Title: IT Security and Risk Management

Catalog Description

This course provides an introduction to the fundamental principles and topics of Information Technology Security and Risk Management at the organizational level. Students will learn critical security principles that enable them to plan, develop, and perform security tasks. The course will address hardware, software, processes, communications, applications, and policies and procedures with respect to organizational IT Security and Risk Management.

Learning Objectives

Students will be able to:

- Understand the fundamental principles of Information Technology Security.
- Understand the concept of threats, information asset identification and evaluation, physical, operational, and information security and how they are related.
- Understand the need for the careful design of a secure organizational information infrastructure.
- Understand risk analysis and risk management.
- Understand both technical and administrative mitigation approaches.
- Understand the need for a comprehensive security model and its implications for the security manager.
- Gain an understanding of security technologies.
- Gain an introductory understanding of basic cryptography, its implementation considerations, and key management.
- Design and guide the development of an organization's security policy.
- Determine appropriate strategies to assure confidentiality, integrity, and availability of information.
- Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls.
- Understand the need for and key components of a disaster recovery plan.

Topics

- Introduction to Information Security
- Inspection
  - Resource Inventory
  - Threat Assessment
  - Identifying Vulnerabilities
  - Assigning Safeguards
- Protection
  - Awareness
  - Access
  - Identification
  - Authentication
  - Authorization

    - Availability
    - Accuracy
    - Confidentiality
    - Accountability
    - Administration
- Detection
    - Intruder Types
    - Intrusion Methods
    - Intrusion Process
    - Detection Methods
    - Monitoring Systems
    - Responding to a Security Event
- Reaction
    - Incident Determination
    - Incident Notification
    - Incident Containment
    - Assessing Damage
    - Incident Recovery
    - Automated Response
- Reflection
    - Incident Documentation
    - Incident Evaluation
    - Legal Prosecution
- Risk Assessment Frameworks, for example:
    - COSO Integrated Control Framework
    - CoBiT – ISACA
    - Australia/New Zealand Standard – Risk Management
    - ISO Risk Management – Draft Standard
    - Audit Control Software
- Security Engineering
    - Protocols
    - Passwords
    - Access Controls
    - Cryptography
- Physical aspects:
    - Biometrics
    - Physical Tamper Resistance
    - Security Printing and Seals
- Security in connected systems and networks:
    - Distributed Systems
    - Telecom System Security
    - Network Attack and Defense
    - Protecting E-Commerce Systems
- Policy and Management Issues
    - Copyright and Privacy Protection
    - E-Policy

- Disaster Planning and Recovery
  - Facilities and data recovery
  - Redundant facilities
  - Recovery Planning
  - Recovery Execution

Discussion

- This course is intended as a first course in Information Assurance at the undergraduate level. This course will be a pre-requisite for additional information and network security courses for an Information Security track in the undergraduate program.
- The course description does not prescribe the specific approaches and methods for inspection, protection, detection, reaction, reflection, risk assessment and mitigation. This will allow instructors and institutions to decide which specific approaches to cover.
- The use of case examples for discussion and reflection in this course is highly recommended.
- It is recommended to include an applied project for a potential client in which students conduct a risk assessment of a part of the client's IT infrastructure.

