



CCISO: Certified Chief Information Security Officer

Course ID #: 1275-265-ZZ-W

Hours: 35

Course Content

Course Description:

The Certified CISO (CCISO) program is the first of its kind training and certification program aimed at producing top-level information security executives. The CCISO does not focus solely on technical knowledge but on the application of information security management principles from an executive management point of view. The program was developed by sitting CISOs for current and aspiring CISOs.

In order to sit for the CCISO exam and earn the certification, candidates must meet the basic CCISO requirements. Candidates who do not yet meet the CCISO requirements but are interested in information security management can pursue the EC-Council Information Security Management (EISM) certification.

Delivery Method:

This course is delivered through a mix of instructor-led training (ILT) and hands-on labs.

Topics:

Domain 1: Governance and Risk Management

1. Define, Implement, Manage, and Maintain an Information Security Governance Program
 - 1.1. Form of Business Organization
 - 1.2. Industry
 - 1.3. Organizational Maturity
2. Information Security Drivers
3. Establishing an Information Security Management Structure
 - 3.1. Organizational Structure
 - 3.2. Where does the CISO fit within the organizational structure?
 - 3.3. The Executive CISO
 - 3.4. Nonexecutive CISO
4. Laws/Regulations/Standards as drivers of Organizational Policy/Standards/Procedures
5. Managing an enterprise information security compliance program

- 5.1. Security Policy
 - 5.1.1. Necessity of a Security Policy
 - 5.1.2. Security Policy Challenges
- 5.2. Policy Content
 - 5.2.1. Types of Policies
 - 5.2.2. Policy Implementation
- 5.3. Reporting Structure
- 5.4. Standards and Best Practices
- 5.5. Leadership and Ethics
6. Introduction to Risk Management
 - 6.1. Risk Management Standards
 - 6.2. The Essentials of a Risk Management Program
 - 6.3. Where Risk Resides
 - 6.4. Risk Ownership
 - 6.5. Risk Assessment Types
 - 6.6. Risk Assessment Process
 - 6.7. Risk Categories



CCISO: Certified Chief Information Security Officer

Course ID #: 1275-265-ZZ-W

Hours: 35

- 6.8. Risk Treatment
 - 6.9. Risk Modification
 - 6.10. Risk Treatment Options
 - 6.10.1. Risk Modification or Mitigation
 - 6.10.2. Risk Retention or Risk Acceptance
 - 6.10.3. Risk Avoidance or Risk Elimination
 - 6.10.4. Risk Sharing or Risk Transfer
 - 6.11. Applying Compensating Controls to Reduce Risk
 - 6.12. Risk Calculation Formula
 - 6.13. Risk Management Frameworks
 - 6.13.1. ISO 27005
 - 6.13.2. Context Establishment
 - 6.13.3. Risk Assessment
 - 6.13.4. Risk Treatment
 - 6.13.5. Risk Acceptance
 - 6.13.6. Risk Feedback
 - 6.13.7. Risk Communication and Consultation
 - 6.13.8. Risk Monitoring and Review
 - 6.13.9. Risk Monitoring
 - 6.13.10. Risk Communications
 - 6.14. NIST Risk Management Framework (RMF)
 - 6.14.1. Step 1: Categorize the Information System
 - 6.14.2. Step 2: Select Security Controls
 - 6.14.3. Step 3: Implement Security Controls
 - 6.14.4. Step 4: Assess the Information System
 - 6.14.5. Step 5: Authorize the Information System
 - 6.14.6. Step 6: Monitor Security Controls
 - 6.15. NIST Risk Management and Assessment
 - 6.16. NIST Risk Management Hierarchy
 - 6.17. NIST Risk Management Process
 - 6.18. Other Frameworks
 - 6.18.1. COBIT Risk Management
 - 6.18.2. COSO Enterprise Risk Management Integrated Framework
 - 6.18.3. Information Technology Infrastructure Library (ITIL)
 - 6.18.4. Factor Analysis of Information Risk (FAIR)
 - 6.18.5. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
 - 6.18.6. Threat Agent Risk Management (TARA)
 - 6.19. Risk Management Policies and Procedures
 - 6.20. Risk Management Lifecycle
 - 6.21. Risk Management Program Implementation Use Case
 - 6.22. Risk Management Program Review
 - 6.23. Conclusion
- Domain 2: Information Security Controls, Compliance and Audit Management**
- 1. Information Security Controls
 - 1.1. Identifying the Organization's Information Security Needs
 - 1.1.1. Identifying the Optimum Information Security Framework
 - 1.1.2. Designing Security Controls
 - 1.1.3. Control Lifecycle Management
 - 1.1.4. Control Classification
 - 1.1.5. Control Selection and Implementation
 - 1.1.6. Control Catalog
 - 1.1.7. Control Maturity
 - 1.1.8. Monitoring Security Controls
 - 1.1.9. Remediating Control Deficiencies
 - 1.1.10. Maintaining Security Controls
 - 1.1.11. Reporting Controls
 - 1.1.12. Information Security Service Catalog
 - 2. Compliance Management
 - 2.1. Acts, Laws, and Statutes
 - 2.1.1. FISMA



CCISO: Certified Chief Information Security Officer

Course ID #: 1275-265-ZZ-W

Hours: 35

- 2.2. Regulations
 - 2.2.1. GDPR
 - 2.3. Standards
 - 2.3.1. ASD – Information Security Manual
 - 2.3.2. Basel III
 - 2.3.3. FFIEC
 - 2.3.4. ISO 27000 Family of Standards
 - 2.3.5. NERC-CIP
 - 2.3.6. PCI DSS
 - 2.3.7. NIST Special Publications
 - 2.3.8. Statement of Standards for Attestation Engagements No. 16 (SSAE 16)
 - 3. Guidelines, Good and Best Practices
 - 3.1. CIS
 - 3.1.1. OWASP
 - 4. Audit Management
 - 4.1. Audit Expectations and Outcomes
 - 4.2. IS Audit Practices
 - 4.2.1. ISO/IEC Audit Guidance
 - 4.2.2. Internal versus External Audits
 - 4.2.3. Partnering with the Audit Organization
 - 4.2.4. Audit Process
 - 4.2.5. General Audit Standards
 - 4.2.6. Compliance-Based Audits
 - 4.2.7. Risk-Based Audits
 - 4.2.8. Managing and Protecting Audit Documentation
 - 4.2.9. Performing an Audit
 - 4.2.10. Evaluating Audit Results and Report
 - 4.2.11. Remediating Audit Findings
 - 4.2.12. Leverage GRC Software to Support Audits
 - 5. Summary
- Domain 3: Security Program Management and Operations**
- 1. Program Management
 - 1.1. Defining a Security Charter, Objectives, Requirements, Stakeholders, and Strategies
 - 1.1.1. Security Program Charter
 - 1.1.2. Security Program Objectives
 - 1.1.3. Security Program Requirements
 - 1.1.4. Security Program Stakeholders
 - 1.1.5. Security Program Strategy Development
 - 1.2. Executing an Information Security Program
 - 1.3. Defining and Developing the Information Security Program 125
 - 1.4. Defining and Developing Information Security Program Staffing Requirements
 - 1.5. Managing the People of a Security Program
 - 1.5.1. Resolving Personnel and Teamwork Issues
 - 1.5.2. Managing Training and Certification of Security Team Members
 - 1.5.3. Clearly Defined Career Path
 - 1.5.4. Designing and Implementing a User Awareness Program
 - 1.6. Managing the Architecture and Roadmap of the Security Program
 - 1.6.1. Information Security Program Architecture
 - 1.6.2. Information Security Program Roadmap
 - 1.7. Program Management and Governance
 - 1.7.1. Understanding Project Management Practices and Controls
 - 1.7.2. Identifying and Managing Project Stakeholders
 - 1.7.3. Measuring the Effectiveness of Projects
 - 1.8. Business Continuity Management (BCM) and Disaster Recovery Planning (DRP)
 - 1.9. Data Backup and Recovery
 - 1.10. Backup Strategy
 - 1.11. ISO BCM Standards
 - 1.11.1. Business Continuity Management (BCM)
 - 1.11.2. Disaster Recovery Planning (DRP)
 - 1.12. Continuity of Security Operations



CCISO: Certified Chief Information Security Officer

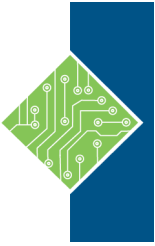
Course ID #: 1275-265-ZZ-W

Hours: 35

- 1.12.1. Integrating the Confidentiality, Integrity and Availability (CIA) Model
- 1.13. BCM Plan Testing
- 1.14. DRP Testing 141
- 1.15. Contingency Planning, Operations, and Testing Programs to Mitigate Risk and Meet Service Level Agreements (SLAs)
- 1.16. Computer Incident Response
 - 1.16.1. Incident Response Tools
 - 1.16.2. Incident Response Management
 - 1.16.3. Incident Response Communications
 - 1.16.4. Post-Incident Analysis
 - 1.16.5. Testing Incident Response Procedures
- 1.17. Digital Forensics
 - 1.17.1. Crisis Management
 - 1.17.2. Digital Forensics Lifecycle
- 2. Operations Management
 - 2.1. Establishing and Operating a Security Operations (SecOps) Capability
 - 2.2. Security Monitoring and Security Information and Event Management (SIEM)
 - 2.3. Event Management
 - 2.4. Incident Response Model
 - 2.4.1. Developing Specific Incident Response Scenarios
 - 2.5. Threat Management
 - 2.6. Threat Intelligence
 - 2.6.1. Information Sharing and Analysis Centers (ISAC)
 - 2.7. Vulnerability Management
 - 2.7.1. Vulnerability Assessments
 - 2.7.2. Vulnerability Management in Practice
 - 2.7.3. Penetration Testing
 - 2.7.4. Security Testing Teams
 - 2.7.5. Remediation
 - 2.8. Threat Hunting
- 3. Summary

Domain 4: Information Security Core Competencies

- 1. Access Control
 - 1.1. Authentication, Authorization, and Auditing
 - 1.2. Authentication
 - 1.3. Authorization
 - 1.4. Auditing
 - 1.5. User Access Control Restrictions
 - 1.6. User Access Behavior Management
 - 1.7. Types of Access Control Models
 - 1.8. Designing an Access Control Plan
 - 1.9. Access Administration
- 2. Physical Security
 - 2.1. Designing, Implementing, and Managing Physical Security Program
 - 2.1.1. Physical Risk Assessment
 - 2.2. Physical Location Considerations
 - 2.3. Obstacles and Prevention
 - 2.4. Secure Facility Design
 - 2.4.1. Security Operations Center
 - 2.4.2. Sensitive Compartmented Information Facility
 - 2.4.3. Digital Forensics Lab
 - 2.4.4. Datacenter
 - 2.5. Preparing for Physical Security Audits
- 3. Network Security
 - 3.1. Network Security Assessments and Planning
 - 3.2. Network Security Architecture Challenges
 - 3.3. Network Security Design
 - 3.4. Network Standards, Protocols, and Controls
 - 3.4.1. Network Security Standards
 - 3.4.2. Protocols
 - 3.4.3. Network Security Controls
 - 3.5. Wireless (Wi-Fi) Security
 - 3.5.1. Wireless Risk
 - 3.5.2. Wireless Controls
 - 3.6. Voice Over IP Security

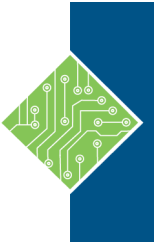


CCISO: Certified Chief Information Security Officer

Course ID #: 1275-265-ZZ-W

Hours: 35

4. Endpoint Protection
 - 4.1. Endpoint Threats
 - 4.2. Endpoint Vulnerabilities
 - 4.3. End User Security Awareness
 - 4.4. End User Device Hardening
 - 4.5. Endpoint Device Logging
 - 4.6. Mobile Device Security
 - 4.6.1. Mobile Device Risk
 - 4.6.2. Mobile Device Security Controls
 - 4.7. Internet of Things Security (IoT)
 - 4.7.1. Protecting IoT Devices
 5. Application Security
 - 5.1. Secure SDLC Model
 - 5.2. Separation of Development, Test, and Production Environments
 - 5.3. Application Security Testing Approaches
 - 5.4. DevSecOps
 - 5.5. Waterfall Methodology and Security
 - 5.6. Other Application Development Approaches
 - 5.7. Application Hardening
 - 5.8. Application Security Technologies
 - 5.9. Version Control and Patch Management
 - 5.10. Database Security
 - 5.11. Database Hardening
 - 5.12. Secure Coding Practices
 6. Encryption Technologies
 - 6.1. Encryption and Decryption
 - 6.2. Cryptosystems
 - 6.2.1. Blockchain
 - 6.2.2. Digital Signatures and Certificates
 - 6.2.3. PKI
 - 6.2.4. Key Management
 - 6.3. Hashing
 - 6.4. Encryption Algorithms
 - 6.5. Encryption Strategy Development
 - 6.5.1. Determining Critical Data Location and Type
 - 6.5.2. Deciding What to Encrypt
 - 6.5.3. Determining Encryption Requirements
 - 6.5.4. Selecting, Integrating, and Managing Encryption Technologies
 7. Virtualization Security
 - 7.1. Virtualization Overview
 - 7.2. Virtualization Risks
 - 7.3. Virtualization Security Concerns
 - 7.4. Virtualization Security Controls
 - 7.5. Virtualization Security Reference Model
 8. Cloud Computing Security
 - 8.1. Overview of Cloud Computing
 - 8.2. Security and Resiliency Cloud Services
 - 8.3. Cloud Security Concerns
 - 8.4. Cloud Security Controls
 - 8.5. Cloud Computing Protection Considerations
 9. Transformative Technologies
 - 9.1. Artificial Intelligence
 - 9.2. Augmented Reality
 - 9.3. Autonomous SOC
 - 9.4. Dynamic Deception
 - 9.5. Software-Defined Cybersecurity
 10. Summary
- Domain 5: Strategic Planning, Finance, Procurement and Vendor Management**
1. Strategic Planning
 - 1.1. Understanding the Organization
 - 1.1.1. Understanding the Business Structure
 - 1.1.2. Determining and Aligning Business Information Security Goals
 - 1.1.3. Identifying Key Sponsors, Stakeholders, and Influencers
 - 1.1.4. Understanding Organizational Financials
 - 1.2. Creating an Information Security Strategic Plan
 - 1.2.1. Strategic Planning Basics
 - 1.2.2. Alignment to Organizational Strategy and Goals



CCISO: Certified Chief Information Security Officer

Course ID #: 1275-265-ZZ-W

Hours: 35

- 1.2.3. Defining Tactical Short, Medium, and Long-Term Information Security Goals
 - 1.2.4. Information Security Strategy Communication
 - 1.2.5. Creating a Culture of Security
 2. Designing, Developing, and Maintaining an Enterprise Information Security Program
 - 2.1. Ensuring a Sound Program Foundation
 - 2.2. Architectural Views
 - 2.3. Creating Measurements and Metrics
 - 2.4. Balanced Scorecard
 - 2.5. Continuous Monitoring and Reporting Outcomes
 - 2.6. Continuous Improvement
 - 2.7. Information Technology Infrastructure Library (ITIL) Continual Service Improvement (CSI)
 3. Understanding the Enterprise Architecture (EA)
 - 3.1. EA Types
 - 3.1.1. The Zachman Framework
 - 3.1.2. The Open Group Architecture Framework (TOGAF)
 - 3.1.3. Sherwood Applied Business Security Architecture (SABSA)
 - 3.1.4. Federal Enterprise Architecture Framework (FEAF)
 4. Finance
 - 4.1. Understanding Security Program Funding
 - 4.2. Analyzing, Forecasting, and Developing a Security Budget
 - 4.2.1. Resource Requirements
 - 4.2.2. Define Financial Metrics
 - 4.2.3. Technology Refresh
 - 4.2.4. New Project Funding
 - 4.2.5. Contingency Funding
 - 4.3. Managing the Information Security Budget
 - 4.3.1. Obtain Financial Resources
 - 4.3.2. Allocate Financial Resources
 - 4.3.3. Information Security Financial Management
 - 4.3.4. Developing an Information Security Program Budget
 - 4.3.5. Managing an Information Security Program Budget
 - 4.3.6. Report Metrics to Sponsors and Stakeholders
 - 4.3.7. Balancing the Information Security Budget
 5. Procurement
 - 5.1. Procurement Program terms and Concepts
 - 5.1.1. Statement of Objectives (SOO)
 - 5.1.2. Statement of Work (SOW)
 - 5.1.3. Total Cost of Ownership (TCO)
 - 5.1.4. Request for Information (RFI)
 - 5.1.5. Request for Proposal (RFP)
 - 5.1.6. Master Service Agreement (MSA)
 - 5.1.7. Service Level Agreement (SLA)
 - 5.1.8. Terms and Conditions (T&C)
 - 5.2. Understanding the Organization's Procurement Program
 - 5.2.1. Internal Policies, Processes, and Requirements
 - 5.2.2. External or Regulatory Requirements
 - 5.2.3. Local versus Global Requirements
 - 5.3. Procurement Risk management
 - 5.3.1. Standard Contract Language
 6. Vendor Management
 - 6.1. Understanding the Organization's Acquisition Policies and Procedures
 - 6.1.1. Procurement Lifecycle
 - 6.2. Applying Cost-Benefit Analysis (CBA) During the Procurement Process
 - 6.3. Vendor management Policies
 - 6.4. Contract Administration Policies
 - 6.4.1. Service and Contract Delivery Metrics
 - 6.4.2. Contract Deliver Reporting
 - 6.4.3. Change Requests
 - 6.4.4. Contract Renewal



CCISO: Certified Chief Information Security Officer

Course ID #: 1275-265-ZZ-W

Hours: 35

6.4.5. Contract Closure

6.5. Delivery Assurance

6.5.1. Validation of Meeting Contractual Requirements

6.5.2. Formal Delivery Audits

6.5.3. Periodic Random Delivery Audits

6.5.4. Third-Party Attestation Services (TPRM)

7. Summary