CISSP - Certified Information Systems Security Professional

Course Outline

1) The Information Security Environment

- Justify an organizational code of ethics
- Relate confidentiality, integrity, availability, non-repudiation, authenticity, privacy and safety to due care and due diligence
- Relate information security governance to organizational business strategies, goals, missions, and objectives
- Apply the concepts of cybercrime to data breaches and other information security compromises
- Relate legal, contractual, and regulatory requirements for privacy and data protection to information security objectives
- Relate transborder data movement and import-export issues to data protection, privacy, and intellectual property protection

2) Information Asset Security

- Relate the IT asset management and data security lifecycle models to information security
- Explain the use of information classification and categorization, as two separate but related processes
- Describe the different data states and their information security considerations
- Describe the different roles involved in the use of information, and the security considerations for these roles
- Describe the different types and categories of information security controls and their use
- Select data security standards to meet organizational compliance requirements

3) Identity and Access Management (IAM)

- Explain the identity lifecycle as it applies to human and nonhuman users
- Compare and contrast access control models, mechanisms, and concepts
- Explain the role of authentication, authorization, and accounting in achieving information security goals and objectives
- Explain how IAM implementations must protect physical and logical assets
- Describe the role of credentials and the identity store in IAM systems

4) Security Architecture and Engineering

- Describe the major components of security engineering standards
- Explain major architectural models for information security
- Explain the security capabilities implemented in hardware and firmware
- Apply security principles to different information systems architectures and their environments
- Determine the best application of cryptographic approaches to solving organizational information security needs
- Manage the use of certificates and digital signatures to meet organizational information security needs

- Discover the implications of the failure to use cryptographic techniques to protect the supply chain
- Apply different cryptographic management solutions to meet the organizational information security needs
- Verify cryptographic solutions are working and meeting the evolving threat of the real world
- Describe defenses against common cryptographic attacks
- Develop a management checklist to determine the organization's cryptologic state of health and readiness

5) Communication and Network Security

- Describe the architectural characteristics, relevant technologies, protocols and security considerations of each of the layers in the OSI model
- Explain the application of secure design practices in developing network infrastructure
- Describe the evolution of methods to secure IP communications protocols
- Explain the security implications of bound (cable and fiber) and unbound (wireless) network environments
- Describe the evolution of, and security implications for, key network devices
- Evaluate and contrast the security issues with voice communications in traditional and VoIP infrastructures
- Describe and contrast the security considerations for key remote access technologies
- Explain the security implications of software-defined networking (SDN) and network virtualization technologies

6) Software Development Security

- Recognize the many software elements that can put information systems security at risk
- Identify and illustrate major causes of security weaknesses in source code
- Illustrate major causes of security weaknesses in database and data warehouse systems
- Explain the applicability of the OWASP framework to various web architectures
- Select malware mitigation strategies appropriate to organizational information security needs
- Contrast the ways that different software development methodologies, frameworks, and guidelines contribute to systems security
- Explain the implementation of security controls for software development ecosystems
- Choose an appropriate mix of security testing, assessment, controls, and management methods for different systems and applications environments

7) Security Assessment and Testing

- Describe the purpose, process, and objectives of formal and informal security assessment and testing
- Apply professional and organizational ethics to security assessment and testing
- Explain internal, external, and third-party assessment and testing

- Explain management and governance issues related to planning and conducting security assessments
- Explain the role of assessment in data-driven security decision-making

8) Security Operations

- Show how to efficiently and effectively gather and assess security data
- Explain the security benefits of effective change management and change control
- Develop incident response policies and plans
- Link incident response to needs for security controls and their operational use
- Relate security controls to improving and achieving required availability of information assets and systems
- Understand the security and safety ramifications of various facilities, systems, and infrastructure characteristics

9) Putting It All Together

- Explain how governance frameworks and processes relate to the operational use of information security controls
- Relate the process of conducting forensic investigations to information security operations
- Relate business continuity and disaster recovery preparedness to information security operations
- Explain how to use education, training, awareness, and engagement with all members of the organization as a way to strengthen and enforce information security processes
- Show how to operationalize information systems and IT supply chain risk management