InterNetwork Academy

# Certified Chief Information Security Officer Version 4

## COURSE *Outline*

*Join The New Generation of*
***Information Security Leaders***

EC-Council
Official Curricula

EC-Council C|CISO Certified Chief Information Security Officer

InterNetwork Academy

CERTIFIED CHIEF INFORMATION SECURITY OFFICER

# Certified Chief Information Security Officer (CCISO)

## Course Outline

*(Version 4)*

### Domain 1: Governance; Risk Management; Security, Compliance, and Privacy; and Audit Management

1. Fundamentals of Information Security Governance
    - 1.1. Introduction to Information Security Governance
    - 1.2. Foundation of Information Security Programs
    - 1.3. Understanding Business Organization Structures
    - 1.4. Understanding Business Organization Structures (cont'd)
    - 1.5. Industry Impact on Governance
    - 1.6. CISO's Impact on Governance
    - 1.7. CMMI Process Model Overview
    - 1.8. Organizational Maturity Models
    - 1.9. Reactive vs. Proactive Organizations
    - 1.10. Aligning IS with Organizational Goals
    - 1.11. Strategic Security Planning
    - 1.12. Organizational Security Architecture
    - 1.13. Security Operating Model Framework
    - 1.14. Governance Structure and Hierarchy
    - 1.15. Governance Structure and Hierarchy Diagram
    - 1.16. Executive vs Non-Executive CISO
    - 1.17. Role of the CISO in Modern Organizations
    - 1.18. C-Suite Attitudes Toward Information Security
    - 1.19. C-Suite Attitudes Toward Information Security – cont.
    - 1.20. Leadership and Management Skills for CISOs
    - 1.21. Ethics in Information Security

1.22. Professional Code of Ethics
1.23. Information Security Documentation Framework

2. Risk Management Foundations
   2.1. Understanding Risk Management Fundamentals
   2.2. Understanding Risk Management Fundamentals – cont.
   2.3. Defining Organizational Risk
   2.4. Risk Management Program Components
   2.5. Risk Categories and Classifications
   2.6. Risk Ownership and Accountability
   2.7. Risk Appetite and Tolerance
   2.8. Asset Identification and Valuation
   2.9. Asset Identification and Valuation – cont.
   2.10. Threat Assessment Methodologies
   2.11. ISO/IEC 27005:2022 Annex A Threats
   2.12. Vulnerability Analysis Framework
   2.13. ISO/IEC 27005:2022 Annex A Vulnerabilities
   2.14. Risk Assessment Process
   2.15. Quantitative Risk Analysis
   2.16. Quantitative Risk Analysis – cont.
   2.17. Qualitative Risk Analysis
   2.18. Qualitative Risk Analysis – cont.
   2.19. Risk Assessment Categories
   2.20. Risk Assessment Focus Types
   2.21. Risk Calculation Methodologies
   2.22. Annualized Loss Expectancy Models
   2.23. Risk Management Lifecycle
   2.24. Risk Register
   2.25. Risk Treatment Options
   2.26. Risk Treatment Options – cont.
   2.27. Risk Treatment Options – cont. 2
   2.28. Risk Treatment Options – cont. 3
   2.29. Risk Modification Strategies
   2.30. Risk Acceptance Criteria
   2.31. Risk Acceptance Criteria – cont.

2.32. Risk Transfer Mechanisms
2.33. Risk Transfer Mechanisms – cont.

3. Security Controls and Implementation
   3.1. Understanding Security Controls
   3.2. CIA Triad Implementation
   3.3. Control Categories and Classifications
   3.4. Control Attributes
   3.5. COSO PDC Defense-In-Depth Model
   3.6. Preventive Control Mechanisms
   3.7. Detective Control Systems
   3.8. Corrective Control Measures
   3.9. Deterrent Control Measures
   3.10. Control Lifecycle Management
   3.11. Control Selection Criteria
   3.12. Control Implementation Strategy
   3.13. Control Maturity Assessment
   3.14. Compensating Controls Framework
   3.15. Security Control Documentation
   3.16. Control Monitoring Systems
   3.17. Control Testing Methodologies
   3.18. Security Control Catalog Management
   3.19. Service Catalog Development
   3.20. Risk Management Frameworks
   3.21. Risk Management Frameworks – cont.
   3.22. Risk Management Frameworks – cont. 2
   3.23. Risk Management Frameworks – cont. 3
   3.24. Risk Management Frameworks – cont. 4
   3.25. Change Management in Control Systems and Updates
4. CISO Role in the AI Era
   4.1. Evolving Cybersecurity Landscape
   4.2. Role of CISO in AI Era
   4.3. Impact of Digital Transformation and AI Adoption
   4.4. Benefits of AI Integration in Cybersecurity
   4.5. Limitations of AI in Cybersecurity

- 4.6. Balancing AI Benefits and Limitations

5. Leveraging AI for Governance and Compliance
   - 5.1. Enhancing Cybersecurity Governance through AI
   - 5.2. Mapping AI to Cybersecurity Frameworks
   - 5.3. Mapping AI to NIST Cybersecurity Framework (CSF)
   - 5.4. Mapping AI to ISO 27001
   - 5.5. Mapping AI to COBIT
   - 5.6. AI-Supported Policy Enforcement and Monitoring
   - 5.7. How AI Supports Policy Enforcement
   - 5.8. Best Practices for Implementing AI in Policy Enforcement and Monitoring
   - 5.9. Continuous Controls Monitoring (CCM) with AI
   - 5.10. Best Practices for Implementing AI in CCM
   - 5.11. AI Governance Board or Committee
   - 5.12. Setting up an AI Governance Board or Committee
   - 5.13. Challenges in Setting Up an AI Governance Board
   - 5.14. Best Practices for AI Governance
6. Establishing Cybersecurity Governance for AI
   - 6.1. AI in Risk Management: A CISO's Strategic Advantage
   - 6.2. AI and Predictive Risk Modeling
   - 6.3. Risk Scoring and Prioritization with AI
   - 6.4. Automated Risk Assessments with AI
   - 6.5. Enhanced Risk Management Decision-Making with AI
   - 6.6. Key Challenges in Leveraging AI for Risk Management
7. Risk Management for AI
   - 7.1. Critical AI Risks
   - 7.2. Critical AI Risks (Cont'd)
   - 7.3. Risk Assessment Templates for AI Projects
   - 7.4. Key Components of an AI Risk Assessment Template
   - 7.5. Example Risk Assessment Template for AI Projects
   - 7.6. Best Practices for Using Risk Assessment Templates in AI Projects
   - 7.7. AI-Specific Threat Modeling
   - 7.8. Operational Risk Controls for AI
   - 7.9. Operational Risk Controls Implementation Checklist

7.10. Establishing AI Risk Registers and Mitigation Controls

7.11. Best Practices for AI Risk Management

8. Tools and Technologies for AI-Driven GRC

8.1. AI Risk Management Frameworks and Platforms

8.2. ENISA Guidelines for AI Systems

8.3. Model Validation and Testing Tools

8.4. Performance Drift and Anomaly Monitoring Tools

8.5. Explainable AI (XAI) Tools

8.6. Governance and Compliance Automation Tools

8.7. AI-Powered Enterprise Tools

8.8. CISO Responsibilities and Considerations for AI Tools

9. Compliance and Regulatory Framework

9.1. Regulatory Compliance Overview

9.2. Legal Framework for Information Security

9.3. International Compliance Standards

9.4. Industry-Specific Regulations

9.5. GDPR Requirements Implementation

- EU Cybersecurity Act (EUCSA)
- ENISA Guidelines
- Digital Operational Resilience Act (DORA)

9.6. HIPAA Compliance Framework

- Japan's Act on the Protection of Personal Information (APPI)
- Brazil's General Data Protection Law (LGPD)

9.7. HITECH

9.8. PCI DSS Standards Overview

9.9. SOX Compliance Requirements

9.10. FISMA Implementation Guidelines

9.11. Australian Privacy Act 1988

9.12. Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)

9.13. Brazilian General Data Protection Law (LGPD)

9.14. Singapore Personal Data Protection Act (PDPA)

9.15. Data Privacy Regulations

9.16. State-Level Privacy Laws

9.17. Cross-Border Data Protection
9.18. Regulatory Reporting Requirements
9.19. Compliance Documentation Standards
9.20. Privacy Impact Assessments
9.21. Regulatory Risk Management
9.22. Compliance Program Development
9.23. Privacy Program Implementation
9.24. Regulatory Change Management

10. Security Frameworks, Standards, Laws, Acts and Directives
    10.1. NIST CSF Cybersecurity Framework
    10.2. NIST CSF Cybersecurity Framework – cont.
    10.3. ISO 27001 Implementation
        - Australian Government Information Security Manual (ISM)
        - Australian Privacy Principles (APPs)
        - Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
    10.4. COBIT Framework Overview
        - Singapore's Cybersecurity Code of Practice
        - Indian IT Act 2000 with CERT-In Guidelines
    10.5. ITIL Security Management
    10.6. ITILv4
    10.7. MITRE ATT&CK® & MITRE ATLAS
    10.8. OWASP SAMM & ASVS
    10.9. Zero Trust Architecture
    10.10. Cloud Security Framework
    10.11. ENISA Guidelines on Cloud Security (EU)
    10.12. Australian Cyber Security Centre (ACSC) Essential Eight Framework
    10.13. CIS Controls (Center for Internet Security – Global)
    10.14. BSI IT-Grundschutz (Germany)
    10.15. Artificial Intelligence in IS
    10.16. Risk Management Frameworks
    10.17. NIST SP 800-37 Framework Steps
    10.18. NIST Security Control Classes
    10.19. NIST SP 800-37: Hierarchy

10.20. NIST SP 800-37: Risk Process
10.21. ISO27005: Risk Process
10.22. Security Control Frameworks
10.23. Risk Management Standards
10.24. NIST Family
10.25. NIST Family – cont.
10.26. ISO27K Family
10.27. ISO27K Family – cont.
10.28. Framework Integration Strategies
10.29. Other Risk Frameworks
10.30. COBIT Risk Framework
10.31. COSO – Enterprise Risk Management Framework
10.32. Information Technology Infrastructure Library (ITIL)
10.33. Factor Analysis of Information Risk (FAIR)
10.34. Operationally Critical Threat, Asset, And Vulnerability Evaluation (OCTAVE)
10.35. Threat Assessment and Remediation Analysis
10.36. ISACA Risk IT Framework
10.37. Security Policy Development
10.38. Security Policy Development - cont.
10.39. Security Policy Challenges
10.40. Security Policy ISO 27001 C5.2
10.41. Types of Policies
10.42. Security Metrics and Measurements
10.43. NIS2 Directive
10.44. EU AI Act
10.45. ePrivacy Directive
10.46. Digital Personal Data Protection Act, 2023 (DPDP Act)
10.47. CERT-In Cybersecurity Directions (2022)
10.48. APPI (Act on Protection of Personal Information)

11. Audit and Assessment
    11.1. Audit Expectations and Outcomes
    11.2. Information Security Audit Practice
    11.3. NIST, COBIT AUDIT GUIDANCE

11.4. INTERNAL Versus EXTERNAL Audits
11.5. Partnering with Organization
11.6. Audit Process
11.7. General Audit Standards
11.8. Type-Based AUDITS
11.9. Performing and Evaluating AUDIT Results in an AUDIT
11.10. Remediating Audit Findings
11.11. Leveraging GRC SOFTWARE to Support AUDITS
11.12. Leveraging AI to Enhance Security Audits
11.13. AI-Driven Security Audit Tools
11.14. AI for Security Audit: Auditing AI Tools

12. Summary
13. Questions

**Domain 2: Organizational Executive Leadership**

1. FOUNDATIONS OF LEADERSHIP
   1.1. Domain Outline
   1.2. Introduction to Leadership's Role and Impact
   1.3. Why Leadership Matters: Core Constituents
   1.4. Definition of a Leader and Leadership Needs
   1.5. Leaders vs Managers: Kotter's Framework
   1.6. Key Similarities Between Leaders and Managers
   1.7. Transitioning from Manager to Leader
   1.8. Building Leadership Confidence
   1.9. Transforming from Boss to Leader
   1.10. Role of Leadership in Organizational Success
   1.11. Why Organizations Exist: Purpose and Goals
   1.12. The Organizational Need for Leaders
   1.13. Leaders as Organizational Change Agents
   1.14. Leadership During Crisis and Failure
   1.15. Information Security Leadership Role
   1.16. Building Security Maturity Capabilities
   1.17. Evolution of Information Security Leadership
   1.18. Ancient Leadership: Mesopotamia to Rome
   1.19. Power and Authority in Leadership

1.20. Types of Authority in Leadership
1.21. Power and Authority in Leadership
1.22. Persuasion and Influence Techniques
1.23. Traditional Leadership Approaches
1.24. Leadership Types and Their Applications
1.25. Leadership Styles
1.26. Leadership Theories and Models
1.27. Leadership Environments and Contexts

2. PERSONAL LEADERSHIP DEVELOPMENT
2.1. Developing Executive Presence: Key Components
2.2. Overcoming Challenges to Executive Presence
2.3. Building and Promoting Personal Brand
2.4. Personal Brand Communication Strategies
2.5. Leadership Self-Awareness Development
2.6. Strategies for Cultivating Self-Awareness
2.7. Emotional Intelligence in Leadership
2.8. Social Intelligence Development
2.9. Cultural Intelligence Enhancement
2.10. Key components of Cultural Intelligence
2.11. Applying Social and Cultural Intelligence
2.12. Building Professional Leadership Networks
2.13. Understanding Team Member Personalities
2.14. Myers-Briggs Type Indicator in Leadership
2.15. Leadership Feedback and Self-Assessment
2.16. Developing Leadership Convictions
2.17. Building Resilience in Uncertain Times
2.18. Building Resilience During Uncertain Times
2.19. Leading and Supporting During Uncertainty
2.20. Adaptability and Agility Development
2.21. Persuasive Business Communication
2.22. Time Management and Priority Setting
2.23. Negotiation and Dispute Resolution
2.24. Leadership Problem-Solving Approaches
2.25. Quantitative Decision-Making Methods

2.26. Behavioral Finance in Leadership
2.27. Personal Development Planning
2.28. Leadership Role Readiness

3. LEADING TEAMS AND PEOPLE
   3.1. Cultivating Future Leaders: Key Strategies
   3.2. Leadership Talent Identification
   3.3. Leadership Talent Retention
   3.4. Succession Planning Implementation
   3.5. Effective Leadership Delegation
   3.6. Team Building for Collaboration
   3.7. Leading Inclusive Teams
   3.8. Virtual Team Management
   3.9. Managing Up: Working with Superiors
   3.10. Managing Down: Supporting Teams
   3.11. Managing Laterally: Cross-Functional Collaboration
   3.12. Performance Evaluation Methods
   3.13. Managing Difficult Conversations
   3.14. Building Team Loyalty and Commitment
   3.15. Team Motivation Strategies
   3.16. Mentoring and Coaching Practices
   3.17. Leading with Empathy
   3.18. Ethical Leadership Development
4. ORGANIZATIONAL LEADERSHIP
   4.1. Board Relationship Management
   4.2. Building Board Trust and Credibility
   4.3. Board Communication Strategies
   4.4. Securing Funding and Sponsorship
   4.5. Organizational Leadership at Scale and Scope
   4.6. Organizational Leadership at Scale and Scope - Cont.
   4.7. T-Shaped Leadership Approach
   4.8. Strategic vs Tactical Leadership
   4.9. Organizational Change Leadership
   4.10. Strategic Analysis Framework
   4.11. Understanding Organizational Internal Context

- 4.12. Understanding Organizational External Context
- 4.13. SWOT Analysis Implementation
- 4.14. Change Planning and Execution
- 4.15. Change Communication Strategies
- 4.16. Building Sustainable Competitive Advantage
- 4.17. Information Security Group Branding
- 4.18. Security Brand Communication
- 4.19. Education and Awareness Leadership
- 4.20. Stakeholder Management Strategies
- 4.21. Regulatory Compliance Leadership
- 4.22. Crisis and Disaster Management
- 4.23. Crisis and Disaster Management – Cont.
- 4.24. Crisis and Disaster Management – Cont.
- 4.25. Business Intelligence Applications
- 4.26. Leading Innovative Projects
- 4.27. Industry-Specific Leadership Challenges
- 4.28. Considerations of Various Industries

5. Responsible and Ethical AI Leadership
   - 5.1. Role of CISO in AI Ethics and Governance Boards
   - 5.2. Key Responsibilities in AI Ethics Governance
   - 5.3. Embedding AI Ethical Principles into Cybersecurity
   - 5.4. Privacy Risks in Large Language Models (LLMs) and Generative AI
   - 5.5. Why Leadership Matters: Core Constituents
   - 5.6. Mitigating Privacy Risks in Large Language Models and Generative AI
   - 5.7. Embedding Fairness, Accountability, and Transparency in AI Development
   - 5.8. Embedding Fairness, Accountability, and Transparency in AI Development (Cont'd)
   - 5.9. Ethical Frameworks: OECD AI Principles
   - 5.10. Ethical Frameworks: UNESCO AI Ethics
6. Cross-Functional AI Innovation Leadership
   - 6.1. Role of CISO in Cross-Functional AI Initiatives
   - 6.2. Strategic Collaboration Activities in AI Initiatives
   - 6.3. Cross-Functional AI Governance
   - 6.4. Responsibilities of the CISO in AI Governance Bodies

6.5. AI Awareness and Training Across Departments
6.6. Role of CISO in AI Awareness and Training Across Departments
6.7. Managing AI Talent Development Within Cybersecurity

7. Strategic AI Alignment and Innovation Management
   7.1. Role of CISO in Aligning AI Innovation with Enterprise Strategy
   7.2. Aligning AI Innovation to Business and Security Strategy
   7.3. Balancing AI Experimentation with Compliance and Control
   7.4. Communicating AI Risk Posture to the Board and Executive Leadership
   7.5. Investment Planning for AI Innovation and Risk Management
   7.6. Vendor Evaluation and Third-Party AI Risk Considerations
8. Summary
9. Practice Questions

**Domain 3: Information Security Controls, Security Program Management and Operations**

1. Introduction and Program Management Fundamentals
   1.1. CISO Evolution: From Tech to Strategy
   1.2. Evolution of CISO's Role
   1.3. Evolution of CISO's Role (Cont'd)
   1.4. Leadership Misconception
   1.5. Knowledge Prerequisites for Information Security Management
   1.6. Core Security Program Execution Principles
   1.7. CISO's Mind Map
   1.8. Business Objective Alignment Strategies
   1.9. Information Security Program Definition Process
   1.10. Program Development Framework
   1.11. Effective Program Management Techniques
   1.12. Program Monitoring and Assessment
   1.13. Key Accounting Concepts in Security
   1.14. Asset Management Fundamentals
   1.15. Asset Lifecycle Management
   1.16. Cost-Benefit Analysis Methods
   1.17. Understanding Security Program Liabilities
   1.18. Net Present Value in Security Investments

1.19. NPV vs IRR
1.20. Profit and Loss Statement Analysis
1.21. ROI Calculation in Security Programs
1.22. Strategic Cost Avoidance
1.23. Security Program Revenue Considerations
1.24. Expense Management Framework
1.25. Security Budget Planning
1.26. Financial Resource Allocation

2. Financial and Resource Management
   2.1. Budget Development Strategies
   2.2. Understanding CapEx in Security
   2.3. Understanding CapEx in Security (Cont'd)
   2.4. OpEx Management Principles
   2.5. CAPEX vs OPEX
   2.6. Budgeting Methodologies Comparison
   2.7. Security Program Cash Flow
   2.8. Burn Rate Monitoring Techniques
   2.9. Strategic Staffing Analysis
   2.10. Administrative Resource Planning
   2.11. Security Delivery Team Structure
   2.12. Technical Competency Requirements
   2.13. Operations Staff Development
   2.14. Digital Forensics Capabilities
   2.15. Cross-Functional Skill Development
   2.16. Team Management Excellence
   2.17. Professional Development Planning
   2.18. Career Advancement Frameworks
   2.19. Security Awareness Strategy
   2.20. Awareness Program Implementation
   2.21. Role-Based Security Education
3. Program Architecture and Operations
   3.1. Security Architecture Principles
   3.2. Program Roadmap Development
   3.3. Project Management Fundamentals

- 3.4. Project Initiation Best Practices
- 3.5. Strategic Project Planning
- 3.6. Execution Phase Management
- 3.7. Monitoring Framework Implementation
- 3.8. Project Closure Procedures
- 3.9. Operations Management Strategy
- 3.10. Conflict Resolution Techniques
- 3.11. Time Management in Disputes
- 3.12. Cost Impact Analysis
- 3.13. Quality Assurance in Operations
- 3.14. Vendor Management Fundamentals
- 3.15. Strategic Vendor Selection
- 3.16. Negotiation Best Practices
- 3.17. Contract Management Principles
- 3.18. Long-term Vendor Relations
- 3.19. Vendor Community Building

4. Stakeholder Management and Project Assessment
   - 4.1. Enhanced Project Management
   - 4.2. Performance Measurement Systems
   - 4.3. Technical Performance Indicators
   - 4.4. Business Alignment Metrics
   - 4.5. Project Success Metrics
   - 4.6. Data Collection Frameworks
   - 4.7. Analysis and Reporting
   - 4.8. Continuous Improvement Process
   - 4.9. Internal Stakeholder Engagement
   - 4.10. External Stakeholder Management
   - 4.11. Communication Strategy Development
   - 4.12. Expectation Management
   - 4.13. Process Enhancement Methods
   - 4.14. Change Management Framework
   - 4.15. Impact Assessment Techniques
   - 4.16. Resource Optimization
   - 4.17. Stakeholder Collaboration

- 4.18. Testing Strategy Development
- 4.19. Implementation Planning
- 4.20. Post-Deployment Review

5. Security Controls and Risk Management
   - 5.1. Operational Process Evaluation
   - 5.2. Control Design Methodology
   - 5.3. Risk Appetite Framework
   - 5.4. Risk Assessment ISO vs NIST
   - 5.5. Control Testing Protocols
   - 5.6. Control Type Classification
   - 5.7. Control Type Classification (Cont'd)
   - 5.8. Preventive Control Implementation
   - 5.9. Detective Control Strategy
   - 5.10. Corrective Control Framework
   - 5.11. Deterrent Control Design
   - 5.12. Recovery Control Design
   - 5.13. Compensating Control Design
   - 5.14. Resource Requirement Analysis
   - 5.15. Human Capital Planning
   - 5.16. Infrastructure Requirements
   - 5.17. Architectural Considerations
   - 5.18. Risk Mitigation Planning
   - 5.19. Performance Metrics Design
   - 5.20. Control Monitoring Systems
   - 5.21. Documentation Standards
   - 5.22. Testing Program Implementation
   - 5.23. Deficiency Management
   - 5.24. Problem Resolution Framework
6. Cloud Security and Program Wrap-up
   - 6.1. Cloud Security Fundamentals
   - 6.2. Shared Responsibility Framework
   - 6.3. Cloud Shared Responsibility Model
   - 6.4. IaaS Security Management
   - 6.5. PaaS Security Framework

6.6. SaaS Security Governance
6.7. Program Management Review
6.8. Financial Management Summary
6.9. Operational Excellence Review
6.10. Security Control Overview
6.11. Future Program Direction

7. Secure AI/ML System Architecture
   7.1. AI and ML System Architecture Security
   7.2. Architecture Security for ML Pipelines
   7.3. Ensuring Secure Model Deployment and Access Control
   7.4. Zero Trust Application to ML/AI Models
   7.5. Securing APIs and ML Endpoints
8. AI in Cybersecurity Operations
   8.1. AI in Cybersecurity Operations
   8.2. Integrating AI into Cybersecurity Operations
   8.3. Role of AI in SOC Operations
   8.4. AI Integration in SIEM and SOAR with Automated Playbooks
   8.5. Threat Hunting using ML-based Tools
   8.6. AI and the CISO's Role in Secure Operations
9. Roadmap for CISOs to Implement AI in Security Programs
   9.1. Roadmap for CISOs to Implement AI in Security Programs
   9.2. Assessing Organizational Readiness
   9.3. Building AI Skillsets in the Security Team
   9.4. Budgeting and Risk Appetite Alignment for AI Adoption
10. Summary
11. Practice Questions

**Domain 4: Information Security Core Competencies**

1. Identity and Access Management (IAM) Fundamentals
   1.1. Introduction to Information Security Core Competencies
   1.2. Identity and Access Management Overview
   1.3. Authentication, Authorization, and Accounting Framework
   1.4. Identity Management Lifecycle
   1.5. Authentication Mechanisms and Factors

1.6. Password-Based Authentication
1.7. Biometric Authentication Methods
1.8. Certificate-Based and Multi-Factor Authentication
1.9. Authorization Models and Access Control
1.10. Role-Based Access Control Implementation
1.11. Rule-Based and Attribute-Based Access Control
1.12. Authorization Controls and Mitigation Strategies
1.13. Access Accounting and Monitoring
1.14. IAM Plan Development
1.15. Identity Theft Prevention
1.16. Social Engineering Attack Lifecycle
1.17. Business Email Compromise Attacks

2. Physical Security and Business Continuity
   2.1. Physical Security Fundamentals
   2.2. Facility Construction and Location Factors
   2.3. Data Center Tier Classifications
   2.4. Physical Security Risk Assessment
   2.5. Physical Security Plans and Design Elements
   2.6. Access Control Implementation
   2.7. Data Backup Fundamentals
   2.8. Backup Technologies and Approaches
   2.9. ISO BCM Standards Overview
   2.10. ISO 22301 Requirements
   2.11. ISO/IEC 27031 Guidelines
   2.12. Business Continuity Management Implementation
   2.13. Disaster Recovery Planning Basics
   2.14. Alternate Recovery Site Options
   2.15. BCP Testing Methodologies
   2.16. DRP Testing Approaches
3. Network Security and Infrastructure
   3.1. Network Security Fundamentals
   3.2. Network Security Technology Planning
   3.3. Firewall Implementation Strategies
   3.4. Intrusion Detection Systems Architecture

3.5. Intrusion Prevention Systems Design
3.6. Secure Web Gateway Implementation
3.7. Virtual Private Network Solutions
3.8. Network Data Loss Prevention
3.9. Network Access Control Systems
3.10. Network Security Design Elements
3.11. Network Address Translation Implementation
3.12. Virtual Private Cloud Architecture
3.13. Network Segmentation Strategies
3.14. Zero Trust Network Access Framework
3.15. Software-Defined WAN Implementation
3.16. Network Security Management Challenges
3.17. ISO Network Security Standards
3.18. Network Protocols Overview
3.19. OSI Model Layers and Security
3.20. Wireless Network Security Fundamentals
3.21. Wireless Security Controls

4. Cloud and Endpoint Security
   4.1. Cloud Computing Security Overview
   4.2. Cloud Service Models
   4.3. Cloud Security Alliance Threats
   4.4. Data Breach Prevention in Cloud
   4.5. Cloud Access Security Management
   4.6. Cloud Control Matrix Implementation
   4.7. Cloud Control Matrix Implementation (Cont'd)
   4.8. Endpoint Security Fundamentals
   4.9. Antivirus Technology Implementation
   4.10. Endpoint Detection and Response
   4.11. Extended Detection and Response
   4.12. Endpoint Encryption Strategies
   4.13. Endpoint Device Hardening
   4.14. Configuration Management Practices
   4.15. Patch Management Lifecycle
   4.16. Mobile Device Security Framework

- 4.17. IoT Security Challenges
- 4.18. Endpoint Threats
- 4.19. Endpoint Vulnerabilities

5. Application Security and Development
   - 5.1. Secure SDLC Model Overview
   - 5.2. Secure Code Training Programs
   - 5.3. Security Requirements Gathering
   - 5.4. Planning and Design Security Integration
   - 5.5. Implementation Security Controls
   - 5.6. Testing and Validation Approaches
   - 5.7. Secure Deployment Strategies
   - 5.8. Waterfall Methodology Security
   - 5.9. Agile Security Implementation
   - 5.10. Threat Modeling and STRIDE Framework
   - 5.11. Application Security Testing Tools
   - 5.12. Static Application Security Testing
   - 5.13. Dynamic Application Security Testing
   - 5.14. Interactive Application Security Testing
   - 5.15. Development Environment Separation
   - 5.16. Secure Coding Best Practices
   - 5.17. DevSecOps Implementation
   - 5.18. Database Security Controls
   - 5.19. Database Hardening Strategies
6. AI System Lifecycle Security
   - 6.1. AI System Lifecycle Security
   - 6.2. Securing the AI System Development Process (AI/ML-SDLC)
   - 6.3. Data Ingestion Pipelines: Securing Training, Validation, and Production Data
7. Encryption and Incident Response
   - 7.1. Cryptography Fundamentals
   - 7.2. Encryption Algorithms Overview
   - 7.3. Symmetric vs. Asymmetric Encryption
   - 7.4. Blockchain Technology Implementation
   - 7.5. Digital Signatures and Certificates

7.6. Public Key Infrastructure Design
7.7. Encryption Strategy Development
7.8. Determining Critical Data Location and Type
7.9. Deciding What to Encrypt
7.10. Selecting, Integrating, and Managing Encryption
7.11. Vulnerability Management and Penetration Testing
7.12. Vulnerability Assessments
7.13. Risk Assessments
7.14. Patching and Remediation
7.15. Vulnerability Management in Practice
7.16. Penetration Testing
7.17. Security Testing Teams
7.18. Threat Management
7.19. Technological Threats
7.20. Threat Intelligence
7.21. Incident Response Model Framework
7.22. Incident Response Communications
7.23. Incident Analysis Methodology
7.24. Incident Analysis
7.25. Incident Response
7.26. Incident Containment
7.27. Incident Eradication
7.28. Incident Recovery
7.29. Incident Postmortem
7.30. Incident Response Scenarios
7.31. Incident Response Plan Testing
7.32. Digital Forensics Framework
7.33. Evidence Collection Procedures
7.34. Evidence Analysis Techniques
7.35. Investigation Reporting Standards

8. AI- Driven Incident and Threat Response Strategies
8.1. AI-Driven Threat Intelligence
8.2. Threat Intelligence Key Responsibilities
8.3. AI-Driven Threat Intelligence

8.4. AI-Driven Incident Response and Forensic Investigations
8.5. Logging, Monitoring, and Incident Response for AI Systems
8.6. Incident Response for AI Systems
8.7. Incident Response Best Practices for AI Systems
8.8. AI Threat Response Strategy
8.9. AI Threat Response Strategy (Cont'd)

9. Summary
10. Practice Questions

**Domain 5: Strategic Planning, Finance, Procurement and Vendor Management**

1. Introduction
2. Key Challenges for CISOs
3. Strategic Planning
   3.1. Strategic Planning in Cybersecurity
   3.2. Key Components of a Strategic Security Plan
   3.3. From Vision to Execution
   3.4. Organic Strategic Planning: A Flexible, Adaptive Approach
   3.5. Issues-Based Strategic Planning Approach
   3.6. Risk-Based Strategic Planning
   3.7. Goal-Based Strategic Planning
   3.8. Strategic Planning Assessment Phase
   3.9. Strategic Planning Formulation Phase
   3.10. Strategic Planning Execution Phase
   3.11. Strategic Planning Evaluation Methods
   3.12. Factors Impacting Strategic Planning Success
   3.13. How CISOs Can Engage with Leadership Effectively?
4. Understanding the Organization
   4.1. General Corporation
   4.2. Close Corporation: Security & Risk Considerations
   4.3. Subchapter Corporation & Security Considerations
   4.4. Limited Liability Company (LLC) Structure
   4.5. Support Pyramid in Security Programs
   4.6. Identifying Key Program Sponsors & Their Security Impact
   4.7. Understanding Stakeholder Dynamics

4.8. Role of Influencers in Security Programs

5. Information Security Strategic Planning & Execution
   5.1. Information Security Strategy Foundation
   5.2. Strategic Plan Component Framework
   5.3. Mission Statement Development Guidelines
   5.4. Vision Statement Creation Process
   5.5. Values Statement Integration
   5.6. SWOT Analysis in Security Programs
   5.7. AI-powered SWOT Analysis
   5.8. AI-powered SWOT Analysis Tools
   5.9. Strategic Objectives Development
   5.10. Security Program Roadmap Design
   5.11. Performance Scorecard Implementation
   5.12. Key Performance Indicators Selection
   5.13. Key Risk Indicators (KRIs) Framework
   5.14. AI-driven KPI and KRI Dashboards
   5.15. Financial Accounting in Security Programs
   5.16. Strategy Communication Planning
   5.17. Communication Goals Development
   5.18. Communication Schedule Design
   5.19. Media Selection for Strategy Communication
   5.20. Message Development Framework
   5.21. Security Awareness Communication
   5.22. Crisis Communication Planning
   5.23. Security Training Program Design
   5.24. AI-Powered Personalized Security Awareness Campaigns
   5.25. AI-Powered Personalized Security Awareness Campaign Tools
   5.26. Security Testing Strategy
   5.27. Creating Security Culture Framework
   5.28. Influencing Organizational Behavior
   5.29. Security Culture Assessment Methods
6. Enterprise Security Program Management
   6.1. Enterprise Security Program Design
   6.2. Blueprint Development Methodology

6.3. Security Program Foundation Elements
6.4. Architectural Views Introduction
6.5. Business View Framework
6.6. Functional View Implementation
6.7. Technical View Design
6.8. Implementation View Strategy
6.9. Security Metrics Development
6.10. Performance Measurement Implementation
6.11. Balanced Scorecard Design
6.12. Continuous Monitoring Framework

7. Enterprise Architecture and Frameworks
   7.1. ITIL Continual Service Improvement Model
   7.2. Enterprise Architecture Introduction
   7.3. Zachman Framework Analysis
   7.4. TOGAF Implementation Strategy
   7.5. TOGAF Implementation Strategy
   7.6. SABSA Framework Components
   7.7. SABSA Framework Components (Cont'd)
   7.8. FEAF Design Elements
   7.9. FEAF Design Elements (Cont'd)
   7.10. AI-Driven Traceability and Impact Analysis in TOGAF, FEAF, and SABSA Frameworks
8. Finance & Budgeting
   8.1. Financial Statement Analysis for Security Leaders
   8.2. Understanding Organizational Assets & Security Implications
   8.3. Business Liabilities
   8.4. Shareholder Equity
   8.5. Operating Activities Analysis
   8.6. Investment Activities Evaluation
   8.7. Financing Activities Assessment
   8.8. Financial Performance Metrics
   8.9. Security Program Funding Fundamentals
   8.10. Budget Analysis Methodology
   8.11. Security Program Forecasting

8.12. Resource Requirements Planning
8.13. Financial Metrics Framework
8.14. Technology Refresh Strategy
8.15. New Project Funding Approaches
8.16. Contingency Funding Planning
8.17. Cryptocurrency Wallet Management
8.18. Disaster Declaration Funding
8.19. License Management Strategy
8.20. Budget Management Principles
8.21. Financial Resource Allocation
8.22. Budget Monitoring Methods
8.23. Financial Reporting Framework
8.24. Cost Per Seat Analysis
8.25. Service Cost Comparison
8.26. Budget Balancing Techniques
8.27. Financial Resource Optimization
8.28. Economic Principles in Security
8.29. AI-Powered Predictive Budgeting and Forecasting for Cybersecurity
8.30. AI-Driven Dashboards for Real-Time ROI Tracking of Cybersecurity Investments

9. Procurement & Vendor Management
9.1. Procurement Program Fundamentals
9.2. Statement of Work Development
9.3. Total Cost of Ownership Analysis
9.4. RFP Development Strategy
9.5. Master Service Agreement (MSA) Design
9.6. Service Level Agreement (SLA) Framework
9.7. Terms and Conditions (T&C) Development
9.8. Procurement Requirements Analysis
9.9. Regulatory Compliance in Procurement
9.10. Global Procurement Requirements
9.11. Local Procurement Requirements
9.12. Procurement Risk Management
9.13. Standard Contract Language Design

- 9.14. Breach Language Requirements
- 9.15. Vendor Management Framework
- 9.16. Vendor Procurement Lifecycle
- 9.17. Contract Negotiation Process
- 9.18. Performance Management Strategy
- 9.19. Cost-Benefit Analysis Methods
- 9.20. Vendor Management Policies
- 9.21. Contract Administration Framework
- 9.22. Service Delivery Metrics
- 9.23. Contract Reporting Requirements
- 9.24. Change Management Process
- 9.25. Contract Renewal Strategy
- 9.26. Contract Closure Procedures
- 9.27. Contract Closure Procedures - continue
- 9.28. Delivery Assurance
- 9.29. Streamlined Procurement Lifecycle Using AI
- 9.30. Leveraging Natural Language Processing (NLP) Tools to Analyze Legal Agreements
- 9.31. NLP Tools to Analyze Legal Agreements
- 9.32. AI-driven Vendor Scoring
- 9.33. AI-driven Vendor Scoring Tools
- 9.34. AI-driven Automated Alerts for SLA Breaches

10. Delivery Assurance Framework
    - 10.1. Delivery Assurance Framework
    - 10.2. Third-Party Attestation Services
11. Summary
12. Practice Questions