CISO — Chief Information Security Officer

Duration: 5 Days

Language: en

Course Code: MG2 - 214

Objective

Participants in this course will be able to:

- Understand the evolving responsibilities and strategic importance of the CISO role.
- Establish and lead enterprise cybersecurity frameworks.
- Analyse emerging threats and implement robust defence strategies.
- Design and lead incident response and crisis management plans.
- Ensure regulatory compliance with global standards (e.g., GDPR, NIS2, ISO/IEC 27001).
- Engage and communicate effectively with executive teams, regulators, and the board.
- Integrate cybersecurity strategy with business continuity and digital transformation goals.

Audience

This course is ideal for:

- Existing and aspiring Chief Information Security Officers (CISOs).
- Information Security Managers and Directors.
- IT Governance and Risk Executives.
- Chief Technology Officers (CTOs).
- Heads of Compliance and Regulatory Affairs.
- Cybersecurity Consultants and Advisors.
- Board Members and Senior Executives involved in security oversight.

Training Methodology

This course uses a blend of interactive lectures, real-world case studies, cyber incident simulations, group discussions, and strategic planning exercises. It is delivered using adult learning principles that enhance comprehension, application, and retention of advanced security leadership concepts. Participants will also receive templates, risk registers, and frameworks applicable to real-world organisational settings.

Summary

This advanced training course is designed for current and aspiring Chief Information Security Officers (CISOs) who are responsible for establishing, managing, and scaling enterprise cybersecurity frameworks. The course explores the evolving threat landscape, regulatory compliance, incident response planning, risk governance, and the CISO's strategic role in aligning cybersecurity with business objectives. Participants will gain the skills to lead cybersecurity operations while fostering a culture of security throughout the organisation.

By the end of the course, participants will be equipped with the knowledge and tools to protect enterprise assets, lead cross-functional security initiatives, and confidently advise boards and executive stakeholders on cyber risk and resilience.

Course Content & Outline

Section 1: The Evolving Role of the CISO

- Defining the CISO’s mandate and reporting structure.
- Cybersecurity trends and executive-level responsibilities.
- Building a strategic cybersecurity vision aligned with business goals.
- Maturity models and the CISO’s journey: reactive to proactive.
- CISO vs CIO vs CTO roles – coordination and boundary setting.

Section 2: Enterprise Security Frameworks & Risk Governance

- Designing an enterprise cybersecurity framework (NIST, ISO, COBIT).
- Risk identification, quantification, and control mapping.
- Third-party and supply chain risk management.
- Building a cyber risk register and board-level dashboards.
- Cyber insurance: coverage, limitations, and evaluation.

Section 3: Threat Intelligence, Detection & Defence

- Understanding modern threats: APTs, ransomware, insider threats.
- Threat intelligence lifecycle and threat hunting techniques.
- SOC maturity and incident detection capabilities.
- Endpoint and network protection strategies.
- Zero trust architecture and segmentation.

Section 4: Crisis Management & Compliance Leadership

- Building and testing incident response and disaster recovery plans.
- Regulatory frameworks: GDPR, HIPAA, NIS2, PCI DSS, ISO 27001.
- Conducting cyber drills, tabletop exercises, and breach simulations.
- Developing a compliance and audit readiness framework.
- Managing communication and stakeholder trust during breaches.

Section 5: Strategic Alignment, Culture, and Reporting

- Developing a cybersecurity culture: training and awareness strategies.
- Aligning cyber strategy with digital transformation and resilience.
- Board reporting: translating cyber risk into business language.

- KPIs, KRIs, and ROI of cybersecurity programs.
- Final Simulation: Leading a cybersecurity crisis from boardroom to SOC.

Certificate Description

Upon successful completion of this training course, delegates will be awarded a Holistique Training Certificate of Completion. For those who attend and complete the online training course, a Holistique Training e-Certificate will be provided.

Holistique Training Certificates are accredited by The CPD Certification Service (CPD), and are certified under ISO 9001 and ISO 29993 standards.

CPD credits for this course are granted by our Certificates and will be reflected on the Holistique Training Certificate of Completion. In accordance with the standards of The CPD Certification Service, one CPD credit is awarded per hour of course attendance. A maximum of 50 CPD credits can be claimed for any single course we currently offer.

Categories

Management & Leadership, Technology, IT & Computer Application

Tags

Information Security Management, Cybersecurity, C-suite, Chief Information Security Officer, CISO

Related Articles

Information Security: Its Importance and Types in Protecting Data and Systems