BİLGİSAYAR BİLİMLERİ VE TEKNOLOJİLERİ DERGİSİ
JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGIES
http://dergipark.org.tr/tr/pub/bibted

Derleme Makalesi

ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi Kapsamında Bilgi Güvenliği Risk Yönetimi ve Risk Analizi

Melis BÖKE YAZICIOĞLU[*1]

[1] İskenderun Teknik Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği, Hatay, Türkiye

Anahtar Kelimeler:
Bilgi Güvenliği
Bilgi Güvenliği Yönetim Sistemi
Bilgi Güvenliği Risk Yönetimi
ISO/IEC 27001
ISO/IEC 27005

ÖZ

Siber saldırılardaki artış ile bilgi güvenliği ve Bilgi Güvenliği Yönetim Sistemi (BGYS) büyük önem kazanmıştır. BGYS'yi kurmak, kurumların bilgi varlıklarını belirleyerek, önemine göre risklerini tanımlayıp yönetmesine ve iş sürekliliğini sağlamasına destek olmaktadır. BGYS'nin oluşturulması, uygulanması ve yönetilmesi sürecinde Risk Yönetim sürecini de kapsayan birçok husus bulunmaktadır. Kurumlar, farkındalık eksikliği, maliyet ve süreç yönteminin zor olması sebepleri ile bu süreci devreye almaktan çekinmektedir. Bu makale, ISO/IEC 27001:2022 standardı çerçevesinde bilgi güvenliği risk yönetimi ve analizi süreçlerini ele almakta ve kurumların bu süreçleri etkin bir şekilde nasıl uygulayabilecekleri konusuna ışık tutmaktadır. Makalede, risk analizi için kullanılan çeşitli teknikler ve metodolojiler ele alınmıştır. İnceleme sonucunda, risk yönetim metodolojilerinin değinmiş olduğu temel noktaların ve temelde işletilmesi beklenen süreçlerin aynı ya da benzer olduğu tespit edilmiştir. Risk yönetim süreci, risklerin belirlenmesi, analiz edilmesi, değerlendirilmesi, yönetilmesi ve izlenmesi adımlarından oluşur. Her bir adımın önemi ve nasıl uygulanabileceği detaylı olarak incelenmiş olup uygulama aşamasında karşılaşılabilecek zorluklar ve çözüm önerileri analiz edilerek detaylandırılmıştır. Sürecin daha net ele alınabilmesi amacıyla edinilmiş deneyimler ve literatürde yapılan araştırmalar sentezlenerek örnek senaryolara yer verilmiştir.

Information Security Risk Management and Risk Analysis within the Scope of ISO/IEC 27001:2022 Information Security Management System

Keywords:
Information Security
Information Security Management System
Information Security Risk Management
ISO/IEC 27001
ISO/IEC 27005

ABSTRACT

With the rise in cyber attacks, information security and the Information Security Management System (ISMS) have become crucial. Establishing an ISMS helps organizations identify their information assets, manage risks based on their significance, and ensure business continuity. The process involves various aspects, including Risk Management. Organizations often hesitate to start due to lack of awareness, cost concerns, and perceived complexity. This article explores information security risk management and analysis within the ISO/IEC 27001:2022 standard and provides guidance on effective implementation. It discusses techniques and methodologies for risk analysis. Fundamental points of risk management methodologies and expected processes are found to be similar or identical. The risk management process includes identifying, analyzing, evaluating, managing, and monitoring risks. Each step's importance and implementation are thoroughly examined, including challenges during implementation and proposed solutions. To clarify the process, example scenarios are provided based on research and practical experiences. This approach helps organizations understand and navigate the complexities of establishing and maintaining an effective ISMS.

[*] **Sorumlu Yazar**

[*](bokemelis@gmail.com) ORCID ID 0009-0007-9055-1576

e-ISSN: 2717-8579

Geliş Tarihi: 05/03/2024; Kabul Tarihi: 18/07/2024

1. GİRİŞ

Bilgi, kâğıt veya başka ortamlar üzerine kaydedilmiş, anlaşılabilen ve iletilebilen veriler topluluğudur veya zihinde herhangi bir biçimde resmi veya gayri resmi olarak iletilen, kaydedilen, yayınlanan fikirlerin gerçek ve hayali ürünleridir (Sağsan, 2010).

Bilgi güvenliği, bilginin bir varlık olarak tehdit veya tehlikelerden korunması için doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak, bilginin varlığının her türlü ortam üzerinde istenmeyen kişiler tarafınca elde edilmesini önleme girişimi olarak tanımlanmaktadır "(URL-7)".Bilgi güvenliği, en değerli kaynaklarından biri olan veri ve bilginin gizliliği, mahremiyeti, bütünlüğü ve kullanılabilirliği ile ilgilendiğinden, kuruluşların yönetiminde kilit bir rol oynar (Antunes vd., 2021). Bilgi güvenliğinde bu kavramlardan en az birinin tehlikede olma ihtimali ve gerçekleşmesi durumunda oluşturabileceği etki riski oluşturmaktadır. Gelişen teknoloji beraberinde birçok fayda getirse de bilinen ya da bilinmeyen pek çok tehdidi de beraberinde getirmektedir. Bu tehditlerin yönetilebilmesi ve azaltılabilmesi Risk Yönetim sürecini oluşturmaktadır.

Dünyaca kabul gören ve 2022 yılında güncellenmiş olan ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi Standardı kapsamında da Risk Değerlendirme sürecine önem verilmektedir. Her bir kurumun bu süreci işletmesinin bilginin güvenliğinin sağlanmasında kritik bir nokta olduğu görülmektedir. Risk Yönetim sürecini oluşturmak isteyen kurumların, temelde bunu nasıl uygulamaları ve yapmaları gerektiğini ve bu süreç içerisinde ne gibi metodolojilerin yer aldığını anlaması gerekir. Bu noktada kurumların veya kişilerin toplanmış, incelenmiş bir bilgiye ve benzer çalışmalara ihtiyaçları ortaya çıkmaktadır. Kurumlarda BGYS özelinde ve teknik kapsamda risklerin nasıl yönetilebileceği ile ilgili literatürdeki kaynaklar araştırılıp incelendiğinde, kapsamlı bir çalışma olmadığı, sunulan çalışmaların yeterli olmadığı ve kısa, özet bilgilere yer verildiği tespit edilmiştir.

Bu çalışmada, risk metodolojileri ve standartları araştırılarak, kurumların ya da kişilerin ihtiyaç duyabileceği risk metodolojilerinin, güncellenmiş olan IEC/ISO 27005:2022 Standardının gereklilikleri ile ortak paydada buluşan noktaları ve bunların risk analizi üzerindeki etkileri detaylı olarak incelenecektir. İnceleme ile kurumda risk yönetim sürecinin nasıl planlanabileceğine, yürütülebileceğine ilişkin önemli noktalar, karşılaşılabilecek zorluklar, çözüm önerileri, ISO 27001:2022'de Risk Yöntemindeki ana değişiklikler ve örnek risk değerlendirme tablosu paylaşılacaktır.

2. YÖNTEM

Araştırmada betimleme yöntemi kullanılmıştır. Betimleme Yöntemi, olayların, grupların, kurumların vb. çeşitli alanların ne olduğu ve bu sırada gerçekleşen eylemleri daha iyi anlayabilme, aktarabilme adına aralarındaki ilişkinin açıklandığı bir unsurdur (Kaptan, 1995).

Araştırma soruları aşağıdaki şekilde belirlenmiştir:

- BGYS ile Risk Yönetimi arasındaki ilişki nedir?
- Bilgi Güvenliği Risk Yönetimi nedir?
- Kurumlar için Bilgi Güvenliği Risk Yönetiminin önemi nedir?
- Kurumlar Risk Yönetimi yapmak için hangi metodolojileri kullanabilir?
- Metodolojilere göre kurumda Risk Yönetim süreci nasıl uygulanabilir?
- Risk Yönetim sürecinde hangi zorluklar ile karşılaşılabilir ve bu zorluklar nasıl çözümlenebilir?
- Araştırma kapsamında elde edilen bilgiler doğrultusunda hangi sonuç ve öneriler paylaşılabilir?

3. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNE GENEL BAKIŞ

BGYS, kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır. BGYS'nin temel amacı hassas bilginin korunmasıdır (Marttin ve Pehlivan, 2010). BGYS, kurumun süreçlerini, çalışanları gibi tüm bilgi sistemlerini kapsamakta olup tüm üst yönetim tarafından desteklenmelidir.

Bir bilgi:

- Dijital sistemler üzerinde
- Bir dokümanda
- Depolama cihazlarında
- Bilgisayarlarda veya telefonlarda
- E-postalarda olmak üzere hemen hemen her yerde bulunabilmektedir.

Bilgi güvenliği, kurumlardaki çalışanlar ile hareket edilerek, iş süreçlerinin desteklenmesinde, işin sürekliliğinin güvenli bir şekilde sağlanmasında, kurumun dış veya iç tehditlerden korunmasında önemli bir role sahip olmakla birlikte bunları gerçekleştirirken 3 ana temel kavramı ele almaktadır.

Gizlilik, bilginin yetkisiz kişilerin erişmesini veya eline geçmesini engellemeyi amaçlamaktadır.

Bütünlük, bir bilginin yetkisiz kişiler tarafından değiştirilmesinin, silinmesinin veya yok edilmesinin engellenmesini ve bilginin bütünlüğünün korunması amaçlamaktadır.

Erişilebilirlik, bilginin veya bilgi bulanan bir sistemin yetkili kişiler tarafından ihtiyaç duyulması durumunda her zaman ulaşılabilir durumda olmasını amaçlamaktadır.

Bilgi varlıklarının korunması, taraflarda güven oluşturulabilmesi ve güvenlik kontrollerinin yeterli ve etkili seviyede uygulanmasını sağlamak için tasarlanmıştır. ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi, kurumsal yapıyı, politikaları,

planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içerir "(URL-3)".

ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi'nin kurum için birçok faydası ve avantajı bulunmaktadır. Bu faydalar "(URL-6)":

- Doğru, güvenilir ve geçerli bilgiler sağlamaktadır.
- Riskin minimize edilmesini sağlamaktadır.
- İş sürekliliğini veya kuruluşun faaliyet sürekliliğini sağlamaktadır.
- Bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunmasını sağlamaktadır.
- Yasal zorunlulukların zorunlu kıldığı bazı gerekliliklerin sağlanmasına olanak tanımaktadır.
- Kurumsal saygınlık korunmasını sağlamaktadır.
- Bilgiye erişimin korunmasını sağlamaktadır.

ISO/IEC 27001:2022 kapsamında bir BGYS kurulurken Şekil 1'de yer alan ve "PUKÖ Döngüsü" olarak adlandırılan bir döngü kullanılmaktadır.

Şekil 1. Pukö Döngüsü

Planla: BGYS politikasının, amaçların, hedeflerin, süreçlerin ve prosedürlerin geliştirilmesidir (Marttin ve Pehlivan, 2010).

Uygula: BGYS politikasının, amaçların, hedeflerin, süreçlerin ve prosedürlerin uygulanmasıdır (Marttin ve Pehlivan, 2010).

Kontrol Et: BGYS politikasının, amaçların, hedeflerin, süreçlerin ve prosedürlerin performansının uygulanmasının değerlendirilmesi, ölçülmesi ve yazılı bir şekilde raporlanmasıdır (Marttin ve Pehlivan, 2010).

Önlem Al: Bir önceki adımda yer alan yönetimin gözden geçirme sonuçlarına bağlı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesidir (Marttin ve Pehlivan, 2010).

Döngüde yer alan her bir adım tüm süreçler için uygulanarak BGYS kurulabilmektedir.

4. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNDE RİSK YÖNETİMİ

Risk yönetimi, potansiyel faydalara göre risk analizini, alternatiflerin değerlendirilmesini ve son olarak yönetimin en iyi eylem planı olarak belirlediği yöntemin uygulanmasını gerektirir (Marianne ve Barbara, 1996).

ISO 27001 Standardı ile Risk Yönetiminin yakın bir ilişkisi bulunmaktadır. ISO 27001 Risk Yönetim sürecini BGYS'nin merkezine yerleştirir ve organizasyonların bilgi güvenliği risklerini etkin bir şekilde yönetmelerini sağlar. Ayrıca, organizasyonların BGYS'yi diğer yönetim sistemleriyle bütünleştirmelerini sağlar. Bu, organizasyonların tüm risk yönetimi süreçlerini birleştirerek daha kapsamlı bir yönetim yaklaşımı benimsemelerine yardımcı olur.

Risk Yönetim süreci genel olarak Şekil 2.'de yer alan riskin tanımlanması, riskin analizi, azaltılması, riskin takibi ve riskin gözden düzenli aralıklarla yeniden gözden geçirilmesi gibi farklı süreçlerden oluşur. Risk yönetim süreçleri metodolojilere göre değişkenlik gösterse de uygulanacak adımlar birbirleriyle benzerlik göstermektedir.

Şekil 2. Risk Yönetim Süreci Yaşam Döngüsü

Seçilen metodoloji doğrultusunda her bir süreç uygulanarak risk yönetimi gerçekleştirilmekte ve alınacak aksiyona karar verilmektedir.

4.1. RİSK DEĞERLENDİRME SÜRECİNE GENEL BAKIŞ VE RİSK DEĞERLENDİRME METODOLOJİLERİ

Risk Değerlendirme, temelde gerçekleşmesi muhtemel risklerin tanımlanmasına ve bu risklerin analizine dayanmaktadır. Kurumlar, belirli bir varlığa yönelik hangi tehditlerin bulunduğunu ve bu tehditlerin risk düzeyini belirleyebilmek amacıyla risk değerlendirme sürecini kullanırlar (Peltier, 2005). Risk düzeyini sıfıra indirgemek olumsuz bir etki oluşturabileceğinden, kurumlar kendi risklerini ve uygun risk seviyelerini belirlemeli ve bunlara uygun aksiyon planı oluşturmalıdır. Risklerin değerlendirilmesinde ve analizi sürecinde Risk Yönetim sürecini kapsayan 3 ana unsur bulunmaktadır (Marianne ve Barbara, 1996). Bu unsurlar:

- Risk Değerlendirme kapsamının ve metodolojisinin belirlenmesi
- Verilerin toplanması ve analizi

- Risk Değerlendirme sonuçlarının yorumlanması

4.1.1. Risk Değerlendirme Sürecinde Kapsamın ve Metodolojinin Belirlenmesi

Riski değerlendirmenin ilk adımı, söz konusu olan BGYS sistemlerinin tanımlanması ve bu sistemler için gerçekleştirilecek olan risk değerlendirme metodolojisinin belirlenmesi veya oluşturulmasıdır. Kullanılabilecek birçok risk metodolojisi bulunmaktadır.

4.1.2. Risk Metodolojileri

EBIOS Risk Metodolojisi: EBIOS metodolojisi, Fransız Ulusal Güvenlik Ajansı SGDN (Secrétariat Générale de la Défense Nationale) bünyesinde Fransa Başbakanına bağlı bir hükümet kuruluşu olan DCSSI (Direction Centrale de la Sécurité des Systèmes d'information) tarafından 1995 yılında oluşturulmuştur. Yöntem, 5 adımı içerir (Mohamed vd., 2014).

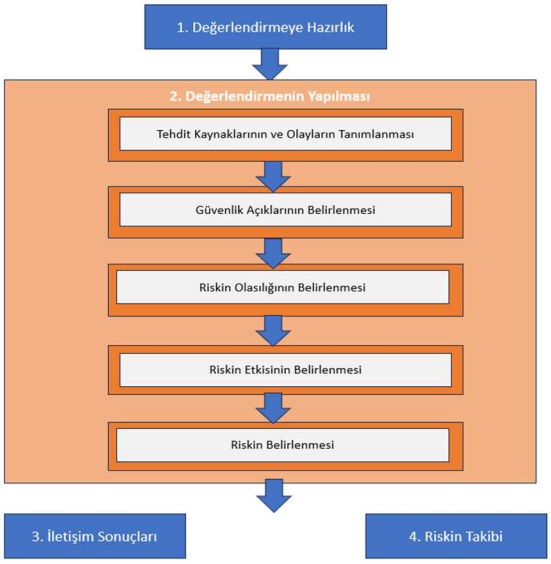
- Bağlam
- Güvenlik ihtiyaçları
- Tehdit analizi
- Güvenlik hedeflerinin belirlenmesi
- Güvenlik gereksinimlerinin belirlenmesi

EBIOS Risk Yönetim Metodolojisinde, risklerin değerlendirilmesi ve analizinde nitel bir yaklaşım benimsenmektedir.

MEHARI Risk Metodolojisi: MEHARI, CLUSIF tarafından geliştirilen ve Risicare (http://www.risicare.fr) şirketi tarafından yönetilen bir yazılım tarafından desteklenen risk analizi ve yöntemidir. İlk olarak 1996 yılında geliştirilen MEHARI, yöneticilere (operasyon yöneticileri, CISO, CIO, risk yöneticisi, denetçi) Bilgi ve BT kaynaklarının güvenliğini yönetme ve ilgili riskleri azaltma çabalarında yardımcı olmayı amaçlamaktadır. MEHARI, ISO/IEC 27001:2022 tarafından tanımlanan BGYS sürecine uygundur. Sürekli iyileştirme döngüsü elde etmek için güvenlik açığı kontrol noktaları listesine ve doğru bir izleme sürecine dayalı güvenlik planları geliştirmesine olanak tanır (Mohamed vd., 2014).

- Risk durumlarına ilişkin bilgileri belirleyin
- Optimum eylem planlarının oluşturulmasıyla sonuçlanan risk analizinin konsolidasyonuna ilişkin kurallar belirleyin
- Önemli riskleri analiz edin
- Güvenlik açıklarını analiz edin
- Riskleri azaltın ve yönetin
- Bilginin güvenliğini izleyin

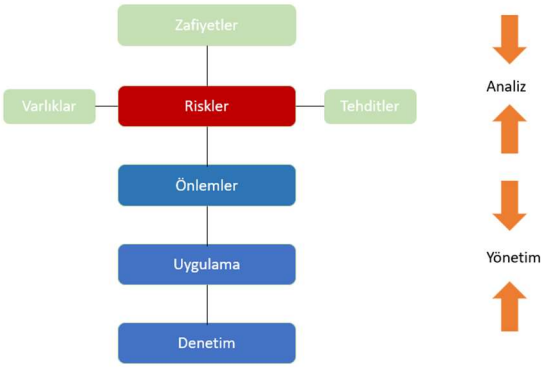
NIST SP 800-30 Risk Metodolojisi: NIST SP 800-30, Ulusal Standartlar ve Teknoloji Enstitüsü tarafından geliştirilen bir standarttır. Bilgi güvenliği risk değerlendirmesi için formüle edilmiş özel bir belge olarak yayınlanmakta ve özellikle BT sistemlerine yöneliktir. NIST SP 800-30'un kurumda nasıl uygulanabileceğini gösteren bir döngü (Şekil 3.) bulunmaktadır.



Şekil 3. NIST SP 800-30

CRAMM Risk Metodolojisi: CRAMM, yazılım tabanlı (Windows tabanlı) bir güvenlik riski değerlendirmesi ve risk yönetimi metodolojisidir. CRAMM, niceliksel bir metodolojiden ziyade niteliksel bir metodolojidir. CRAMM Şekil 4.'te yer alan üç temel aşamaya dayanmaktadır:

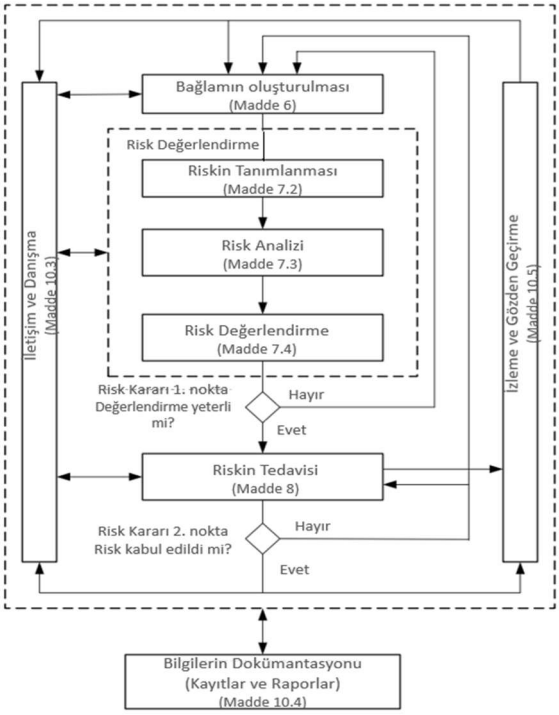
- Bilginin değerinin değerlendirilmesi ve iş sürecini destekleyen varlıkların belirlenmesi
- Hangi tehditlerin sistemi etkileyebileceğinin ve sistemin bu tehditlere karşı ne kadar savunmasız olduğunun belirlenmesi; riskler hakkında bir sonuca varmak
- Bir sonraki adım risk ölçümlerinin türetilmesidir ve bunlar tehdit, güvenlik açığı ve varlık değerinin birleşiminden elde edilir. Risk ölçümleri, oluşturulacak güvenlik gereksinimlerinin risk derecesine uygun olmasını sağlayacak şekilde ölçeklendirilir
- Mevcut kontrol önlemlerinde hangi iyileştirmelerin gerekli olduğu da dahil olmak üzere, risklerle nasıl mücadele edilebileceği belirlenir.



Şekil 4. CRAMM Risk Metodolojisi

ISO/IEC 27005:2022 Bilgi Güvenliği Risk Yönetim Standardı: ISO 27005'in amacı bilgi güvenliği risk yönetimi için yönergeler sağlamaktır. ISO/IEC 27001:2022'de belirtilen genel kavramları desteklemek ve risk yönetimi yaklaşımına dayalı olarak bilgi güvenliğinin etkin bir şekilde uygulanmasına yardımcı olmak için tasarlanmıştır. Risk analizinden risk tedavi planının oluşturulmasına kadar yapılandırılmış, sistematik ve titiz bir süreci belirtmesine rağmen, herhangi bir spesifik risk analizi yöntemini belirtmez. Birçok bilgi güvenliği kontrol hedefini ve genel kabul görmüş güvenlik kontrollerini açıklayan, bilgi güvenliği yönetimine yönelik uygulama kurallarını kapsayan bir standarttır (Mohamed vd., 2014).

ISO/IEC 27005:2022 Standardı kapsamında uygulanan ve Şekil 5'te belirtilen 8 adımdan oluşan bir risk yönetim süreci bulunmaktadır.



Şekil 5. ISO 27005 Bilgi Güvenliği Risk Yönetim Süreci (ISO/IEC 27005:2022 International Standard, 2022)

Süreç adımları:

- Bağlamın oluşturulması
- Riskin tanımlanması
- Riskin analizi
- Risk değerlendirilme
- Riskin tedavisi
- Bilgilerin dokümantasyonu
- İzleme ve gözden geçirme
- İletişim ve danışma

Risk Yönetim sürecinde risklerin değerlendirilmesine ve tedavi sürecindeki değişikliklere bağlı olarak Risk Yönetim süreci "Stratejik" ve "Operasyonel" olarak iki sürece ayrılabilir.

Stratejik Döngü; iş varlıkları, tehditler, hedefler, risk kaynakları, kuruluşun bağlamında yer alan değişiklikler olarak tanımlanmaktadır. Bunlar risk tedavi planının oluşturulmasında veya riskin değerlendirilmesi için girdi niteliğindedir.

Operasyonel Döngü ise, stratejik döngüde yer alanları kapsayan ve yapılan risk değerlendirmenin veya tedavinin gözden geçirilmesi gereken durumları kapsamaktadır.

Stratejik döngü daha uzun zaman bazında veya büyük değişiklikler meydana geldiğinde ve kuruluşun hedeflerine ulaşmaya çalıştığı ortam için uygulanırken, operasyonel döngü ise belirlenen ve değerlendirilen ayrıntılı risklere ve ilgili risk tedavisine bağlı olmanın yanı sıra risk yönetim süreci bağlamı dikkate alınarak yapılan tüm risk değerlendirmelerini içermekte ve daha kısa süreyi kapsayacak şekilde işletilmektedir.

6. RİSK DEĞERLENDİRME VE RİSK ANALİZİ

Risk değerlendirme sürecine başlayacak olan kurumlar kullanacağı risk metodolojisini belirlemiş olmalıdır. Risk metodolojisini belirleyen kurumların, sonraki süreçleri planlaması ve uygulaması gerekmektedir. Bu süreçlerin uygulanması sırasında zorluklar ile karşı karşıya kalınabilmektedir.

6.1. Risk Değerlendirme ve Analiz Sürecinde Karşılaşılabilecek Zorluklar ve Öneriler

Risk değerlendirme analiz sürecinde karşılaşılan zorluklar, genellikle bilgi yetersizliği, kapsam belirsizliği, tahmin hataları, önyargı ve ön kabuller, karmaşıklık, değerlendirme yöntemleri ve araçlarının karmaşıklığı, süreç yönetimi zorlukları gibi faktörlerden kaynaklanır.

- **Bilgi yetersizliği,** doğru risk analizi yapmak için gerekli olan bilgilere eksik erişim sağlanmasına veya belirli bilgilerin eksik olmasına neden olabilir.
- **Kapsam belirsizliği,** analizin doğru bir şekilde yönetilmesini zorlaştırabilir ve hangi varlıkların veya süreçlerin risk analizine dahil edileceği konusunda belirsizlik yaratabilir.

- **Tahmin hataları,** risklerin olasılığının veya etkisinin yanlış tahmin edilmesine yol açabilir ve yanlış kararlar alınmasına neden olabilir.
- **Önyargı ve ön kabuller,** analizin nesnel olmasını engelleyebilir ve doğru sonuçlara ulaşmayı zorlaştırabilir.
- **Karmaşıklık,** büyük ve karmaşık organizasyonlarda risk analizi sürecini yönetmeyi zorlaştırabilir ve analizin doğruluğunu etkileyebilir.
- **Değerlendirme yöntemleri ve araçlarının karmaşıklığı,** sürecin yürütülmesini zorlaştırabilir ve gereksiz karmaşıklığa yol açabilir.
- **Süreç yönetimi zorlukları**, paydaşlar arasında iş birliğini sağlamak ve iletişimi sürdürmek için ek bir engel oluşturabilir.

Bu zorlukların üstesinden gelmek için:

- İyi bir hazırlık ve planlama yapılmalı
- Kapsam net bir şekilde belirlenmeli
- Risk analizi için ihtiyaç duyulan tüm bilgilere erişim sağlanmalı
- Farklı görüş ve deneyimlere önem verilmeli
- Analiz yapılırken objektif olunmalı
- Basit ve uygulanabilir yöntemler tercih edilmeli
- İletişim ve iş birliği sağlanmalı
- Sürekli iyileştirme benimsenmeli

Zorluklar ile karşılaşılmaması adına sürecin başlangıcında yukarıda yer alan önerilerin uygulanması sonraki süreçlerin daha yönetilebilir olmasını sağlayacaktır. Risk metodolojisi ve kapsam net bir şekilde belirlendikten sonra bir sonraki süreçler uygulanmalıdır.

6.1.1. Verilerin Toplanması ve Analizi

Ebios veya ISO 27005 Risk Metodolojileri tercih edilecekse verilerin toplanması ve analiz aşamasından önce kurumların bağlamını oluşturması beklenmektedir. Bağlam, faaliyetleri etkileyen ya da faaliyetler sonucunda etkilenen yönetim sistemini iç ve dış hususlar olmak üzere belirlenmesini sağlayan bir kavramdır. ISO 27005 Standardına göre kuruluşun bağlamı tanımlanırken ya da belirlenirken, kurum bağlamını aşağıda yer alan gereksinimler kapsamında oluşturmalıdır.

- Organizasyonel hususlar
- İlgili tarafların temel gereksinimlerinin belirlenmesi
- Risk değerlendirmenin uygulanması
- Bilgi güvenliği risk kriterlerinin oluşturulması ve sürdürülmesi
- Uygun bir yöntemin seçilmesi

Diğer metodolojilerden biri ile devam edilmesi durumunda ise, verilerin toplanabilmesi için bakılabilecek çok sayıda alan bulunmaktadır. Riskin birçok bileşeni bulunmakta ve bir bilgi birçok alanda bulunabilmektedir. Verileri toplamak ve bunların analizini yapmak riskin tespit edilmesini ve tanımlanmasına destek olmaktadır.

6.1.2. Varlık Envanteri ve Varlıkların Değerlendirilmesi

Varlıklar; bilgi, yazılım, donanım, süreç, insan gibi içerisinde bilginin bulunduğu alanlardır. BGYS kapsamında bir kurum varlıklarını belirlemiş ise bu varlıklar üzerinden risklerin belirlenmesi için veriler toplayabilmekte ve analiz ederek riskini belirleyebilmektedir. Eğer kurum varlıklarını henüz belirlememiş ve bir varlık envanterine sahip değilse, kurumda yer alan departmanlar ile görüşmeler yapılarak varlık envanterleri çıkarılabilir. Varlık envanteri oluşturulurken aşağıda yer alan noktalar belirlenmelidir:

- Varlıkların gizlilik, bütünlük ve erişilebilirlik dereceleri
- Varlığın sahibi
- Varlıkların türü

6.1.3. Tehditlerin Tanımlanması

Tehdit, sisteme zarar verme potansiyeli olan varlıklar veya olaylardır. Tehditler, 3 kategoride değerlendirilmektedir.

Doğal Tehditler: Sel, deprem, kasırga, hortum gibi doğal afetler gibi olaylardır.

İnsan Kaynaklı Tehditler: İnsan kaynaklı tehditler kasıtlı ve kasıtsız olarak değerlendirilmektedir. Kasıtsız eylemler, hatalar veya ihmaller sebebiyle, kasıtlı eylemler ise insanlar tarafından bilinçli olarak yapılan dolandırma, kötü amaçlı yazılım gibi büyük kayba neden olabilecek tehditlerdir.

Çevresel Tehditler: Uzun süreli elektrik kesintileri, kirlilik, kimyasal atıklar gibi tehditlerdir.

Tehditler, ortaya çıkma olasılıklarını ve varlıklara zarar verme potansiyellerini belirlemek için tanımlanmalı ve analiz edilmelidir (Marianne ve Barbara, 1996).

ISO 27005:2022 kapsamında riskler tanımlanırken Olaya Dayalı Yaklaşım ve Varlığa Dayalı Yaklaşım olmak üzere 2 farklı yaklaşım türü uygulanmaktadır.

Olaya Dayalı Yaklaşım: Risk kaynaklarını, riskleri ve bu risklerin hedefe ulaşmayı ne ölçüde etkilediğine bağlı olarak stratejik senaryolar belirlenmektedir. Bu yaklaşımda olaylar ve sonuçlar genellikle üst yönetimin endişelerinin, risk sahiplerinin ve kuruluşun bağlamını belirlerken ortaya çıkan gereksinimler ile belirlenebilmektedir.

Varlığa Dayalı Yaklaşım: Varlıklar, tehditler ve güvenlik açıklarına bağlı olarak ayrıntılı bir operasyonel senaryolar belirlenmektedir. Bu yaklaşım, varlığa özgü tehditleri ve güvenlik açıklarını belirleyebilir ve kurumun bazı riskleri ayrıntılı şekilde incelemesine imkân

tanıyabilmektedir (ISO/IEC 27005:2022 International Standard, 2022).

Bu tehditlere ek olarak, kurumlar sektörü tanımalı ve sektörel tehditlerini ve var ise özel tehditlerini ve zafiyetlerini de belirlemelidir.

6.1.4. Güvenlik Açığı Analizi

Güvenlik açığı; güvenlik prosedürleri, teknik kontroller, fiziksel kontroller veya bir tehdit tarafından istismar edilebilecek diğer kontrollerdeki (veya bunların bulunmaması) bir durum veya zayıflıktır (Marianne ve Barbara, 1996).
Bu zayıflıklar sonucunda varlıkların ve bilgi güvenliğinin zarar görme ihtimali bulunmaktadır. Bu potansiyel açıklar belirlenmeli ve analiz edilmelidir. Bu noktada sızma testleri, tarama araçları, iç ve dış denetimlerde tespit edilen bulgular güvenlik açığı hususunda hem bir referans hem de risk için girdi oluşturmaktadır. Güvenlik açığı olarak tespit edilen zafiyet ya da bulgular risk olarak tanımlanabilmektedir.

6.1.5. Olasılıkların Belirlenmesi ve Değerlendirilmesi

Olasılık, bir tehdidin gerçekleşme sıklığının ya da ihtimalinin tahminidir. Kurumların kullandığı metodolojiye göre genellikle 3 ya da 5 dereceye sahiptir. 3 (Tablo 2) ve 5 (Tablo 1) dereceye ilişkin çizelgeler aşağıda detaylandırılmıştır.

Tablo 1. 5 Dereceli Olasılık Skalası

Olasılık Düzeyi	Açıklama
5- Neredeyse Kesin	Neredeyse her zaman gerçekleşebilir. Mevcut tedbirlerin yeterli olmaması nedeniyle sıklıkla tekrarlanabilir.
4- Muhtemel	Sıklıkla olabilir. Mevcut tedbirlerin yeterli olmaması nedeniyle yılda birkaç kez tekrarlanabilir.
3- Orta	Bazen olabilir. Mevcut tedbirlerin yeterli olmaması nedeniyle yılda bir kez tekrarlanabilir.
2- Muhtemel değil	Meydana gelmesi çok mümkün olmasa bile olabilir. Mevcut kontroller ve tedbirler kısmen yeterli seviyededir.
1- Nadir	Meydana gelmesi oldukça nadir. Mevcut kontroller yeterli seviyededir. Bu sayede tehdidin oluşması önlenebilmektedir.

Tablo 2. 3 Dereceli Olasılık Skalası

Düzey	Açıklama
3- Yüksek	Sıklıkla meydana gelebilir
2 -Orta	Ara sıra meydana gelmesi muhtemel
1- Düşük	Çok mümkün olmasa da nadiren gerçekleşebilir.

6.1.6. Tehditlere Göre Etkinin Belirlenmesi ve Değerlendirilmesi

Bir tehdidin meydana gelme olasılığı değerlendirildikten sonra, tehdidin kurum üzerinde oluşturabileceği etkisi belirlenmektedir. Etki değerinin belirlenmesinde de olasılıkta olduğu gibi genellikle 3 (Çizelge 4) ve 5 (Çizelge 3) dereceye sahip skala kullanılmaktadır. Riskin etki değeri belirlenirken kurumun genel misyonu, değer ve hedeflerinin nasıl etkileneceğine ek olarak Bilgi Güvenliğinin 3 temel prensibi olarak bilinen Gizlilik, Bütünlük ve Erişilebilirlik üzerindeki etkileri de göz önünde bulundurulmalıdır. Kurum, riskin gerçekleşmesi durumunda itibar kaybı, finansal kayıp, operasyonel süreçlerde aksama gibi zararlar görebilir.

Tablo 3. 5 Dereceli Etki Skalası

Düzey	Açıklama
5- Kritik	Çok ciddi kayıplara sebep olabilir.
4- Yüksek	Ciddi kayıplara olabilir.
3- Orta	Önemli kayıplara sebep olabilir.
2- Düşük	Kurum için minör kayıplara sebep olabilir.
1- Çok Düşük	Kurum için neredeyse önemsiz kayıplardır.

Tablo 4. 3 Dereceli Etki Skalası

Düzey	Açıklama
3-Yüksek/ Kritik	Çok ciddi veya ciddi kayıplara sebep olabilir.
2 – Orta	Önemli kayıplara sebep olabilir.
1- Düşük	Kurum için minör kayıplara sebep olabilir.

6.2. Olasılık ve Etki Analizine Göre Risklerin Değerlendirilmesi

Olasılık ve etki analizi kurumların riski doğru şekilde değerlendirmesini, ölçülebilmesini ve bu

değerlendirme neticesinde kontrollerin ve önlemlerin tanımlanarak etkin bir şekilde uygulanmasına destek sağlamaktadır. Riskler belirlendikten sonra ve sonuçların hem olasılık hem de etki değerleri belirlendikten sonra kurumlar risklerin kabul edilip edilmeyeceğini belirlemek için risk kabul kriterlerini uygulamalıdır (ISO/IEC 27005:2022 International Standard, 2022).
Riskin değeri,

$$Risk\ (R) = OxE \qquad (1)$$

Formülü ile hesaplanır. Hesaplamada yer alan O değeri Olasılık (Likelihood), E değeri ise Etki (Impact) olarak değerlendirilmektedir.

Tanımlanan risk için uygulanan mevcut bir kontrol var ise, kontrol metni içerisinde kontrolün ne olduğu ve nasıl çalıştığının detaylandırılması riskin yönetiminin kolaylaşmasında önemli bir rol oynamaktadır. Detaylandırma ISO 27005'te belirtilen bilgilerden yararlanılarak yapılabilir.

- Belgelenmiş bir kontrol olup olmadığı
- Kontrolün sahibinin kim veya hangi departman olduğu
- Nasıl izlendiği
- Nasıl kanıtlanabileceği
- İstisnalar

Bir risk, olasılık ve etkisine göre değerlendirilirken sanki herhangi bir kontrol uygulanmıyormuş gibi değerlendirilmelidir. Bu değerlendirme, doğal risk olarak tanımlanan riskin gerçek değerini göstermektedir.

Mevcutta uygulanan kontroller risk değerlendirme aşamasında yapılan skorlamaya dahil edilmemelidir. Bunun sebebi (ISO/IEC 27005:2022 International Standard, 2022):

- Bir veya daha fazla bilgi güvenliği riskini yönetmek için gerekli bir kontrol olmayabilir.
- BGYS tarafından yönetilmek için yeterince etkili olmayan bir kontrol olabilir.
- Halihazırda bilgi güvenliği ile ilgili olmayan başka bir konuda uygulanıyor olabilir.
- Bilgi Güvenliği için uygun olmayabilir.

Bu tespit yapıldıktan sonra mevcutta uygulanan kontroller var ise bu kontroller ile yeniden risk değerlendirme yapılır ve riskin mevcut skoru belirlenir. Uygulanması gereken ek kontrol veya önlemlerin gerekliliği tespit edilmelidir.

ISO 27005:2022 Standardı kapsamında uygulanan kontroller Önleyici, Tespit Edici ve Düzeltici olmak üzere 3 sınıfa ayrılmaktadır.

Önleyici Kontrol, bir veya daha fazla sonucun ortaya çıkmasına yol açabilecek bir bilgi güvenliği olayının meydana gelmesini engellemeyi amaçlamaktadır (ISO/IEC 27005:2022 International Standard, 2022).

Tespit Edici Kontrol, bir bilgi güvenliği olayının meydana geldiğini tespit etmeyi amaçlayan bir kontroldür (ISO/IEC 27005:2022 International Standard, 2022).

Düzeltici Kontrol, bir bilgi güvenliği olayının sonuçlarını sınırlamayı amaçlayan kontroldür (ISO/IEC 27005:2022 International Standard, 2022).

- Tespit edici kontroller, önleyici kontrollerin başarısız olması durumunda riski azaltmalıdır.
- Düzeltici kontroller, eğer tespit edici kontrollerin başarısız olması durumunda riski azaltmalıdır.
- Önleyici kontroller ise, düzeltici kontrollerin kullanılma olasılığını azaltmalıdır.

Riskin değerlendirilmesinde genellikle 3x3 (Şekil 6) veya 5x5'lik (Şekil 7) risk matrisleri kullanılmaktadır. Bu matrisler her ne kadar yaygın kullanılıyor olsa da kurumsal kendi risk matrislerini de belirleyebilmektedir.

OLASILIK \ ETKİ	YÜKSEK	ORTA	DÜŞÜK
YÜKSEK	YÜKSEK	YÜKSEK	ORTA
ORTA	YÜKSEK	ORTA	DÜŞÜK
DÜŞÜK	ORTA	DÜŞÜK	DÜŞÜK

Şekil 6. 3x3 Risk Değerlendirme Matrisi

OLASILIK x ETKİ			Çok Yüksek	Yüksek	Orta	Düşük	Çok Düşük
			5	4	3	2	1
OLASILIK	Çok Yüksek	5	25	20	15	10	5
	Yüksek	4	20	16	12	8	4
	Orta	3	15	12	9	6	3
	Düşük	2	10	8	6	4	2
	Çok Düşük	1	5	4	3	2	1

Şekil 7. 5x5 Risk Değerlendirme Matris ("URL-4")

Peltier 'in Bilgi Güvenliği Risk Analiz kitabında yer alan "Aksiyon Gereklilik Matrisi" risklerin olasılık ve etkisine göre aksiyon gerekliliği olup olmadığının tespitini desteklemek amacıyla kullanılmaktadır.

OLASILIK \ ETKİ	YÜKSEK	ORTA	DÜŞÜK
YÜKSEK	A	B	C
ORTA	B	B	C
DÜŞÜK	C	C	D

Şekil 8. Aksiyon Gereklilik Matrisi(Peltier, 2005)

Şekil 8'de yer alan Aksiyon Gereklilik Matrisi 'ne göre A, B, C ve D değerlerinin açılımları:

A – Mutlaka düzeltici faaliyet uygulanmalıdır.
B – Düzeltici faaliyet uygulanmalıdır.
C – Takip edilmeli ve izlenmelidir.
D – Şu anda herhangi bir aksiyon alınmasına gerek bulunmamaktadır.

6.3. Risk Değerlendirme Sonuçlarının Yorumlanması

Risk değerlendirme, kuruluş için gerçekten neyin önemli olduğunu yansıtan anlamlı bir çıktı üretmelidir. Risk değerlendirme birbiriyle ilişkili iki işlev olan riskin kabulü ve uygun maliyetli kontrollerin seçimini desteklemek için kullanılır (Marianne ve Barbara, 1996). Riskin değerlendirme sonuçları, risk skoruna (R) bağlı olarak mevcut kontroller, aksiyon planları, mevcut kontrollerin efektiflik derecesine göre yorumlanmalı ve riskin kabul edilebilir seviyede olması sağlanmalıdır. Kabul edilebilir seviye, kurum tarafından belirlenmiş olan ve kurumun kabul edebileceği seviyeye indirilmiş risk olarak tanımlanmaktadır. ISO 27001:2022 Standardını uygulayan her kurum ya da kuruluşta, üst yönetim tarafından karar verilmiş bir kabul edilebilir risk seviyesi bulunmaktadır (Durankaya vd., 2018). Kabul edilebilir seviye belirlenirken kurum tarafından belirlenmiş olan risk iştahı göz önünde bulundurulmalıdır.

Risk iştahı, üst yönetim tarafından belirlenen ve kurumun kabul edebileceği ya da tahammül edebileceği en yüksek risk seviyesidir. Aynı zamanda bu düzeyin üzerinde kalan risklerin onaylanamayacağını ve bu konuda önlem almanın gerekli olduğunu göstermektedir ("URL-2)".

Risk değerlendirme adımı tamamlandıktan sonra riskin ne yapılacağına karar verilmesi beklenmektedir. Bu karar sonucunda aşağıda yer alan 4 yöntemden biri uygulanmaktadır.

- Risk Kabulü
- Riskin Azaltılması
- Riskten Kaçınma
- Riskin Transferi

6.3.1. Riskin Kabulü

Riskin kabulü, kurum tarafından güvenlik riskinin varlığının kabul edilmesini fakat ilgili risk için belirli gerekçeler sebebi ile herhangi bir iyileştirici aksiyon alınmayacağını ifade etmektedir. Risk iştahının üzerinde kalan fakat önlem ya da aksiyon alınması mümkün olmayan durumlarda risk kabulü yapmak uygulanabilecek yöntemlerden biridir. Bir kurumun risk kabul kriterleri, risk yöntem sürecinde genel bir yaklaşım olarak tanımlanır ve bilgi güvenliği politikası içerisinde yer alır. Sadece risk kabulü yapmak ve herhangi bir iyileştirici aksiyon almamak bazı durumlarda etkisiz olabilmekte ve potansiyel sonuçlar doğurabilmektedir.

Bir kuruluşun riskleri etkin bir şekilde azaltmadan kabul etmesi, zaman içinde kalan risklerin yüksek oranda birikmesine neden olabilir ve bu da güvenlik ihlalleri ve veri ihlalleri olasılığını artırabilir ("URL-1").

Risk kabul kararı, risklerin kabul edilebilir olduğu durumlarda ya da azaltma maliyetinin riskin potansiyel etkisinden daha ağır bastığı durumlarda verilebilir.

6.3.2. Riskten Kaçınma

Riski tespit edilen bir varlığın kullanımından vazgeçmek riskten kaçınma olarak tanımlanmaktadır. Riskten kaçınma, güvenlik risklerini azaltmak için cazip bir yöntem gibi görünse de bazı dezavantajları bulunmaktadır.

- Daha güvenli bir teknolojiye geçiş gibi çeşitli ve daha yüksek maliyet gerektiren alternatifler doğurabilir.
- Güvenlik ihtiyaçlarını tam olarak karşılayabilecek güvenilir bir tedarikçi bulma konusunda zorluklarla karşılaşabilir. Bu durum, riskten kaçınma stratejilerinin uygulanmasında gecikmelere veya aksaklıklara yol açarak kurumu potansiyel tehditlere karşı savunmasız bırakabilir ("URL-1").
- Kurumun operasyonları üzerinde, işlerin aksamasına neden olabileceğinden olumsuz potansiyel etkileri olabilir.

Riskten kaçınmak her zaman uygulanabilir ve sürdürülebilir olamayabileceğinden uzun vadeli bir çözüm olarak kullanılması önerilmemektedir. Teknolojinin gelişmesiyle birlikte çok sayıda yeni güvenlik açıkları ve tehditleri de ortaya çıkmaktadır. Bu nedenle sadece riskten kaçınma stratejisini kullanmak uzun vadede olası tehditlere karşı kurum için tam bir koruma sağlama noktasında yetersiz kalabilmektedir ("URL-1").

6.3.3. Riskin Transferi

Riskin transferi, potansiyel risklerin sorumluluğunun ya da yükünün üçüncü bir tarafa aktarılmasını içeren bir yöntemdir. Riskin transferi, hizmet sağlayıcı veya harici satıcılar ile yapılan sözleşmeler yolu ile gerçekleştirilebilir. Kurumlar riski transfer ederek, olası bir güvenlik ihlalinden doğacak olan maddi veya repütasyonel kayıpları indirgeyebilmekte ve aynı zamanda bu sayede hizmet satın alarak maliyeti de azaltabilmektedir.
Riskin transferinin getirmiş olduğu bazı dezavantajlar bulunmaktadır. Bu dezavantajlardan bir tanesi tüm risklerin aktarılamaması veya eksik aktarılmasıdır. Ayrıca, maliyet ve performans etkileri de dahil olmak üzere güvenlik risklerinin sonuçlarının aktarılması her zaman mümkün veya etkili olmayabilir ("URL-1").

Tablo 5. Risk Değerlendirme Rapor Örneği

Risk ID	**Tespit Yılı**	**Riskin Tanımı**	**Riskin Sahibi**	**Riskin Tipi**	**Riskin Gizliliğe Etkisi**	**Riskin Bütünlüğe Etkisi**	**Riskin Erişilebilirliğe Etkisi**	**Riskin Gerçekleşme Olasılığı**	**Riskin Etkisi**	**Doğal Risk Seviyesi**	**Risk Değerlendirme Sonucu**	**Mevcut Aksiyon(lar)**	**Aksiyon Efektiflik Derecesi**	**Mevcut Kontrol Sonrası Riskin Değeri**	**Planlanan Aksiyon(lar)**	**Aksiyon Sonrası Riskin Gerçekleşme Olasılığı**	**Etkisi**	**Riskin Yeni Değeri**	**Riskin Durumu**
001	2024	Riskin tanımı	Riskin Sahibi	İtibari (Repütasyonel), Finansal, Bilgi Kaybı Riski	Düşük, Orta Yüksek	Düşük, Orta, Yüksek	Düşük, Orta, Yüksek	Düşük, Orta, Yüksek	Düşük, Orta, Yüksek	Düşük, Orta, Yüksek	Riskin Azaltılması, Kabulü vb.		Efektif, Az efektif, Efektif değil	Düşük, Orta, Yüksek		Düşük, Orta, Yüksek	Düşük, Orta, Yüksek	Düşük, Orta, Yüksek	Açık, Kapalı

6.4. Riskin İyileştirilmesi ve İyileştirme Planı

6.4.1. Riskin Azaltılması

Risk azaltma, riski yönetim tarafından kabul edilebilir bir düzeye indirmek için güvenlik kontrollerinin seçilmesini ve uygulanmasını içerir. Risk azaltma sürecinde aşağıda yer alan kontroller ve aksiyonlar uygulanabilmektedir.

Koruma sağlayacak kontrollerin belirlenmesi: Uygun kontrolleri seçerken aşağıdakiler dikkate alınmalıdır (Marianne ve Barbara, 1996).

- Kurumsal politika, mevzuat veya regülasyonlar
- Güvenlik, güvenilirlik ve kalite gereksinimleri
- Sistem performans gereksinimleri
- Güncellik, doğruluk ve bütünlük gereklilikleri
- Güvenlik önlemlerinin yaşam döngüsü maliyetleri
- Teknik gereksinimler
- Kültürel kısıtlamalar

Risk tedavi planı oluşturulurken dikkat edilmesi gereken bazı hususlar bulunmaktadır. Bu hususlar (ISO/IEC 27005:2022 International Standard, 2022):

- Risk düzeyi ve iyileştirmenin aciliyeti ile ilgili öncelikler
- Farklı kontrol türlerinin ve bu kontrollerin birleşiminin uygun olup olmadığını,
- Kontrolün uygulamaya konduğu an ile tamamen etkili ve çalışır duruma geldiği an arasında bir gecikme olup olmadığı.

Artık riskin kabul edilmesi: Riskin azaltılmasına yönelik gerekli aksiyonlar alındıktan sonra geriye kalan risk "Artık Risk" olarak adlandırılmaktadır. Artık riskler, kalan olasılık ve etkilerine göre yeniden değerlendirilmelidir. Yönetimin veya ekiplerin, kalan risklerin türünü ve ciddiyetini göz önünde bulundurarak, BT sisteminin işleyişinin kabul edilebilir olup olmadığına karar vermesi gerekir (Marianne ve Barbara, 1996). Karar doğrultusunda gerekiyorsa yeni bir aksiyon planı oluşturulmalıdır.

6.5. Riskin Dokümante Edilmesi

Tespit edilen ve değerlendirilen tüm risklerin dokümante edilmesi risk yönetim sürecinde kritik bir öneme sahiptir. Tespit edilen risklerin sayısı artmaya başladıkça, risklerin takibi ve hatırlanması güçleşmeye başlamaktadır. Bu nedenle risklerin dokümantasyonu bu noktada ve riskin detaylarını inceleme ya da yeniden hatırlama konusunda kaynak sağlayacaktır. Bir riski dokümante ederken aşağıda yer alan başlıklar veya Tablo 5'te yer alan örnek rapor taslağı kullanılabilir.

- Riskin tanımı/detayı
- Riskin sahibi
- Riskin kritiklik derecesi
- Alınmış veya alınması gereken aksiyon detayları

6.6. Riskin Takibi ve Gözden Geçirilmesi

Risk takibi ve gözden geçirilmesi Risk Yönetim Süreç Döngüsünün son halkasıdır. Bu bölümde risk değerlendirme süreci her ne kadar sona ermiş gibi görünse de aslında hala yaşayan bir süreç bulunmaktadır. İlgili risk için gerekli kontroller sağlanmış ve etkin önemler alınmış olsa bile risk

unsuru tamamen ortadan kalkmayabilir. Bazı riskler gerekli önlemler etkin bir şekilde alındıktan sonra kapanabilirken bazı riskler her zaman açık kalabilmektedir. Açık kalacak olan bu riskler kabul edilebilir seviyede ve her zaman gerçekleşme ihtimali devam eden risklerdir. Bu risklere:

- Deprem, yangın gibi doğal afet riskleri
- İnsan tarafından oluşabilecek riskler örnek verilebilir.

7. RİSK DEĞERLENDİRME VE ANALİZİ UYGULAMA ÖRNEKLERİ

Bir yazılım şirketinin risklerinin değerlendirme aşamalarının aşağıdaki gibi olduğu bir senaryo incelenmektedir.

Hazırlık ve Planlama Aşaması:

Bilgi güvenliği risklerini belirlemek amacıyla, uzmanlık alanları ve deneyimleri dikkate alınarak, bilgi güvenliği uzmanları, sistem yöneticileri ve ilgili departman temsilcilerinden oluşan bir risk yönetim ekibi kuruldu. Ekip, proje planını hazırlayarak sürecin adımlarını belirleyecektir. Proje planı, risk analiz sürecinin başlangıcından sonuna kadar olan zaman çizelgesini ve ekip üyelerinin sorumluluklarını belirtmektedir. Zaman çizelgesi içerisinde her adım için belirlenen süreler ve süre sonunda gerçekleştirilmesi gereken faaliyetler belirlenmelidir.

Risklerin Tanımlanma Aşaması:

Şirketin varlık envanteri oluşturuldu ve kritik bilgi varlıkları belirlendi. Varlıklar yazılım kodları, müşteri veri tabanları, proje belgeleri gibi kritik bilgi varlıklarını içermektedir. Bu varlıkların yanı sıra, şirketin sahip olduğu diğer önemli bilgi kaynakları (patent başvuruları vb.) da belirlenerek envantere eklenmiştir.

Potansiyel tehditler göz önüne alınarak, risk kaynakları belirlendi ve riskler dokümante edildi. Risklerin kataloglanması sürecinde, her bir tehdidin potansiyel etkisi ve olasılığı detaylı bir şekilde değerlendirildi. Örneğin, yazılım kodlarının yetkisiz erişime açık olması durumunda şirketin itibarı ve müşteri güveni ciddi şekilde zarar görebilirken, müşteri veri tabanının sızdırılması durumunda ise veri ihlali ve yasal yaptırımlar söz konusu olabilir. Bu adımla birlikte riskler kapsamlı şekilde değerlendirilmiştir.

Risklerin Analiz Edilme Aşaması:

Bu aşamada belirlenen risklerin olasılığı ve etkisi dikkate alınarak detaylı bir değerlendirme yapılmıştır. Her riskin potansiyel etkisi ve gerçekleşme olasılığı titizlikle incelenerek belirlenmiştir. Önceliklendirme yapılırken, risklerin kritiklik düzeyi ve etkileri göz önünde bulunduruldu. Özellikle, şirketin faaliyetleri üzerindeki potansiyel etkileri ve olası zararları değerlendirilerek risklerin önem sırası belirlendi. Örneğin, yazılım kodlarının sızdırılması gibi yüksek etkili ve yüksek olasılıklı riskler öncelikli olarak ele alındı. Bu tür bir olayın gerçekleşmesi durumunda, şirketin itibarı ciddi şekilde zarar görebilir, müşteri güveni sarsılabilir ve yasal yaptırımlarla karşılaşabilir. Bu nedenle, bu tür risklerin etkilerini azaltmak için öncelikli olarak çözüm stratejileri belirlendi ve uygulanması için gerekli kaynaklar tahsis edildi.

Diğer yandan, düşük etkili veya düşük olasılıklı riskler daha düşük öncelikle ele alındı. Bu tür riskler, şirketin operasyonları üzerindeki etkileri daha sınırlı olduğu için, daha az acil bir şekilde çözülmesi gereken riskler olarak değerlendirildi. Ancak, bu risklerin de göz ardı edilmemesi ve uygun önlemler alınarak yönetilmesi önemlidir,

Risk Değerlendirme Aşaması:

Riskleri değerlendirme aşamasında, belirlenen risklerin kabul edilebilirlik düzeyi belirlendi. Bu, risklerin şirketin tolerans seviyesine uygun olup olmadığının değerlendirilmesini içeriyordu. Kabul edilebilirlik düzeyi aşılan riskler için risk azaltma stratejileri geliştirildi ve uygulanması için gerekli önlemler alındı.

Örneğin, yazılım kod güvenliğinin artırılması, veri tabanı erişim kontrollerinin sıkılaştırılması gibi çeşitli önlemler bu stratejilere örnek olarak belirlendi. Yazılım kod güvenliğinin artırılması için, kod inceleme süreçleri güçlendirildi, güvenlik açıklarını tespit etmek için otomatik test araçları kullanıldı ve geliştiricilere güvenli kodlama eğitimleri verildi. Ayrıca, veri tabanı erişim kontrolleri sıkılaştırılarak, yetkisiz erişim girişimlerinin önlenmesi amaçlandı ve bu yönde teknik ve politika bazlı önlemler alındı.

Risklerin yönetilmesi için gereken kaynaklar ve bütçe belirlenirken, risk azaltma stratejilerinin uygulanması için gereken kaynakların ve maliyetlerin hesaplanması yapıldı. Bu, güvenlik yazılımlarının satın alınması, güvenlik eğitimlerinin düzenlenmesi gibi kaynak ve bütçe gereksinimlerini içeriyordu. Belirlenen kaynak ve bütçe gereksinimleri, risk azaltma stratejilerinin etkin bir şekilde uygulanmasını ve risklerin yönetilmesini sağlamak amacıyla kullanıldı. Bu sayede, şirketin bilgi güvenliğini artırmak için gerekli kaynakların ve bütçenin sağlanması ve yönetilmesi sağlandı.

Risklerin Yönetilme Aşaması:

Kabul edilebilirlik düzeyini aşan risklerin kontrol ve koruma önlemleri titizlikle uygulanarak, risklerin azaltılması ve etkilerinin minimize edilmesi sağlandı. Bu süreç, şirketin bilgi varlıklarını korumak ve olası güvenlik açıklarını kapatmak için kritik öneme sahipti.

Örneğin, yazılım kod güvenliğinin artırılması için otomatik test araçlarının kullanılması gibi önlemler alındı. Bu sayede, yazılım geliştirme sürecinde olası güvenlik açıkları daha erken tespit edilebilir hale geldi ve hızla çözüme kavuşturulabildi. Ayrıca, veri tabanı erişim yetkilerinin revize edilmesi gibi kontroller de

uygulandı. Bu sayede, yetkisiz erişim girişimlerini önlemek ve veri güvenliğini sağlamak amaçlandı.

Her bir kontrol ve koruma önlemi, riskin özelliğine ve potansiyel etkisine uygun olarak belirlendi ve sistematik bir şekilde hayata geçirildi. Bu önlemler sayesinde, şirketin bilgi güvenliği riskleri etkin bir şekilde yönetildi ve olası güvenlik tehditlerine karşı daha güçlü bir savunma mekanizması oluşturuldu.

Risklerin İzlenmesi ve Gözden Geçirilme Aşaması:

Uygulanan önlemlerin etkinliği düzenli aralıklarla izlendi ve değerlendirildi. Bu süreçte, değişen tehditler ve organizasyonel değişiklikler göz önünde bulunduruldu ve risk analizi sürekli olarak gözden geçirildi. Bu sayede, güvenlik önlemlerinin güncel kalması ve şirketin bilgi güvenliğinin sürekli olarak sağlanması amaçlandı.

Bu izleme ve değerlendirme süreci, aylık olarak düzenlenen toplantılar ve güvenlik raporlarının incelenmesi yoluyla gerçekleştirildi. Bu toplantılarda, risklerin güncel durumu değerlendirilerek, yeni tehditler ve güvenlik zafiyetleri hakkında bilgi paylaşımı yapıldı. Ayrıca, mevcut güvenlik önlemlerinin etkinliği tartışıldı ve alınması gereken ek önlemler belirlendi.

Bu süreç, şirketin bilgi güvenliğini sürekli olarak güçlendirmek ve olası risklere karşı hazırlıklı olmak için kritik bir rol oynadı. Değerlendirme sonuçlarına dayanarak, mevcut önlemlerin etkinliği artırıldı ve yeni güvenlik stratejileri belirlendi. Bu sayede, şirketin bilgi varlıklarını koruma kapasitesi sürekli olarak iyileştirildi ve güncel tehditlere karşı daha etkili bir şekilde savunma sağlandı.

Sonuç olarak, yazılım şirketi bilgi güvenliği risk yönetimi sürecinde başarılı bir ilerleme kaydederek kapsamlı bir varlık ve risk tanımlaması yapmış ve önemli tehditleri belirlemiştir. Kabul edilebilirlik düzeyini aşan riskler için etkili kontrol ve koruma önlemleri uygulanmıştır. Süreç sürekli izlenmiş ve değerlendirilmiş, böylece güvenlik önlemleri sürekli olarak güncel tutulmuştur. Bu sürecin şirketin bilgi güvenliğini güçlendirdiği ve sürdürülebilir bir güvenlik çerçevesi oluşturduğu belirlenmiştir.

8. SONUÇ ve ÖNERİLER

ISO 27001 Standardı çerçevesinde bilgi güvenliği risk yönetimi ve analizi süreçleri detaylı olarak incelenmiş ve bu süreçler kapsamında en sık kullanılan risk metodolojileri ele alınarak kurumların bu süreçleri etkin bir şekilde uygulayabilmesi noktasına ışık tutulmaktadır. Ekiplerin risk yönetimi konusunda sade ve yalın bir bilgiye ulaşabilmesi sağlanmakla birlikte, risk yönetimi konusunda ihtiyaç duyabileceği birçok konu ve soru detaylı olarak incelenmiştir. Bu inceleme akademik bir makale olmasının yanı sıra edinilmiş deneyimlerin ve uygulamaların da süzgeçten geçirilerek paylaşılmasını sağlamaktadır.

Teknolojinin son derece hızlı bir şekilde gelişmesi ile ortaya çıkabilecek pek çok bilgi güvenliği riski bulunmaktadır. Bilgi güvenliği risk yönetimi süreçlerinin önemi ve etkin uygulanmasının kurumların bilgi varlıklarını korumak ve güvenliklerini sağlamak açısından kritik olduğu ve bunun yanı sıra yasal uyumun sağlanmasında da gereklilik haline geldiği sonucu tespit edilmektedir. Bu gerekliliklerin sağlanması hususunda, kurumların hangi metodolojiyi seçmesi gerektiği ve nasıl bir süreç işletmesi gerektiği bilgisi, genellikle kurumlar için gerek sürecin tasarlanması gerek ise işletilmesi ve yönetilmesi konusunda zor olmaktadır. Bazı kurumlar düşük maliyet ve yönetim kolaylığı nedeniyle hizmet olarak satın almayı tercih etmektedir. Bu konuda kurumların çekimser davranmasında çeşitli sebepler bulunmakta, bu sebeplerden biri de sürecin tam anlaşılamaması ve anlaşılabilmesi için yeterli kaynağın bulunmamasıdır. Literatürde yapılan araştırmalar sonucunda da bilgi güvenliği risklerinin yönetimi konusunda yeterli kaynağın olmaması veya var olan kaynaklardaki bilgilerin yetersiz kalması bunu destekler niteliktedir.

Kurumsal bilgi güvenliği risklerinin tespit edilmesi, analizi ve doğru aksiyon planlanlarının belirlenmesi kurumlarda oluşabilecek olası bir tehditin ortaya çıkmasını azaltmaya ya da engellemeye olanak tanıması noktasında büyük önem oluşturmaktadır. Bu sayede kurumlar risklerini azaltarak kabul edilebilir seviyelere indirgeyebilmektedir.

Makalede incelenen risk yönetimi metodolojileri, temelde benzer adımları içermekte ve kurumların bu süreçleri etkin bir şekilde uygulayabilmelerine olanak tanımaktadır.

Hedef ve ihtiyaçlar belirlendikten sonra kurumlar kendi yöntemlerini de geliştirip uygulayabilirler ya da mevcut yöntemleri kullanmayı tercih edebilirler. Bu tamamen kurumun beklentilerine ve ihtiyaçlarına bağlı şekilde yapılanmaktadır.

Sonuçlar kapsamında öneriler ve gelecek çalışmalara yön verebilecek husular:

- Risk Yönetim Sürecinin uygulanabilmesi için BGYS kurma zorunluluğu bulunmasa da kurumların BGYS'yi kurmaları risk yönetimini kolaylaştırmaktadır.
- Risk Yönetim Sürecinin öneminin anlaşılması amacıyla hem üst yönetim hem de kurum çalışanları için farkındalık eğitimi verilebilir.
-
- Risk analizi adımlarının ayrıntılı bir şekilde incelenmesi ve örnek senaryolar üzerinde değerlendirilmesi, kurumların riskleri daha iyi anlamalarına ve uygun önlemleri alabilmelerine yardımcı olmaktadır.

- Risk yönetim sürecinde karşılaşılabilecek zorlukların farkında olunması ve uygun çözümlerin geliştirilmesi önemlidir.

Son olarak, BGYS'de sürekli izleme ve değerlendirme sürecinin önemi vurgulanmaktadır. Değişen tehditler ve organizasyonel değişiklikler göz önünde bulundurularak, risk analizi sürekli olarak gözden geçirilmeli ve güncellenmelidir. Bu şekilde, kurumlar bilgi güvenliğini sürekli olarak güçlendirebilir ve olası risklere karşı hazırlıklı olabilirler.

KAYNAKÇA

Antunes, M., Maximiano, M., Gomes, R., ve Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 1(2), 219-238.

Durankaya, İ., Gökşen, Y., Eminağaoğlu, M. (2018, Ekim) ISO/IEC 27001 ISO27001 Bilgi Güvenliği Yönetim Sisteminde Risk Analizi. IMISC 2018 Conference Proceedings, 29-33.

ISO/IEC 27005:2022 Information Security Risk Management International Standard. (2022).

ISO/IEC 27001:2022 Information Security Management System International Standard. (2022).

Kaptan, S., (1995), Bilimsel Araştırma ve İstatistik Teknikleri, Tekışık Web Ofset Yayınları. Ankara

Marianne S. ve Barbara G. (1996). NIST- Generally Accepted Principles and Practices, Special Publication (NIST SP)- 800-14.

Mohamed G., Sophia F., Hicham M., Adil S. (2014). Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk, International Journal of Computer Applications (0975 – 8887).

Peltier, T. R. (2005). Information Security Risk Analysis (15-42).

Sağsan, M. (2010). Gelişmişliğin Vazgeçilmez Unsuru: Ulusal Bilgi Politikası.

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

URL-1: https://www.6clicks.com/resources/answers/what-are-the-four-4-cybersecurity-risk-treatment-mitigation-methods
[Erişim Tarihi: 30.11.2023]

URL-2: https://finans.mynet.com/haber/detay/r/risk-istahi-nedir-risk-istahi-nasil-belirlenir/453728/
[Erişim Tarihi: 26.02.2024]

URL-3:https://it.bilgi.edu.tr/tr/guvenlik/iso-27001/
[Erişim Tarihi: 18.11.2023]

URL-4: https://ishayativedenetim.com/2021/03/26/risk-matrisi-nedir/
[Erişim Tarihi: 10.11.2023]

URL-5: https://www.beyaz.net/tr/guvenlik/makaleler/bilgi_guvenligi.html
[Erişim Tarihi: 17.05.2024]

URL-6: https://belgelendirme.ctr.com.tr/iso-27001.html
[Erişim Tarihi: 24.12.2023]