Cybersecurity Specialization: Governance, Risk, and Compliance Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Overview

Governance, Risk, and Compliance (GRC) has become a critical component of modern cybersecurity strategies. As cyber threats evolve and regulatory requirements increase, organizations must establish structured governance frameworks to ensure security, accountability, and compliance.

The Cybersecurity Specialization: Governance, Risk and Compliance program provides professionals with the knowledge needed to design and implement governance structures that align with legal requirements and security best practices.

Participants will gain the ability to:

- understand cybersecurity governance frameworks
- develop effective risk management strategies
- interpret regulatory compliance requirements
- strengthen organizational security culture

Why Governance, Risk, and Compliance Matters

In modern organizations, cybersecurity is not limited to technical teams. Governance and risk management must be integrated across the entire organization.

A strong GRC framework helps organizations:

- maintain regulatory compliance
- identify and manage risks early
- standardize security processes
- promote organization-wide security awareness

This approach is particularly important in industries such as finance, healthcare, technology, and government.

Prerequisites

Before attending this program, participants are recommended to have basic knowledge in the following areas:

- cybersecurity fundamentals
- information security principles

Cybersecurity Specialization: Governance, Risk, and Compliance Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- general IT infrastructure concepts

Knowledge equivalent to **Cybersecurity Foundations** or **CompTIA Security+ level** is beneficial for getting the most out of the course.

Who Should Attend

This program is designed for professionals working in areas such as:

- cybersecurity operations
- risk management
- IT leadership
- compliance and governance
- auditing and internal control
- DevOps and security engineering

It is also valuable for mid-career professionals who want to strengthen their expertise in cybersecurity governance.

What You Will Learn

By the end of this program participants will be able to:

- develop strategies to mitigate compliance risks related to IT regulations
- contribute to organizational risk management frameworks
- design security policies supported by effective controls
- improve an organization's risk maturity level
- strengthen enterprise-wide security culture
- contribute to business continuity planning
- evaluate and select eGRC tools for risk management

Outline

1. Why GRC Matters

Cybersecurity Specialization: Governance, Risk, and Compliance Training

BILGINC IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Duration: **3 Day**

Introduction to key concepts of governance, risk, and compliance.

Topics include:

- fundamental GRC terminology
- asset value and information assets
- the growing importance of governance and compliance

2. Industry Compliance Standards

This module explores major regulatory frameworks that influence cybersecurity governance.

Examples include:

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

3. Privacy Compliance

This section focuses on privacy regulations and data protection principles.

Key topics include:

- personally identifiable information (PII)
- protected health information (PHI)
- data architecture and handling
- encryption methods

4. Risk Assessment

Risk assessment is a core component of cybersecurity governance.

Topics include:

- CIA triad

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- threat modeling
- quantitative vs qualitative risk assessment
- business impact analysis (BIA)

5. Risk Management

This module explores strategies for managing and mitigating cybersecurity risks.

Topics include:

- risk mitigation strategies
- risk avoidance and transfer
- risk management frameworks
- continuous monitoring and incident response

6. Corporate Security Culture

A strong cybersecurity program depends on organizational culture as much as technology.

Topics include:

- enterprise security awareness
- security policies
- employee engagement in security practices

7. Governance and Policy Management

This module focuses on governance processes and policy implementation.

Topics include:

- business continuity planning (BCP)
- disaster recovery planning (DRP)
- redundancy strategies

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- organizational accountability models

8. GRC Tools and Technologies

This section introduces tools used to support governance, risk, and compliance management.

Examples include:

- eGRC platforms
- compliance reporting tools
- risk monitoring systems