MERCURY

GRC Cyber Security Training Course

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

GRC Cyber Security Training Course

Introduction:

The GRC Cyber Security training course introduces Governance, Risk Management, and Compliance GRC principles within cybersecurity. Participants will learn the knowledge and skills to manage cyber risks effectively, ensure compliance with regulatory requirements, and implement robust governance structures. They will explore the interplay between governance, risk, and compliance, focusing on how they can be integrated to strengthen an organization's cybersecurity posture.

Through a combination of theoretical insights and practical applications, this GRC Cyber Security course prepares professionals to navigate the complexities of cyber threats in today's digital landscape, ensuring that their organizations are protected and compliant with industry standards. The acronym GRC stands for Governance, Risk Management, and Compliance in this digital era. It plays a role in the cybersecurity sector.

Understanding what GRC means in the context of cyber security is crucial for any professional wishing to develop expertise in this area. In this GRC Cyber Security course, participants will understand GRC applications within cybersecurity and learn how these three components work synergistically to protect an organization's information assets.

Discover how GRC tools can fortify cybersecurity measures, streamline compliance processes, and deliver structured methods for managing the landscape of risks. In this GRC Cyber Security course, participants will get hands-on experience with various GRC tools, providing practical skills to enhance their role as cybersecurity GRC analysts and contributing to a robust cybersecurity GRC framework for their organizations.

Targeted Groups:

- Chief Information Security Officers CISOs.
- IT Governance Managers.
- Risk Management Professionals.
- Compliance Officers.
- Cybersecurity Analysts.
- Information Security Managers.
- IT Auditors.
- Data Protection Officers.
- Legal and Regulatory Professionals in Cybersecurity.
- Senior IT and Security Executives.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

Course Objectives:

At the end of this GRC Cyber Security course, the participants will:

- Understand cybersecurity's Governance, Risk Management, and Compliance GRC principles.
- Identify and assess cyber risks within an organization.
- Develop and implement effective cybersecurity policies and procedures.
- Ensure compliance with industry regulations and standards.
- Integrate GRC practices to enhance cybersecurity frameworks.
- Prepare for and manage cybersecurity incidents and breaches.
- Align cybersecurity strategies with organizational goals and governance structures.
- Evaluate and improve existing cybersecurity controls and measures.
- Foster a culture of compliance and risk awareness within the organization.
- Utilize best practices for data protection and privacy management.

Targeted Competencies:

By the end of this GRC Cyber Security training, participants' competencies will:

- Cyber Risk Assessment and Management.
- Regulatory Compliance Understanding.
- Information Security Governance.
- Policy Development and Implementation.
- Threat and Vulnerability Management.
- Incident Response Planning.
- Cybersecurity Frameworks and Standards.
- Internal Audit and Control.
- Data Privacy and Protection Strategies.
- Strategic Decision-Making in Cybersecurity.

Course Content:

Unit 1: Introduction to GRC in Cybersecurity:

- Define the concepts of Governance, Risk Management, and Compliance GRC.
- Explore the role of GRC in strengthening cybersecurity frameworks.
- Understand the interrelationships between governance, risk, and compliance.
- Examine the importance of GRC in the modern cyber threat landscape.
- Identify key regulatory frameworks and standards relevant to GRC.

Unit 2: Cyber Risk Management:

- Learn the process of identifying and assessing cyber risks.
- Analyze different types of cyber threats and vulnerabilities.
- Develop risk mitigation strategies to address identified risks.
- Implement risk management frameworks aligned with organizational goals.
- Explore the use of risk assessment tools and methodologies.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Unit 3: Compliance and Regulatory Requirements:

- Understand the key regulations affecting cybersecurity compliance.
- Explore global cybersecurity laws and standards, such as GDPR, HIPAA, and ISO 27001.
- Develop strategies to ensure compliance with legal and regulatory requirements.
- Implement compliance monitoring and reporting processes.
- Understand the role of audits in maintaining cybersecurity compliance.

Unit 4: Governance and Policy Development:

- Explore the principles of cybersecurity governance.
- Develop and implement cybersecurity policies and procedures.
- Align cybersecurity governance with overall corporate governance.
- Understand the role of leadership in establishing effective governance.
- Review case studies on successful cybersecurity governance frameworks.

Unit 5: Incident Response and Management:

- Learn the fundamentals of cybersecurity incident response.
- Develop an effective incident response plan IRP.
- Understand the roles and responsibilities within an incident response team.
- Explore the steps to detect, respond to, and recover from a cyber incident.
- Examine post-incident activities, including reporting and continuous improvement.