Miami Dade College

Course Description

CIS3361 |Information Security Management | 4.00 credits

This course covers how to manage, design, oversee and assess an organization's information security. The student will learn how to develop an information security strategy, how to write information security policies, and how to manage information risk. Other topics include security program development and management, business continuity planning and disaster recovery planning. Prerequisite: CIS3360.

Course Competencies:

Competency 1: The student will be able to demonstrate an understanding of information security governance by:

1. Developing an information security strategy aligned with business goals and objectives
2. Aligning information security strategy with corporate governance
3. Developing business cases justifying investment in information security
4. Identifying current and potential legal and regulatory requirements affecting information security
5. Identifying drivers affecting the organization and their impact on information security
6. Obtaining senior management commitment to information security
7. Defining roles and responsibilities for information security throughout the organization
8. Establishing internal and external reporting and communication channels that support information security

Competency 2: The student will be able to demonstrate an understanding of information risk management by:

1. Comparing various risk assessment/analysis methodologies
2. Comparing various risk measurement and evaluation methodologies
3. Evaluating various risk management models
4. Discussing various risk management strategies, including acceptance, avoidance, transference, and mitigation
5. Establishing a process for information asset classification and ownership
6. Implementing a systematic and structured information risk assessment process
7. Ensuring that business impact assessments are conducted periodically
8. Ensuring that threat and vulnerability evaluations are performed continuously
9. Ensuring that a configuration and patch management program is implemented
10. Identifying and periodically evaluating information security controls and countermeasures to cost-effectively mitigate risk to acceptable levels
11. Integrating risk, threat, and vulnerability identification and management into life cycle processes (e.g., project management, development, procurement, and employment life cycles)
12. Reporting significant changes in information risk to appropriate levels of management for acceptance on both a periodic and event-driven basis

Competency 3: The student will be able to demonstrate an understanding of information security program development by:

1. Explaining the goals and objectives of a security program
2. Developing and maintaining plans to implement the information security strategy
3. Selecting best practices and frameworks to guide the development of the security program
4. Specifying the activities to be performed within the information security program
5. Ensuring alignment between the information security program and other assurance functions (e.g., physical, human resources (HR), quality, IT)
6. Identifying internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program
7. Ensuring the development of information security architectures (e.g. people, processes, technology)

8. Establishing, communicating, and maintaining information security policies that support the security strategy and are in compliance with applicable laws and regulations
9. Establishing policies for system and data identification and system configuration management
10. Designing and developing a program for information security awareness, training, and education
11. Ensuring the development, communication, and maintenance of standards, procedures, and other documentation (e.g., guidelines, baselines, codes of conduct) that support information security policies.
12. Integrating information security requirements into the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement)
13. Establishing a system security plan
14. Developing a process to integrate information security controls into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, and third parties)
15. Establishing metrics to evaluate the effectiveness of the information security program
16. Developing an appropriate certification and accreditation process

Competency 4: The student will be able to demonstrate an understanding of information security program management by:

1. Managing internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program
2. Ensuring that processes and procedures are performed in compliance with the organization's information security policies and standards
3. Ensuring the performance of contractually agreed (e.g., with joint ventures, outsourced providers, business partners, customers, and third parties) information security controls
4. Ensuring that information security is an integral part of the systems development process and acquisition processes
5. Ensuring that information security is maintained throughout the organization's processes (e.g., change control, mergers, and acquisitions) and life cycle activities (e.g., development, employment, procurement)
6. Providing information security advice and guidance (e.g., risk analysis, control selection) in the organization;
7. Providing information security awareness, training, and education to stakeholders (e.g. business process owners, users, information technology)
8. Monitoring, measuring, testing, and reporting on the effectiveness and efficiency of information security controls and compliance with information security policies
9. Ensuring that noncompliance issues and other variances are resolved promptly

Competency 5: The student will be able to demonstrate an understanding of incident management and response by:

1. Developing and implementing processes for detecting, identifying, analyzing, and responding to information security incidents
2. Establishing escalation and communication processes and lines of authority
3. Developing plans to respond to and document information security incidents
4. Establishing the capability to investigate information security incidents (e.g. forensics, evidence collection and preservation, log analysis, interviewing)
5. Developing a process to communicate with internal parties and external organizations (e.g., media, law enforcement, customers)
6. Integrating information security incident response plans with the organization's disaster recovery (DR) and business continuity plan

7. Organizing, training, and equipping teams to respond to information security incidents
8. Periodically testing and refining information security incident response plans
9. Managing the response to information security incidents
10. Conducting reviews to identify causes of information security incidents, develop corrective actions, and reassess risk

Competency 6: The student will evaluate the legal, ethical, and professional issues in information security by:

1. Differentiating between laws and ethics in information security
2. Assessing ethical and professional issues relevant to information security
3. Analyzing international laws and their legal bodies
4. Distinguishing between unethical and illegal behavior
5. Discussing applicable laws and regulations about information security management

Learning Outcomes:

1. Solve problems using critical and creative thinking and scientific reasoning
2. Formulate strategies to locate, evaluate, and apply information
3. Use computer and emerging technologies effectively