



Certified Information Systems Security Professional

5 Days + 1 Day Refresher

CISSP Exam Preparation Boot Camp Plus 1 Day Memory Refresher

The Certified Information Systems Security Professional (CISSP®) certification provides information security professionals with not only an objective measure of competence but also a globally recognized standard of achievement. This designation is the first credential accredited by ANSI to ISO Standard 17024:2003 in the field of information security. The CISSP credential demonstrates competence in the 10 domains of the International Information Systems Security Certification Consortium (ISC)² CISSP® CBK®.

ABOUT THE COURSE

The course covers the 10 CISSP® CBK® Domains

1. Access Control
2. Application Security
3. Business Continuity and Disaster Recovery Planning
4. Cryptography
5. Information Security and Risk Management
6. Legal, Regulations, Compliance and Investigations
7. Operations Security
8. Physical (Environmental) Security
9. Security Architecture and Design
10. Telecommunications and Network Security

Each section of the course contains an Introduction to the Domain covered, a Summary and CBK (Components and Examples).

Prerequisites

There are no pre-requisites to attend the course. However, not everyone will be qualified to take the exam or receive certification.

COURSE OUTLINE

Domain 1: Access Control

- Definitions and Key Concepts
- Information Classification and Access Control
- Information Protection Requirements
- Information Protection Environment
- Security Technology and Tools
 - Centralized Access Control Methodologies
 - Decentralized/Distributed Access Control Methodologies
 - Access to Data
- Access Control Categories and Types
- Access Control Threats
- Access Control Technologies
- Assurance Mechanisms
- Assurance, Trust, and Confidence Mechanisms
- Intrusion Detection
- Information Protection and Management Services

Domain 2: Application Security

- Information Protection Requirements
 - The C-I-A Triad
- Information Protection Environment
 - Open Source Code and Closed Source Code
 - Software Environment
- The Database and Data Warehousing Environment
 - DBMS Architecture
- Databases and Data Warehouses
 - Database Interface Languages
 - Security Assertion Markup Language (SAML)
 - Data Warehousing
 - Database Vulnerabilities and Threats
- Security Technology and Tools
 - System Life Cycle and Systems Development
 - System (Software) Development Methods
 - Including Security in a Systems Development Method
 - Programming Language and Security
 - Software Protection Mechanisms
 - DBMS Controls
- Assurance, Trust, and Confidence Mechanisms
 - Information Integrity
 - Information Accuracy
 - Information Auditing
 - Evaluation/Certification and Accreditation
- Applications Systems Threats and Vulnerabilities
- Applications Security Controls
- Information Protection and Management Services
- Configuration Management

Domain 3: Business Continuity Planning and Disaster Recovery Planning

- Defining a Disaster
- Information Protection Requirements
- Information Protection Environment
- Project Scope Development and Planning
- Business Impact Analysis
- Emergency Assessment
- Continuity and Recovery Strategy
- Plan Design and Development
- Implementation
- Restoration

- Plan Management
- Security Technology and Tools
 - Phase I: Project Management and Initiation
 - Phase II: Business Impact Analysis (BIA)
 - Phase III: Recovery Strategies
 - Phase IV: Plan Development and Implementation
 - Phase V: Testing, Maintenance, Awareness, and Training
- Assurance, Trust, and Confidence Mechanisms
- Information Protection and Management Services

Domain 4: Cryptography

- Key Concepts and Definitions
- History
- Information Protection Requirements
 - The C-I-A Triad
- Information Protection Environment
 - Introduction
 - Definitions
 - Cryptanalysis and Attacks
 - Import/Export Issues
- Security Technology and Tools
 - Basic Concepts of Cryptography
 - Encryption Systems
 - Symmetric Key Cryptography Algorithms
 - Asymmetric Key Cryptography Algorithms
 - Message Integrity Controls
- Assurance, Trust, and Confidence Mechanisms
 - Digital Signatures and Certificate Authorities
 - Public Key Infrastructure (PKI)
- Management of Cryptographic Systems
- Information Protection and Management Services
 - Key Management
 - Key Management Functions
 - Key Generation
 - Distribution
 - Installation
 - Storage
 - Change
 - Control
 - Disposal
 - Modern Key Management
 - Principles of Key Management
- Threats and Attacks

Domain 5: Information Security and Risk Management

- Purposes of Information Security Management
- Concepts: Confidentiality, Integrity, Availability
- Risk Analysis and Assessment
 - Information Protection Requirements
 - Information Protection Environment
 - Security Technology and Tools
 - Assurance, Trust, and Confidence Mechanisms
 - Information Protection Management Service
- Information Classification
 - Information Protection Requirements
 - Information Protection Environment
 - Security Technology and Tools
 - Assurance, Trust, and Confidence Mechanisms
 - Information Protection and Management Services

- Policies, Procedures, Standards, Baselines, Guidelines
 - Information Protection Requirements
 - Information Protection Environment
 - Security Technology and Tools
 - Information Protection Requirements
- Security Awareness Training and Education
 - Information Protection Environment
 - Social Engineering
- Risk Management
- Ethics
- Implementation (Delivery) Options
 - Security Technology and Tools
 - Assurance, Trust, and Confidence Mechanisms
 - Information Protection Management Services

Domain 6: Legal, Regulations, Compliance and Investigation

- Introduction to Law
- Major Legal Systems
- Legal Concepts
 - Information Protection Requirements
 - Information Protection Environment
 - Privacy
 - Recommended Course of Action
 - Security Technology and Tools
 - Assurance, Trust, and Confidence Mechanisms
 - Information Protection and Management Services
- Introduction to Regulations
 - Regulatory Issues
- Introduction to Investigations
 - Information Protection Requirements
 - Information Protection Environment
 - Security Technology and Tools
 - Assurance, Trust, and Confidence Mechanisms
 - Information Protection and Management Services
- Introduction to Computer Forensics
- Introduction to Ethics
 - Information Protection Requirements
 - Computer Ethics
 - Information Protection Environment
 - Security Technology and Tools
 - Assurance, Trust and Confidence Mechanisms
 - Information Protection and Management Services

Domain 7: Operations Security

- Information Protection Requirements
 - Resource Protection
- Information Protection Environment
- Security Technology and Tools
 - Change Control Management
 - Physical Security Controls
 - Privileged Entity Control
- Assurance, Trust, and Confidence Mechanisms
 - Information Protection and Management Services

Space is limited.
To register, call (613) 727-7729.
Email -training@algonquincollege.com

Domain 8: Physical (Environmental) Security

- Definitions and Key Concepts
- Layered Defense Model
 - Information Protection Requirements
 - The C-I-A Triad
- Information Protection Environment
 - Site Location
 - Equipment Protection
 - Crime Prevention through Environmental Design (CPTED)
- Infrastructure Support Systems
- Security Technology and Tools
 - Perimeter and Building Grounds Boundary Protection
 - Building Entry Points
 - Inside the Building: Building Floors, Office Suites, Offices
 - Penetration (Intrusion) Detection Systems
- Assurance, Trust, and Confidence Mechanisms
 - Drills/Exercises/Testing
 - Vulnerability/ Penetration Tests
 - Creating a Checklist
 - Maintenance and Service
- Information Protection and Management Services
 - Awareness and Training

Domain 9: Security Architecture and Design

- Security Architecture and Design Components and Principles
 - Hardware
 - Software
- System Security Techniques
- Information Protection Requirements
- The C-I-A Triad
- Information Protection Environment
 - Platform Architecture
 - Network Environment
 - Enterprise Architecture
 - Security Models
- Security Technology and Tools
 - Network Protection
- Assurance, Trust, and Confidence Mechanisms
 - Trusted Computer Security Evaluation Criteria (TCSEC)
 - The Trusted Network Interpretation (TNI)
 - Information Technology Security Valuation Criteria (ITSEC)
 - The Common Criteria (CC)
 - Certification and Accreditation
- Security Models and Architecture Theory
- Security Evaluation Methods and Criteria
- Information Protection and Management Services

Domain 10: Telecommunications and Network Security

- Key Concepts and Definitions
- Information Protection Requirements
- Information Protection Environment
 - Data Networks
 - Remote Access Services
 - Network Protocols
 - Network Threats and Attacks

- Network Components
- Telephony
- Security Technology and Tools
 - Content Filtering and Inspection
 - Intrusion Detection
- Assurance, Trust, and Confidence Mechanisms
- Information Protection and Management Services

Course Conclusion

Added Features:

- A one-day Memory Refresher with Patrick Malcolm
- Throughout the course you will be given assessment tests so that you can test your knowledge level
- Register 3 weeks or more prior to the course date and you'll receive a pre-test assessment so that you know what your baseline knowledge is before taking the boot camp

ATTEND THIS WORKSHOP IF YOU...

- Are seeking comprehensive knowledge of security and CISSP certification.
- This course will help you to prepare for the CISSP Certified Information Systems Security Professional exam.

NOTE: This course supports those wanting to write the CISSP Exam, but does not guarantee a student will pass the exam.

Student Materials include a comprehensive workbook and other materials that are necessary.

HOW TO REGISTER

To register, call **(613) 727-7729**
Or email training@algonquincollege.com

Schedule:

October 26 to 30, 2009

December 7 to 11, 2009

One-day Memory Refresher: (scheduled quarterly)

Date: To be scheduled. Past participants will be informed of scheduled date.

Class Times: 8:30 a.m. to 4:00 p.m.

Location: 340 Albert Street, 11th Floor
Constitution Square, Ottawa

Class check-in, coffee and muffins start at 8:00 a.m.

Afternoon refreshment provided on class days.

Group size is limited to 25.

PATRICK MALCOLM is a frequent speaker at major security conferences and author of numerous courses and focuses on the development of an integrated IT risk and security management, processes, policies and guidelines.

Throughout his 23-year career in computer networking and security, Patrick has been devoted to solving security problems in a manner that balances mission requirements and cost-effectiveness constraints.