BLACKBIRD FOR TRAINING

Cybersecurity Governance, Risk, and Compliance (GRC)

3 – 7 October 2027
Online



Cybersecurity Governance, Risk, and Compliance (GRC)

Ref: 3254809_212534 **Date:** 3 – 7 October 2027 **Location:** Online **Fees:** 2700 GBP

Introduction

In the rapidly evolving digital landscape, cybersecurity governance has become a critical priority for organizations aiming to protect their digital assets, maintain regulatory compliance, and manage cyber risks effectively. This comprehensive training course is designed to equip professionals with the necessary skills to manage cybersecurity governance, cybersecurity risk management, and compliance GRC frameworks in alignment with global standards like ISO 27001, NIST, GDPR, and COBIT.

Participants will learn how to design and implement integrated GRC programs, perform risk analysis, and ensure regulatory compliance through real-world examples, simulations, and practical exercises. This program empowers attendees to proactively identify, assess, and mitigate cybersecurity risks, ensuring robust cybersecurity governance solutions that support business continuity and regulatory confidence.

Course Objectives

By the end of this course, participants will be able to:

- Understand the core principles of cybersecurity governance and how it aligns with organizational strategy.
- Apply national and international legal and regulatory requirements to information security and cybersecurity compliance.
- Design and implement an effective GRC framework that aligns with global cybersecurity compliance standards.
- Perform cyber risk governance and analysis to identify vulnerabilities and mitigate risks effectively.
- Improve cybersecurity maturity through continuous monitoring, reporting, and audit readiness.
- Communicate cybersecurity governance strategies to executive leadership and stakeholders effectively.

Course Outlines

Day 1 - Cybersecurity Governance Foundations

- Introduction to cybersecurity governance and its strategic importance.
- Overview of key cybersecurity frameworks: NIST, ISO 27001, COBIT.
- Defining roles, responsibilities, and accountability within GRC structures.
- Developing organizational cybersecurity strategies and policies.
- Integrating GRC with enterprise IT governance to enhance cybersecurity compliance.



Day 2 - Risk Management Principles

- Understanding the cybersecurity risk management lifecycle.
- Techniques for identifying and assessing cyber risks in various environments.
- Selecting appropriate risk treatment and mitigation options.
- Comparing quantitative vs. qualitative risk assessments.
- Using risk registers and visual dashboards for ongoing tracking and decision-making.

Day 3 - Compliance and Legal Aspects

- Overview of global regulatory standards: GDPR, HIPAA, SOX.
- Addressing legal and ethical issues in cybersecurity compliance.
- Preparing for and managing compliance audits efficiently.
- Understanding privacy regulations and data handling obligations.
- Aligning cybersecurity compliance with corporate strategy and operations.

Day 4 - Operationalizing GRC

- Building and maintaining a cybersecurity GRC program aligned with global cybersecurity compliance.
- Automating compliance and risk workflows using GRC tools.
- Planning for incident response and managing cyber crises effectively.
- Integrating GRC with business continuity and disaster recovery strategies.
- Communicating GRC status and risks to executives and boards with clarity.

Day 5 - Case Studies, Assessment & Roadmap

- Reviewing real-world cybersecurity GRC implementations.
- Conducting a simulated risk assessment and control mapping.
- Group workshop: designing a tailored GRC framework.
- Knowledge check and optional certification exam.
- Creating a personal or organizational GRC roadmap for strategic planning.



Why Attend This Course: Wins & Losses!

- Master Cybersecurity Governance: Understand how cybersecurity governance aligns with organizational strategy and compliance requirements.
- Develop Proactive Cyber Risk Management Strategies: Learn to identify, assess, and mitigate cybersecurity risks before they become critical.
- Enhance Global Cybersecurity Compliance: Apply international standards such as ISO 27001, NIST, and GDPR confidently.
- Boost Regulatory Confidence: Prepare for compliance audits and maintain strong cybersecurity compliance solutions.
- Strengthen Business Continuity Plans: Ensure business continuity with effective cybersecurity governance solutions and disaster recovery planning.
- Communicate Cyber Risks Effectively: Gain the skills to report cybersecurity performance and risk levels to stakeholders and executive boards.

Conclusion

This course is a vital investment for professionals in cybersecurity, IT risk management, audit, and compliance. It equips participants with the knowledge and tools to design and implement effective GRC programs that align with global cybersecurity governance standards.

By the end of the program, attendees will be capable of leading secure and compliant digital environments that support business continuity, regulatory confidence, and long-term resilience.

Join this course to become a leader in cybersecurity governance, mastering the skills to protect your organization's digital assets, ensure compliance, and mitigate cyber risks effectively.

