HDTC Training Center

Provide

Technical proposal of the Training program

Cyber Governance, Risk, and Compliance (Cyber GRC)

9200 15661 | +966 55 744 4070 | info@hdtc-ksa.com | www.hdtc-ksa.com
+971 4 220 8780 | +971 52 937 6837 | info@hdtc.ae | www.hdtc.ae

Course Overview:

This training program provides a comprehensive understanding of Cybersecurity Governance, Risk Management, and Compliance (GRC) frameworks. Participants will learn how to align cybersecurity practices with business objectives, manage risks effectively, and ensure compliance with regulatory standards and industry frameworks. The course bridges the gap between cybersecurity, business strategy, and regulatory requirements.

General Objective:

To equip participants with the knowledge and skills required to implement and manage effective cyber governance, risk management, and compliance strategies within organizations.

Program Objectives:

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

- Understand the core concepts of Cyber GRC and its significance in modern organizations.
- Analyze and manage cyber risks using recognized risk management frameworks.
- Design and implement cybersecurity governance structures aligned with organizational goals.
- Interpret and apply key regulations and standards (e.g., ISO 27001, NIST, GDPR).
- Integrate GRC practices into business and IT processes.
- Conduct effective audits and compliance assessments.
- Develop policies, procedures, and controls to support GRC programs.

Program Outlines:

Day 1 Introduction to Cyber GRC

- Overview of cybersecurity trends and challenges
- Key definitions: Governance, Risk, Compliance
- Importance of GRC in enterprise cybersecurity
- Introduction to frameworks (ISO, NIST, COBIT, etc.)

Day 2 Cybersecurity Governance

- Building a governance structure for cybersecurity
- Roles and responsibilities (CISO, IT, Board, etc.)
- Policies, standards, and strategic alignment
- Cybersecurity maturity models

Day 3: Risk Management

- Risk identification and assessment techniques
- Risk registers and impact-likelihood matrices
- Risk treatment and mitigation strategies
- Business Continuity and Disaster Recovery (BC/DR)

Day 4: Regulatory Compliance & Standards

- Overview of global and regional regulations:
    - GDPR, HIPAA, PCI-DSS, NCA ECC, etc.
- ISO/IEC 27001 & NIST CSF frameworks
- Mapping compliance to operational controls
- Internal auditing and assessment

Day 5: Integrated GRC Program and Final Workshop

- Designing an enterprise GRC strategy
- Tools and platforms for GRC (e.g., RSA Archer, ServiceNow)
- Case studies and group exercises
- Final project: Simulating a GRC implementation plan

Target Audience:

- Information Security Officers (ISOs & CISOs)
- Risk and Compliance Officers
- IT Governance Professionals
- Auditors and Internal Control Managers
- Cybersecurity Consultants
- Legal and Regulatory Officers
- Professionals pursuing a role in cybersecurity management

Training methods:

- Technology-Based Learning.
- Simulation in Training.
- On-the-job guidance.
- Trainer-Led Training.
- Work Teams and Roles.
- Films and Videos.
- Case Studies and Workshops.