€TRAINING

Chief Information Security Officer CISO

1 - 5 December 2024
Cairo (Egypt)

Chief Information Security Officer CISO

REF: B1940 DATE: 1 - 5 December 2024 Venue: Cairo (Egypt) - Fee: 4095 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 of a CISO and align cybersecurity leadership with business strategy.

- Implement effective cybersecurity governance, manage risks, and ensure regulatory compliance.

- Develop and execute strategic cybersecurity plans, including incident management and performance measurement.

- Lead high-performing cybersecurity teams and promote a culture of accountability and awareness.

- 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 the CISO Role and Cybersecurity Leadership:

- Overview of the Chief Information Security Officer CISO role and responsibilities.

- The importance of cybersecurity leadership in modern organizations.

- Aligning cybersecurity initiatives with broader business strategies.

- Ethical considerations and professional standards for CISOs.

- Balancing cybersecurity with business objectives and operational needs.

- The evolving role of CISOs in response to emerging cyber threats.

Unit 2:

Cybersecurity Governance, Risk Management, and Compliance:

- Methods of implementing cybersecurity governance frameworks NIST, ISO/IEC 27001.

- Establishing cybersecurity policies, standards, and operational procedures.

- Conducting comprehensive cyber risk assessments and gap analysis techniques.

- Compliance requirements: GDPR, HIPAA, and other regulatory frameworks.

- Developing risk mitigation strategies and implementing control measures.

- Continuous monitoring, auditing, and improving cybersecurity controls.

Unit 3:

Strategic Cybersecurity Planning and Incident Management:

- Developing a cybersecurity strategy aligned with organizational goals.

- Budgeting and allocating resources for cybersecurity initiatives.

- Incident response planning and management: preparation and execution.

- Business continuity and disaster recovery in case of cyber incidents.

- Evaluating and selecting cybersecurity technologies and solutions.

- Measuring cybersecurity performance, metrics, and effectiveness.

Unit 4:

Leading and Building Effective Cybersecurity Teams:

- Strategies of building and leading high-performing cybersecurity teams.

- Talent acquisition, development, and retention strategies in cybersecurity.

- Fostering collaboration between cybersecurity, IT, legal, and business units.

- Importance of effective communication and stakeholder engagement for cybersecurity awareness.

- Promoting a culture of cybersecurity accountability and vigilance.

- Enhancing team capabilities through continuous learning and skill development.

Unit 5:

Certification Exam Preparation:

- Detailed review of the exam requirements.

- Review of key topics and concepts covered in the certification syllabus.

- Sample questions and their potential answers.

- Resources and materials for further study.

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