interface

SECURITY

SEC275: CISSP (Certified Information Systems Security Professional)

Information security is part of every IT professional's job. Hackers are constantly trying to compromise your networks, steal sensitive data, and overwhelm your systems. Planning, implementing, enforcing, or even removing security are tasks we all do to keep users and systems safe. Performing these tasks properly and in alignment with industry best practices is critical to virtually every technology role, from decision maker to developer to operator. This scenario-based course focuses on computer security as an applied process across job roles and industries. The course also helps to prepare students for achieving the Certified Information Systems Security Professional (CISSP) certification. CISSP is widely regarded as the most valuable vendor-neutral credential a computer security professional can hold. It is frequently identified as a prerequisite for security jobs across all industries including security design, implementation, maintenance, policy development, and management of secured systems, process/procedures, policies, applications and networks. This course is primarily for Information Technology Security Professionals who want to advance their security certifications such as Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified Ethical Hacker (CEH), and related courses. This course also covers most of the knowledge required to prepare for the Systems Security Certified Practitioner (SSCP) certification exam.

AUDIENCE

This course is primarily designed for the IT professional whose role includes some information security tasks or responsibilities. Common job titles for students include CISO, Director, Manager, Supervisor, Analyst, Information Architect, Program Manager, Lead, Information Security Officer, Security Specialist, and Auditor. The ideal student has some practical experience in the information security industry. Experienced information security professionals will also find value in this course to update their security skills, expand their knowledge of theoretical security, practice security exercises in areas that require a "safe" environment, and deepen exposure to areas outside their current role. DoD Directive 8570.1-M- CISSP meets Government and DoD agencies compliance with Federal Information Security Management Act (FISMA) and DoD Directive 8570.1-M Exams.

PREREQUISITES

Before taking this course, students should have six to nine months in a role that is relevant to security practices. It is also recommended that student have successfully completed the following courses or have equivalent experience..

- ICND1 v3.0 Interconnecting Cisco Networking Devices CCNA Part 1
- A+901: CompTIA A+ Certification with Exam 220-901

WHAT YOU WILL LEARN

- Security Architecture and Design
- Implementing Governance Compliance Strategies and Risk Management
- Security Access Control models, methods and implementations.
- Disaster Recovery Planning
- Cryptography Methodology
- Operations in Information Security
- Legal, Regulations, Investigations and Compliance in Security
- Vulnerability Assessment
- Continuous Security Lifecycle
- Physical and Software Development Security
- Network Security Considerations

"Interface never disappoints – first class all the way!"

Interface Student
Phoenix, AZ

$3095.00

- 5-day course
- Promo and package discounts may apply

QUESTIONS?
Call 602-266-8585

CAN'T MAKE IT TO CLASS IN PERSON?

Attend many classes online with RemoteLive.™
Call 602-266-8585 today for a live demo.

(course outline on back side)

COURSE OUTLINE

SEC275: CISSP (Certified Information Systems Security Professional)

1. Access Control
- Security Principles and the Principle of Least Privilege
- Confidentiality
- Integrity
- Availability
- Identification, Authentication, Authorization, Access and Accounting
- Authentication Techniques and Standards
- Access Control Models
- Access Control Methods and Implementations
- Access Control Accounting and Auditing

2. Information Security Governance and Risk Management
- Fundamental Principles of Security
- Confidentiality
- Integrity
- Availability
- Balancing the Security Principles
- Security vs. Usability vs. Cost
- Security Definitions
- Types of Security Controls
- Security Frameworks
- ISO/IEC 27001
- COSO
- COBIT
- Process Management
- Security Management
- Risk Management
- Risk Assessment and Analysis
- Asset Classification
- Data Classification
- Risk Mitigation Strategies
- Policies
- Standards
- Guidelines
- Baselines
- Procedures
- Executive Leadership in Risk Management
- Implementing Governance and Compliance Strategies

3. Security Architecture and Design
- Computer System Architecture
- Operating System Security Architecture
- Application Security Architecture
- System Security Models
- Security Architecture Evaluation and Certification
- Trusted Computer System Evaluation Criteria (TCSEC, or Orange Book)
- Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
- System Testing and Certification

4. Business Continuity and Disaster Recovery Planning
- Standards and Best Practices
- Planning for Incidents
- The Business Continuity Process
- Implementing A Disaster Recovery Plan

5. Cryptography
- Overview of Cryptography
- The History of Cryptography (Without Math)
- The Use of Cryptography (With Math)
- Symmetric Key (Shared Secret Key) Cryptography
- Diffie-Hellman Key Agreement
- Asymmetric Key (Public – Private Key) Cryptography
- Digital Signature (Hash) Cryptography
- Implementing All Types of Cryptography in Cryptosystems
- Public Key Infrastructure (PKI) and Certificates
- Encrypted VPN Tunnels
- Digitally Signed Documents and Email
- Encrypting Data At Rest and In Transit

6. Legal, Regulations, Investigations and Compliance
- The Complexity of Cybercrime
- Regions
- Laws
- Law Enforcement
- Privacy Laws
- Intellectual Privacy Laws
- Eavesdropping & Workplace Spying Laws
- Legal Liability and Security Compliance
- Conducting a Security Investigation
- Ethics of Information Security

7. Operations Security (formerly Security Operations)
- The Role of Operations in Information Security
- Personnel Management and Administration
- Planning System Security
- Implementing and Maintaining System Security
- Applying Controls
- System Hardening
- Trusted Recovery
- Configuration Management
- Change Control Process
- Change Control Documentation
- Change Control Compliance and Auditing
- Vulnerability Assessment
- Continuous Security Lifecycle

8. Physical (Environmental) Security
- The Importance of Physical Security in Information Security
- Planning Physical Security
- Identifying and Protecting Assets
- Internal Physical Security Threats and Controls
- Perimeter Physical Security Threats and Controls
- External Physical Security Threats and Controls

9. Software Development Security
- Security as a Part of Software Development
- System Development Lifecycle
- Secure Software Development Lifecycle
- Software Development Models
- Change Control and Update Management
- Cloud Computing
- Web and Mobile Applications
- Database Management and Security
- Malicious Software
- Viruses
- Trojan Horses
- Worms
- Rootkits
- Backdoors

10. Telecommunications and Network Security
- The Open Systems Interconnect Model
- TCP/IP Security
- IPv4 Security and Threats
- IPv6 Security and Threats
- Network Cabling Types and Security Considerations
- Network Devices
- Hubs
- Switches
- Routers
- Bridges
- Gateways
- Security Network Devices
- Firewalls and Content Filters
- Proxy Servers
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Firewalls
- WAN Security
- Dial-Up Network Security
- Virtual Private Network (VPN) Security
- Internet Protocol Security (IPSec)

Register by phone at 602-266-8585, or online at www.InterfaceTT.com.