Course 1 – Security Awareness Training for Executives (SATE)

Duration – 1 day

Course Content – Course will give attendees a realistic view of the current threat landscaping that shall lead executives for a better understanding of what Information security means, what needs to be protected and the legal obligations. Attendees will gain expertise on how to address security incidents within the organisation. Furthermore, the course will help executives in adopting Cyber hygiene within their professional and personal life.

Who is this course for?

The course is intended for business owners and executives whom their business operation is connected to the cyber space.

Agenda:

1. **Introduction – Threat Landscape**
    a. The world around us
    b. Examples of incidents
    c. Cost of incidents
    d. Attacker's viewpoint

2. **Fundamentals of Cyber Security**
    a. Technical Terms
    b. Understanding Information security and privacy basics
    c. What needs to be protected and why

3. **The Role of the Executive**
    a. Executives' legal and operational responsibilities
    b. GDPR compliance
    c. Risk management fundamentals

4. **How / Why did they get hacked?**
    a. Case studies of internal and external attacks

5. **The Internal Threat**
    a. A deep dive into the risk associated with internal threat actors (employees)
    b. Brand reputation impact from leakage to Social networks

6. **Security Incidents – Preparing, Responding and Recovering**
    a. How to plan for an incident
    b. Measures to implement in order to recover from an incident

7. **Securing the Executives**
    a. Cyber hygiene' – Practical tips and guidelines for security in the daily, personal and family life of the executive

Course 2 – The Certified Information Systems Auditor (CISA) certification[1]

Duration – 4 days

Course Content – Course is aligned with ISACA and will give attendees the tools to take the official exam. It will give attendees the skillsets to govern and control enterprise IT and perform an effective security audit on any organisation. Attendees will gain expertise in the acquisition, development, testing, and implementation of information systems and learn the guidelines, standards and best practices of protecting them.

Who is the course for?

The course is intended for professionals who have a minimum of 5 years of professional work experience in information systems auditing, control or security.

Agenda:

Day 1

1. **The Process of Auditing Information Systems**
    a. Risk-based IS Audit Strategy
    b. Plan Audits
    c. Conduct Audits
        i. Process & Procedures
        ii. Important Concepts
    d. Control Self-Assessments (CSA)
    e. Communicate Audit Results & Follow-up

2. **Governance & Management of IT**
    a. Evaluate the IT Strategy
    b. Evaluate the IT Governance Structure
    c. Evaluate the IT Organisation Structure & HR Management, IT Policies, Standards, & Procedures
    d. Evaluate IT Resource Management & IT Portfolio Management
    e. Evaluate Risk Management Practices & IT Management
    f. Evaluate Controls & KPIs
    g. Evaluate the Organisation's BCP

Day 2

3. **Information Systems Acquisition, Development, & Implementation**
    a. Evaluate the Business Case for Proposed Investments

[1] *ISACA exam & certificate are not included and can be taken up directly with ISACA.*

b. Evaluate the IT Supplier Selection & Contract Management Processes
c. Evaluate the Project Management Framework
d. Conduct Project Reviews
e. Virtualization & Cloud Service Provider (CSP) Architecture
f. Evaluate Controls for Information Systems during Acquisition
g. Evaluate Readiness for Implementation
h. Conduct Post-Implementation Reviews

Day 3

4. Information Systems Operations, Maintenance, & Service Management

a. Evaluate IT Service Management Framework & Practices
b. Conduct Periodic Reviews of Information Systems
c. Evaluate IT Operations & IT Maintenance
d. Evaluate Database Management Practices & Data Quality
e. Evaluate Problem & Incident Management
f. Change and Release Management Practices
g. Evaluate End User Computing, & IT Continuity & Resilience
h. Disaster Recovery Testing

Day 4

5. Protection of Information Assets

a. Evaluate Information Security & Privacy
b. Evaluate Physical & Environmental Controls
c. Evaluate the System & Logical Security Controls
d. Evaluate Data Classification & Information Asset Safeguards
e. Evaluate Information Security Programs

6. Mock exams

After completing this course, the student will be able to:

- Prepare for the Certified Information Systems Auditor (CISA) exam
- Develop and implement a risk-based IT audit strategy in compliance with IT audit standards
- Evaluate the effectiveness of an IT governance structure
- Ensure that the IT organisational structure and human resources (personnel) management support the organisation's strategies and objectives
- Review the information security policies, standards, and procedures for completeness and alignment with generally accepted practices

Course 3 – The Certified Information Security Manager (CISM) certification [1]

Duration – 4 days

Course Content – Course will give attendees the requisite skillsets to design, deploy and manage security architecture for your organisation. The course is aligned with ISACA best practices and is designed to help attendees pass the CISM exam.

Who is the course for?

The course is intended for professionals who have a minimum of 5 years of professional work experience in information systems, security and management.

Agenda:

Day 1

1. **Information Security Governance**
    a. Explain the need for and the desired outcomes of an effective information security strategy
    b. Create an information security strategy aligned with organisational goals and objectives
    c. Gain stakeholder support using business cases
    d. Identify key roles and responsibilities needed to execute an action plan
    e. Establish metrics to measure and monitor the performance of security governance

Day 2

2. **Information Risk Management**
    a. Explain the importance of risk management as a tool to meet business needs and develop a security management program to support these needs
    b. Identify, rank, and respond to a risk in a way that is appropriate as defined by organisational directives
    c. Assess the appropriateness and effectiveness of information security controls
    d. Report information security risk effectively

Day 3

3. **Information Security Program Development and Management**
    a. Align information security program requirements with those of other business functions
    b. Manage the information security program resources
    c. Design and implement information security controls
    d. Incorporate information security requirements into contracts, agreements and third-party management processes

Day 4

4. Information Security Incident Management

a. Understand the concepts and practices of Incident Management
b. Identify the components of an Incident Response Plan and evaluate its effectiveness
c. Understand the key concepts of Business Continuity Planning, or BCP and Disaster Recovery Planning, or DRP
d. Be familiar with techniques commonly used to test incident response capabilities

5. Mock exams

After completing this course, the student will be able to:

- Prepare for the Certified Information Security Manager (CISM) exam
- Develop an information security strategy and plan of action to implement the strategy
- Manage and monitor information security risks
- Build and maintain an information security plan both internally and externally
- Implement policies and procedures to respond to and recover from disruptive and destructive information security events