeni bir adım atmadan önce sonuçların görülmesi için ayrılan zaman,
- Faaliyetleri gerçekleştirmede kullanılacak finansal kaynaklar,
- Doğru kararları almada ve faaliyetlerin performansını ölçmede kullanılacak bilgiler,
- Bilgi sistemleri ürünü olup olmadıklarına bakılmaksızın, teknoloji, araç ve gereçler gibi edinilebilecek veya üretilebilecek altyapı ve diğer araçlar.

Görüldüğü üzere, BGYS'nin ihtiyaç duyduğu kaynaklar, yalnızca finansal kaynaklarla sınırlı değildir. Çalışanlar, zaman, bilgiler ve araçlar da BGYS kaynakları arasında değerlendirilmektedir. Düzenli olarak bu kaynaklara duyulan ihtiyaç gözden geçirilmeli ve BGYS'nin ihtiyaçlarına uygun olarak sağlanan kaynak güncellenmelidir. Kurum kronolojik olarak sırasıyla:

- BGYS ile ilgili tüm faaliyetler için gerekli kaynakları hesap etmelidir. Bu hesaplama yapılırken kaynakların sadece miktarını (kapasitesini) değil aynı zamanda kalitesini (örn. çalışanlar için yetkinlik, araçlar için performans ve yetenekler) de göz önünde bulundurmalıdır;
- İhtiyaç kadar kaynağı gerektiğinde edinmelidir;
- Kaynakların teminini tüm BGYS süreçleri boyunca sürdürmelidir; ve
- Sağlanan kaynakları BGYS'nin ihtiyaçlarına göre gözden geçirerek gerektiği şekilde düzenlemelidir.

Bu faaliyet ve sonucu ile ilgili bilgilerin belgelenmesi, kurumun yönetim sisteminin etkinliği için gerekli olduğu ölçüde yapılmalıdır.

2.9 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN İHTİYAÇ DUYDUĞU YETKİNLİK SEVİYESİNİN TEMİNİ

Yetkinlik, amaçlanan sonuçlara ulaşmak için bilgi ve becerileri uygulama yeteneğidir. İhtiyaç duyulan yetkinlik, iş tanımına özel olan risk yönetimi, hukuksal bilgi gibi alanlarda olabileceği gibi; iş tanımından bağımsız olarak, analitik düşünme, hızlı karar alabilme, sürekli öğrenme, takım çalışmasına yatkınlık gibi özellikleri de içerebilir. Kurum, BGYS'nin performansı için gerekli kişilerin sahip olması gereken yetkinlikleri belirlemeli ve kişilerin bu yetkinlik düzeyinde olmasını sağlamalıdır.

BGYS'nin performansını etkileyebilecek kişiler, kurum ya da müşteri firma çalışanları olabilir. Dolayısıyla, ilgili tüm çalışanların yetkinliğinin yönetilmesi gereklidir. Yeni bir yetkinliğin edinilmesi ya da var olan bir yetkinliğin yükseltilmesi; eğitim, danışmanlık alma, işe alma veya sözleşme yapma gibi çok çeşitli yollarla hem kurum içerisinde hem de kurum dışında sağlanabilir.

Geçici olarak (belirli bir faaliyet için veya kısa bir süreliğine) ihtiyaç duyulan yetkinlik için kurum, yeterliliklerini doğruladıktan dış kaynak çalışanlar ile sözleşme yapabilir. Bu doğrulama yapılırken ihtiyaç duyulan yetkinlikle ilgili sertifikaların veya benzer iş tecrübelerinin varlığı aranabilir.

Kurum, BGYS'nin ihtiyaç duyduğu yetkinliğin temin edilebilmesi için;

- BGYS içindeki her bir role karşılık gelen yetkinliği belirlemeli ve bu yetkinliğin belgelenmesi gerekip gerekmediğine karar vermelidir. Örneğin; belirli bir lisans bölümünden mezun olunduğunu gösteren bir diploma ya da ihtiyaç duyulan seviyede yetkinliği belgeleyen bir sertifikanın varlığı iş tanımında şart koşulabilir. Dış taraf ile yapılacak bir sözleşmede ise, dış tarafın sahip olması gereken sertifika veya iş tecrübeleri sözleşme içerisinde yer alabilir.
- BGYS içindeki rolleri, gerekli yetkinliğe sahip kişilere atamalıdır. Çalışanların eğitimlerine, iş deneyimlerine, sertifikalarına bakılarak yetkin çalışanlar belirlenip atama gerçekleştirilebilir. Kurum içerisinde aranan yetkinliğe sahip çalışan bulunamıyorsa:
  - Çalışanların yetkinliği elde etmesini sağlamak için eğitim, rehberlik, mevcut çalışanların yeniden atanması vb. yöntemlerle veya
  - Yetkinliğe sahip yeni çalışanlar kuruma dahil ederek (örn. işe alma veya dış tarafla yapılacak sözleşme yoluyla) yetkinliğin temini sağlanmalıdır.
- İkinci maddedeki eylemlerin etkinliği değerlendirilmelidir. Bu etkinliği değerlendirirken aşağıdaki örnek yöntemler izlenebilir:
  - Çalışanların eğitimden sonra yetkinlik kazanıp kazanmadıklarını ölçme,

  - Yeni işe alınan veya sözleşmeli dış taraf çalışanlarının kuruma geldikten bir süre sonra yeterliliklerini analiz etme,
  - İşe alım planının beklendiği gibi tamamlandığını doğrulama.
- Yeterliliğin zaman içinde gerektiği gibi gelişmesini ve beklentileri karşılamasını sağlamalıdır.

Yetkinlik kanıtı olarak dokümante edilmiş bilgi gereklidir. Bu nedenle kurum, bilgi güvenliği performansını etkileyen gerekli yetkinliğe ve bu yetkinliğin ilgili kişiler tarafından nasıl karşılandığına ilişkin belgeleri saklamalıdır.

2.10 BİLGİ GÜVENLİĞİ FARKINDALIĞI

Bilgi güvenliği bir zincir gibidir ve çalışanlar bu zincirin halkalarıdır. Bilgi güvenliği seviyesi, zincirin en zayıf halkası tarafından belirlenir. Bu nedenle, çalışanların bilgi güvenliği farkındalığının artırılması BGYS için zorunludur. Çalışanların farkındalığı, bilgi güvenliği konusunda kendilerinden ne beklendiğine dair gerekli anlayış ve motivasyona sahip olmayı ifade eder. Çalışanlar; aşağıdaki konularda mutlaka bilgilendirilmelidir:

- Mevcut BGYS politika ve prosedürleri,
- Bu politika ve prosedürlere erişimin yöntemi,
- BGYS kapsamında uyulması gerekli kurallar,
- BGYS gerekliliklerine uymamanın etkileri (hem bilgi güvenliği seviyesi üzerindeki olumsuz etki hem de çalışana uygulanacak yaptırımlar konusunda),
- BGYS'nin etkinliğine katkıları (örn. kendilerini ilgilendiren amaç ve hedefler yönüyle),
- Bilgi güvenliği performansının iyileştirilmesi noktasındaki rolleri.

Ayrıca, dış tarafların da BGYS gerekliliklerine uymamanın etkilerini bilmesi, anlaması ve kabul etmesi gerekir. Aksi durumda, bilgi güvenliği ve çalışanlar açısından olumsuz sonuçlar oluşabilir. Bu kişilerin, bir bilgi güvenliği politikasının var olduğunu ve bu konuda nereden bilgi edinebileceklerini bilmeleri önemlidir.

Bir kurumda, birçok çalışan için politika ve prosedürlerin ayrıntılı içeriğini bilmek şart değildir; ancak sahip oldukları rolleri etkileyen ve bilgi güvenliği politikasından türetilmiş olan bilgi güvenliği amaçlarını ve gereksinimlerini bilmeli, anlamalı, kabul etmeli ve uygulamalıdırlar. Bu gereksinimler, işlerini yapmak için izlemeleri beklenen standartlara veya prosedürlere dâhil edilebilir.

Kurumun aşağıdakileri yapması gereklidir:

- İlgili taraflara özel, belirli mesajlar içeren bir program hazırlanmalı (örn. iç ve dış taraflar, insan kaynakları çalışanları veya proje personeli gibi gruplara özel farkındalık eğitimleri);
- Bilgi güvenliği gereksinimlerini ve beklentilerini, kurumun BGYS dışındaki faaliyetlerinin de içerisine katabilmek için; bu gereksinimler ve beklentiler, farkındalık ve eğitim materyallerine dahil edilmeli;
- Mesajları düzenli aralıklarla iletmek için bir duyuru planı hazırlanmalı (Tablo 6);
- Hem farkındalık oturumunun sonunda hem de oturumlar arasında mesajların anlaşıldığı doğrulanmalı (örn. eğitim öncesi ve sonrası sınavlar ile); ve
- Kişilerin BGYS gerekliliklerine göre hareket edip etmedikleri kontrol edilmeli.

Tablo 6. Örnek Duyuru Planı

Duyuru Numarası	Duyuru Konusu	Planlanan Duyuru Tarihi	Gerçekleşen Duyuru Tarihi
01	e-Posta Kullanımında Güvenlik	Mayıs 2020	11/05/2020
02	Güçlü Parola Belirleme Yöntemleri	Haziran 2020	15/06/2020
03	Kritik WPA2 Zafiyeti Hakkında Bilgilendirme	Plansız	12/06/2020

Bu faaliyet ve sonucu ile ilgili bilgilerin dokümante edilmesi, kurumun yönetim sisteminin etkinliği için gerekli olduğu ölçüde yapılmalıdır.

2.11 İLETİŞİM

İletişim, BGYS içindeki önemli bir süreçtir. İlgili iç ve dış taraflarla yeterli seviyede iletişimin sağlanması zorunludur. Yeterli seviyede iletişimin temini için kurum öncelikle, BGYS ile ilgili iç ve dış iletişim ihtiyaçlarını belirlemelidir. İletişim, kurumun tüm düzeylerindeki ilgili iç taraflar arasında veya ilgili dış taraflar ile kurum arasında olabilir. İletişimi başlatan taraf, iç ya da dış taraf olabilir. Kurumun şunları belirlemesi gerekir:

- Hangi içeriğin hangi taraflara iletilmesi gerektiğini belirten iletişim konusu ve ilgili taraflar sütunları;
- İletişim için planlanan veya en uygun zaman (örn. bir ihlal olayı gerçekleştiği anda iletişim kurulması gerekirken; iş sürekliliği tatbikatlarının tetiklenmesi için iletişim, planlanmış periyotlarda gerçekleştirilebilir);

- İletişimde yer alan taraflar (iletişimi başlatan ve iletişim kurulan taraflar);
- İletişim faaliyetlerini kimin başlatacağı (belirli bir iletişim konusu için iletişimin belirli bir kişi veya kurum tarafından başlatılacağı belirtilmelidir); ve
- İletişim faaliyetlerinin etkilendiği, dolayısıyla bir değişiklik sonrasında iletişim planlarını etkileyebilecek süreçler

Kurum yukarıda belirtilen maddeleri dikkate alarak iki ayrı tablo oluşturmalıdır. Bunlardan ilki olan "İletişim Planı Tablosu" tüm çalışanlar ile paylaşılabilir olan ve rollerin yer aldığı plandır. Bu plan ilgili tüm taraflar ile paylaşılmalı, belirlenen noktalarda bir kopyası hazır bulundurulmalıdır. İletişim Planı Tablosu, bina girişinde yer alan danışma noktası, toplantı odaları, çalışma ofisleri vb. çok çeşitli alanlarda tüm çalışanlar ile paylaşılabilir.

"İletişim Listesi" ise İletişim Planı Tablosu'ndan yola çıkılarak hazırlanmış ve bu tabloda yer alan rollerin sahibi olan çalışanların bilgisini içeren listedir. İletişim Listesi içerdiği kişisel bilgiler göz önünde bulundurularak tüm kullanıcılara açık olacak şekilde paylaşılmamalıdır. Bunun yerine her bir ilgili taraf için, ilgili tarafın ihtiyaçlarını karşılayacak şekilde listenin filtrelenmesi ve bilmesi gereken prensibine uygun hale getirildikten sonra paylaşılması önerilir.

Örnek olarak hazırlanmış olan "İletişim Planı Tablosu" ve "İletişim Listesi", Tablo 7 ve Tablo 8 olarak rehber içerisinde yer almaktadır. İletişim Listesi'nin örnekte verilen haline benzer filtre uygulanmamış haline, sadece Bilgi Güvenliği Çalışanları tarafından erişilebilir olmalıdır. İletişim düzenli olarak veya ihtiyaç duyuldukça gerçekleşebilir. Proaktif veya reaktif olabilir. İletişim süreçlere, kanallara ve protokollere dayanır. Bunlar, iletilen mesajın bütünüyle alınmasını, doğru bir şekilde anlaşılmasını ve mesaja uygun şekilde hareket edilmesini sağlamak için özenle seçilmelidir.

Tablo 7. İletişim Planı Tablosu

Sıra No	1	2
İletişim Yönü	Kurum İçi	Kurum Dışı
İletişim Konusu	Bilgi Güvenliği İhlal Olayı	Elektrik Altyapısı
İletişimi Başlatan Kişi / Kurum	Tüm Çalışanlar	Tesis Yönetimi Çalışanı
İletişim Kurulan Kişi / Kurum	Bilgi Güvenliği Yöneticisi	Elektrik Hizmeti Sağlayıcı Firma
İletişim Zamanı	Bilgi Güvenliği İhlal Olayı Yaşandığında	Elektrik Arızası Durumunda
İletişim Yöntemi	• Talep • E-posta	• Talep • E-posta • Telefon
İletişimin Etkilendiği Süreçler	• Yardım Masası Hizmeti • e-Posta Sistemi	• Yardım Masası Hizmeti • e-Posta Sistemi • Santral Hizmeti

Tablo 8. İletişim Listesi

Sıra No	1	2
İletişim Yönü	Kurum İçi	Kurum Dışı
İletişim Konusu	Bilgi Güvenliği İhlal Olayı	Elektrik Altyapısı
İletişimi Başlatan Kişi / Kurum	A Kurumu Çalışanları	Ali Er
İletişim Kurulan Kişi / Kurum	Fatma Özet	B Elektrik Çağrı Merkezi
İletişim Bilgisi (Telefon/e-Posta)	bgymail[at]kurum.com.tr	info[at]bfirması.com 0555 555 55 55
İletişim Zamanı	Bilgi Güvenliği İhlal Olayı Yaşandığında	Elektrik Arızası Durumunda

Kurum hangi içeriğin iletilmesi gerektiğini belirlemelidir. Örneğin;

- Risklerin tanımlanması, analizi, değerlendirilmesi ve tedavisinde kullanılmak üzere risk yönetimi planları ve sonuçları (gerektiğinde ve uygun olan şekilde sadece ilgili taraflara);
- Ulaşılan bilgi güvenliği hedefleri (örn. ISO / IEC 27001 sertifikası, kişisel veri koruma yasalarına uygunluk belgesi vb. Bunlar özellikle kurum itibarına katkı sağlamaktadır);
- Kurumun bilgi güvenliği yönetiminin, beklenmedik durumlarla başa çıkma yeteneğine olan güveni artırmayı sağlayan olaylar veya krizler (paylaşılması uygunsa);
- Roller, sorumluluklar ve yetkiler (sadece ilgili taraflarla paylaşılması önemlidir);
- BGYS'deki değişiklikler;
- BGYS kapsamındaki kontroller ve süreçler gözden geçirilerek tespit edilen diğer hususlar;
- Düzenleyici kurumlarla veya diğer ilgili taraflarla iletişim gerektiren konular (örn. ihlal olayı veya kriz bildirimi); ve
- Müşteriler, potansiyel müşteriler, hizmet kullanıcıları ve otoriteler gibi dış taraflardan gelen talepler veya diğer iletişim konuları.

Kurum, aşağıdaki konularda iletişim için gereksinimleri belirlemelidir:

- Uygun yetki ile belirli bir role atanmış ve iç ve dış iletişim kurmasına izin verilen çalışan (veri sızıntısı gibi özel durumlarda vb.). Dış iletişim için bir halkla ilişkiler görevlisi ve iç iletişim için bir güvenlik görevlisi olabilir;
- İletişim tetikleyicileri veya sıklığı (örn. bir olayın iletişimi için tetikleyici, ilgili olayın tanımlanmasıdır);
- Asli ilgili taraflara (örn. müşteriler, düzenleyiciler, genel kamuoyu, önemli iç kullanıcılar) yönelik mesajların içeriği. Bir iletişim planının, ihlal olayı müdahale planının veya iş sürekliliği planının bir parçası olarak uygun bir yönetim seviyesi tarafından hazırlanan ve önceden onaylanan mesajlara dayanarak iletişim daha etkili olabilir;
- İletişimin planlanan alıcıları. Bazı durumlarda bir liste tutulmalıdır (örn. hizmetlerdeki değişikliklerin veya krizlerin iletilmesi için);
- İletişim araçları ve kanalları. İletişimde, mesajın resmi ve uygun yetki düzeyinde olduğundan emin olmak için özel araçlar ve kanallar kullanılmalıdır. İletişim kanalları, iletilen bilgilerin gizliliğinin ve bütünlüğünün korunması için tüm ihtiyaçları karşılamalıdır. Örneğin; e-posta aracılığıyla iletilmesi gereken bir belgenin

kendisini e-posta ekinde göndermek yerine, bu belgenin bulunduğu sürüm takip sisteminden alınacak linki e-postaya eklemek daha uygundur. Böylece e-posta alıcısının belgeyi görmeye yetkisi olmadığı durumlarda, alıcı linki açamayacağından gizlilik korunmuş olur.

İletişim, kuruluşun gereksinimlerine göre sınıflandırılmalı ve ele alınmalıdır. Bu faaliyet ve sonucu ile ilgili bilgilerin dokümante edilmesi, kurumun yönetim sisteminin etkinliği için gerekli olduğu ölçüde yapılmalıdır.

2.12 DOKÜMANTE EDİLMİŞ BİLGİ

2.12.1 GENEL

Bilgi güvenliği politikasını, hedeflerini, yönergelerini, talimatlarını, kontrollerini, süreçlerini, prosedürlerini ve çalışanların ne yapmalarının ve nasıl davranmalarının beklendiğini tanımlamak ve bu bilgileri iletmek için dokümante edilmiş bilgiye ihtiyaç vardır. Dokümante edilmiş bilgi, BGYS denetimlerinde BGYS sisteminin varlığını göstermek için gereklidir. Kritik rollerde olan çalışanlar değiştiğinde, göreve yeni atananların var olan işleyişe adapte olabilmeleri, dolayısıyla istikrarlı bir BGYS sağlamak için de dokümante edilmiş bilgi bulunmalıdır. Ayrıca, BGYS süreçlerinin ve bilgi güvenliği kontrollerinin faaliyetlerini, kararlarını ve sonuçlarını kaydetmek için dokümante edilmiş bilgiye ihtiyaç vardır.

Dokümante edilmiş bilgiler şunları içerebilir:

- Bilgi güvenliği hedefleri, riskleri, gereksinimleri ve standartları hakkında bilgi,
- İzlenecek süreçler ve prosedürler hakkında bilgi,
- Yönetimin gözden geçirme toplantıları gibi süreçlerden gelen katkıların kayıtları,
- iş sürekliliği tatbikatları gibi operasyonel faaliyetlerin planları ve sonuçları.

BGYS içinde, başka bir faaliyet için girdi olarak kullanılan dokümante edilmiş bilgiler üreten birçok etkinlik vardır. Bir dizi dokümante edilmiş bilginin hazırlanması zorunludur (örn. Bilgi Güvenliği Politikası).

Zorunlu dokümante edilmiş bilgi miktarı genellikle kurumun büyüklüğü ile ilgilidir. Kurumun büyüklüğü ile beraber; iç ve dış tarafların beklentileri, analiz edilmesi gerekli risklerin sayısı, iletişim ihtiyaçları, aktarılacak bilginin büyüklüğü gibi gerekliliklerde artış gözlenir. Bu nedenle, kurumun büyüklüğü arttıkça BGYS yönetilebilirliğinin ve sürekliliğinin sağlanabilmesi için dokümante bilgilere olan ihtiyaç da artmaktadır. Zorunlu ve ek dokümante bilgiler, 2.13'te belirtilen performans değerlendirme gereksinimlerinin yerine getirilebilmesi için yeterli bilgi içermelidir.

Kurum, standartlar tarafından zorunlu tutulmasa da, BGYS'nin etkinliğini sağlamak için bazı bilgilerin dokümante edilmesinin gerekli olduğuna karar verebilir. Kurumun yapısı göz

önünde bulundurularak bu bilgilerin dokümante edilmesi denetimler sırasında bir gereklilik olarak dahi görülebilir. Kurum tarafından BGYS'nin etkinliğini sağlamak için gerekli olabilecek dokümante edilmiş bilgilere örnekler aşağıda verilmiştir:

- Kuruluşun bağlamının sonuçları,
- Roller, sorumluluklar ve yetkililer,
- Risk yönetiminin farklı aşamalarının raporları,
- Belirlenen ve sağlanan kaynaklar,
- Beklenen yeterlilik,
- Farkındalık faaliyetlerinin planları ve sonuçları,
- İletişim faaliyetlerinin planları ve sonuçları,
- BGYS için gerekli olan dış kaynaklı dokümante edilmiş bilgi,
- Dokümante edilmiş bilgileri kontrol etme süreci,
- Bilgi güvenliği faaliyetlerini yönetmek ve işletmek için politikalar, kurallar ve direktifler,
- BGYS'yi ve genel bilgi güvenliği statüsünü uygulamak, sürdürmek ve geliştirmek için kullanılan süreçler ve prosedürler,
- Faaliyet planları,
- BGYS süreçlerine ait çıktıların kanıtı (örn. ihlal olayı yönetimi, erişim kontrolü, bilgi güvenliği sürekliliği, ekipman bakımı vb.).

Dokümante edilmiş bilgi dâhili veya harici kaynaklara sahip olabilir. Kurum dokümante edilmiş bilgilerini bir belge yönetim sisteminde yönetmeli ve versiyon bilgisini tutmalıdır.

2.12.2 OLUŞTURMA VE GÜNCELLEME

Doküman oluşturulurken ve güncellenirken, kurum dokümanın uygun bir isme, tanıma, formata, içeriğe, gözden geçirmeye ve onaya sahip olduğundan emin olmalıdır. Bu niteliklerin sağlanabilmesi için uygun bir dokümantasyon süreci tanımlanmalıdır. Yönetimin gözden geçirmesi ve onaylaması ile; dokümante edilen bilgilerin doğru, amaca uygun ve hedeflenen grup için uygun bir formda ve detayda olduğu teyit edilmiş olur. Bu onaylama; dokümanların basılı hallerine ıslak imza ile yapılabileceği gibi, elektronik ortamda gerçekleşecek onay ile ya da toplantı tutanağının gündem maddelerinde belirtilerek de yapılabilir. Düzenli gözden geçirmeler ise, dokümante edilmiş bilgilerin uygunluğunun ve yeterliliğinin sürekli olmasını sağlar. Düzenli gözden geçirmeler kayıt altına alınmalı, yapılan değişiklikler belirtilmeli, dokümanların sürümleri tutulmalıdır.

Dokümante bilgi çok çeşitli biçimlerde saklanabilir. Basılı veya elektronik ortamdaki geleneksel dokümanlar, web sayfaları, veri tabanları, log kayıtları, ses ve video dosyaları bu formatlardan bazılarıdır. Ayrıca, dokümante bilgiler amacın beyanından (örn. bilgi

güvenliği politikası), performans kayıtlarından (örn. iç denetim raporu) veya her ikisinin birleşiminden oluşabilir. Aşağıdaki yönlendirmeler ve rehberlik doğrudan basılı ve elektronik ortamdaki geleneksel dokümanlar için geçerlidir, diğer dokümante bilgi formlarına uygulandığında ilgili forma uygun şekilde yorumlanmalıdır.

Kurum, bir "dokümante bilgi kütüphanesi" oluşturarak aşağıdakileri uygulamalı ve dokümante edilmiş bilgiler için ortak bir yapı oluşturmalıdır:

- Hangi bilgilerin ne detayda dokümante edileceğini netleştirerek;
- Farklı dokümante bilgi türleri için şablonlar sağlayarak;
- Dokümante edilmiş bilgiyi hazırlama, onaylama, yayınlama ve yönetme sorumluluklarını belirleyerek; ve
- Uygunluğun ve yeterliliğin sürekliliğini sağlamak için revizyon ve onay sürecini belirleyip belgeleyerek.

Örneğin, risk listesi oluşturulacağında bu listede projelere özel riskler yer alacak mı yoksa sadece kurumsal riskler mi listelenecek kararı verilmelidir. Risk Listesi Şablonu'nda, listede yer alması istenen sütunlar belirlenmeli (tehdit, açıklık, risk tanımı gibi zorunlu sütunlara ek olarak risk müdahalesi için maliyet bilgisi gibi ek sütunlar da belirlenebilir. Bu karar alınırken kurumun büyüklüğü ve BGYS olgunluğu göz önünde bulundurulmalıdır). Risk listesinin hazırlanması, onaylanması, yayınlanması, yönetilmesi ve sürekliliğinin sağlanması için sorumluluklar; kılavuzlar ve görev listeleri kullanılarak rollerle eşleştirilmelidir.

Kurum, her belgenin ortak niteliklerini içeren, açık ve benzersiz tanımlamaya izin veren bir dokümantasyon yaklaşımı tanımlamalıdır. Bu özellikler genellikle belge türü (örn. politika, yönerge, kılavuz, plan, form, süreç veya prosedür), amaç ve kapsam, başlık, yayın tarihi, sınıflandırma, referans numarası, sürüm numarası ve bir düzeltme geçmişi bilgilerini içerir. Dokümana dahil edilmesi gereken diğer bazı alanlar, yazar(lar), belgeden sorumlu kişi(ler), belgenin uygulaması ve değişimi, onaylayan(lar) veya onay otoritesi şeklindedir. İfadeler ve yazma tarzı, belgelerin hedef grubuna ve kapsamına göre şekillenmelidir.

Dokümante edilmiş bilgilerdeki bilgilerin çoğaltılmasından kaçınılmalı ve aynı bilgileri farklı belgelerde çoğaltmak yerine çapraz referanslar kullanılmalıdır. Bu yaklaşımın sürdürülmesi önemlidir. Aynı konuda birden fazla dokümanda bilgi verilmesi durumunda, bu konuda yaşanan bir değişiklik durumunda, konunun yer verildiği tüm dokümanların güncellenmesi gerekir. Hem iş gücü verimliliği hem de dokümanların birbiri ile tutarlılığının sağlanabilmesi açısından bu uygulama olumsuz bir duruma zemin hazırlamaktadır. Dolayısıyla, bilginin tek bir dokümanda verilmesi, gerekli diğer dokümanlarda ise bilginin verildiği bu ilk dokümana referansta bulunulması uygun olanıdır.

Dokümantasyon yaklaşımı, dokümante edilmiş bilgilerin zamanında gözden geçirilmesini ve tüm dokümantasyon değişikliklerinin onaya tabi olmasını sağlamalıdır. Uygun inceleme kriterleri zamanlamayla (örn. belge incelemeleri arasındaki maksimum zaman dilimleri) veya içerikle ilgili olabilir. Dokümante bilgilerin doğru, amaca uygun ve hedeflenen grup için uygun bir biçimde ve detayda olmasını sağlayan onay kriterleri tanımlanmalıdır.

2.12.3 DOKÜMANTE EDİLMİŞ BİLGİLERİN KONTROLÜ

Kurum, dokümante edilmiş bilgileri dokümanların yaşam döngüleri boyunca yönetir. Onaylandıktan sonra, dokümante bilgiler hedeflenen gruba iletilir. Dokümante bilginin, tüm yaşam döngüsü boyunca bütünlüğünü, gizliliğini ve erişilebilirliğini koruması için gerekli önlemler alınır.

Dokümante tüm bilgiler, kurumun sınıflandırma şemasına uygun olarak sınıflandırılmalıdır (örn. gizlilik derecelendirme dokümanı dikkate alınarak). Daha sonra bu bilgiler, sınıflandırma seviyesinin gerekliliklerine uygun olarak korunmalı ve ele alınmalıdır.

Dokümante bilgiler için bir değişiklik yönetimi süreci tanımlanmalı ve yalnızca yetkili kişilerin, uygun ve önceden tanımlanmış yollarla, gerektiğinde değiştirme ve dağıtma hakkına sahip olması sağlanmalıdır.

Dokümante bilgiler, yetkisi bulunan ilgili taraflara dağıtılmalıdır. Bunun için kurum, dokümante her bilgi (veya bilgi grubu) için ilgili tarafların kim olduğunu ve dağıtım, erişim, geri alma ile kullanım için yararlanılacak araçları (örn. uygun erişim kontrol mekanizmalarına sahip bir web sitesi) belirlemelidir. Dağıtım, gizli bilgilerin korunması ve işlenmesiyle ilgili tüm gerekliliklere uygun olmalıdır.

Kurum, dokümante bilgiler için bir saklama süresi belirlemelidir. Saklama süresi belirlenirken planlanan geçerlilik ve diğer ilgili gereklilikler (örn. yasal mevzuatlar) dikkate alınır. Bilgilerin saklama süresi boyunca okunaklı olması sağlanmalıdır (örn. mevcut yazılım tarafından okunabilen dosya formatlarının kullanılması veya basılı evrağın yıpranmadığının doğrulanması). Kurum, saklama süresi dolduktan sonra belgelenmiş bilgilerle ne yapacağını belirlemelidir (örn. imha etme ya da arşive kaldırma).

Kurum ayrıca dış kaynaklı (müşterilerden, ortaklardan, tedarikçilerden, düzenleyici kurumlardan vb. gelen) dokümante bilgileri yönetmelidir. Bu dokümanların yönetiminde de iç dokümanların yönetimi ile benzer prensipler esas alınır.

Bu faaliyet ve sonucu ile ilgili bilgilerin dokümante edilmesi, kurumun yönetim sisteminin etkinliği için gerekli olduğu ölçüde yapılmalıdır.

2.13 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ'NİN PERFORMANSININ DEĞERLENDİRİLMESİ

2.13.1 İZLEME, ÖLÇME, ANALİZ VE DEĞERLENDİRME

Kurum, bilgi güvenliği performansını ve BGYS'nin etkinliğini değerlendirmelidir. İzleme ve ölçümün amacı, kurumun risk değerlendirmesi ve tedavisi de dâhil olmak üzere bilgi güvenliği faaliyetlerinin, hedeflenen sonuca planlanan şekilde ulaşıp ulaşmadığını anlamasına yardımcı olmaktır.

İzleme; bir sistemin, bir sürecin veya bir faaliyetin durumunu belirler; ölçüm ise bu duruma bir değer belirleme işlemidir. Örneğin; internet trafiğinin aktif olduğunu belirtmek izlemenin sonucu iken, bu trafiğin bant genişliğini ölçerek kullanılan bant genişliği oranını belirlemek bir ölçümün sonucudur. Bu nedenle izleme, belirli zaman aralıklarında benzer ölçümlerin art arda yapılmasıyla gerçekleştirilebilir. İzleme ve ölçüm için kurum şunları belirler:

- Neyin izleneceği ve ölçüleceği;
- İzleme ve ölçmenin ne zaman kim tarafından yapılacağı; ve
- Geçerli ölçüm sonuçları (karşılaştırılabilir ve tekrarlanabilir) elde etmek için kullanılacak yöntemler.

Analiz ve değerlendirme için ise kurum şunları belirler:

- İzleme ve ölçümden elde edilen sonuçları kim, ne zaman analiz eder ve değerlendirir; ve
- Geçerli analiz sonuçları üretmek için kullanılacak yöntemler.

İki genel ölçüm türü vardır:

- Planlanan faaliyetlerin verimliliğini ifade eden performans ölçümleri; ve
- Planlanan faaliyetlerin gerçekleştirilmesinin kuruluşun bilgi güvenliği hedefleri üzerindeki etkisini ifade eden etkinlik ölçümleri.

Değerlendirmenin de iki yönü bulunur:

- Kurumun beklendiği gibi çalışıp çalışmadığını belirlemek için bilgi güvenliği performansını değerlendirmek (bunun için BGYS içindeki süreçlerin ilgili süreçlerden beklentileri ne kadar iyi karşıladığını belirlemek gerekir); ve
- Kurumun doğru şeyleri yapıp yapmadığını belirlemek için BGYS'nin etkinliğini değerlendirmek (bunun için ise bilgi güvenliği hedeflerine ne ölçüde ulaşıldığını belirlemek gerekir).

Aşağıda performans izleme ve ölçüm gerekliliklerini yerine getirmek için kullanılabilecek örnek bir tablo bulunmaktadır (Tablo 9).

Tablo 9. Örnek Ölçüm Metrikleri

Kullanım Amacı	İzleme Sorumlusu	İzleme Sıklığı	İzlenen Kaynak
Zemin Kat Ağ Hizmeti	Ali Er	Alarmlar günlük, Raporlama haftalık	Bant Genişliği Kullanımları
Depolama	Hakan Uzun	Alarmlar günlük, Raporlama aylık	CPU, RAM, Disk, Alarmlar

Belirlenmiş olan ölçülecek niteliklerin ölçüm sonuçları yeni bir tabloda kayıt altına alınır. Bu tablo üzerinden analiz ve değerlendirme çalışması yapılabilir. Bu nedenle, tablonun ölçüm hedeflerini ve sonuçlarını, ölçüm ve değerlendirme sorumlularını, ölçümün sıklığını göstermesi gerekir. Aşağıda örnek bir performans ölçüm ve değerlendirme tablosunun sahip olması gereken sütun isimleri verilmiştir:

- Ölçüm Açıklaması
- İlgili Kontroller
- Ölçüm Hedefi
- Ölçüm Sıklığı
- Veri Kaynağı ve Veri Toplama Yöntemi
- Seçilen Göstergeler (ölçüm sonucu hesaplanırken dikkate alınacak göstergeler, örn. yapılan eğitim sayısı, bulguların kapatılma süresi, disk kullanım yüzdesi vb.)
- Ölçüm Sorumlusu
- Değerlendirme Sorumlusu
- Ölçüm Sonuç Raporunun Paylaşılacağı Kişiler
- Ölçüm Sonucu

İzleme, ölçüm, analiz ve değerlendirmeyi planlarken 'bilgi ihtiyacını' tanımlamak tavsiye edilen bir uygulamadır. Bilgi ihtiyacı genellikle, kurumun bilgi güvenliği performansını ve BGYS etkinliğini değerlendirmesine yardımcı olan üst düzey bir bilgi güvenliği sorusu veya ifadesi olarak ifade edilir. Başka bir deyişle, bir “bilgi ihtiyacı” tanımlanmalı, daha sonra izleme ve ölçüm bu ifadeyi elde etmek için yapılmalıdır. Örneğin; bilgi ihtiyacı, “BGYS Farkındalığının Çalışanlara Kazandırılma Oranı” olarak tanımlandığında, bu ihtiyacı gidermek için yapılacak ölçüm “Farkındalık Eğitimlerine Katılım Oranı” veya “Çalışanlar Tarafından Bildirilen Bilgi Güvenliği İhlal Olaylarının Oranı” olarak belirlenebilir. Bir bilgi ihtiyacını karşılamak için birden fazla ölçüm yapmak da mümkündür. Dolayısıyla, örnekte yer alan ölçümlerin her ikisi de kullanılabilir.

Ölçülecek nitelikler belirlenirken dikkatli olunmalıdır. Çok fazla veya yanlış niteliklerin ölçülmesi pratiklikten uzak, maliyetli ve üretkenliğe zarar vericidir. Çok sayıda özelliği ölçme, analiz etme ve değerlendirme maliyetlerinin yanı sıra, kritik konuların tamamen gözden kaçırılması olasılığı da vardır.

İzleme, ölçme, analiz ve değerlendirmeye katılanlara ayırt edici roller belirlemek ve atamak uygun olabilir. Bu roller ölçüm istemcisi, ölçüm planlayıcısı, ölçüm inceleyicisi, bilgi sahibi, bilgi toplayıcı, bilgi analisti ve değerlendirme girdi veya çıktısının bilgi iletişimcisi olabilir. İzleme ve ölçme ile analiz ve değerlendirme sorumlulukları genellikle farklı yetkinliğe sahip olan ayrı kişilere verilir.

2.13.2 İÇ DENETİM

Kurum, BGYS'nin gereksinimlere uygunluğunu görmek için iç denetimler gerçekleştirir. İç denetimler planlı aralıklarla yapılır. İç denetimlerin düzenli ve kriterlere uygun olarak düzenleniyor olması, BGYS'nin durumu ile ilgili üst yönetime güvence verir. Denetim bir dizi ilke ile nitelendirilir: bütünlük, adil temsil, profesyonel özen, gizlilik, bağımsızlık ve kanıta dayalı yaklaşım.

İç denetimler, iki çeşit gereksinimin uygunluğunu test etmek içindir: Kurumun BGYS içerisinde belirlediği kendi gereksinimleri ve varsa tabii olunan standardın (örn. ISO / IEC 27001) getirdiği gereksinimler.

Kurumun BGYS için kendi gereksinimleri şunları içerir:

- Bilgi güvenliği politikası ve prosedürlerde belirtilen şartlar;
- Risk müdahale sürecinin sonuçları da dahil olmak üzere bilgi güvenliği hedeflerinin gerçekleştirilmesi için belirlenen gereksinimler;
- Yasal ve sözleşmeye bağlı gereksinimler; ve
- Dokümante bilgilerle ilgili gereksinimler.

Denetçiler ayrıca BGYS'nin etkin bir şekilde uygulanıp uygulanmadığını da değerlendirir. Bu kapsamda çalışanların BGYS ve BGYS'nin kendilerini ilgilendiren süreçleri (örn. bilgi güvenliği politakası, bilgi güvenliği ihlal olayı bildirimi, bilgi güvenliği rolleri ve sorumlulukları vb.) ile ilgili farkındalığı sorgulanabilir. Buna ek olarak kayıtların incelenmesi sırasında BGYS'nin etkin bir şekilde işletildiğini görmek adına güncel olaylara dair kanıtlar aranabilir. Örneğin; yeni açıklanmış kritik bir zafiyetle ilgili risk sürecinin başlatılması ya da duyuru yayınlanması BGYS'nin aktif olarak sürdürüldüğünün bir göstergesidir.

Bir denetim programı; belirli zaman dilimleri için planlanmalı, kapsamı net bir şekilde belirlenmeli ve denetim kriterleri rehberliğinde sürdürülmelidir. Denetim kriterleri, denetim kanıtlarının karşılaştırılacağı bir referans olarak kullanılan bir dizi politika, prosedür veya

gerekliliktir. Bir başka deyişle denetim kriterleri, denetçinin ne olmasını beklediğini açıklar. Denetim kriterleri, bağlı bulunan standarttan gelebileceği gibi, kurumun belirlediği gereksinimlerden de ortaya çıkabilir.

İç denetim; uygunsuzlukları, riskleri ve fırsatları belirleyebilir. Uygunsuzluklar 2.14.1'deki talimatlara göre; riskler ise 2.7'deki rehberliğe göre yönetilir.

Kurumun, denetim programları ve denetim sonuçlarına dair dokümante edilmiş bilgileri mutlaka saklaması gerekmektedir.

2.13.2.1 BİR DENETİM PROGRAMINI YÖNETME

Bir denetim programı; denetim faaliyetlerinin planlanması, yürütülmesi, raporlanması ve takip edilmesi için yapı ve sorumlulukları tanımlar. Bu nedenle, yapılan denetimlerin uygun olmasını, kapsamının doğru belirlenmesini, kurumun faaliyetleri üzerindeki olumsuz etkisini en aza indirmesini ve gerekli denetim kalitesini sürdürmesini sağlamalıdır. Bir denetim programı; denetim ekiplerinin yetkinliğini, denetim kayıtlarının uygun şekilde korunmasını ve operasyonların, risklerin, denetimin etkinliğinin izlenmesini ve gözden geçirilmesini de sağlamalıdır. Ayrıca, bir denetim programı, BGYS'nin (tüm ilgili süreçler, fonksiyonlar ve kontroller) belirli bir zaman dilimi içerisinde tümüyle denetlenmesini sağlamalıdır. Son olarak, bir denetim programı, denetimin türü (örn. iç denetim, sertifikalandırma denetimi, gözetim denetimi), süresi, yeri ve zamanı hakkında dokümante edilmiş bilgileri içermelidir.

İç denetimlerin kapsamı ve sıklığı, organizasyonun büyüklüğüne ve niteliğine; ayrıca BGYS'nin doğasına, işlevselliğine, karmaşıklığına ve olgunluk düzeyine dayandırılmalıdır (riske dayalı denetim).

Uygulanan kontrollerin etkinliği, iç denetimler kapsamında incelenmelidir. Gerekli tüm kontrolleri kapsayacak bir denetim programı tasarlanmalı ve seçilen kontrollerin zaman içindeki etkinliğinin değerlendirilmesi yapılmalıdır. Kurumun bağlamı, liderlik, risk yönetimi, performans değerlendirmesi, iyileştirme gibi BGYS'nin temelini oluşturan kontrol maddeleri her denetimin kapsamına kesinlikle dahil edilmelidir. Kriptografi, tedarikçi güvenliği, yasal gereksinimler gibi ek kontrol maddeleri ise her denetimin kapsamına alınmayabilir. Bu karar alınırken ek kontrol maddelerinin yakın bir tarihteki denetimde kapsama alınıp alınmadığına bakılabilir. Belirli periyotlarla tüm BGYS kontrol maddelerinin denetimden geçirilmesi gerekliliği unutulmamalıdır. Kapsam dışına çıkarılacak olan kontrol maddeleri belirlenirken kurumun iş süreçleri mutlaka göz önünde bulundurulmalıdır. Elektronik imza sertifikasyonu sağlayan bir kurum için kriptografi kontrol maddesi en az BGYS'nin temel kontrol maddeleri kadar değerlidir.

Denetim programı, uygun kanıtların değerlendirilebilmesi için süreçlerin ve kontrollerin bir süredir faaliyette olması gerektiğini de göz önünde bulundurmalıdır. Yeni kurulmuş ve ilk denetimine girmekte olan bir BGYS denetiminde, tüm süreçlerin kayıt üretmesi mümkün olamayabilir. Üretilen kayıtlar ise sıklıkla olgunluktan uzaktır. Bu nedenle, denetçiler kayıtlardaki makul eksiklikleri anlayışla karşılamalıdır.

Bir BGYS ile ilgili iç denetimler, kurumun diğer iç denetimlerinin bir parçası olarak veya onlarla işbirliği içinde etkin bir şekilde gerçekleştirilebilir. Denetim programı, ayrı ayrı veya birlikte yürütülen bir veya daha fazla yönetim sistemi standardıyla ilgili denetimleri içerebilir. Yapılan bir iç denetimin BGYS denetimi ile örtüşen yanları, denetim programından çıkartılarak iş gücünün verimli kullanımı sağlanabilir.

Bir denetim programı şunlarla ilgili dokümante bilgileri içermelidir: denetim kriterleri, denetim yöntemleri, denetim ekiplerinin seçimi, gizlilikle ilgili işlemler, bilgi güvenliği, denetçiler için sağlık ve güvenlik hükümleri ve benzeri konular.

2.13.2.2 DENETÇİLERİN YETERLİLİĞİ VE DEĞERLENDİRİLMESİ

Denetçilerin yeterliliği ve değerlendirilmesi ile ilgili olarak kurum:

- Denetçiler için yeterlilik şartlarını belirlemeli;
- Uygun yetkinliğe sahip iç veya dış denetçileri seçmeli;
- Denetçilerin ve denetim ekiplerinin performansını izlemek için bir süreç oluşturmalı (örn. denetlenen çalışanlar ile denetim sonrasında yapılacak anketler);
- Sektörün içinden ve bilgi güvenliği bilgisine sahip çalışanları iç denetim ekiplerine dahil etmelidir.

Denetçiler; yetkin, bağımsız ve yeterli eğitim almış olmaları göz önünde bulundurularak seçilmelidir. Denetçilerin sahip olması gereken şartlar BGYS prosedürleri içerisinde belirlenebilir.

İç denetçilerin seçilmesi küçük şirketler için zor olabilir. Gerekli kaynaklar ve yetkinlik dahili olarak mevcut değilse, iç denetimde görev almaları için kurum dışından denetçiler atanmalıdır. Kurum dışarıdan denetçiler kullandığında, denetçilerin kuruluşun bağlamı hakkında yeterli bilgiye sahip olduklarından emin olunmalı, bu bilgi kurum çalışanları tarafından sağlanmalıdır.

2.13.2.3 DENETİMİN YAPILMASI

Denetim yapılırken, denetim ekibi lideri, önceki denetimlerin sonuçlarını ve daha önce bildirilen uygunsuzluklar ile kabul edilebilir seviyenin üzerindeki riskleri takip etme ihtiyacını karşılayacak bir denetim planı hazırlamalıdır. Denetim planı dokümante bilgi olarak tutulmalı ve denetim kriterlerini, kapsamını ve yöntemlerini içermelidir.

Denetim ekibi şunları gözden geçirmelidir:

- Süreçlerin ve belirlenmiş kontrollerin yeterliliği ve etkinliği;
- Bilgi güvenliği hedeflerinin yerine getirilmesi;
- Kurumun kendi bilgi güvenliği gereksinimlerine uygunluk;
- Bilgi güvenliği risk müdahale sürecinin sonuçları ile eşleştirilmiş Uygulanabilirlik Bildirgesi'nin tutarlılığı;
- Bilgi güvenliği risk müdahale planının, değerlendirmesi yapılmış riskler ve risk kabul kriterleri ile tutarlılığı;
- Yönetim gözden geçirme girdileri ve çıktılarının bütünlüğü (kurumun büyüklüğü ve karmaşıklığı dikkate alınarak);
- Yönetim gözden geçirme çıktılarının (iyileştirme ihtiyaçları dahil) kurum üzerindeki etkileri; ve
- Sertifikalandırılan standardın getirdiği şartlar.

Performans izleme, ölçüm, analiz ve değerlendirme çalışmalarının etkinliği ve güvenilirliği doğrulanmış ise, denetçiler bu verileri BGYS tarafından getirilen kontrollerin etkinliğini değerlendirmek için kullanabilir. Böylece denetçilerin kendi değerlendirme çabalarını azaltmaları sağlanabilir.

Denetimin sonucu uygunsuzlukları içeriyorsa, denetlenen kişi, denetim ekibi lideri ile kararlaştırılacak her uygunsuzluk için bir "faaliyet planı" hazırlamalıdır. Bir faaliyet planı tipik olarak şunları içerir:

- Tespit edilen uygunsuzluğun tanımı;
- Uygunsuzluğun neden(ler)inin tanımlanması (kök-neden analizi);
- Tespit edilen uygunsuzluğu belirli bir zaman dilimi içinde ortadan kaldırmak için kısa vadeli düzeltmenin ve uzun vadeli düzeltici faaliyetin tanımı. Kısa vadeli düzeltme uygunsuzluğun ortadan kalkmasını sağlasa da tekrarlanmasını engellemez. Uzun vadeli düzeltici faaliyet ise uygunsuzluğun kök-nedeninin ortadan kaldırılmasıdır, uygunsuzluğun tekrarlanmasını engelleyen çözümdür; ve
- Planın uygulanmasından sorumlu kişiler.

Denetim sonuçları ile birlikte denetim raporları da üst yönetime sunulmalıdır.

Önceki denetimlerin sonuçları mümkünse denetim öncesinde gözden geçirilmeli ve denetim programı, uygunsuzluk nedeniyle daha yüksek risk taşıyan alanları daha kapsamlı denetleyecek şekilde düzenlenmelidir.

2.13.3 YÖNETİMİN GÖZDEN GEÇİRMESİ

Üst yönetim BGYS'yi, planlanan aralıklarla gözden geçirir. Yönetimin gözden geçirmesinin amacı; BGYS'nin sürekli uygunluğunu, yeterliliğini ve etkililiğini sağlamaktır. Sürekli uygunluk, kuruluşun hedefleri ile sürekli uyumu ifade eder. Yeterlilik ve etkililik ise, BGYS tarafından yönlendirilen süreçlerin ve kontrollerin etkili bir şekilde uygulanmasının yanı sıra BGYS'nin uygun tasarımını ve organizasyonun dokusuna işlemesini, süreçlerle bütünleşmesini ifade eder.

Genel olarak, yönetimin gözden geçirmesi kurumun çeşitli düzeylerinde gerçekleştirilen bir süreçtir. Bu etkinlikler günlük, haftalık veya aylık birim toplantılarından basit rapor sunumlarına kadar değişebilir. Üst yönetim, organizasyondaki tüm seviyelerden gelen girdilerden faydalanarak yönetimin gözden geçirilmesinden sorumludur. Üst yönetim, BGYS'nin performansının raporlanmasını zorunlu tutmalı ve düzenli olarak gözden geçirmelidir.

Ölçümleri ve raporları teslim alma ve inceleme, elektronik iletişim, sözlü güncellemeler gibi yönetimin BGYS'yi gözden geçirmesinin birçok yolu vardır. Kritik girdiler, bilgi güvenliği ölçümlerinin sonuçları, iç denetimlerin sonuçları, risk değerlendirme sonuçları ve risk tedavi planının durumudur. Bilgi güvenliği risk değerlendirmesi sonuçlarını ve risk tedavi planının durumunu incelerken yönetim, artık risklerin risk kabul kriterlerini karşıladığını ve risk tedavi planının ilgili tüm riskleri ve risk tedavi seçeneklerini ele aldığını doğrulamalıdır.

BGYS'nin tüm kapsamı, yönetim toplantılarında uygun programlar ve gündem maddeleri oluşturularak, en az yılda bir kez olacak şekilde planlanan aralıklarla gözden geçirilmelidir. Yeni veya daha az olgunlaşmış BGYS'ler, daha etkin olabilmek için yönetim tarafından daha sık gözden geçirilmelidir. Bununla beraber, olgunlaşmış bir BGYS'nin kapsamına yeni dahil olmuş süreçler de daha sık gözden geçirilmelidir.

Yönetimin gözden geçirme gündemi aşağıdaki konuları ele almalıdır:

- Önceki yönetim gözden geçirmelerinden gelen eylemlerin durumu;
- BGYS ile ilgili iç ve dış hususlardaki değişiklikler;
- Bilgi güvenliği performansı hakkında geri bildirim ve bu bilgilerin trend analizi:
  - Uygunsuzluklar ve düzeltici faaliyetler;
  - İzleme ve ölçüm sonuçları;
  - Denetim sonuçları; ve
  - Bilgi güvenliği hedeflerinin yerine getirilmesi.
- İyileştirme önerileri, değişiklik talepleri ve şikayetler de dahil olmak üzere ilgili taraflardan gelen BGYS ile ilişkili geri bildirimler;

- Bilgi güvenliği risk değerlendirmelerinin sonuçları ve bilgi güvenliği risk tedavi planının durumu; ve
- Hem BGYS'nin hem de bilgi güvenliği kontrollerinin verimliliğinin yükseltilmesini içeren sürekli iyileştirme fırsatları.

Gözden geçirmeyi gerçekleştiren yönetim için belirlenen hedefler göz önünde bulundurularak, yönetimin gözden geçirmesine yapılan girdiler uygun ayrıntı düzeyinde tutulmalıdır. Örneğin; üst yönetim bilgi güvenliği hedeflerine veya yüksek seviye hedeflere odaklı olarak tüm öğelerin sadece bir özetini değerlendirmelidir.

Yönetimin gözden geçirme sürecinden elde edilen çıktılar; sürekli iyileştirme fırsatları ve BGYS'deki değişikliklere ilişkin kararları içermelidir. Ayrıca aşağıdakilerle ilgili kararların kanıtlarını da içerebilirler:

- Bilgi güvenliği politikası ve hedeflerindeki değişiklikler, örn. ilgili tarafların iç ve dış hususlarındaki ve gereksinimlerindeki değişikliklerden kaynaklanan;
- Risk kabul kriterlerindeki ve bilgi güvenliği risk değerlendirmelerini gerçekleştirme kriterlerindeki değişiklikler;
- Bilgi güvenliği performansının değerlendirilmesini takiben gerekli görülen eylemler;
- BGYS için kaynak veya bütçe değişiklikleri;
- Güncellenmiş bilgi güvenliği risk tedavi planı veya uygulanabilirlik bildirgesi; ve
- İzleme ve ölçüm faaliyetlerinde gerekli iyileştirmeler.

Yönetim gözden geçirmelerinde dokümante bilgiler gereklidir. Hiçbir eylemin gerekli olmadığına karar verildiğinde bile, listelenen tüm alanlar (en azından), değerlendirilmeye alındığını göstermek için muhafaza edilmelidir.

Kurumun farklı düzeylerinde birkaç yönetim gözden geçirme yapıldığında, bunlar uygun bir şekilde birbiri ile ilişkilendirilmelidir.

2.14 İYİLEŞTİRME

2.14.1 UYGUNSUZLUK VE DÜZELTİCİ FAALİYET

Uygunsuzluk, BGYS'nin bir gereksiniminin yerine getirilmemesidir. Gereksinimler; dokümanlarda belirtilen, bu dokümanlardan yorumlama sonucunda çıkartılan veya bilgi güvenliğinin sağlanabilmesi için zorunlu olan ihtiyaçlar veya beklentilerdir. Kurum uygunsuzlukları gidermek için aksiyon almalı, değerlendirme sonucunda gerekliyse düzeltmelere ek olarak düzeltici faaliyetler başlatmalıdır. Aşağıdakiler gibi çeşitli uygunsuzluk türleri vardır:

- Tabii olunan standardın bir şartının (tamamen/kısmen) yerine getirilmemesi;

- BGYS tarafından belirtilen bir gereksinim, kural veya kontrolün doğru bir şekilde uygulanmaması; ve
- Yasalara, sözleşmelere veya üzerinde mutabık kalınan müşteri gereksinimlerine uyulmaması.

Bazı örnek uygunsuzluklar aşağıdakiler olabilir:

- Prosedür ve politikaların beklediği gibi davranmayan kişiler;
- Üzerinde anlaşmaya varılan ürün veya hizmetleri sağlamayan tedarikçiler;
- Beklenen sonuçları üretmeyen projeler; ve
- Tasarıma göre çalışmayan kontroller.

Uygunsuzluklar şu şekilde ayırt edilebilir:

- Yönetim sistemi kapsamında gerçekleştirilen faaliyetlerin eksiklikleri;
- Uygun şekilde düzeltilmeyen etkisiz kontroller;
- BGYS'nin bir gerekliliğinin yerine getirilmediğini gösteren bilgi güvenliği ihlal olaylarının analizi;
- Müşterilerden gelen şikayetler;
- Çalışanlardan veya tedarikçilerden gelen uyarılar;
- Kabul kriterlerini karşılamayan izleme ve ölçüm sonuçları; ve
- Ulaşılmayan hedefler.

Düzeltmeler, uygunsuzluğa derhal müdahale etmeyi ve sonuçlarını ele almayı amaçlamaktadır. Düzeltici faaliyetler ise, uygunsuzluğun nedenini ortadan kaldırmayı ve tekrarlanmasını önlemeyi amaçlamaktadır. Bir uygunsuzluğu düzeltmek için önlem alınabileceği durumda bunun yapılması gereklidir.

Bilgi güvenliği ihlal olayları ile uygunsuzlukların ayırt edilmesi önemlidir. Bilgi güvenliği ihlal olayları; herhangi bir bilgi varlığının gizlilik, bütünlük veya erişilebilirliği üzerine olumsuz etki eden olaylardır. Bu olumsuzluk gerçekleşse de (örn. açık kalan sistem odası kapısından giren saldırganın sistemlere zarar vermesi) gerçekleşmesine ramak kalsa da (örn. sistem odası kapısının açık kalması) bilgi güvenliği ihlal olayı olarak değerlendirilmelidir.

Bazı durumlarda ihlal olayları uygunsuzluk olarak da değerlendirilebilir. Özellikle süreçteki bir eksiklikten, yanlış uygulamadan kaynaklandığı fark edilen bilgi güvenliği ihlal olayları için uygunsuzluk süreci de işletilerek sürecin düzeltilmesi ve ihlalin tekrarının önüne geçilmesi gereklidir.

Bilgi güvenliği ihlal olayları mutlaka bir uygunsuzluğun var olduğu anlamına gelmez, ancak uygunsuzlukların tespitinde önemli kaynaklardan biridir. İç ve dış denetimler ile müşteri şikayetleri ise uygunsuzlukların tespitinde yardımcı olan diğer önemli kaynaklardır.

Uygunsuzluk durumunda başlatılacak aksiyonlar, tanımlanmış bir süreç çerçevesinde ilerlemelidir. Süreç şunları içermelidir:

- Uygunsuzluğun kapsamını ve etkisini belirlemek;
- Uygunsuzluğun etkisini sınırlamak için gerekli müdahalelere karar vermek (bu aşamada yapılacak müdahaleler ile durum kontrollü bir güvenlik seviyesine getirilir ve uygunsuzluk sonucu yeni zararların oluşması engellenir);
- Düzeltmelerin yapılmasını sağlamak için ilgili çalışan ile iletişim kurmak;
- Verilen karar doğrultusunda düzeltmeler yapmak;
- Düzeltmelerin hedeflenen etkiye sahip olmasını ve istenmeyen yan etkiler üretmemesini sağlamak için durumu izlemek;
- Hala düzeltilmedi ise, uygunsuzluğu düzeltmek için daha fazla aksiyon almak; ve
- Uygunsa diğer ilgili taraflarla iletişim kurmak.

Tek başına düzeltmeler uygunsuzluğun tekrarlanmasını önleyemez. Düzeltici faaliyetler düzeltmelerden sonra veya bunlara paralel olarak gerçekleştirilebilir. Aşağıdaki adımlar düzeltici faaliyet süreci içerisinde atılmalıdır:

- Belirlenmiş kriterlere göre (örn. uygunsuzluğun etkisi, tekrarlanabilirlik) düzeltici bir eylemin yürütülmesinin gerekip gerekmediğine karar verilmesi;
- Aşağıdakileri dikkate alarak uygunsuzluğun gözden geçirilmesi:
  - Benzer uygunsuzluklar kaydedilmiş mi;
  - Uygunsuzluğun neden olduğu tüm sonuçlar ve yan etkiler; ve
  - Yapılan düzeltmeler.
- Aşağıdakileri göz önünde bulundurarak uygunsuzluğun derinlemesine bir kök-neden analizinin gerçekleştirilmesi ve bu çalışmaya uygunsuzluğa müdahale etmekten sorumlu çalışanların da katılımının sağlanması:
  - Yanlış giden şey, uygunsuzluğa yol açan belirli bir tetikleyici veya durum (örn. kişiler, yöntemler, süreçler veya prosedürler tarafından belirlenen hatalar, donanım veya yazılım araçları, yanlış ölçümler, çevre); ve
  - Gelecekte benzer durumların belirlenmesine yardımcı olabilecek modeller ve kriterler.
- Aşağıdakileri göz önünde bulundurarak BGYS üzerindeki potansiyel sonuçların bir analizinin gerçekleştirilmesi:

  - Diğer alanlarda benzer uygunsuzlukların olup olmadığı (örn. kök-neden analizi sırasında bulunan örüntüleri ve kriterleri kullanarak); ve
  - Diğer alanların belirlenen modeller veya kriterlerle eşleşip eşleşmediği (eşleşme varsa benzer bir uygunsuzluğun ortaya çıkması sadece bir zaman meselesidir).
- Kök-nedeni ortadan kaldırmak için gereken faaliyetlerin belirlenerek, uygunsuzluğun sonuçları ve etkileri ile orantılı olup olmadığının değerlendirilmesi (örn. fayda-maliyet analizi ile) ve diğer uygunsuzluklara veya kritik yeni bilgi güvenliği risklerine yol açabilecek yan etkilere sahip olmadıklarının kontrol edilmesi;
- Mümkünse, tekrarlama olasılığının daha yüksek olduğu ve uygunsuzluğun daha önemli sonuçlarının olduğu alanlara öncelik verecek şekilde düzeltici faaliyetlerin planlanması (planlama, düzeltici faaliyetten sorumlu bir kişi ve düzeltici faaliyetin uygulanması için bir son tarih içermelidir);

Düzeltmeler ve düzeltici faaliyetlerin bir sonucu olarak, iyileştirme için yeni fırsatların tanımlanması mümkündür. Tanımlanan iyileştirmeler uygulamaya alınmalıdır.

Kurumun, uygunsuzluğu gidermek için uygun şekilde hareket ettiğini ve ilgili sonuçları ele aldığını göstermek için yeterli seviyede dokümante edilmiş bilginin saklanması gerekmektedir. Uygunsuzluk yönetiminin (keşif ve düzeltmelerden başlayarak) tüm önemli adımları ve başlatılırsa, düzeltici faaliyet yönetiminin (kök-neden analizi, inceleme, faaliyetlerin uygulanması hakkında karar, gözden geçirme ve BGYS için alınan değişiklik kararları) dokümante edilmelidir. Dokümante bilgilerin ayrıca, alınan önlemlerin hedeflenen etkilere ulaşıp ulaşmadığına dair kanıt içermesi gerekmektedir.

2.14.2 SÜREKLİ İYİLEŞTİRME

Kurum, BGYS'nin uygunluğunu, yeterliliğini ve etkinliğini sürekli olarak geliştirmelidir. Bilgi sistemlerine yönelik riskler ve bunları istismar etme yolları hızlı ve sürekli bir değişim içerisindedir. Hiçbir BGYS mükemmel değildir; organizasyon ve içeriği değişmese bile, her zaman BGYS'nin geliştirilebileceği bir yol vardır.

İyileştirmeler sadece uygunsuzlukların ya da risk çalışmalarının sonucu olarak belirlenmezler. Uygunsuzluklarla veya risklerle bağlantılı olmayan iyileştirmelere bir örnek olarak, BGYS'nin bir unsurunun (uygunluk, yeterlilik ve etkililik açısından) değerlendirilmesi sonucu BGYS'nin gereksinimlerini aştığı veya verimlilikten yoksun olduğunun belirlenmesi gösterilebilir. Eğer öyleyse, değerlendirilen unsuru değiştirerek BGYS'yi iyileştirme fırsatı doğabilir.

Sürekli iyileştirmeyi kullanan sistematik bir yaklaşım, kurumun bilgi güvenliğini artıracak daha etkili bir BGYS'ye zemin hazırlayacaktır. Üst yönetim, sürekli iyileştirme için hedefler belirleyebilir, örn. etkinlik, maliyet veya süreç olgunluğu ölçümleri yoluyla.

Sonuç olarak; kurum, BGYS'sini iş süreçlerinin gelişen, öğrenen, yaşayan bir parçası olarak görür. BGYS'nin değişikliklere ayak uydurması için BGYS'yi, hedef, etkinlik ve kurumun amaçlarına uygunluğu açısından düzenli olarak değerlendirir.

Değerlendirme aşağıdakilerin bir analizini içermelidir:

- BGYS'nin uygunluğu (iç ve dış hususlar, ilgili tarafların beklentileri, tespit edilen bilgi güvenliği hedefleri ve riskler uygun şekilde ele alınmış mı düşünülerek);
- BGYS'nin yeterliliği (BGYS faaliyetlerinin kurumun genel amaçlarına, faaliyetlerine ve süreçlerine uygun olup olmadığı dikkate alınarak);
- BGYS'nin etkinliği (BGYS'nin hedeflenen sonuçlarına ulaşması, ilgili tarafların beklentilerinin karşılanması, bilgi güvenliği risklerinin bilgi güvenliği hedeflerini karşılayacak şekilde yönetilmesi, uygunsuzlukların yönetilmesi düşünülerek); ve
- BGYS'nin verimliliği (kaynak kullanımının uygunluğu, verimliliği artırma fırsatları göz önünde bulundurularak).

Uygunsuzluklar ve düzeltici faaliyetler yönetilirken iyileştirme fırsatları da tanımlanabilir. İyileştirme fırsatları belirlendikten sonra, organizasyon şunları gerçekleştirir:

- Uygulamaya değer olup olmadıklarını tespit etmek için onları değerlendirmek;
- İyileştirmeyi sağlamak için BGYS ve unsurlarında yapılması gerekli değişiklikleri belirlemek;
- Faydaların gerçekleşmesini ve uygunsuzlukların ortaya çıkmamasını sağlayacak fırsatları ele almak için faaliyetleri planlamak ve uygulamak; ve
- Faaliyetlerin etkinliğini değerlendirmek.

Bu faaliyetler, riskleri ve fırsatları ele alan faaliyetlerin bir alt kümesi olarak düşünülmelidir.

EKLER

EK-A: KONTROL SORULARI

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
2.1	Bilgi Güvenliği Yönetimi Sisteminin Temelleri	BGYS'ye neden ihtiyaç duyulduğu kavramsal olarak analiz edildi mi?
2.1	Bilgi Güvenliği Yönetimi Sisteminin Temelleri	BGYS kurulumunda üst yönetim liderlik ediyor mu?
2.1	Bilgi Güvenliği Yönetimi Sisteminin Temelleri	BGYS'nin ihtiyaç duyduğu kaynakların temin edilmesi hızlı bir şekilde gerçekleştiriliyor mu?
2.2	Kurumun ve İçinde Bulunduğu Ortamın Anlaşılması	BGYS ile kurum amaç ve hedefleri arasındaki ilişki uygun bir şekilde kurulmuş mudur?
2.2	Kurumun ve İçinde Bulunduğu Ortamın Anlaşılması	Kurum risk ve fırsatları değerlendirirken iyileştirme fırsatlarını dikkate alıyor mu?
2.2	Kurumun ve İçinde Bulunduğu Ortamın Anlaşılması	BGYS ile kurumun diğer iş süreçleri arasında yaşanabilecek uyuşmazlıkların önüne geçilmesi için gerekli çalışmalar yapılıyor mu?
2.2	Kurumun ve İçinde Bulunduğu Ortamın Anlaşılması	BGYS sürecine etki edebilecek iç etkenler tanımlanmış mıdır?
2.2	Kurumun ve İçinde Bulunduğu Ortamın Anlaşılması	BGYS sürecine etki edebilecek dış etkenler tanımlanmış mıdır?
2.3	İlgili Tarafların Tespit Edilmesi	İlgili iç ve dış taraflar tespit edildi mi?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
2.4	Bilgi Güvenliği Yönetim Sisteminin Kapsamının Belirlenmesi	BGYS süreçleri kurumun hangi alanları için zorunlu hangi alanları için zorunlu değil tanımlandı mı?
2.4	Bilgi Güvenliği Yönetim Sisteminin Kapsamının Belirlenmesi	BGYS'nin diğer kurum süreçleriyle bağlantıları ve bağımlılıkları kesin bir şekilde belirlendi mi?
2.5	Bilgi Güvenliği Politikalarının Oluşturulması	Kuruma ait temel bir bilgi güvenliği politikası oluşturuldu mu?
2.5	Bilgi Güvenliği Politikalarının Oluşturulması	Kurumun diğer politikaları temel bilgi güvenliği politikası ile uyumlu mu?
2.6	Bilgi Güvenliği Yönetim Sistemi Organizasyonunun Kurulması	BGYS ile ilişkili tüm rol ve sorumluluklar resmi bir şekilde tanımlandı ve kayıt altına alındı mı?
2.6	Bilgi Güvenliği Yönetim Sistemi Organizasyonunun Kurulması	BGYS ile ilili kritik olan rol ve sorumlulukların onayı Üst Yönetim tarafından alındı mı?
2.6	Bilgi Güvenliği Yönetim Sistemi Organizasyonunun Kurulması	Kurumda bir Bilgi Güvenliği Yönetim Komitesi oluşturuldu mu?
2.6	Bilgi Güvenliği Yönetim Sistemi Organizasyonunun Kurulması	BGYÖK'de her iş birimi aynı seviye yöneticiler veya çalışanlar tarafından temsil ediliyor mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
2.6	Bilgi Güvenliği Yönetim Sistemi Organizasyonunun Kurulması	Bilgi Güvenliği Yöneticisi rolü, diğer iş birimlerini bağımsız bir şekilde denetleyebilecek bir çalışana atandı mı?
2.6	Bilgi Güvenliği Yönetim Sistemi Organizasyonunun Kurulması	Risk yöneticisinin görev ve sorumlukları belirlendi mi?
2.6	Bilgi Güvenliği Yönetim Sistemi Organizasyonunun Kurulması	Varlıklar ve sahipleri açık ve net bir şekilde tespit edildi mi?
2.6	Bilgi Güvenliği Yönetim Sistemi Organizasyonunun Kurulması	Varlık sahiplerine sorumlulukları duyuruldu mu?
2.7	Bilgi Güvenliği Risk Yönetimi	Kurumda risk yönetimi sürecinin adımları belirlendi mi?
2.7	Bilgi Güvenliği Risk Yönetimi	Risk yönetim sürecinde uyulması gerekli temel gereksinimler belirlendi mi?
2.7	Bilgi Güvenliği Risk Yönetimi	Kurumda risk değerlendirme çalışmaları yapılıyor mu?
2.7	Bilgi Güvenliği Risk Yönetimi	Risk belirleme çalışmalar düzenli olarak gerçekleştiriliyor mu?
2.7	Bilgi Güvenliği Risk Yönetimi	Tespit edilen riskler, risk yönetim süreci kapsamında nasıl analiz edileceği tanımlandı mı?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
2.7	Bilgi Güvenliği Risk Yönetimi	Risk yanıt stratejileri belirlendi mi?
2.7	Bilgi Güvenliği Risk Yönetimi	Riskler sürekli olarak izlenip gözden geçiriliyor mu?
2.8	Bilgi Güvenliği Yönetim Sistemine Kaynakların Sağlanması	Kurum, BGYS'nin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekli kaynakları belirleyip sağlıyor mu?
2.9	BGYS'nin İhtiyaç Duyduğu Yetkinlik Seviyesinin Temini	BGYS ile ilgili çalışanların tümünün yetkinliği yönetiliyor mu?
2.9	BGYS'nin İhtiyaç Duyduğu Yetkinlik Seviyesinin Temini	Kurum, BGYS 'nin ihtiyaç duyduğu yetkinlik seviyesinin teminini gerçekleştiriyor mu?
2.10	Bilgi Güvenliği Farkındalığı	Çalışanlar mevcut BGYS politika ve prosedürleri ile ilgili düzenli olarak bilgilendiriliyorlar mı?
2.10	Bilgi Güvenliği Farkındalığı	Çalışanların BGYS politika ve prosedürlerine erişim yetkileri var mı?
2.10	Bilgi Güvenliği Farkındalığı	Çalışanlar, kurumun bilgi güvenliği performansının iyileştirilmesi noktasındaki rollerini biliyorlar mı?
2.11	İletişim	BGYS ile ilgili iç ve dış iletişim ihtiyaçları belirlendi mi?
2.11	İletişim	Rehberde belirtilen hususlar dikkate alınarak bir iletişim planı tablosu oluşturuldu mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
2.12	Dokümante Edilmiş Bilgi	Kurum dokümante edilmiş bilgilerini bir belge yönetim sisteminde yönetiyor ve versiyon bilgisi tutuyor mu?
2.12	Dokümante Edilmiş Bilgi	Dokümante edilen bilgilerin yaşam döngüsü boyunca gizliliği, bütünlüğü ve erişilebilirliğinin korunması için gerekli önlemler alınıyor mu?
2.12	Dokümante Edilmiş Bilgi	Dokümante bilgiler için saklama süreleri belirlendi mi?
2.13	BGYS'nin Performansının Değerlendirilmesi	Ölçülecek olan nitelilkler belirlendi mi?
2.13	BGYS'nin Performansının Değerlendirilmesi	İç denetimler yapılıyor mu?
2.13	BGYS'nin Performansının Değerlendirilmesi	Denetçilerin yeterliliği değerlendiriliyor mu?
2.13	BGYS'nin Performansının Değerlendirilmesi	Üst Yönetim BGYS'yi gözden geçiriyor mu?
2.14	İyileştirme	Uygunsuzluk durumlarında başlatılacak olan aksiyonlar tanımlanmış bir süreç çerçevesinde ilerliyor mu?

TÜBİTAK BİLGEM
Yazılım Teknolojileri Araştırma Enstitüsü

İşçi Blokları Mahallesi Muhsin Yazıcıoğlu Caddesi
No:51/C 06530 Çankaya - ANKARA
T 0312 284 92 22 **F** 0312 286 52 22
E epid.yte@tubitak.gov.tr

www.yte.bilgem.tubitak.gov.tr
www.dijitalakademi.gov.tr