EC-Council Certified Chief Information Security Officer (CCISO) – Course Outline

EC-Council Accredited Training Center

Domain 1 – Policy, Legal and Compliance

- Defining, implementing, managing and maintaining IS governance programs with leadership, organizational structures and procedures
- Aligning the IS framework with organizational goals and governance
- Creating IS management structures
- Creating an IS governance monitoring framework
- Comprehending standards, directives, regulations, policies, procedures and legal concerns relating information security programs
- Comprehending the different provisions of laws affecting organizational security
- Gramm-Leach-Bliley Act
- Family Educational Rights and Privacy Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- Clinger-Cohen Act
- Privacy Act
- Sarbanes-Oxley
- Familiarity with various standards - ISO 27000 series, Federal Information Processing Standards (FIPS)
- Comprehending federal and organization related public documents for managing operations in computing environments
- Assessing enterprise risk factors related to compliance
- Managing application of IS strategies, plans, procedures and policies for reducing regulatory risk
- Understanding relevance of regulatory IS organizations and correct industry groups, forums and stakeholders
- Comprehending IS changes, trends and best practices
- Managing enterprise compliance program controls
- Understanding IS compliance procedures and processes
- Compiling, analyzing and reporting compliance programs
- Understanding compliance auditing and certification programs
- Understanding and following organizational ethics

Domain 2 - Information Security (IS) Management Controls and Auditing Management

- IS Management Controls
  - Identifying organization operational processes, objectives and risk tolerance levels
  - Designing IS controls aligned with operational needs, goals and performing testing before implementation to ensure efficiency and effectiveness
  - Identifying and choosing resources to implement and maintain IS controls such as:
  - Human capital, information, infrastructure, and architecture

  - Overseeing IS control processes for ensuring implementation that aligns with budgets and scope
  - Communicating progress and successes to stakeholders
  - Designing and implementing IS controls for mitigating risk
  - Monitoring and documenting IS control performance for organizational objectives when they identify and measure metrics and key performance indicators (KPIs)
  - Designing and performing testing of IS controls for ensuring effectiveness, identifying deficiencies and reinforcing alignment with organizational standards, procedures and policies
  - Designing and implementing processes for remediating deficiencies
  - Evaluating problem management practices to ensuring errors are documented, analyzed and solved efficiently
  - Assessing and implementing tools and methods for automating IS control processes
  - Creating IS control status reports for ensuring processes for IS operations, maintenance and support align with organization strategy and objectives
  - Communicating status reports to appropriate stakeholders for executive decisions
- Auditing Management
  - Comprehending IT audit processes and standards
  - Applying IS audit skills, methods and principles to review and test IS technology and applications for designing and implementing risk-based IT audit strategies
  - Performing audit processes that align with set standards and interpreting results against established criteria for ensuring information systems are controlled, effective and secure for supporting objectives and organizations
  - Evaluating audit results, comparing relevancy, accuracy and relevant perspective of conclusions with the audit evidence gathered
  - Assessing exposures produced from ineffective and missing control practices
  - Producing practical and cost-effective plans for enhancing exposures
  - Building IT audit documentation processes and sharing reports with appropriate stakeholders pertinent for decision making
  - Ensuring that audit results are addressed and solutions are implemented efficiently

Domain 3 - Managing Projects and Operations

- Creating clear project scope statements aligning with an organization's objectives
- Defining activities necessary to perform the information systems program, calculating activity time and creating staffing and scheduling plans
- Developing, managing and monitoring the IS program budget, estimate and control costs for projects
- Identifying, negotiating, gaining and managing resources for designing and implementing the IS program
- Acquiring, developing and managing information security project teams
- Assigning information security personnel job functions and supplying continual training for ensuring performance and accountability
- Managing information security personnel and establishing communications and team activities between information systems team members and other security personnel

- Identifying solutions for personnel and team problems regarding time, cost and quality constraints
- Identifying, negotiating and managing vender communication and agreements
- Working with vendors and stakeholders for reviewing and assessing suggested solutions, including:
- Identity incompatibilities
- Challenges
- Problems with suggested solutions
- Evaluating project management controls and practices for seeing if business requirements are accomplished in cost-effects ways while effectively managing risks
- Creating plans to consistently measuring information systems project effectiveness for ensuring system performance
- Identifying stakeholders, managing expectations and communicating documented progress and performance
- Ensuring changes and enhancements to information systems processes are implemented

Domain 4 - Information Security Fundamental Competencies

- Access Control
    - Identifying criteria for mandatory and discretionary access control
    - Understanding various factors related to the design and implementation of access control plans
    - Implementing and managing access control plans that align with principles that manage access control systems such as need-to-know
    - Identifying various access control systems - ID cards and biometrics
    - Comprehending relevancy of warning banners to implement access rules
    - Creating procedures for ensuring system user awareness of IA responsibilities prior to allowing access to information systems
- Social Engineering, Phishing Attacks and Identity Theft
    - Comprehending social engineering terminology, concepts and the role of insider attacks
    - Developing best practices to prevent social engineering attacks
    - Designing response plans for identifying theft
    - Identifying and designing plans for handling phishing attacks
- Physical Security
    - Identifying standards, directives, policies, procedures, regulations and laws relating to physical security
    - Deciding physical asset value and impact
    - Identifying resources for implementing physical security plans
    - Designing, implementing and managing holistic physical security plans for organizational security
    - Setting objectives for personnel security for making sure they align with enterprise security goals
    - Designing and managing physical security audit and update concerns
    - Developing systems to measure physical security performance
- Risk Management
    - Identifying risk mitigation and treatment processes
    - Understanding acceptable risk

  - Identifying resource requirements pertaining to implementing risk management plans
  - Designing systematic and structured risk assessment processes
  - Establishing IT security risk management programs that align with security standards, procedures, and organizational goals
  - Developing and managing risk management teams
  - Setting relationships between incident response and other internal teams in organizations
  - Creating programs to measure incident management
  - Managing risk management tools and methods
  - Comprehending information infrastructure risk
  - Assessing vulnerabilities and threats for identifying security risks and updating security controls
  - Identifying changes for relevant risk management processes and policies
  - Ensuring that current risk management programs align with organizational goals
  - Ensuring that security controls and processes integrate successfully with investment planning processes related to IT and security reports
- Disaster Recovery and Business Continuity Planning
  - Developing, implementing and monitoring business continuity plans in the potential disruptive events
  - Establishing the enterprise continuity scope of operations for:
  - Business continuity
  - Business recovery
  - Contingency planning
  - Disaster recovery
  - Identifying resources and stakeholders for business continuity programs
  - Identifying and prioritizing vital business functions while designing:
  - Emergency delegations of authority
  - Orders of succession for critical roles
  - Enterprise continuity of operations organization structure and staffing models
  - Overseeing contingency planning, operations and programs for risk management
  - Comprehending the results from testing, training and exercising related to critical events
  - Designing and performing test and update plans for operations program continuity
  - Understanding critical nature of IA requirement integration with Continuity of Operations Plan (COOP)
  - Identifying processes for measuring emergency preparedness for:
  - Backup and recovery solutions
  - Designing standard operational procedures to implement in case of disasters
- Firewall, IDS/IPS and Network Defense Systems
  - Identifying intrusion detection and prevention systems
  - Designing and building programs for monitoring firewalls and locating configuration problems
  - Comprehending the perimeter defense systems:
    - Grid sensors and access control lists (ACLs) for network devices such as firewalls and routers
  - Understanding and identifying various components for network security such as network architecture, protocols, models, software and hardware (routers, hubs, etc.)

  - Network segmentation
  - Managing PBX, VOIP and additional VPN, DMZs and telecommunication technologies
  - Hardware and software monitoring, testing and troubleshooting
  - Accounts, system access, and network rights and permissions management
- Wireless Security
  - Managing network security tools
  - Understanding and identifying common wireless network attacks and vulnerabilities
- Virus, Trojans and Malware Threats
  - Measuring risk of threats such as viruses, Trojans, malware and other threats for organizational security
  - Locating potential sources for malware
  - Anti-virus system deployment and management
  - Constructing processes to combat system threats such as malware, Trojans and viruses
- Secure Coding Best Practices and Securing Web Applications
  - Development and maintenance for software assurance programs
    - Ensuring program alignment with System Development Life Cycle (SDLC) phases and secure coding principles
  - Comprehending system-engineering practices
  - Configuring and deploying tools essential in aiding secure program development
  - Software vulnerability analysis methods
  - Installing and operating IT systems in a test configuration scope without affecting program code or security controls and principles
  - Pointing out vulnerabilities and attacks for web applications
  - Security tools for protecting web applications against attacks
- Operating System Hardening
  - Understanding and identifying operating system attacks and vulnerabilities
  - Developing plans for hardening operation systems
  - Utilizing system logs, configuration management and patch management processes
- Encryption Technologies
  - Grasping concepts and terminology for:
    - Encryption and decryption
    - Digital certificates
    - public key infrastructure (PKI)
    - Cryptography and steganography
  - Understanding and identifying cryptosystem components
  - Creating plans for implementing and using information security encryption
- Penetration Testing and Vulnerability Assessment
  - Designing, constructing and implementing programs for penetration testing with pen testing methodologies for verifying organizational security
  - Understanding and identifying penetration testing legal problems and information system vulnerabilities
  - Creating pre and post procedures for testing
  - Planning for penetration testing reporting and implementing technical vulnerability fixes
  - Constructing vulnerability management systems for organizational security
- Incident Response and Computer Forensics

- Creating plans for identifying security violations and actions for reporting incidents
- Ensuring compliance for system termination procedures and incident reporting requirements for potential incidents and breaches
- Reviewing potential security violations for making decisions in the event that network security policies are breached while measuring impact and saving breach evidence
- Diagnosing and developing solutions IA programs resulting from incidents reported
- Designing procedures for incidence response
- Creating guidelines for deciding if security incidents violates laws that require legal action
- Identifying and categorizing persistently volatile system information
- Forensic labs and related programs implementation and management
- Developing an understanding of e-discovery principles, digital media devices, and various file systems
- Constructing and managing teams for forensic investigation
- Constructing and managing digital forensic programs
- Developing processes for investigation:
  - Imaging, data acquisition, analysis and evidence collection
- Evaluating and specifying best practices for acquiring, storing and processing digital evidence
- Configuring and utilizing forensic investigation tools
- Developing and implementing anti-forensic methods

Domain 5 - Strategic Planning and Finance

- Strategic Planning
  - Designing, developing and maintaining enterprise information security architectures (EISA) that follow:
    - IT software and hardware
    - Business processes
    - Local and wide area networks (LANs and WANs)
    - Organizational operations, projects and people that impact enterprise security
  - Executing external analysis of organizations that align with organizational objectives
    - Analyzing competitors, customers, markets, industry environments, etc.
  - Utilizing internal analysis that align with organizational objectives
    - Organizational abilities, measuring system performance, risk management, etc.
  - Identifying and consulting with critical stakeholders for verifying and ensuring complete comprehension of organizational objectives
  - Foreseeing future information security program strategies that align with organizational objectives and goals
  - Identifying and defining critical performance indicators and measuring effectiveness consistently
  - Evaluating and changing IT investments for supporting organizational strategies and objectives
  - Monitoring and updating organizational activities to reinforce security progress and accountability

- Finance
  - Analyzing, projecting and creating IT department operational budgets
  - Acquiring and managing resources to implement and management information security plans
  - Distributing financial resources for processes, projects and units in information security programs
  - Monitoring and reviewing information security cost management, return on investment (ROI) of critical buys for IT infrastructures
    - Align cost management with organizational objectives and overall strategies
  - Identifying and developing reports of financial spending for stakeholders
  - Using Enterprise Information Security Architecture (EISA) suggestions and security priorities for balancing IT security investment portfolios
  - Developing an understanding of the how important of Business Impact Analysis for procurement and the acquisition life cycle
  - Understanding and selecting various procurement strategies
    - Comprehending cost-benefit analysis in procurement of information systems
  - Developing a grasp on procurement concepts
    - Statement of Objectives (SOO)
    - Statement of Work (SOW)
    - Total Cost of Ownership (TCO)
  - Working with stakeholders on IT security service/product procurement
  - Ensuring the implementation of risk-based IT security requirements for:
    - Acquisition plans, statements of work, contracts, cost estimates, and evaluation factors related to service level agreements, award, and additional documents for procurement
  - Designing and developing vendor selection processes and management policies
  - Creating policies for contract administration that dictate IT security services and products evaluations and acceptance
    - Includes security evaluations for software and IT in procurement
  - Creating standards for measuring and reporting on critical objectives in procurement
    - Ensuring alignment with IT security procedures and policies
  - Developing an understanding of Information Assurance (IA) requirements for statements of work (SOW) and additional procurement documents