Day 1 – Information Security Governance

Students will understand the broad requirements for effective information security governance, the elements and actions required to develop an information security strategy, and be able to formulate a plan of action to implement this strategy.

- Develop an information security strategy and align the strategy with corporate governance
- Develop a business case
- Understand legal and regulatory issues
- Identify the drivers affecting the organization and the impact they have to security
- Obtain management commitment
- Define roles and responsibilities
- Establish clear communication channels

Day 2 – Information Risk Management

Students will be able to manage information security risks.

- Establish a process for information asset classification and ownership
- Implement a systematic and structured information risk assessment process
- Ensure that business impact assessments are conducted periodically
- Ensure that threat and vulnerability evaluations are performed on an ongoing basis
- Identify and periodically evaluate information security controls and countermeasures to mitigate risk to acceptable levels
- Integrate risk, threat and vulnerability identification and management into life cycle processes
- Report significant changes in information risk to appropriate levels of management for acceptance on both a periodic and event-driven basis

Day 3 – Information Security Program Development

Students will be able to develop an information security plan.

- Create and maintain plans to implement the information security strategy
- Specify the activities to be performed in the program
- Ensure alignment between the information security program and other assurance functions
- Identify internal and external resources required to execute the security program
- Ensure the development of information security architectures
- Establish communicate and maintain information security policies that support the security strategy
- Design and develop a program for information security awareness, training and education
• Ensure the development, communication, and maintenance of standards, procedures and other documentation
• Integrate information security requirements into the organization’s processes and life cycle activities
• Develop a process to integrate information security controls into contracts
• Establish metrics to evaluate the effectiveness of the information security program

Day 4 – Information Security Program Management & Incident Management & Response

Students will effectively manage information security within an enterprise and develop policies and procedures to respond to and recover from disruptive and destructive information security events.

• Manage internal and external resources required to execute the information security program
• Ensure that processes and procedures are performed in compliance with the organization’s information security policies and standards
• Ensure the performance of contractually agreed information security controls
• Ensure that information security is an integral part of the systems development process and acquisition processes
• Ensure that information security is maintained throughout the organization’s processes life cycle activities
• Provide information security advice and guidance in the organization
• Provide information security awareness, training and education to stakeholders
• Monitor, measure, test and report on the effectiveness and efficiency of information security controls and compliance with information security policies
• Ensure that noncompliance issues and other variances are resolved in a timely manner
• Develop and implement processes for detecting, identifying and analyzing security incidents
• Establish escalation and communication processes and lines of authority
• Develop plans to respond to and document information security incidents
• Establish the capability to investigate information security incidents
• Develop a process to communicate with internal parties and external organizations
• Integrate information security incident response plans with the organization’s disaster recovery and business continuity plan
• Organize, train, and equip teams to respond to information security incidents
• Periodically test and refine information security incident response plans
• Manage the response to information security incidents
• Conduct reviews to identify causes of information security incidents, develop corrective actions and reassess risk

*Topics covered per day may vary per instructor.*