

Certified Information Systems Security Professional (CISSP) Course Outline

1. Controlling Access to Information Systems
 - Control Data Access
 - Control System Access
 - Determine an Access Control Administration Method
 - Perform a Penetration Test
2. Networking Systems and Telecommunications
 - Design Data Networks
 - Provide Remote Access to a Data Network
 - Secure a Data Network
 - Manage a Data Network
3. Defining Security Management
 - Determine Security Management Goals
 - Classify Information
 - Develop a Security Program
 - Manage Risk
4. Creating Applications Security
 - Perform Software Configuration Management
 - Implement Software Controls
 - Secure Database Systems
5. Performing Cryptography
 - Apply a Basic Cipher
 - Select a Symmetric Key Cryptography Method
 - Select an Asymmetric Key Cryptography Method
 - Determine Email Security
 - Determine Internet Security
6. Securing System Architecture
 - Evaluate Security Models
 - Choose a Security Mode
 - Provide System Assurance

7. Executing Operations Security

- Control Operations Security
- Audit and Monitor Systems
- Handle Threats and Violations

8. Performing Business Continuity Planning

- Sustain Business Processes
- Perform Business Impact Analysis
- Define Disaster Recovery Strategies
- Test the Disaster Recovery Plan

9. Applying Physical Security

- Control Physical Access
- Monitor Physical Access
- Establish Physical Security Methods
- Design Secure Facilities

10. Applying Law, Investigations, and Ethics

- Interpret Computer Crime Laws and Regulations
- Apply the Evidence Life Cycle
- Perform an Investigation
- Identify Codes of Conduct

11. Appendix A: CISSP Certification Exam Objectives

12. Appendix B: SSCP Certification Exam Objectives