OUTCOMES BASED LEARNING MATRIX

Course: CTIM 180 - Computer and Information Security (3 credits, 45 hours)
Department: Computer Technology and Information Management

Description:

This course is designed to give those in the computer and security professions an understanding of the challenges of protecting information assets and the resources available to meet those challenges. An introduction to information/computer security is followed by an examination of the need for security and the legal, ethical, and professional issues faced by professionals in this field. Students will then examine the methodologies within the five stages (Security Analysis, Logical Design, Physical Design, Implementation, and Maintenance and Change) of the development, implementation, and maintenance of a new security system within an organization or the improvement of an existing security system.

Prerequisite: None

While completing the table below, remember that the individual outcomes you list in the first column should answer this question: **What must the learner know and be able to do at the end of the course?** Items in the third column should answer the question: **How do we know?** The second column is where teachers can be most creative; it's for pedagogy. Each rectangle in column one should contain just one outcome; the corresponding rectangles in columns two and three, however, may contain more than one item. Using the code at the end of the matrix, indicate the core competencies being strengthened by the outcomes activities and the assessment tools.

Approved by CTIM Department: January 2004

*COURSE OUTCOMES	OUTCOMES ACTIVITIES	ASSESSMENT TOOLS
At the end of this course, the student will have an understanding of the field of computer and information security to include:		
1. access control systems and methodology	a) Accountability (CCT, OC, QL, IL, WC, IG) b) Access Control techniques (CCT, OC, QL, IL, WC, IG) c) Access Control Administration (CCT, OC, QL, IL, WC, IG) d) Access Control Models (CCT, OC, QL, IL, WC, IG) e) Identification and Authentication Techniques (CCT, OC, QL, IL, WC, IG) f) Access Control Methodologies and Implementation (CCT, OC, QL, IL, WC, IG) g) File and Data Ownership and Custodianship h) Methods of Attack (CCT, OC, QL, IL, WC, IG) i) Monitoring and Analysis (CCT, OC, QL, IL, WC, IG)	1. Quizzes, tests, projects, class participation, homework assignments (CCT, OC, QL, IL, WC, IG)

2. telecommunications and network security	a) International Standards Organization/ Open Systems Interconnection (CCT, OC, QL, IL, WC, IG) (ISO/OSI) Layers and Characteristics (CCT, OC, QL, IL, WC, IG) b) Data Communications and Network Security (CCT, OC, QL, IL, WC, IG) c) Remote Access (CCT, OC, QL, IL, WC, IG) d) Secure Internet/Intranet/Extranet (CCT, OC, QL, IL, WC, IG) e) Network Attacks and Countermeasures (CCT, OC, QL, IL, WC, IG)	2. Referenced above (CCT, OC, QL, IL, WC, IG)

3. security management practices	a) Security Management Concepts and Principles b) CIA Triad (CCT, OC, QL, IL, WC, IG) c) Protection Mechanisms (CCT, OC, QL, IL, WC, IG) d) Change Control/Management (CCT, OC, QL, IL, WC, IG) e) Security Assessment (CCT, OC, QL, IL, WC, IG) f) Information/Data Classification (CCT, OC, QL, IL, WC, IG) g) Employment Policies and Practices (CCT, OC, QL, IL, WC, IG) h) Policies, Standards, Guidelines and Procedures (CCT, OC, QL, IL, WC, IG) i) Risk Management (CCT, OC, QL, IL, WC, IG) j) Risk Identification (CCT, OC, QL, IL, WC, IG) k) Risk Assessment (CCT, OC, QL, IL, WC, IG) l) Roles , Responsibilities and Organization (CCT, OC, QL, IL, WC, IG) m) Security Awareness Training (CCT, OC, QL, IL, WC, IG) n) Security Management Planning (CCT, OC, QL, IL, WC, IG)	3. Referenced above

4. applications and systems development security	a) Systems Development Controls (CCT, OC, QL, IL, WC, IG) b) System Development Life Cycle (CCT, OC, QL, IL, WC, IG) c) Malicious Code (CCT, OC, QL, IL, WC, IG) d) Methods of attack (CCT, OC, QL, IL, WC, IG)	4. Referenced above
5. cryptography	a) Use of Cryptography to achieve Confidentiality, Integrity, Authentication, Non-repudiation (CCT, OC, QL, IL, WC, IG) b) Digital Signatures, Message Digests (CCT, OC, QL, IL, WC, IG) c) Cryptographic Concepts, Methodologies, and Practices (CCT, OC, QL, IL, WC, IG) d) Symmetrical Key Algorithms (Secret) (CCT, OC, QL, IL, WC, IG) e) Asymmetrical Key Algorithms (Public/Private) (CCT, OC, QL, IL, WC, IG) f) Key Management Techniques (CCT, OC, QL, IL, WC, IG) g) Public Key Infrastructure (PKI) (CCT, OC, QL, IL, WC, IG) h) Encryption Techniques (CCT, OC, QL, IL, WC, IG) i) SSL, PGP, PEM, Steganography (CCT, OC, QL, IL, WC, IG) j) System Architecture for Implementing Cryptographic Functions (CCT, OC, QL, IL, WC, IG) k) Methods of Attack (CCT, OC, QL, IL, WC, IG)	5 . Referenced above

6. security architecture and models	a) Principles of common computer and network organizations, architectures and designs (CCT, OC, QL, IL, WC, IG) b) Principles of common security models, architectures, and evaluation criteria (CCT, OC, QL, IL, WC, IG) c) Rainbow Books (CCT, OC, QL, IL, WC, IG)	6. Referenced above
7. operations security	a) Administrative Management (CCT, OC, QL, IL, WC, IG) b) Operations Controls and Concepts (CCT, OC, QL, IL, WC, IG) c) Control Types (CCT, OC, QL, IL, WC, IG) d) Administrative controls (separation of duties and responsibilities, rotation of duties, least privilege, etc.) e) Resource Protection (CCT, OC, QL, IL, WC, IG) f) Monitoring / Monitoring tools and techniques g) Auditing / Audit trails (CCT, OC, QL, IL, WC, IG) h) Intrusion detection Systems (network-based/host-based) (CCT, OC, QL, IL, WC, IG) i) Penetration testing techniques (CCT, OC, QL, IL, WC, IG) j) Threats and Countermeasures (CCT, OC, QL, IL, WC, IG) k) Violations, Incidents, Breaches, and Reporting (CCT, OC, QL, IL, WC, IG)	7. Referenced above

8. business continuity planning (BCP) and disaster recovery planning (DRP)	a) Business Continuity Planning (CCT, OC, QL, IL, WC, IG) b) Project Scope and Planning (CCT, OC, QL, IL, WC, IG) c) Business Impact Assessment (CCT, OC, QL, IL, WC, IG) d) Incident Response Plan (CCT, OC, QL, IL, WC, IG) e) Backup/Recovery Strategy (CCT, OC, QL, IL, WC, IG) f) Recovery Techniques (CCT, OC, QL, IL, WC, IG) g) Training/Testing/Maintenance (CCT, OC, QL, IL, WC, IG) h) Disaster Recovery Planning (CCT, OC, QL, IL, WC, IG) i) Recovery Plan Development (CCT, OC, QL, IL, WC, IG) j) Emergency Response (CCT, OC, QL, IL, WC, IG) k) Implementation (CCT, OC, QL, IL, WC, IG) l) Training/Testing/Maintenance (CCT, OC, QL, IL, WC, IG) m) BCP/DRP Events (Fire, Earthquake, Power Outage, etc.) (CCT, OC, QL, IL, WC, IG)	8 . Referenced above

9. law, investigations, and ethics	a) Laws (Common Law, Civil Law) (CCT, OC, QL, IL, WC, IG) b) Investigations (CCT, OC, QL, IL, WC, IG) c) Major categories of computer crime (CCT, OC, QL, IL, WC, IG) d) Incident Handling (CCT, OC, QL, IL, WC, IG) e) General Ethics (CCT, OC, QL, IL, WC, IG) f) Professional Code of Ethics (CCT, OC, QL, IL, WC, IG)	9. . Referenced above
10. physical security	a) Facility Requirements (CCT, OC, QL, IL, WC, IG) b) Technical Controls (CCT, OC, QL, IL, WC, IG) c) Environment/Life Safety (CCT, OC, QL, IL, WC, IG) d) Physical security threats (CCT, OC, QL, IL, WC, IG) e) Mechanisms of physical security (CCT, OC, QL, IL, WC, IG) f) Elements of physical security (CCT, OC, QL, IL, WC, IG)	10 . Referenced above

*Try to express an outcome as an infinitive phrase that concludes this sentence: **At the end of the course, the students should be able to . . ..** Finding the line between too general and too specific can be difficult. In an English Composition course, for instance, it is probably too general to say, "The student should be able to write effective essays." It is probably too specific to say, "The student should be able to write an introductory paragraph of at least 50 words, containing an attention-getting device, an announcement of the narrowed topic, and an explicit thesis sentence." Just right might read, "The student will write introductions that gather attention and focus the essay."

**Indicate the Core Competencies that apply to the outcomes activities and assessment tools: critical and creative thinking (CCT); oral communications (OC); quantitative literacy (QL); information literacy (IL); written communication (WC); civic engagement (CE); integrative learning (IG); global learning (GL).