TMMOB BİLGİSAYAR MÜHENDİSLERİ ODASI 2012

Siber Güvenlikte Yönetişim Risk ve Uyumluluk

www.bmo.org.tr

TMMOB

BİLGİSAYAR MÜHENDİSLERİ ODASI

SİBER GÜVENLİKTE YÖNETİŞİM, RİSK VE UYUMLULUK

Bu çalışma ile ilgili istek, görüş ve önerileriniz için;

TMMOB BİLGİSAYAR MÜHENDİSLERİ ODASI

Necatibey Cad. No. 88/7 Çankaya – ANKARA

Telefon: 0312 230 31 45

Belgeç (Faks): 0312 230 31 46

e-Posta: iletisim@bmo.org.tr

www.bmo.org.tr

Kapak Tasarım : R. Savaş Uluçay

Editör : Alper Dönmez

1.Basım Kasım 2025

TMMOB

BİLGİSAYAR MÜHENDİSLERİ ODASI

SİBER GÜVENLİK ÇALIŞMA GRUBU

SİBER GÜVENLİKTE YÖNETİŞİM, RİSK VE UYUMLULUK

Hazırlayan

R. Savaş ULUÇAY

ÖNSÖZ

Siber güvenlik söz konusu olduğunda, kuruluşlar güvenliği sağlamak için farklı çerçeveler, en iyi uygulamalar ve standartlar kullanır. Bu yönetişim çerçeveleri, çoğunlukla kurumsal yönetişim gerekliliklerine veya yasal gerekliliklere uygun olarak seçilir. Kontroller, siber ihlal geçmişi ve mali konular; teknik, idari, ve fiziksel kontroller dahil olmak üzere genellikle yönetişim belgelerinde belirtilir. Ayrıca, işletmelerin siber alanlarını güvence altına almak için geliştirmeleri gereken belirli yetenekleri tanımlayan bir dizi belge de mevcuttur. Bu nedenle, tehditlerden SQL (Structured Query Language - Yapılandırılmış Sorgu Dili) enjeksiyon saldırılarına, bulut bilişime, yük dengelemeye ve siber koruma gerektiren Nesnelerin İnternetine kadar her şey GRC (Governance, Risk, and Compliance – Yönetişim, Risk ve Uygunluk) çerçevesine dahil edilmeli ve GRC'nin kuruluşlara sağladığı ticari faydalar hakkında bilgi verilmelidir. Bu nedenle, bu makaledeki sonuçlar; kötü yönetimi önlemek, riski azaltmak ve kuruluşlarda uyumu sağlamak için Bilgi Teknolojileri GRC uygulamasının anlaşılması ve değerlendirilmesi olmalıdır. Bu, yalnızca uygulama güvenliği, nesnelerin interneti güvenliği, ağ güvenliği, altyapı güvenliği gibi yöntemler kullanılarak; siber ve ağ saldırıları gibi dış risklerin azaltılması, hassas bilgilere erişimi sınırlandırılması ve GRC'nin siber güvenlikle olan ilişkisinin ortaya konulmasıyla sağlanabilir.

R. Savaş ULUÇAY

TMMOB BMO

Siber Güvenlik Çalışma Grubu Başkanı

SUNUŞ

Değerli Meslektaşlarımız,

Bilgi ve iletişim teknolojilerinin toplumsal yaşamın her alanına nüfuz ettiği günümüzde, bu sistemlerin güvenli, sürdürülebilir ve etik biçimde işletilmesi hem bireylerin hem kurumların hem de kamusal yapıların varlığını sürdürebilmesi için kritik bir zorunluluk haline gelmiştir. Siber güvenlik yalnızca teknik bir alan değil, ulusal güvenlikten kişisel mahremiyete kadar geniş bir yelpazede toplumsal refahı doğrudan etkileyen stratejik bir konudur.

Anayasamızın 135. maddesi uyarınca kamu kurumu niteliğinde bir meslek kuruluşu olan TMMOB Bilgisayar Mühendisleri Odası olarak, mesleğimizin kamusal sorumluluğunu gözetmek ve toplumsal fayda üretmek en temel görevlerimiz arasındadır. Bu kapsamda, siber güvenliğin ve bilgi güvenliği yönetiminin yalnızca teknik değil, yönetişim, risk ve uyum (GRC) boyutlarıyla da ele alınması gerektiğine inanıyoruz.

Günümüzde yapay zekâ, büyük veri, bulut bilişim ve nesnelerin interneti gibi teknolojilerle karmaşıklaşan dijital ekosistemlerde; kurumların bilgi varlıklarını korumaları, yasal düzenlemelere uyum sağlamaları ve etik ilkeler çerçevesinde hareket etmeleri giderek zorlaşmaktadır. Bu noktada, yönetişim, risk ve uyum süreçlerinin mühendislik ilkeleriyle bütünleştirilmesi; yalnızca teknik bir gereklilik değil, aynı zamanda toplumsal bir sorumluluktur.

Öte yandan, kamusal denetim mekanizmalarının zayıflatıldığı, veri gizliliği ihlallerinin arttığı, kritik altyapıların güvenliğinin yeterince gözetilmediği günümüz koşullarında; meslektaşlarımızın bilgi güvenliği, siber savunma, risk yönetimi ve uyum süreçlerinde aktif rol üstlenmeleri her zamankinden daha büyük bir önem taşımaktadır.

Bu el kitabı, siber güvenlik alanında görev yapan mühendislerimizin temel kavramlara, standartlara, süreçlere ve en iyi uygulamalara erişimini kolaylaştırmayı amaçlamaktadır. Aynı zamanda, kamu ve özel sektörde siber güvenlik ve GRC süreçlerinin tanımlanması, mesleki denetim altyapısının güçlendirilmesi ve kurumsal farkındalığın artırılması hedeflenmektedir.

Hazırlık sürecinde büyük özveriyle katkı sunan Siber Güvenlik Çalışma Grubu'nun tüm üyelerine, değerli meslektaşlarımıza ve emeği geçen herkese teşekkür eder, bu el kitabının mesleğimizin gelişimine ve toplumun dijital güvenliğine katkı sağlamasını temenni ederim.

Saygılarımla,

Cem Nuri ALDAŞ

TMMOB Bilgisayar Mühendisleri Odası Yönetim Kurulu Başkanı

Kasım 2025

KISALTMALAR

BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BT	Bilgi Teknolojileri
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technology
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
GDPR	General Data Protection Regulation
GRC	Governance, Risks, and Compliance
HIPAA	Health Insurance Portability and Accountability Act
IAM	Identity and access management
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KOBİ	Küçük ve Orta Büyüklükteki İşletmeler
KPI	Key Performance Indicator
KVKK	Kişisel Verilerin Korunması Kanunu

MASAK	Mali Suçları Araştırma Kurulu
MTTD	Mean Time to Detect
MTTR	Mean Time to Respond
NIST	National Institute of Standards and Technology
OCEG	Open Compliance and Ethics Group
PCI DSS	Payment Card Industry Data Security Standard
SIEM	Security Information and Event Management
SOC	Security Operations Center

TERİM KARŞILIKLARI

AI Act / Yapay Zeka Yasası

Acceptance / Risk Kabulü

Avoidance / Riskten Kaçınma

Chief Executive Officer / İcra Kurulu Başkanı, Genel Müdür

Chief Information Officer / Baş Bilgi[BT] Sorumlusu

Chief Information Security Officer / Baş Bilgi Güvenliği Sorumlusu

Compliance / Uyumluluk

Control Objectives for Information and Related Technology / Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri

Cyber Resilience / Siber Dayanıklılık

Data Loss Prevention / Veri Kaybı Önleme

Detect / Tespit Et

Distributed Denial of Service / Dağıtılmış Hizmet Reddi

General Data Protection Regulation / Genel Veri Koruma Tüzüğü

Governance / Yönetişim

Governance, Risk, and Compliance / Yönetişim, Risk(yönetimi) ve Uyumluluk

Health Insurance Portability and Accountability Act / Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası

Identify / Tanımla

Internet of Things / Nesnelerin interneti

International Electrotechnical Commission / Uluslararası Elektroteknik Komisyonu

Information Systems Audit and Control Association / Bilgi Sistemleri Denetim ve Kontrol Birliği

International Organization for Standardization / Uluslararası Standardizasyon Örgütü

Information Technology / Bilgi Teknolojisi

Information Technology Infrastructure Library / Bilgi Teknolojisi Altyapı Kütüphanesi

International Organization for Standardization /

Key Performance Indicator / Anahtar[Temel] Performans Göstergesi

Mean Time to Detect / Ortalama tespit Süresi

Mean Time to Respond / Ortalama Müdahale Süresi

Mitigation / Risk Azaltma

National Institute of Standards and Technology / Ulusal Standartlar ve Teknoloji Enstitüsü

NIST Cybersecurity Framework NIST **/** Siber Güvenlik Çerçevesi

Open Compliance and Ethics Group / Açık Uyumluluk ve Etik Grubu

Payment Card Industry Data Security Standard / Ödeme Kartı Sektörü Veri Güvenliği Standardı

Protect / Koru

Recover / Kurtar

Respond / Yanıtla

Risk Heatmap / Risk Matrisi

Risk(Management) / Risk(yönetimi)

Security Information and Event Management / Güvenlik Bilgi ve Olay Yönetimi

Security Operations Center / Güvenlik Operasyon Merkezi

Zero Trust / Sıfır Güven

İÇERİK

1. GİRİŞ

1.1. GRC Nedir?

GRC, İngilizce Governance, Risk, and Compliance kelimelerinin baş harflerinden oluşur. Türkçede Yönetişim, Risk[Yönetimi] ve Uyumluluk anlamına gelir.

- **Yönetişim:** Bir kurumun siber güvenlik stratejilerini, politikalarını ve süreçlerini belirleyen; karar mekanizmalarını yöneten çerçevedir.
- **Risk [Yönetimi]:** Kurumun karşı karşıya olduğu siber tehditleri analiz eden, bunların olasılığını ve etkisini ölçerek uygun önlemler geliştiren süreçtir.
- **Uyumluluk:** Kurumun faaliyetlerini ilgili yasal düzenlemeler, standartlar ve regülasyonlarla uyumlu hale getirmesini ifade eder.

Bu üç unsur birlikte ele alındığında kurumun yalnızca teknik açıdan değil, stratejik ve yasal açıdan da güvenli olması sağlanır.

1.2. Siber Güvenlikte GRC'nin Önemi

Günümüzde siber saldırılar yalnızca teknik hasarlara yol açmakla kalmayıp; aynı zamanda finansal kayıplar, yasal yaptırımlar, marka değerinde düşüş ve müşteri güveninde erozyon gibi sonuçlar doğurmaktadır.

- ✓ GRC yaklaşımı, teknik güvenlik önlemlerinin ötesine geçerek organizasyonel yapıyı güçlendirir.
- ✓ Yönetim kurulu, üst yönetim ve çalışanlar arasında ortak bir güvenlik kültürü oluşmasına yardımcı olur.
- ✓ Kurumun sürdürülebilir siber güvenlik olgunluğunu artırır.

Örneğin, bir banka için yalnızca güvenlik duvarı veya antivirüs yazılımı kullanmak yeterli değildir. Risklerin doğru yönetilmesi, BDDK ve KVKK mevzuatına uyum sağlanması ve yönetim kurulu seviyesinde doğru raporlamaların yapılması da gerekmektedir. İşte GRC, bu bütüncül yaklaşımı sağlamaktadır.

1.3. Dünyada ve Türkiye'de GRC Yaklaşımları

- Dünya Genelinde;
  - Amerika ve Avrupa'da özellikle NIST Cybersecurity Framework, COBIT ve ISO 27001 standartları GRC uygulamalarının temelini oluşturmaktadır.
  - GDPR (Avrupa Birliği Genel Veri Koruma Tüzüğü) uyum süreçleri, GRC programlarının hızla yaygınlaşmasına sebep olmuştur.
- Türkiye'de;
  - KVKK (Kişisel Verilerin Korunması Kanunu), kurumların veri koruma uyumluluğunu zorunlu kılmaktadır.
  - BDDK düzenlemeleri, finans sektörü için kapsamlı siber güvenlik yükümlülükleri sağlamaktadır.
  - Kamu kurumlarında BTK tarafından yayımlanan rehberler, GRC süreçlerinin gelişimini hızlandırmaktadır.
  - Türkiye'de özellikle son yıllarda regülasyonların artmasıyla GRC uygulamalarının yalnızca büyük kuruluşlarda değil, KOBİ'lerde de hızla yaygınlaştığı görülmektedir.

2. YÖNETİŞİM

Yönetişim, kurumun siber güvenlik yol haritasını belirleyen ve tüm paydaşların sorumluluklarını netleştiren üst düzey çerçevedir.

2.1. Siber Güvenlik Stratejisi ve Politika Yönetimi

2.1.1. Siber Güvenlik Stratejisi

Kurumun iş hedefleriyle uyumlu, uzun vadeli güvenlik vizyonudur. Örneğin, dijital dönüşüm sürecinde bulut altyapısına geçiş yapan bir şirketin, bulut güvenliği stratejisini de buna entegre etmesi anlamına gelir.

2.1.2. Politika Yönetimi

Tüm çalışanların uyması gereken yazılı kuralların oluşturulmasıdır. Örneğin, Parola politikaları, E-posta ve internet kullanım kuralları, Mobil cihaz yönetimi, Uzaktan çalışma

güvenliği kuralları. Politikaların yalnızca yazılı olması yetmez, düzenli aralıklarla güncellenmesi, çalışanlara eğitimlerle aktarılması gerekmektedir.

2.2. Kurumsal Roller ve Sorumluluklar

Etkili bir yönetişim yapısı, kurum içinde rollerin ve sorumlulukların net bir şekilde tanımlanmasını gerektirir.

- ✓ Yönetim Kurulu: Siber güvenliğin stratejik öncelik olduğunu kabul etmeli ve bu doğrultuda bütçe ile kaynak ayırmalıdır.
- ✓ CISO: Kurumun siber güvenlik lideridir. Strateji oluşturur, uygulamayı denetler ve raporlama yapar.
- ✓ Risk Yönetimi Birimi: Siber risklerin ölçüm ve raporlamasından sorumludur.
- ✓ Uyum Ekibi: Mevzuat ve standartlara uygunluğu denetler.
- ✓ IT ve SOC ekipleri: Teknik önlemleri uygular, izleme ve müdahale süreçlerini yönetir.
- ✓ Çalışanlar: En zayıf halka olmamaları için farkındalık eğitimleri ile desteklenmelidir.

2.3. Siber Güvenlik Komiteleri ve Raporlama Yapısı

Kurumlarda siber güvenlik yalnızca IT'nin işi değildir, tüm iş birimlerini kapsayan bir yönetişim mekanizması gerekmektedir. Bu nedenle birçok kurumda Siber Güvenlik Komiteleri kurulmaktadır. Komite üyeleri genellikle CIO, CISO, Risk Direktörü, Hukuk Direktörü, İnsan Kaynakları Direktörü ve bazen CEO'dan oluşmaktadır. *Komite düzenli aralıklarla toplanır;*

a. Siber tehdit raporlarını inceler,

b. Risk seviyelerini değerlendirir,

c. Yatırım ve bütçe kararları alır,

d. İhlal durumunda kriz yönetimi planlarını devreye sokar.

2.3.1. Raporlama Yapısı

CISO, düzenli olarak üst yönetime ve yönetim kuruluna rapor sunmalıdır. Bu raporlar yalnızca teknik terimlerden ibaret

olmamalı ve iş diliyle hazırlanmalıdır. Örneğin; "%25 fidye yazılımı riski" yerine "Fidye yazılımı saldırısı gerçekleşirse finansal kayıp 2 milyon TL olabilir" gibi anlaşılır metrikler sunulmalıdır.

2.4. Yönetişimde Başarı İçin Kritik Unsurlar

- ✓ Üst Yönetim Desteği: yönetim kurulu güvenlik konusunu maliyet değil yatırım olarak görmelidir.
- ✓ Şeffaf iletişim: riskler ve ihlaller gizlenmemeli, zamanında raporlanmalıdır.
- ✓ Sürekli Eğitim: Tüm çalışanlar düzenli olarak bilinçlendirilmelidir.
- ✓ Uyumlu Çerçeve: ISO 27001, NIST veya COBIT gibi uluslararası standartlar referans alınmalıdır.

3. RİSK[YÖNETİMİ]

3.1. Siber Risk Kavramı ve Türleri

Siber risk, bir kurumun bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliğinin tehdit altında olması durumudur. Risk, tehditlerin (ataklar, doğal afetler, iç tehditler vb.) kurumun zafiyetleriyle (açık portlar, güncel olmayan yazılımlar, eğitimsiz çalışanlar) buluşması sonucu ortaya çıkmaktadır.

Başlıca siber risk türleri:

- ❖ Veri İhlalleri: Kişisel verilerin veya müşteri bilgilerin çalınmasıdır.
- ❖ Fidye Yazılımları: Sistemlerin şifrelenerek fidye talep edilmesidir.
- ❖ İç Tehditler: Çalışanların hataları veya kasıtlı zarar vermesidir.
- ❖ Hizmet Kesintileri: DDoS saldırıları veya altyapı arızalarını kapsar.
- ❖ Tedarikçi Kaynaklı Riskler: Üçüncü taraf yazılım veya hizmet sağlayıcıların güvenlik açıklarını kapsar.

3.2. Risk Analizi ve Değerlendirme Yöntemleri

Risk yönetimi, sadece tehditleri tanımayı değil, bunların olasılığını ve etkisini ölçerek önceliklendirmeyi de içermektedir.

- Nitel Analiz: Riskler düşük, orta, yüksek şeklinde sınıflandırılır. Örneğin, fidye yazılımı riski yüksek.
- Nicel Analiz: Risklerin finansal karşılığı hesaplanır. Örneğin, bir fidye yazılımı saldırısının maliyeti çok yüksek olabilir.
- Risk Matrisi: Olasılık ve etki ekseninde riskler görselleştirilir.
- Formül: Risk = Olasılık × Etki

Örneğin; Yüksek olasılıklı ama düşük etkili bir risk öncelikli değil iken, düşük olasılıklı ama yüksek etkili risk (kritik altyapıya saldırısı) stratejik öneme sahiptir.

3.3. Risk Azaltma, Kabul ve Transfer Stratejileri

Risk yönetimi dört temel yaklaşımı kapsamaktadır;

i. Risk Azaltma: Güvenlik duvarı, antivirüs, SIEM sistemleri, çalışan eğitimi.

ii. Risk Kabulü: Bazı düşük seviye risklerin kabul edilmesi (düşük etkili e-posta spam riski).

iii. Risk Transferi: Siber sigorta poliçeleri ile riskin finansal etkisinin başka kuruma aktarılması.

iv. Riskten Kaçınma: Çok riskli bir teknolojiden veya iş modelinden tamamen vazgeçilmesi.

3.4. Siber Risk Metrikleri ve KPI'lar

Üst yönetimin siber riskleri anlayabilmesi için ölçülebilir göstergeler gerekir. Örnek metrikler;

- Tespit Süresi: Bir saldırının ortalama ne kadar sürede fark edildiği.
- Müdahale Süresi: Bir saldırıya ortalama müdahale süresi.
- Açık Yönetimi: Kritik yamaların uygulanma süresi. Örneğin %90'ı ilk 30 gün içinde kapatıldı gibi.

- ❖ Olay Sayısı: Belirli bir dönemde yaşanan güvenlik olaylarının adedi.
- ❖ Finansal Kayıp: İhlallerin mali etkisi. Örneğin, 2024'te toplam 2 milyon TL kayıp.

Bu metrikler yönetim kuruluna iş diliyle raporlandığında, güvenlik yatırımlarının önemi daha net anlaşılmaktadır.

3.5. Risk Yönetiminde Başarı İçin İpuçları

Risk yönetiminde başarı için dört temel ipucu:

- ✓ Riskler yalnızca BT'nin değil, tüm iş birimlerinin sorumluluğu olmalıdır.
- ✓ Her risk değerlendirmesi yılda en az bir kez güncellenmelidir.
- ✓ Kritik riskler için iş sürekliliği planı hazırlanmalıdır.
- ✓ Tedarikçi risk yönetimi süreçleri mutlaka uygulanmalıdır.

4. UYUMLULUK

4.1. Uyumluluk Nedir?

Uyumluluk, bir kurumun faaliyetlerini ulusal ve uluslararası kanunlar, standartlar ve düzenlemelerle uyumlu hale getirmesidir. Siber güvenlikte uyumluluk, yalnızca yasal yaptırımlardan kaçınmak için değil, aynı zamanda müşteri güveni ve kurumsal itibar için kritik öneme sahiptir.

4.2. Uluslararası Standartlar ve Çerçeveler

Kurumların siber güvenlik uyumluluğu için takip ettiği başlıca uluslararası standartlar;

- ➢ ISO/IEC 27001: Bilgi güvenliği yönetim sistemi standardıdır. Politikaların, risk yönetiminin ve kontrollerin çerçevesini belirler.
- ➢ NIST Cybersecurity Framework (ABD): "Tanımla, Koru, Tespit Et, Yanıtla, Kurtar" olmak üzere beş temel fonksiyon üzerine kuruludur (Identify, Protect, Detect, Respond, Recover).

- COBIT (ISACA): BT yönetişimi ve kontrol hedeflerini belirler.
- GDPR (Avrupa): Kişisel verilerin korunması konusunda en kapsamlı regülasyonlardan biridir.
- PCI-DSS: Ödeme kartı verilerini işleyen kurumlar için güvenlik standartlarıdır.

Bu standartlar yalnızca teknik önlemleri değil, organizasyonel yapıyı ve süreçleri de kapsar.

4.3. Türkiye'de Mevzuatlar

Türkiye'de kurumların uyması gereken birçok yasal düzenleme bulunmaktadır.

- KVKK (Kişisel Verilerin Korunması Kanunu)
  - 2016'dan beri yürürlüktedir.
  - Kişisel verilerin işlenmesi, saklanması ve aktarılması süreçlerini düzenler.
  - Veri ihlali yaşandığında 72 saat içinde KVKK Kurumu'na bildirim zorunluluğu vardır.

- BDDK Düzenlemeleri (Bankacılık Sektörü)
  - Finansal kuruluşların bilgi sistemleri ve siber güvenlik kontrollerine yönelik yükümlülükler içerir.
  - Yedekleme, log (kayıt, kütük) yönetimi ve olay müdahale planı zorunludur.

- MASAK Düzenlemeleri
  - Kara para aklama ve terör finansmanı ile mücadele kapsamında veri güvenliği ve kayıt tutma yükümlülükleri içerir.

- BTK Rehberleri
  - Kritik altyapı sağlayıcıları için siber güvenlik önlemleri ve uyum süreçlerini içerir.

4.4. Uyumluluk Denetimi ve Süreçleri

Uyumluluk yalnızca belgeler hazırlamak değil, aynı zamanda düzenli denetimlerle kontrol edilen bir süreçtir.

- İç Denetim: Kurum içindeki denetim birimleri tarafından yapılır.
- Dış Denetim: Bağımsız denetim kuruluşları veya regülatör kurumlar tarafından yapılır.
- Uyumluluk Raporları: Yönetim kuruluna ve regülatörlere düzenli rapor sunulur.
- Sürekli İzleme: Uyumluluk statik değil, dinamik bir süreçtir. Yeni düzenlemeler çıktığında kurum politikaları güncellenmelidir.

Örneğin, KVKK'ya uyumlu bir kurumun;

- ✓ Açık rıza metinleri,
- ✓ Aydınlatma yükümlülükleri,
- ✓ Veri işleme envanteri,
- ✓ Saklama ve imha politikaları hazır olmalıdır.

4.5. Uyumluluk Sağlamanın Faydaları

- Yasal Risklerden Kaçınma: Para cezaları ve yaptırımlardan korunma.
- Müşteri Güveni: "Verilerim güvende" algısı yaratma.
- Rekabet Avantajı: ISO 27001 sertifikalı şirketlerin iş ortaklığı şansı artar.
- Kriz Yönetimi Kolaylığı: Veri ihlali durumunda hazırlıklı olunmasını sağlar.

4.6. Uyumlulukta Karşılaşılan Zorluklar

- ❖ Sürekli değişen regülasyonlara ayak uyduramamak.
- ❖ Yüksek uyum maliyetleri.
- ❖ Küçük ölçekli şirketlerde yetersiz insan kaynağı.

Uyumluluk ile gerçek güvenlik arasındaki fark şudur: Bazı kurumlar sadece kâğıt üzerinde uyumlu olmaya odaklanırken, gerçek güvenlik kültürünü atlamaktadır.

5. SİBER GÜVENLİK GRC UYGULAMALARI

5.1. GRC Yazılımları ve Teknolojileri

Kurumların GRC süreçlerini manuel yönetmesi hem zahmetli hem de hataya açık olabilmektedir. Bu nedenle GRC yazılımları kullanılmaktadır.

Yazılımların başlıca işlevleri:

- Politika Yönetimi: Güvenlik politikalarının yayınlanması, çalışanlarla paylaşılması ve uyum takibinin yapılması.
- Risk Yönetimi Modülleri: Risklerin kaydı, değerlendirilmesi ve önceliklendirilmesi.
- Uyumluluk Takibi: ISO 27001, KVKK, GDPR gibi regülasyonlara uyum durumunun izlenmesi.
- Raporlama ve Gösterge Panelleri: Üst yönetime görsel ve anlaşılır rapor sunulması.
- Örnek GRC Araçları: RSA Archer, MetricStream, ServiceNow GRC, LogicGate.

5.2. Otomasyon ve Yapay Zekâ Kullanımı

Modern GRC çözümleri yalnızca statik raporlamadan ibaret değildir. Otomasyon ve yapay zekâ desteği ile daha etkin hale gelmektedir.

- Olay Yönetimi: SIEM sistemlerinden gelen veriler GRC'ye entegre edilerek otomatik risk kaydı oluşturulur.
- Uyumluluk Kontrolleri: Yapay zekâ, log verilerini analiz ederek uyumsuzlukları otomatik raporlar.
- Tahmine Dayalı Analiz: Makine öğrenmesi ile gelecekte oluşabilecek riskler tahmin edilir.
- Süreç Otomasyonu: Örneğin bir çalışanın işe girişinde otomatik olarak KVKK eğitim modülüne atanması yapılır.

5.3. Olay Yönetimi ve İhlal Bildirimleri

Bir kurumun GRC olgunluğu, siber olaylara nasıl tepki verdiğiyle ölçülür.

- Olay Tespiti: SOC ekipleri veya otomasyon sistemleri tarafından yapılır.
- Olay Kaydı: GRC platformuna işlenir ve ilgili risk kategorisine atanır.
- İhlal Bildirimi: KVKK'ya 72 saat içinde, müşterilere/iş ortaklarına ise makul sürede yapılır.
- Düzeltici faaliyetler: Açığın kapatılması, yamaların yapılması ve süreçlerin güncellenmesidir.
- Kapanış ve Raporlama: Yönetim kuruluna ve regülatörlere sonuç raporu hazırlanır.

Yasal uyum ve kurumsal itibar korunması için süreç sistematik yürütülmelidir.

5.4. GRC ile Entegre Güvenlik Süreçleri

GRC uygulamaları, yalnızca risk ve uyum değil, tüm siber güvenlik döngüsünü kapsayacak şekilde tasarlanmalıdır.

- Varlık Yönetimi: Hangi sistemlerde hangi verilerin bulunduğu net olmalıdır.
- Açık Yönetimi: Zafiyet tarama sonuçları GRC'ye bağlanmalıdır.
- Eğitim Yönetimi: Çalışanların eğitim katılımı takip edilmelidir.
- İş Sürekliliği ve Felaket Kurtarma: GRC çerçevesinde yedekleme ve test süreçleri izlenmelidir.

5.5. GRC Uygulamalarında Başarı Faktörleri

- Üst Yönetim Katılımı: Komiteler aktif çalışmalıdır.
- Kültür ve Farkındalık: Çalışanlar sadece imza atmakla kalmamalı, süreci anlamalıdır.
- Teknoloji Entegrasyonu: SIEM, DLP, IAM gibi güvenlik araçları GRC platformuna bağlanmalıdır.
- Sürekli İyileştirme: Olaylardan ders çıkarılarak süreçler güncellenmelidir.

6. VAKA ÇALIŞMALARI

6.1. Uluslararası Şirketlerde GRC Örnekleri

- Örnek 1 - Global Banka (ABD)
  - Durum: Banka, fidye yazılımı saldırısı sonucu müşteri verilerinin şifrelenmesiyle karşılaşmıştır.
  - GRC Yaklaşımı: Risk analizi sonucunda fidye yazılımlarının yüksek olasılık-yüksek etki kategorisinde olduğu belirlenmiştir. Banka, olay müdahale planını önceden hazırlamıştır. Saldırı sonrasında ise hızlıca iş sürekliliği planını devreye almış ve müşteri verilerinin yedeklerini geri yüklemiştir.
  - Sonuç: Banka, finansal kaybı minimize etmiştir ve regülatörlere 48 saat içinde rapor sunmuştur. Bu, GRC'nin kriz yönetiminde ne kadar kritik olduğunu göstermiştir.
- Örnek 2 - Avrupa'da E-ticaret Şirketi
  - Durum: GDPR gereği, kullanıcı verilerinin Avrupa dışına aktarılırken açık rıza alınması gerekmektedir. Şirket, ilk denetiminde uyumsuzluk nedeniyle 500.000 € ceza almıştır.
  - GRC Yaklaşımı: Uyumluluk ekibi, veri işleme envanterini güncellemiştir. Müşterilere sunulan aydınlatma metinleri ile çerez politikaları yeniden düzenlemiş ve otomatik uyum takibi için GRC yazılımını devreye almıştır.
  - Sonuç: Kurum tekrar denetimde ceza almamıştır ve müşteri güvenini yeniden kazanmıştır.

6.2. Türkiye'de GRC Örnekleri

- Örnek 3 - Bankacılık Sektörü
  - Durum: BDDK'nın bilgi sistemleri denetimlerinde, birçok banka uyumluluk eksikleri nedeniyle uyarı almıştır.
  - Uygulama: Büyük bir banka, GRC yazılımı entegre ederek tüm politikalarını tek merkezden yönetmeye başlamıştır. Risk komitesi, düzenli toplantılarla raporları

incelemeye başlamıştır. KVKK ihlallerini izlemek için SIEM sistemi ile GRC platformu birbirine bağlanmıştır.

- ❖ Sonuç: Banka hem BDDK hem de KVKK denetimlerinden eksiksiz geçmiştir.

- ➢ Örnek 4 - Telekom Sektörü
  - ❖ Durum: BTK, kritik altyapı sağlayıcılarının siber olay bildirimlerini zorunlu kılmıştır.
  - ❖ Uygulama: Telekom şirketi, GRC sistemine olay yönetim modülü eklemiştir. SOC merkezinden gelen alarmlar, otomatik olarak GRC'de kayıt altına alınmıştır. Bu sayede 24 saat içinde BTK'ya rapor gönderme süreci otomatize edilmiştir.
  - ❖ Sonuç: Yasal uyumluluk hızlanmış ve manuel raporlama hataları ortadan kalkmıştır.

6.3. Ders Çıkarılan Siber Olaylar

- ➢ Yahoo Veri İhlali (2013–2014)
  - 3 milyar hesabın verileri sızdırılmıştır. Zayıf şifreleme (MD5) ve geç fark edilen saldırılar nedeniyle hasar büyümüştür.
  - Alınan Ders: Risk yönetimi ve erken tespit metriklerinin önemi.

- ➢ Equifax Veri İhlali (2017)
  - Apache Struts güvenlik açığı yamalanmadığı sebebiyle 147 milyon kişinin verileri sızdırılmıştır.
  - Alınan Ders: Zafiyet yönetiminin uyumluluk süreçlerine entegre edilmesi şart haline gelmiştir.

- ➢ TurkNet Veri İhlali (2021)

- KVKK'ya bildirilen bir veri sızıntısı yaşanmıştır. KVKK ihlal bildirim sürecine uygun hareket edilmiştir.
- Alınan Ders: Yasal zorunluluklara uyum, itibar kaybını azaltabilir.

6.4. Vaka Çalışmalarından Çıkarılan Ortak Sonuçlar

- ✓ GRC süreçleri etkin işletildiğinde kriz yönetimini kolaylaştırmaktadır.
- ✓ Uyumluluk eksikliği, yüksek maliyetli cezalar doğurmaktadır.
- ✓ Risk analizleri sadece kâğıt üzerinde kalmamalı, düzenli güncellenmelidir.
- ✓ Bütünleşmiş teknolojiler (SIEM + GRC), olaylara hızlı müdahale sağlamaktadır.

7. GRC VE GELECEK EĞİLİMLERİ

7.1. Yapay Zeka ve Makine Öğrenmesi ile GRC

- ➢ Otomatik Risk Tespiti: Yapay zekâ, sistem loglarını inceleyerek anormal davranışları tespit edebilir.
- ➢ Tahmine Dayalı Güvenlik: Makine öğrenmesi, geçmiş saldırılardan ders çıkararak gelecekteki riskleri öngörebilir.
- ➢ Uyum Kontrolü: YZ destekli sistemler, yeni regülasyonları analiz ederek kurumun hangi alanlarda eksik olduğunu raporlayabilir.
- ➢ Chatbot Denetçiler: Çalışanların güvenlik sorularına anında yanıt veren yapay zekâ destekli danışmanlar gelişmektedir.

7.2. Siber Dayanıklılık

Klasik güvenlik yaklaşımı, yalnızca saldırıyı önlemeye odaklanırken; siber dayanıklılık ise saldırının kaçınılmaz olduğunu kabul edip, saldırı sonrası toparlanma sürecini de planlamayı kapsar.

Dayanıklılığın Unsurları;

- Önleme
- Tespit
- Müdahale
- İyileşme

GRC çerçevesi, bu unsurların her birini kapsayan politikalar ve süreçler tanımlayarak kurumların saldırılar karşısında hızlıca toparlanmasını sağlamaktadır.

7.3. Bulut ve Dijital Dönüşümde GRC Yaklaşımları

Modern GRC çözümleri yalnızca statik raporlamadan ibaret değildir. Otomasyon ve yapay zekâ desteği ile daha etkin hale gelmektedir.

7.3.1. Bulut Servisleri

Kurumlar verilerini AWS, Azure veya Google Cloud gibi ortamlara taşıyor. Burada GRC'nin rolü:

- ✓ Paylaşılan sorumluluk modelini anlamak (sağlayıcı – müşteri).
- ✓ Bulut güvenliği uyumluluk sertifikaları (ISO 27017, ISO 27018) kullanmak.

7.3.2. Dijital Dönüşüm

IoT, 5G ve yapay zekâ tabanlı hizmetler yeni riskler doğurmaktadır. GRC, bu riskleri stratejik çerçeveye entegre etmektedir.

7.4. Sıfır Güven Modeli ve GRC

- "Kimseye güvenme, her zaman doğrula" prensibine dayalı Zero Trust yaklaşımı, klasik güvenlik modellerini değiştirmektedir.
- GRC, Zero Trust politikalarının kurum genelinde benimsenmesini sağlamaktadır.
- Erişim yönetimi, çok faktörlü kimlik doğrulama ve sürekli izleme süreçleri GRC ile entegre edilmektedir.

7.5. Regülasyonların Geleceği

- Türkiye'de: KVKK'nın GDPR'a daha da yakınlaştırılması beklenmektedir.
- Avrupa'da: Yapay zekâ düzenlemeleri (AI Act) şirketlerin GRC süreçlerine yeni uyum zorunlulukları getirecektir.
- Küresel: Uluslararası siber güvenlik standartlarının birleşmesi gündemdedir (örneğin NIST + ISO hibrit çerçeveler).

7.6. Gelecek Trendlerinde Öne Çıkanlar

- Otomatik Uyumluluk: GRC yazılımları mevzuatları kendiliğinden güncelleyip uyumsuzlukları raporlayacaktır.
- Siber Sigorta Entegrasyonu: Risk skorları doğrudan sigorta primlerini belirleyecektir.
- Kuantum Çağına Hazırlık: Kuantum bilgisayarların mevcut şifreleme yöntemlerini tehdit etmesi, GRC politikalarını kökten etkileyecektir.
- Global İş birliği: Ülkeler arasında zorunlu veri ihlali raporlama standartları gündeme gelecektir.

8. SONUÇ VE ÖNERİLER

8.1. GRC ile Güçlü Siber Güvenlik Kontrolü

Siber güvenlik yalnızca teknoloji yatırımlarına dayalı bir alan değildir; aynı zamanda kurumsal kültürün bir parçasıdır. GRC yaklaşımı, kurumların güvenliği stratejik, risk odaklı ve uyumlu şekilde yönetmesini sağlamaktadır. Güçlü bir GRC yapısı, kriz anlarında kurumun dayanıklılığını arttırmaktadır. Çalışanların bilinçlenmesi ve üst yönetimin desteği olmadan hiçbir teknoloji tek başına yeterli değildir.

8.2. Yönetim Kurullarına Öneriler

- ✓ Siber güvenlik finansal risk gibi ele alınmalıdır. (Her saldırının potansiyel maliyeti var.)
- ✓ Düzenli olarak CISO raporları istenmelidir.
- ✓ GRC yatırımları sadece uyumluluk için değil, rekabet avantajı için de değerlendirilmelidir.

- ✓ Siber güvenlik, kurumsal risk yönetimi ajandasında öncelikli konular arasına konulmalıdır.

8.3. CISO'lara (Bilgi Güvenliği Yöneticilerine) Öneriler

- ✓ Yönetimle teknik değil, iş diliyle konuşulmalıdır. (Riskin finansal etkisi vurgulanmalıdır.)
- ✓ Risk analizleri düzenli güncellenmeli; raporlar ise basit ve anlaşılır şekilde sunulmalıdır.
- ✓ SIEM, IAM, DLP gibi sistemler, GRC platformu ile entegre edilmelidir.
- ✓ Olay sonrası ders çıkarma (post-incident review) süreçleri kurum kültürüne oturtulmalıdır.

8.4. Çalışanlara Öneriler

- ✓ Parola, e-posta ve cihaz güvenliği konusunda kurum politikalarına uyulmalıdır.
- ✓ "Benim başıma gelmez" düşüncesinden uzak durulmalıdır.
- ✓ Siber güvenlik farkındalık eğitimlerine aktif katılım sağlanmalıdır.
- ✓ Şüpheli bir durumla karşılaşıldığında hemen BT veya güvenlik ekibine bildirilmelidir.

8.5. Geleceğe Yönelik Yol Haritası

- ✓ Dijital dönüşümle birlikte riskler daha da artacaktır, bu nedenle GRC süreçleri sürekli güncellenmelidir.
- ✓ Yapay zekâ ve otomasyon destekli GRC araçları kurumların ana yardımcısı olacak.
- ✓ Uyumluluk sadece regülasyonlara uymak değil, aynı zamanda itibar yönetimi olarak görülmeli.
- ✓ Siber dayanıklılık yaklaşımı her kurumun stratejik planına entegre edilmeli.

Genel Sonuç:

- ❖ Siber güvenlikte GRC, kurumların yalnızca bugünkü değil, gelecekteki tehditlere karşı da hazırlıklı olmasını sağlayan bütüncül bir kalkandır.

- Yönetişim: Güvenlik stratejisini ve politikaları kurar.
- Risk Yönetimi: Tehditleri ölçer ve önceliklendirir.
- Uyumluluk: Kurumu yasal ve etik çerçevede güvence altına alır.
- Üçü bir araya geldiğinde, kurumlar sadece saldırılardan korunmakla kalmaz, aynı zamanda krizlere karşı daha dirençli, daha şeffaf ve daha güvenilir hale gelmektedir.

KAYNAKÇA

Uluçay, R. Savaş (2025). İşletmelerde Dijital Dönüşüm, BT Güvenliği, Yapay Zeka, VTN Yayıncılık

Pekel, Ahmet (2024). Siber Güvenlik Yönetimi Tehditler ve Önlemler, ODTÜ Yayıncılık

Uluçay, R. Savaş (2024). Bilgi Güvenliği, VTN Yayıncılık

Uluçay, R. Savaş (2024). Siber Güvenlik Terimleri Sözlüğü, VTN Yayıncılık

Uluçay, R. Savaş (2022). Siber Güvenlik Saldırı ve Savunma, VTN Yayıncılık

Unal Perendi. (2020, January 2). "*The GRC approach to Cyber Security"*. GOVERNIFY. Retrieved April 3, 2022, from https://governify.com/2020/01/02/the-grc-approach-to-cyber-security/

Swinhoe, D., & Hill, M. (2021, July 16). "*The 18 biggest Data breaches of the 21st Century"*. CSO Online. https://www.csoonline.com/article/2130877/the-biggest-Data-breaches-of-the-21st-century./

Cybersecurity & GRC Services HCL Technologies. "*Dynamic Cybersecurity*" www.hcltech.com. https://www.hcltech.com/cyber-security-grc-services

Hamilton, S., 2018. "*What is GRC And How It Empowers Cyber Security?* ". 360factors.com. https://www.360factors.com/Blog/what-is-GRc/

Hamilton, S., 2018. "*What is GRC And How It Empowers Cyber Security?* ". 360factors.com. https://www.360factors.com/Blog/What-is-grc/ .

Lindros, K. (Ed.). (2017, July 31). What is it governance? A formal way to align IT & business strategy. CIO. Retrieved April 6, 2022, from https://www.cio.com/article/272051/governanceit-governance-definition-and-solutions.html

"*Expert GRC Cyber Security Services*". ESecurity Solutions. https://www.esecuritysolutions.com/security-services/ Jacobs, P., von

Solms, S. and Grobler, M., 2016. "*Towards a framework for the growth of business cybersecurity capabilities.*" Cberuk.com https://cberuk.com/cdn/conference_proceedings/conference_40254.pdf

ITGI: '*Global Status Report on the Governance of Enterprise IT (GEIT)*' (ISACA & IT Governance Institute, 2011. 2011)

Polkard, C.E., Gupta, D., and Satzinger, J.W.: '*Teaching Systems Development*: A Compelling Case for Integrating the SDLC with the ITSM Lifecycle', Information Systems Management, 2010, 27, (2)

Hamaker, S.: '*Spotlight on Governance'*, Information Systems Control Journal, 2003,