€TRAINING

Chief Information Security Officer CISO

18 - 22 November 2024
Kuala Lumpur (Malaysia)

Chief Information Security Officer CISO

REF: B1940 DATE: 18 - 22 November 2024 Venue: Kuala Lumpur (Malaysia) - Fee: 5850 Euro

Introduction:

This program is designed to prepare participants for the certification exam only.

This training program equips participants with the essential skills and knowledge required to excel in the role of a Chief Information Security Officer CISO. It focuses on strategic cybersecurity leadership, risk management, and ensuring alignment with organizational objectives.

Program Objectives:

At the end of this program, participants will be able to:

- Understand the role and responsibilities of a Chief Information Security Officer CISO.
- Develop and implement effective cybersecurity strategies aligned with business goals.
- Lead and manage cybersecurity teams to safeguard organizational assets.
- Conduct risk assessments and establish robust security controls.
- Communicate cybersecurity risks and strategies to senior management and stakeholders effectively.
- Prepare for the certification exam.

Targeted Audience:

- Current and aspiring Chief Information Security Officers CISOs.
- Senior IT Managers and Directors.
- Cybersecurity Professionals aiming for leadership roles.
- Risk and Compliance Managers.

Program Outline:

Unit 1:

Introduction to CISO Role and Responsibilities:

- Overview of the Chief Information Security Officer CISO role.
- Importance of cybersecurity leadership in modern organizations.

- Responsibilities and expectations of a CISO.
- Relationship between cybersecurity and business strategy.
- Ethical considerations and professional standards for CISOs.

Unit 2:

Cybersecurity Governance and Frameworks:

- Implementing cybersecurity governance frameworks NIST Cybersecurity Framework, ISO/IEC 27001.
- Establishing cybersecurity policies, standards, and procedures.
- Roles and responsibilities of cybersecurity governance committees.
- Compliance requirements and regulatory frameworks GDPR, HIPAA.
- Continuous monitoring and auditing of cybersecurity controls.

Unit 3:

Cyber Risk Management:

- Principles of cyber risk management and assessment.
- Conducting cybersecurity risk assessments and gap analysis.
- Developing risk mitigation strategies and action plans.
- Incident response planning and management.
- Business continuity and disaster recovery planning.

Unit 4:

Leading Cybersecurity Teams:

- Building and leading high-performing cybersecurity teams.
- Talent acquisition, development, and retention strategies.
- Collaboration with IT, legal, and business units.
- Effective communication and stakeholder engagement.
- Promoting a culture of cybersecurity awareness and accountability.

Unit 5:

Strategic Cybersecurity Planning and Execution:

- Developing and implementing a cybersecurity strategy aligned with organizational objectives.
- Budgeting and resource allocation for cybersecurity initiatives.
- Evaluating and selecting cybersecurity technologies and solutions.
- Measuring cybersecurity performance and effectiveness.
- Case studies and simulations of real-world cybersecurity challenges.
- Prepare for the certification exam.

Note: This program is designed to prepare participants for the certification exam only.