CCISO

Total Duration: 5 Days, 40 Hours

Domain 1: Governance

Qualifying areas under Domain 1 include (but are not limited to) the following:

- Define, implement, manage and maintain an information security governance program that includes leadership, organizational structures and processes.
- Align information security governance framework with organizational goals and governance, i.e., leadership style, philosophy, values, standards and policies.
- Establish information security management structure.
- Establish a framework for information security governance monitoring (considering cost/benefits analyses of controls and ROI).
- Understand standards, procedures, directives, policies, regulations, and legal issues that affect the information security program.
- Understand the enterprise information security compliance program and manage the compliance team.
- Analyze all the external laws, regulations, standards, and best practices applicable to the organization.
- Understand the various provisions of the laws that affect the organizational security such as 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, etc.
- Be familiar with the different standards such as ISO 27000 series, Federal Information Processing Standards [FIPS].
- Understand the federal and organization specific published documents to manage operations in a computing environment.
- Assess the major enterprise risk factors for compliance.
- Coordinate the application of information security strategies, plans, policies, and procedures to reduce regulatory risk.
- Understand the importance of regulatory information security organizations and appropriate industry groups, forums, and stakeholders.

- Understand the information security changes, trends, and best practices.
- Manage enterprise compliance program controls.
- Understand the information security compliance process and procedures.
- Compile, analyze, and report compliance programs.
- Understand the compliance auditing and certification programs.
- Follow organizational ethics.

Domain 2 Management Controls and Auditing Management

Information Security Management Controls:

- Identify the organization's operational process and objectives as well as risk tolerance level.
- Design information systems controls in alignment with the operational needs and goals and conduct testing prior to implementation to ensure effectiveness and efficiency.
- Identify and select the resources required to effectively implement and maintain information systems controls. Such resources can include human capital, information, infrastructure, and architecture (e.g., platforms, operating systems, networks, databases, applications).
- Supervise the information systems control process to ensure timely implementation in accordance with the outlined budget and scope, and communicate progress to stakeholders.
- Design and implement information systems controls to mitigate risk. Monitor and document the information systems control performance in meeting organizational objectives by identifying and measuring metrics and key performance indicators (KPIs).
- Design and conduct testing of information security controls to ensure effectiveness, discover deficiencies and ensure alignment with organization's policies, standards and procedures.
- Design and implement processes to appropriately remediate deficiencies and evaluate problem management practices to ensure that errors are recorded, analyzed and resolved in a timely manner.
- Assess and implement tools and techniques to automate information systems control processes.
- Produce information systems control status reports to ensure that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives, and share with relevant stakeholders to support executive decisi

Auditing Management

- Understand the IT audit process and be familiar with IT audit standards.

- Apply information systems audit principles, skills and techniques in reviewing and testing information systems technology and applications to design and implement a thorough risk-based IT audit strategy.
- Execute the audit process in accordance with established standards and interpret results against defined criteria to ensure that the information systems are protected, controlled and effective in supporting organization's objectives.
- Effectively evaluate audit results, weighing the relevancy, accuracy, and perspective of conclusions against the accumulated audit evidence.
- Assess the exposures resulting from ineffective or missing control practices and formulate a practical and cost-effective plan to improve those areas.
- Develop an IT audit documentation process and share reports with relevant stakeholders as the basis for decision-making.
- Ensure that the necessary changes based on the audit findings are effectively implemented in a timely manner.
- on-making.

Domain 3 Management Projects and Operations.

Qualifying areas under Domain 3 include (but are not limited to) the following:

- For each information systems project develop a clear project scope statement in alignment with organizational objectives.
- Define activities needed to successfully execute the information systems program, estimate activity duration, and develop a schedule and staffing plan.
- Develop, manage and monitor the information systems program budget, estimate and control costs of individual projects.
- Identify, negotiate, acquire and manage the resources needed for successful design and implementation of the information systems program (e.g., people, infrastructure, and architecture).
- Acquire, develop and manage information security project team.
- Assign clear information security personnel job functions and provide continuous training to ensure effective performance and accountability.
- Direct information security personnel and establish communications, and team activities, between the information systems team and other security-related personnel (e.g., technical support, incident management, security engineering).
- Resolve personnel and teamwork issues within time, cost, and quality constraints.
- Identify, negotiate and manage vendor agreement and communication.
- Participate with vendors and stakeholders to review/assess recommended solutions; identify incompatibilities, challenges, or issues with proposed solutions.

- Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization.
- Develop a plan to continuously measure the effectiveness of the information systems projects to ensure optimal system performance.
- Identify stakeholders, manage stakeholders' expectations and communicate effectively to report progress and performance.
- Ensure that necessary changes and improvements to the information systems processes are implemented as required.

Domain 4 Information Security Core Competence

Access Control

- Identify the criteria for mandatory and discretionary access control, understand the different factors that help in implementation of access controls and design an access control plan.
- Implement and manage an access control plan in alignment with the basic principles that govern the access control systems such as need-to-know.
- Identify different access control systems such as ID cards and biometrics.
- Understand the importance of warning banners for implementing access rules.
- Develop procedures to ensure system users are aware of their IA responsibilities before granting access to the information systems.

Social Engineering, Phishing Attacks, Identity Theft

- Understand various social engineering concepts and their role in insider attacks and develop best practices to counter social engineering attacks.
- Design a response plan to identity theft incidences.
- Identify and design a plan to overcome phishing attacks.

Physical Security

- Identify standards, procedures, directives, policies, regulations and laws for physical security.
- Determine the value of physical assets and the impact if unavailable.
- Identify resources needed to effectively implement a physical security plan.
- Design, implement and manage a coherent, coordinated, and holistic physical security plan to ensure overall organizational security.
- Establish objectives for personnel security to ensure alignment with overall security goals for the enterprise.
- Design and manage the physical security audit and update issues.

- Establish a physical security performance measurement system.

Risk Management

- Identify the risk mitigation and risk treatment processes and understand the concept of acceptable risk.
- Identify resource requirements for risk management plan implementation.
- Design a systematic and structured risk assessment process and establish, in coordination with stakeholders, an IT security risk management program based on standards and procedures and ensure alignment with organizational goals and objectives.
- Develop, coordinate and manage risk management teams.
- Establish relationships between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals)
- Develop an incident management measurement program and manage the risk management tools and techniques.
- Understand the residual risk in the information infrastructure.
- Assess threats and vulnerabilities to identify security risks, and regularly update applicable security controls.
- Identify changes to risk management policies and processes and ensure the risk management program remains current with the emerging risk and threat environment and in alignment with the organizational goals and objectives.
- Determine if security controls and processes are adequately integrated into the investment planning process based on IT portfolio and security reporting.

Disaster Recovery and Business Continuity Planning

- Develop, implement and monitor business continuity plans in case of disruptive events and ensure alignment with organizational goals and objectives.
- Define the scope of the enterprise continuity of operations program to address business continuity, business recovery, contingency planning, and disaster recovery/related activities.
- Identify the resources and roles of different stakeholders in business continuity programs.
- Identify and prioritize critical business functions and consequently design emergency delegations of authority, orders of succession for key positions, the enterprise continuity of operations organizational structure and staffing model.
- Direct contingency planning, operations, and programs to manage risk.
- Understand the importance of lessons learned from test, training and exercise, and crisis events.
- Design documentation process as part of the continuity of operations program.

- Design and execute a testing and updating plan for the continuity of operations program.
- Understand the importance of integration of IA requirements into the Continuity of Operations Plan (COOP).
- Identify the measures to increase the level of emergency preparedness such as backup and recovery solutions and design standard operating procedures for implementation during disasters.

Firewall, IDS/IPS and Network Defense Systems

- Identify the appropriate intrusion detection and prevention systems for organizational information security.
- Design and develop a program to monitor firewalls and identify firewall configuration issues.
- Understand perimeter defense systems such as grid sensors and access control lists on routers, firewalls, and other network devices.
- Identify the basic network architecture, models, protocols and components such as routers and hubs that play a role in network security.
- Understand the concept of network segmentation.
- Manage DMZs, VPN and telecommunication technologies such as PBX and VoIP.
- Identify network vulnerabilities and explore network security controls such as use of SSL and TLS for transmission security.
- Support, monitor, test, and troubleshoot issues with hardware and software.
- Manage accounts, network rights, and access to systems and equipment.

Wireless Security

- Identify vulnerability and attacks associated with wireless networks and manage different wireless network security tools.

Virus, Trojans and Malware Threats

- Assess the threat of virus, Trojan and malware to organizational security and identify sources and mediums of malware infection.
- Deploy and manage anti-virus systems.
- Develop process to counter virus, Trojan, and malware threats.

Secure Coding Best Practices and Securing Web Applications

- Develop and maintain software assurance programs in alignment with the secure coding principles and each phase of System Development Life Cycle (SDLC).
- Understand various system-engineering practices.

- Configure and run tools that help in developing secure programs.
- Understand the software vulnerability analysis techniques.
- Install and operate the IT systems in a test configuration manner that does not alter the program code or compromise security safeguards.
- Identify web application vulnerabilities and attacks and web application security tools to counter attacks.

Hardening OS

- Identify various OS vulnerabilities and attacks and develop a plan for hardening OS systems.
- Understand system logs, patch management process and configuration management for information system security.

Encryption Technologies

- Understand the concept of encryption and decryption, digital certificates, public key infrastructure and the key differences between cryptography and steganography.
- Identify the different components of a cryptosystem.
- Develop a plan for information security encryption techniques.

Vulnerability Assessment And Penetration Testing

- Design, develop and implement a penetration testing program based on penetration testing methodology to ensure organizational security.
- Identify different vulnerabilities associated with information systems and legal issues involved in penetration testing.
- Develop pre and post testing procedures.
- Develop a plan for pen test reporting and implementation of technical vulnerability corrections.
- Develop vulnerability management systems.

Computer Forensics And Incident Response

- Develop a plan to identify a potential security violation and take appropriate action to report the incident.
- Comply with system termination procedures and incident reporting requirements related to potential security incidents or actual breaches.
- Assess potential security violations to determine if the network security policies have been breached, assess the impact, and preserve evidence.
- Diagnose and resolve IA problems in response to reported incidents.
- Design incident response procedures.

- Develop guidelines to determine whether a security incident is indicative of a violation of law that requires specific legal action.
- Identify the volatile and persistent system information.
- Set up and manage forensic labs and programs.
- Understand various digital media devices, e-discovery principles and practices and different file systems.
- Develop and manage an organizational digital forensic program.
- Establish, develop and manage forensic investigation teams.
- Design investigation processes such as evidence collection, imaging, data acquisition, and analysis.
- Identify the best practices to acquire, store and process digital evidence.
- Configure and use various forensic investigation tools.
- Design anti-forensic techniques.

Domain 5 Strategic Planning and Finance.

- **Strategic Planning**
    - Design, develop and maintain enterprise information security architecture (EISA) by aligning business processes, IT software and hardware, local and wide area networks, people, operations, and projects with the organization's overall security strategy.
    - Perform external analysis of the organization (e.g., analysis of customers, competitors, markets and industry environment) and internal analysis (risk management, organizational capabilities, performance measurement etc.) and utilize them to align information security program with organization's objectives.
    - Identify and consult with key stakeholders to ensure understanding of organization's objectives.
    - Define a forward-looking, visionary and innovative strategic plan for the role of the information security program with clear goals, objectives and targets that support the operational needs of the organization.
    - Define key performance indicators and measure effectiveness on continuous basis.
    - Assess and adjust IT investments to ensure they are on track to support organization's strategic objectives.
    - Monitor and update activities to ensure accountability and progress.

Finance

- Analyze, forecast and develop the operational budget of the IT department.

- Acquire and manage the necessary resources for implementation and management of information security plan.
- Allocate financial resources to projects, processes and units within information security program.
- Monitor and oversee cost management of information security projects, return on investment (ROI) of key purchases related to IT infrastructure and security and ensure alignment with the strategic plan.
- Identify and report financial metrics to stakeholders.
- Balance the IT security investment portfolio based on EISA considerations and enterprise security priorities.
- Understand the acquisition life cycle and determine the importance of procurement by performing Business Impact Analysis.
- Identify different procurement strategies and understand the importance of cost-benefit analysis during procurement of an information system.
- Understand the basic procurement concepts such as Statement of Objectives (SOO), Statement of Work (SOW), and Total Cost of Ownership (TCO).
- Collaborate with various stakeholders (which may include internal client, lawyers, IT security professionals, privacy professionals, security engineers, suppliers, and others) on the procurement of IT security products and services.
- Ensure the inclusion of risk-based IT security requirements in acquisition plans, cost estimates, statements of work, contracts, and evaluation factors for award, service level agreements, and other pertinent procurement documents.
- Design vendor selection process and management policy.
- Develop contract administration policies that direct the evaluation and acceptance of delivered IT security products and services under a contract, as well as the security evaluation of IT and software being procured.
- Develop measures and reporting standards to measure and report on key objectives in procurements aligned with IT security policies and procedures.
- Understand the IA security requirements to be included in statements of work and other appropriate procurement documents.