Center for Curriculum and Transfer Articulation

Information Security Essentials

Course: **CIS271DB**	Lec + Lab **3** Credit(s) **4** Period(s) **3.7** Load
	Course Type: **Occupational**
First Term: **2014 Fall**	Load Formula: **S- Standard**
Final Term: **Current**	

Description: Overview of information security principles, access control, risk management, and compliance. Provides partial preparation for certification in one or all of the following: Comptia Security + exam, International Information Systems Security Certification Consortium (ISC)2, Systems Security Certified Practitioner (SSCP) exam, the Committee on National Security Systems (CNSS) 4011 certification, or GIAC Security Essentials Certificate (GSEC).

Requisites: Prerequisites: CNT140AA and (MST150SV or CIS126DL) and CIS250.

MCCCD Official Course Competencies

1. Explain the fundamental components, concepts and application of information security principles (I, V).
2. Describe access control concepts, methodologies and practices designed to protect the IT Infrastructure (II, IV).
3. Explain the core principles related to Risk Management including risk identification, analysis and mitigation (III).
4. Describe basic Information Technology principles, which are related to information security (IV).
5. Explain how US Law has created the information security compliance environment and what the various laws and compliance standards are
(V).
6. Describe training opportunities that lead to certifications, which are needed for entry into the Information Security Field (VI).

MCCCD Official Course Outline

I. Information Security Fundamentals
A. Tenants of Information Security
1. Confidentiality
2. Integrity
3. Availability
B. IT Infrastructure Definition
1. Users
2. Workstations
3. Networks
4. Remote Access

4. Remote Access
5. Systems
6. Applications and Databases

C. IT Security Policy Framework
1. Security Policy Definition
2. Foundational IT Security Policies

D. Data Classification Standards
1. Data Types
2. Importance of Data

E. Asset Classifications
1. Critical
2. Non-Critical

F. Defense in Depth
1. Perimeter Security
2. Systems Security
3. Application Security
4. Remote Access Security
5. Corporate Security

G. Security Types
1. Asset based
2. Information based Security

II. Access Control

A. Access Control Parts
1. Identification
2. Authentication
3. Authorization
4. Accountability

B. Access Control Types
1. Physical
2. Logical

C. Authentication Process and Requirements
1. Authentication Types
2. Single Sign-On (SSO)

D. Accountability Policies and Procedures
1. Log Files
2. Data Retention
3. Media Disposal
4. Compliance Requirements

E. Formal Models of Access Control
1. Discretionary Access Control
2. Mandatory Access Control
3. Non-Discretionary Access Control
4. Rule-Based Access Control
5. Content-Dependent Access Control
6. Constrained User Interface
7. Other Access Control Models

F. Centralized and Decentralized Access Control
1. Authentication, authorization, and accounting (AAA) Servers
2. Decentralized Access Control

2. Decentralized Access Control

G. Access Controls
1. Remote Access Controls
2. Network Access Controls
3. System Access Controls
4. Application Access Controls

III. Risk Response and Recovery
A. Risk Management and Information Security
1. Definitions of Risk
2. Elements of Risk
3. Purpose of Risk Management
4. Risk Equation
5. Risk Identification
6. Risk Analysis
7. Risk Response Planning

B. Risk Assessment Approaches
1. Calculating Quantified Risk
2. Qualitative Risk Analysis

C. Risk Management
1. Acceptable Risk Levels
2. Countermeasure Evaluation

D. Business Continuity Planning
1. Terminology
2. Assessing Maximum Tolerable Downtime (MTD)
3. Business Impact Analysis

E. Disaster Recovery
1. Activating a Disaster Recovery (DR) Plan
2. Operating in a Reduced/Modified Environment
3. Restoring Damaged Systems
4. Disaster Recovery Issues
5. Recovery Alternatives
6. Interim or Alternate Processing Strategies

F. Incident Response
1. Incident Identification
2. Incident Containment
3. Incident Root Cause Analysis
4. Incident Eradication
5. Incident Recovery

IV. Infrastructure, Networks and Telecommunications Security
A. The Open System Interconnection Reference Model
B. Network Types
1. Wide Area Networks
2. Local Area Networks
3. Personal Area Networks

C. Transmission Control Protocol/Internet Protocol (TCP/IP)
1. TCP/IP Overview
2. IP Addressing
3. Internet Control Message Protocol (ICMP)

D. Network Security Risks

D. Network Security Risks
1. Risk Categories
E. Basic Network Security Defense Tools
1. Firewalls
2. Virtual Private Networks (VPNs) and Remote Access
3. Network Access Control
F. Wireless Networks
1. Wireless Access Points (WAPs)
2. Wireless Network Security Controls
V. Standards, Laws, and Compliance
A. Standards Organizations
1. National Institute of Standards and Technology (NIST)
2. International Organization for Standardization (ISO)
3. International Electrotechnical Commission (IEC)
4. World Wide Web Consortium (W3C)
5. American National Standards Institute (ANSI)
6. Institute of Electrical and Electronics Engineers (IEEE)
B. Standards, Requirements and Frameworks
1. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-Series
2. North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)
3. Nuclear Energy Institute (NEI) 08/09
4. ISO/IEC 27002
5. Payment Card Industry (PCI) Data Security Standards (DSS)
6. Health Insurance Portability and Accountability Act (HIPAA)
7. Sarbanes-Oxley Act (SOX)
8. Gramm-Leach-Bliley Act (GLBA)
9. Committee on National Security Systems (CNSS)
C. US Compliance Laws
1. Federal Information Security Management Act
2. Health Insurance Portability and Accountability Act
3. Gramm-Leach-Bliley Act
4. Sarbanes-Oxley Act
5. Family Educational Rights and Privacy Act
6. Children?s Internet Protection Act
7. Energy Independence and Security Act
VI. Training, Certifications and Career Opportunities
A. Continuing Education Programs
B. Post-Secondary Degree Programs
C. Background Check and Security Clearance Requirements
D. Vendor-Neutral Professional Certifications
1. International Information Systems Security Certification Consortium (ISC)2
2. Global Information Assurance Certification (GIAC)/SysAdmin, Audit, Networking, and Security (SANS) Institute
3. Certified Internet Web Professional (CIW)
4. Computing Technology Industry Association (CompTIA)
5. Security Certified Program (SCP)
6. Information Systems Audit and Control Association (ISACA)

6. Information Systems Audit and Control Association (ISACA)
7. Council of Electronic Commerce Consultants (EC Council)
8. Committee on National Security Systems (CNSS)
9. CMU
10. Certified SCADA (Supervisory Control and Data Acquisition) Security Architect (CSSA)

E. Information Security Careers

1. Compliance
2. Security Operations
3. Security Assessor
4. Penetration Tester
5. Architecture
6. Management

Last MCCCD Governing Board Approval Date: **June 24, 2014**