Cybersecurity Specialization: Governance, Risk, and Compliance Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Siber güvenlik alanında yönetişim, risk yönetimi ve uyumluluk (GRC), kurumların dijital varlıklarını koruyabilmesi için kritik bir rol oynar. Günümüzde hızla değişen tehdit ortamı ve artan regülasyonlar, kurumların yalnızca teknik güvenlik önlemleriyle değil aynı zamanda güçlü bir yönetişim ve risk yönetimi yapısıyla hareket etmesini gerektirir.

Cybersecurity Specialization: Governance, Risk and Compliance eğitimi, kurumların yasal düzenlemelere ve sektör standartlarına uygun bir güvenlik yönetim sistemi kurabilmeleri için gerekli bilgi ve becerileri kazandırmayı hedefler.

Bu eğitim sayesinde katılımcılar:

- siber güvenlik yönetişim süreçlerini anlayabilir
- risk yönetimi stratejileri geliştirebilir
- uyumluluk gereksinimlerini analiz edebilir
- organizasyon içinde güvenlik kültürü oluşturabilir

Neden GRC (Governance, Risk ve Compliance) Önemlidir?

Modern organizasyonlarda siber güvenlik yalnızca IT departmanının sorumluluğu değildir. Kurumsal yönetişim yapısının bir parçası olarak risklerin belirlenmesi, değerlendirilmesi ve yönetilmesi gerekir.

GRC yaklaşımı sayesinde şirketler:

- regülasyonlara uyum sağlayabilir
- riskleri daha erken tespit edebilir
- güvenlik süreçlerini standartlaştırabilir
- kurum genelinde güvenlik farkındalığı oluşturabilir

Bu yaklaşım, özellikle finans, sağlık, teknoloji ve kamu sektörlerinde kritik önem taşır.

Prerequisites

Programa katılmadan önce aşağıdaki konularda temel bilgi sahibi olunması önerilir:

- siber güvenlik temelleri
- bilgi güvenliği prensipleri

Cybersecurity Specialization: Governance, Risk, and Compliance Eğitimi

Süre: **3 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

- IT altyapısı ve sistemleri hakkında genel bilgi

Özellikle **Cybersecurity Foundations** veya **CompTIA Security+ seviyesinde bilgi** katılımcıların eğitimden daha fazla verim almasını sağlar.

Who Should Attend

Bu program özellikle şu alanlarda çalışan profesyoneller için tasarlanmıştır:

- siber güvenlik uzmanları
- risk yönetimi profesyonelleri
- IT yöneticileri
- uyumluluk ve regülasyon ekipleri
- denetim ve iç kontrol uzmanları
- DevOps ve güvenlik mühendisleri

Ayrıca siber güvenlik yönetişimi alanında kariyer yapmak isteyen orta seviyedeki profesyoneller için de oldukça faydalıdır.

What You Will Learn

Program sonunda katılımcılar aşağıdaki konularda güçlü bir bilgi birikimi kazanır:

- IT regülasyonlarına dayalı uyumluluk risklerini analiz etmek
- kurumun risk toleransını belirleyen risk yönetimi stratejileri oluşturmak
- kontrol mekanizmaları ile desteklenen güvenlik politikaları geliştirmek
- organizasyonun risk olgunluk seviyesini artıracak yöntemler belirlemek
- kurum içinde güvenlik kültürünü güçlendirmek
- iş sürekliliği planlamasına katkı sağlamak
- risk yönetimi için uygun eGRC araçlarını seçmek

Outline

1. GRC Neden Önemlidir?

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Bu bölümde yönetişim, risk ve uyumluluk kavramlarının temel prensipleri ele alınır.

Konular:

- temel GRC terimleri
- varlık değeri ve bilgi varlıkları
- kurumlar için GRC yaklaşımının önemi

2. Sektörel Uyumluluk Standartları

Bu modülde kurumların uyması gereken sektörel standartlar incelenir.

Ele alınan bazı standartlar:

- PCI DSS
- Sarbanes-Oxley (SOX)
- FINRA
- GDPR

Ayrıca şirket politikaları ile uyumluluk süreçlerinin nasıl yönetileceği açıklanır.

3. Veri Gizliliği ve Uyumluluk

Bu bölüm veri gizliliği ile ilgili düzenlemeleri ele alır.

Örnek konular:

- kişisel veriler (PII)
- sağlık verileri (PHI)
- veri mimarisi
- veri işleme süreçleri
- şifreleme yöntemleri

HIPAA, HITECH ve GLBA gibi düzenlemeler de incelenir.

4. Risk Değerlendirme

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Risk analizi, siber güvenlik yönetiminin en kritik adımlarından biridir.

Bu modülde şu konular ele alınır:

- CIA üçlüsü (Confidentiality, Integrity, Availability)
- tehdit modelleme
- risk değerlendirme yöntemleri
- nicel ve nitel risk analizi
- risk olasılığı ve etki analizi
- iş etki analizi (BIA)

5. Risk Yönetimi

Risklerin nasıl yönetileceği bu bölümde detaylı şekilde ele alınır.

Başlıca konular:

- risk azaltma stratejileri
- riskten kaçınma
- risk transferi
- risk kabulü
- risk yönetim çerçeveleri
- sürekli izleme ve olay müdahalesi

6. Kurumsal Güvenlik Kültürü

Başarılı bir siber güvenlik programı yalnızca teknoloji ile değil, aynı zamanda kurum kültürü ile de ilgilidir.

Bu bölümde ele alınan konular:

- kurum genelinde güvenlik farkındalığı
- güvenlik politikaları
- çalışan davranışları
- güvenlik eğitimleri

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

7. Yönetişim ve Politika Yönetimi

Bu modülde kurumların güvenlik politikalarını nasıl oluşturacağı ve yöneteceği ele alınır.

Konular:

- iş sürekliliği planı (BCP)
- felaket kurtarma planı (DRP)
- tek hata noktası (single point of failure)
- yedeklilik
- organizasyonel sorumluluk modelleri

8. GRC Araçları ve Teknolojileri

Bu bölümde kurumsal risk yönetimini destekleyen araçlar incelenir.

Örnek araçlar:

- eGRC platformları
- risk raporlama sistemleri
- uyumluluk yönetim araçları