Certified Information Security Manager (CISM)

Course Duration: 10 Days

Course Overview

In this course, students will establish processes to ensure that information security measures align with established business needs.

Who Should Attend?

The intended audience for this course is information security and IT professionals, such as network administrators and engineers, IT managers, and IT auditors, and other individuals who information about information security management, who are looking for career advancement in IT security, or who are interested in earning the CISM certification.

Course Objectives

- Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations. Identify and manage information security risks to achieve business objectives. Create a program to implement the information security strategy.
- Implement an information security program. Oversee and direct information security activities to execute the information security program. Plan, develop, and manage capabilities to detect, respond to, and recover from information security incidents.

Course Outline

1 - Information Security Governance

- Establish and maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and ongoing management of the information security program.
- Establish and maintain an information security governance framework to guide activities that support the information security strategy.
- Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program.
- Establish and maintain information security policies to communicate management's directives and guide the development of standards, procedures and guidelines.
- Develop business cases to support investments in information security.
- Identify internal and external influences to the organization (for example, technology, business environment, risk tolerance, geographic location, legal and regulatory

requirements) to ensure that these factors are addressed by the information security strategy.
- Obtain commitment from senior management and support from other stakeholders to maximize the probability of successful implementation of the information security strategy.
- Define and communicate the roles and responsibilities of information security throughout the organization to establish clear accountabilities and lines of authority.
- Establish, monitor, evaluate and report metrics (key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs]) to provide management with accurate information regarding the effectiveness of the information security strategy.

2 - Information Risk Management and Compliance

- Establish and maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value.
- Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.
- Ensure that risk assessments, vulnerability assessments and threat analyses are conducted periodically and consistently to identify risk to the organization's information.
- Determine appropriate risk treatment options to manage risk to acceptable levels.
- Evaluate information security controls to determine whether they are appropriate and effectively mitigate risk to an acceptable level.
- Identify the gap between current and desired risk levels to manage risk to an acceptable level.
- Integrate information risk management into business and IT processes (for example, development, procurement, project management, mergers and acquisitions) to promote a consistent and comprehensive information risk management process across the organization.
- Monitor existing risk to ensure that changes are identified and managed appropriately
- Report noncompliance and other changes in information risk to appropriate management to assist in the risk management decision-making process.

3 - Information Security Program Development and Management

- Establish and maintain the information security program in alignment with the information security strategy.
- Ensure alignment between the information security program and other business functions (for example, human resources [HR], accounting, procurement and IT) to support integration with business processes.
- Identify, acquire, manage and define requirements for internal and external resources to execute the information security program.
- Establish and maintain information security architectures (people, process, technology) to execute the information security program.

- Establish, communicate and maintain organizational information security standards, procedures, guidelines and other documentation to support and guide compliance with information security policies.
- Establish and maintain a program for information security awareness and training to promote a secure environment and an effective security culture.
- Integrate information security requirements into organizational processes (for example, change control, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security baseline.
- Integrate information security requirements into contracts and activities of third parties (for example, joint ventures, outsourced providers, business partners, customers) to maintain the organization's security baseline.
- Establish, monitor and periodically report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

4 - Information Security Incident Management

- Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate identification of and response to incidents.
- Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents.
- Develop and implement processes to ensure the timely identification of information security incidents.
- Establish and maintain processes to investigate and document information security incidents to be able to respond appropriately and determine their causes while adhering to legal, regulatory and organizational requirements.
- Establish and maintain incident escalation and notification processes to ensure that the appropriate stakeholders are involved in incident response management.
- Organize, train and equip teams to effectively respond to information security incidents in a timely manner.
- Test and review the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities.
- Establish and maintain communication plans and processes to manage communication with internal and external entities.
- Conduct post-incident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions.
- Establish and maintain integration among the incident response plan, disaster recovery plan and business continuity plan.

Plus, Exam Preparation Session

OA, *Information Security expert*

Mr. OA is an Information Security expert with more than 15 years of industry experience. Over the last 10 years, his focus has been on Security Assessments, Risk Management, IT Governance, Information Security Program Maturity, Disaster Recovery and Business Continuity. He has consulted and conducted training for many large customers in the Middle East and Africa across various industries, and still acts as an advisor for selected clients within the region. As the Director Cyber Security Academy, OA leads a team of consultants developing practical contents in different domains in information security. Before joining IT Security C&T, he was part of the Intel Security(McAfee)/Found stone team in EMEA, helping customers in the region improve their security posture and resilience to cyber-attacks. As Director of Found stone Services EMEA, OA was responsible for managing the EMEA team conducting assessments and emergency incident response services out of the Dubai offices.

OA has been a public speaker in several regional events such as IDC and BCI Middle East Summit, CIO East Africa, $(ISC)^2$ and others. He is also associated with international organizations like $(ISC)^2$, Mile2, ISACA, BCI, BSI, and EC|Council. He holds multiple international certifications, and as a trainer has been delivering IT & IT Security training across multiple geos. He has taught internationally recognized certification programs such as Novell's CNE and Microsoft's MCSE, and has worked as a Senior Consultant with a wide array of companies leading major projects.

Accreditation and Certifications:

- Bachelor's Degree in management of Information Systems (MIS), Rochville University, Florida
- Certified Business Continuity Institute (CBCI)
- BS25999 Lead Auditor (BSI)
- Certified Information Systems Security Professional (CISSP), $(ISC)^2$
- Certified Information Security Manager (CISM), ISACA
- Certified Information Systems Auditor (CISA), ISACA
- Member of the BCI Middle East Working Group
- Certified Ethical Hacker (CEH), EC-Council
- Certified Hacking Forensics Investigator (CHFI), EC-Council
- EC-Council Certified Security Analyst (ECSA), EC-Council
- Juniper Networks Certified Internet Specialist (JNCIS-FWV), Juniper
- Juniper Network Certified Internet Associate (JNCIA-IDP), Juniper
- Microsoft Certified Systems Engineer (MCSE), Microsoft
- Certified Novell Engineer (CNE), Novell
- Certified and Authorized Instructor for the following:
  - Certified Information Systems Security Professional – CISSP
  - Systems Security Certified Professional – SSCP
  - Mile2: CIHE, CDRE, CDFE, CPTE
  - Certified Business Continuity Institute (CBCI)
  - Ethical Hacking – CEH
  - Certified Hacking Forensics Investigator – CHFI
  - EC-Council Certified Security Analyst/Licensed Penetration Tester – ECSA/LPT
  - Security Principles – SP
  - Network & Host Security – N&H Security
  - Microsoft – MCT
  - Novell - CNI

Standards and Frameworks

- BCI – GPG
- BS 25999
- ISO 22301
- TOGAF 9.1
- ISO 27001
- NIST
- ISO 31000
- COBIT
- ITIL
- ISO 20000

Public Speaking:

CIO East Africa – CIO Series 2016, Nairobi, Kenya

IDC IT Security Roadshow 2015, Dec, Riyadh, Saudi Arabia

Panelist at the Middle East BCM Summit 2012 – Abu Dhabi - UAE

IDC IT Security Roadshow 2011, May 2011, Jeddah, Saudi Arabia. “Risk Management in the Era of Mobile Devices”

IDC IT Security Roadshow 2011, June 2011, Riyadh, Saudi Arabia. “Risk Management in the Era of Mobile Devices”

Application Security Technical Day, Dec 2010, Saudi Aramco, Dhahran, Saudi Arabia “Secure Coding Case Study”