C-ID Descriptor
Introduction to Information Systems Security

Descriptor Details

- **Descriptor Title**: Introduction to Information Systems Security
- **C-ID Number**: 160
- **Units**: 3.0
- **Date of Last Revision**: 2/26/2025 07:19:25 PM GMT+0000

General Description

An introduction to the fundamental principles and topics of Information Technology Security and Risk Management at the organizational level. It addresses hardware, software, processes, communications, applications, and policies and procedures with respect to organizational Cybersecurity and Risk Management. Preparation for the CompTIA Security+ certification exams.

Prerequisites

None

Corequisites

None

Advisories

ITIS 150 Computer Network Fundamentals

The use of case examples for discussion and reflection in this course is highly recommended.

Content

1. Introduction to Information Systems Security
2. Malware and Social Engineering Attacks
3. Application and Network Attacks
4. Vulnerability Assessment and Mitigating Attacks
5. Host, Application, and Data Security
6. Network Security
7. Administering a Secure Network
8. Wireless Network Security
9. Access Control Fundamentals
10. Authentication and Account Management
11. Basic Cryptography
12. Advanced Cryptography
13. Business Continuity
14. Risk Mitigation

Lab Activities

No information provided

Objectives

At the conclusion of this course, the student should be able to:

1. Describe the fundamental principles of information systems security.
2. Define the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related.
3. Evaluate the need for the careful design of a secure organizational information infrastructure.
4. Perform risk analysis and risk management.
5. Determine both technical and administrative mitigation approaches.
6. Explain the need for a comprehensive security model and its implications for the security manager or Chief Security Officer (CSO).

7. Create and maintain a comprehensive security model.
8. Apply security technologies.
9. Define basic cryptography, its implementation considerations, and key management.
10. Design and guide the development of an organization’s security policy
11. Determine appropriate strategies to assure confidentiality, integrity, and availability of information.
12. Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls.

Evaluation Methods

Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments.

Textbooks

• Ciampa, M. - Security+ Guide to Network Security Fundamentals, Cengage
• Whitman, M. E. & Mattord, H. J. - Principles of Information Security, Cengage