Cover the 10 domains required for Certified Information Systems Security Professional (CISSP) certification in 40 hours at the University of Arizona South Continuing Education in Sierra Vista. This class is ideal for information security professionals attempting to achieve CISSP certification. Classes are offered during the day or evening. See www.uasce.org for pricing and schedule details.

INFORMATION SECURITY AND RISK MANAGEMENT

The Business Case for Information Security Management
Core Information Security Principles: Availability, Integrity,
Information Security Management Governance
Organizational Behavior
Security Awareness, Training, and Education
Risk Management
Ethics
Data Classification Policy
Data Handling Policy

ACCESS CONTROL

Definitions and Key Concepts
Access Control Categories and Types
Access Control Threats
Access to Systems
Access to Data
Intrusion Detection and Prevention Systems
Access Control Assurance

CRYPTOGRAPHY

Key Concepts and Definitions
Encryption Systems
Message Integrity Controls
Digital Signatures
Encryption Management
Cryptanalysis and Attacks
Encryption Usage
References
Sample Questions

PHYSICAL (ENVIRONMENTAL) SECURITY

Site Location
The Layered Defense Model
Information Protection and Management Services
SECURITY ARCHITECTURE AND DESIGN

Security Architecture and Design Components and Principles
Security Models and Architecture Theory
Security Product Evaluation Methods and Criteria

BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

Organization of the BCP/DRP Domain Chapter
Terminology
Appendix A: Addressing Legislative Compliance within Business Continuity Plans

TELECOMMUNICATIONS AND NETWORK SECURITY

Basic Concepts
Layer 1: Physical Layer
Layer 2: Data-Link Layer
Layer 3: Network Layer
Layer 4: Transport Layer
Layer 5: Session Layer
Layer 6: Presentation Layer
Layer 7: Application Layer
Trivial File Transfer Protocol (TFTP)

APPLICATION SECURITY

Domain Description and Introduction
Applications Development and Programming Concepts and Protection
Audit and Assurance Mechanisms
Malicious Software (Malware)
The Database and Data Warehousing Environment
Web Application Environment

OPERATIONS SECURITY

Privileged Entity Controls
Resource Protection
Continuity of Operations
Change Control Management

LEGAL, REGULATIONS, COMPLIANCE AND INVESTIGATIONS

Major Legal Systems
Information Technology Laws and Regulations
Incident Response
Computer Forensics