

## Certified Chief Information Security Officer (CCISO)

CODICE	DT0184
DURATA	5 gg
PREZZO	3.790,00 €
EXAM	

### DESCRIZIONE

**Il corso in partenza il 7 luglio si svolgerà nei giorni 7, 8, 9, 14 e 15 luglio**

Il Certified Chief Information Security Officer (C|CISO) è un programma incentrato sui dirigenti, progettato appositamente per formare e certificare i leader responsabili dello sviluppo e della guida della strategia di sicurezza informatica di un'organizzazione.

Il programma C|CISO assicura ai partecipanti non solo una profonda comprensione della sicurezza informatica, ma anche le competenze di leadership, finanziarie e di pianificazione strategica necessarie per avere successo in un ruolo dirigenziale. Il C|CISO prepara i leader a integrare l'intelligenza artificiale nella gestione dei rischi di sicurezza informatica, nella conformità, nelle previsioni e nella governance con responsabilità e trasparenza. Il conseguimento della certificazione C|CISO dimostra che sei in grado di allineare le strategie di sicurezza e le strategie di sicurezza dell'intelligenza artificiale agli obiettivi aziendali, gestire efficacemente i rischi aziendali e comunicare con i consigli di amministrazione e la leadership esecutiva.

C|CISO v4 vi fornisce gli strumenti per:

- Allineare la sicurezza informatica agli obiettivi aziendali
- Guidare la governance dell'IA, la conformità e la strategia di rischio
- Comunicare in modo efficace con i consigli di amministrazione e i dirigenti
- Gestire i programmi e i budget di sicurezza a livello aziendale

Ottenere la certificazione C|CISO dimostra che siete pronti per ricoprire ruoli dirigenziali e di leadership in materia di sicurezza. Il programma C|CISO è un corso di formazione e certificazione unico nel suo genere, che mira a formare dirigenti di sicurezza informatica di altissimo livello e con un'etica impeccabile. Il programma di studi C|CISO, sviluppato da da CISO esperti per professionisti in ruolo o aspiranti tali, adotta un punto di vista tipico del management esecutivo che incorpora sia i principi di gestione della sicurezza delle informazioni sia le conoscenze tecniche generali.

## TARGET

---

Questa formazione è rivolta ai manager che desiderano sviluppare le loro competenze imparando ad adattare le loro conoscenze tecniche alle problematiche generali di impresa.

## PREREQUISTI

---

Nessuno

## CONTENUTI

---

# Domini

- [Domain 1: Governance; Risk Management; Security, Compliance, and Privacy; and Audit Management](#)
- [Domain 2: Organizational Executive Leadership](#)
- [Domain 3: Information Security Controls, Security Program Management and Operations](#)
- [Domain 4: Information Security Core Competencies](#)
- [Domain 5: Strategic Planning, Finance, Procurement and Vendor Management](#)

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

- **Fundamentals of Information Security Governance**
  - Introduction to Information Security Governance
  - Foundation of Information Security Programs
  - Understanding Business Organization Structures
  - Understanding Business Organization Structures (cont'd)
  - Industry Impact on Governance
  - CISO's Impact on Governance
  - CMMI Process Model Overview
  - Organizational Maturity Models
  - Reactive vs. Proactive Organizations
  - Aligning IS with Organizational Goals
  - Strategic Security Planning
  - Organizational Security Architecture
  - Security Operating Model Framework
  - Governance Structure and Hierarchy
  - Governance Structure and Hierarchy Diagram
  - Executive vs Non-Executive CISO
  - Role of the CISO in Modern Organizations
  - C-Suite Attitudes Toward Information Security
  - C-Suite Attitudes Toward Information Security – cont.

- Leadership and Management Skills for CISOs
- Ethics in Information Security
- Professional Code of Ethics
- Information Security Documentation Framework

## • Risk Management Foundations

- Understanding Risk Management Fundamentals
- Understanding Risk Management Fundamentals – cont.
- Defining Organizational Risk
- Risk Management Program Components
- Risk Categories and Classifications
- Risk Ownership and Accountability
- Risk Appetite and Tolerance
- Asset Identification and Valuation
- Asset Identification and Valuation – cont.
- Threat Assessment Methodologies
- ISO/IEC 27005:2022 Annex A Threats
- Vulnerability Analysis Framework
- ISO/IEC 27005:2022 Annex A Vulnerabilities
- Risk Assessment Process
- Quantitative Risk Analysis
- Quantitative Risk Analysis – cont.
- Qualitative Risk Analysis
- Qualitative Risk Analysis – cont.
- Risk Assessment Categories
- Risk Assessment Focus Types
- Risk Calculation Methodologies
- Annualized Loss Expectancy Models
- Risk Management Lifecycle
- Risk Register
- Risk Treatment Options
- Risk Treatment Options – cont.
- Risk Treatment Options – cont. 2
- Risk Treatment Options – cont. 3
- Risk Modification Strategies
- Risk Acceptance Criteria
- Risk Acceptance Criteria – cont.
- Risk Transfer Mechanisms
- Risk Transfer Mechanisms – cont.

## • Security Controls and Implementation

- Understanding Security Controls

- CIA Triad Implementation
- Control Categories and Classifications
- Control Attributes
- COSO PDC Defense-In-Depth Model
- Preventive Control Mechanisms
- Detective Control Systems
- Corrective Control Measures
- Deterrent Control Measures
- Control Lifecycle Management
- Control Selection Criteria
- Control Implementation Strategy
- Control Maturity Assessment
- Compensating Controls Framework
- Security Control Documentation
- Control Monitoring Systems
- Control Testing Methodologies
- Security Control Catalog Management
- Service Catalog Development
- Risk Management Frameworks
- Risk Management Frameworks – cont.
- Risk Management Frameworks – cont. 2
- Risk Management Frameworks – cont. 3
- Risk Management Frameworks – cont. 4
- Change Management in Control Systems and Updates

## • CISO Role in the AI Era

- Evolving Cybersecurity Landscape
- Role of CISO in AI Era
- Impact of Digital Transformation and AI Adoption
- Benefits of AI Integration in Cybersecurity
- Limitations of AI in Cybersecurity
- Balancing AI Benefits and Limitations

## • Leveraging AI for Governance and Compliance

- Enhancing Cybersecurity Governance through AI
- Mapping AI to Cybersecurity Frameworks
- Mapping AI to NIST Cybersecurity Framework (CSF)
- Mapping AI to ISO 27001
- Mapping AI to COBIT
- AI-Supported Policy Enforcement and Monitoring
- How AI Supports Policy Enforcement
- Best Practices for Implementing AI in Policy Enforcement and Monitoring

- Continuous Controls Monitoring (CCM) with AI
- Best Practices for Implementing AI in CCM
- AI Governance Board or Committee
- Setting up an AI Governance Board or Committee
- Challenges in Setting Up an AI Governance Board
- Best Practices for AI Governance
- Establishing Cybersecurity Governance for AI
  - AI in Risk Management: A CISO's Strategic Advantage
  - AI and Predictive Risk Modeling
  - Risk Scoring and Prioritization with AI
  - Automated Risk Assessments with AI
  - Enhanced Risk Management Decision-Making with AI
  - Key Challenges in Leveraging AI for Risk Management
- Risk Management for AI
  - Critical AI Risks
  - Critical AI Risks (Cont'd)
  - Risk Assessment Templates for AI Projects
  - Key Components of an AI Risk Assessment Template
  - Example Risk Assessment Template for AI Projects
  - Best Practices for Using Risk Assessment Templates in AI Projects
  - AI-Specific Threat Modeling
  - Operational Risk Controls for AI
  - Operational Risk Controls Implementation Checklist
  - Establishing AI Risk Registers and Mitigation Controls
  - Best Practices for AI Risk Management
- Tools and Technologies for AI-Driven GRC
  - AI Risk Management Frameworks and Platforms
  - ENISA Guidelines for AI Systems
  - Model Validation and Testing Tools
  - Performance Drift and Anomaly Monitoring Tools
  - Explainable AI (XAI) Tools
  - Governance and Compliance Automation Tools
  - AI-Powered Enterprise Tools
  - CISO Responsibilities and Considerations for AI Tools
- Compliance and Regulatory Framework
  - Regulatory Compliance Overview
  - Legal Framework for Information Security
  - International Compliance Standards
  - Industry-Specific Regulations

- GDPR Requirements Implementation
  - EU Cybersecurity Act (EUCSA)
  - ENISA Guidelines
  - Digital Operational Resilience Act (DORA)
- HIPAA Compliance Framework
  - Japan's Act on the Protection of Personal Information (APPI)
  - Brazil's General Data Protection Law (LGPD)
- HITECH
- PCI DSS Standards Overview
- SOX Compliance Requirements
- FISMA Implementation Guidelines
- Australian Privacy Act 1988
- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- Brazilian General Data Protection Law (LGPD)
- Singapore Personal Data Protection Act (PDPA)
- Data Privacy Regulations
- State-Level Privacy Laws
- Cross-Border Data Protection
- Regulatory Reporting Requirements
- Compliance Documentation Standards
- Privacy Impact Assessments
- Regulatory Risk Management
- Compliance Program Development
- Privacy Program Implementation
- Regulatory Change Management

## • Security Frameworks, Standards, Laws, Acts and Directives

- NIST CSF Cybersecurity Framework
- NIST CSF Cybersecurity Framework – cont.
- ISO 27001 Implementation
  - Australian Government Information Security Manual (ISM)
  - Australian Privacy Principles (APPs)
  - Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
- COBIT Framework Overview
  - Singapore's Cybersecurity Code of Practice
  - Indian IT Act 2000 with CERT-In Guidelines
- ITIL Security Management
- ITILv4
- MITRE ATT&CK® & MITRE ATLAS
- OWASP SAMM & ASVS
- Zero Trust Architecture
- Cloud Security Framework

- ENISA Guidelines on Cloud Security (EU)
- Australian Cyber Security Centre (ACSC) Essential Eight Framework
- CIS Controls (Center for Internet Security – Global)
- BSI IT-Grundschutz (Germany)
- Artificial Intelligence in IS
- Risk Management Frameworks
- NIST SP 800-37 Framework Steps
- NIST Security Control Classes
- NIST SP 800-37: Hierarchy
- NIST SP 800-37: Risk Process
- ISO27005: Risk Process
- Security Control Frameworks
- Risk Management Standards
- NIST Family
- NIST Family – cont.
- ISO27K Family
- ISO27K Family – cont.
- Framework Integration Strategies
- Other Risk Frameworks
- COBIT Risk Framework
- COSO – Enterprise Risk Management Framework
- Information Technology Infrastructure Library (ITIL)
- Factor Analysis of Information Risk (FAIR)
- Operationally Critical Threat, Asset, And Vulnerability Evaluation (OCTAVE)
- Threat Assessment and Remediation Analysis
- ISACA Risk IT Framework
- Security Policy Development
- Security Policy Development - cont.
- Security Policy Challenges
- Security Policy ISO 27001 C5.2
- Types of Policies
- Security Metrics and Measurements
- NIS2 Directive
- EU AI Act
- ePrivacy Directive
- Digital Personal Data Protection Act, 2023 (DPDP Act)
- CERT-In Cybersecurity Directions (2022)
- APPI (Act on Protection of Personal Information)

## • Audit and Assessment

- Audit Expectations and Outcomes

- Information Security Audit Practice
- NIST, COBIT AUDIT GUIDANCE
- INTERNAL Versus EXTERNAL Audits
- Partnering with Organization
- Audit Process
- General Audit Standards
- Type-Based AUDITS
- Performing and Evaluating AUDIT Results in an AUDIT
- Remediating Audit Findings
- Leveraging GRC SOFTWARE to Support AUDITS
- Leveraging AI to Enhance Security Audits
- AI-Driven Security Audit Tools
- AI for Security Audit: Auditing AI Tools
- Summary
- Questions

## Domain 2: Organizational Executive Leadership

- Foundation of leadership
  - Domain Outline
  - Introduction to Leadership's Role and Impact
  - Why Leadership Matters: Core Constituents
  - Definition of a Leader and Leadership Needs
  - Leaders vs Managers: Kotter's Framework
  - Key Similarities Between Leaders and Managers
  - Transitioning from Manager to Leader
  - Building Leadership Confidence
  - Transforming from Boss to Leader
  - Role of Leadership in Organizational Success
  - Why Organizations Exist: Purpose and Goals
  - The Organizational Need for Leaders
  - Leaders as Organizational Change Agents
  - Leadership During Crisis and Failure
  - Information Security Leadership Role
  - Building Security Maturity Capabilities
  - Evolution of Information Security Leadership
  - Ancient Leadership: Mesopotamia to Rome
  - Power and Authority in Leadership
  - Types of Authority in Leadership
  - Power and Authority in Leadership
  - Persuasion and Influence Techniques

- Traditional Leadership Approaches
- Leadership Types and Their Applications
- Leadership Styles
- Leadership Theories and Models
- Leadership Environments and Contexts

## • Personal leadership development

- Developing Executive Presence: Key Components
- Overcoming Challenges to Executive Presence
- Building and Promoting Personal Brand
- Personal Brand Communication Strategies
- Leadership Self-Awareness Development
- Strategies for Cultivating Self-Awareness
- Emotional Intelligence in Leadership
- Social Intelligence Development
- Cultural Intelligence Enhancement
- Key components of Cultural Intelligence
- Applying Social and Cultural Intelligence
- Building Professional Leadership Networks
- Understanding Team Member Personalities
- Myers-Briggs Type Indicator in Leadership
- Leadership Feedback and Self-Assessment
- Developing Leadership Convictions
- Building Resilience in Uncertain Times
- Building Resilience During Uncertain Times
- Leading and Supporting During Uncertainty
- Adaptability and Agility Development
- Persuasive Business Communication
- Time Management and Priority Setting
- Negotiation and Dispute Resolution
- Leadership Problem-Solving Approaches
- Quantitative Decision-Making Methods
- Behavioral Finance in Leadership
- Personal Development Planning
- Leadership Role Readiness

## • Leading teams and people

- Cultivating Future Leaders: Key Strategies
- Leadership Talent Identification
- Leadership Talent Retention
- Succession Planning Implementation
- Effective Leadership Delegation

- Team Building for Collaboration
- Leading Inclusive Teams
- Virtual Team Management
- Managing Up: Working with Superiors
- Managing Down: Supporting Teams
- Managing Laterally: Cross-Functional Collaboration
- Performance Evaluation Methods
- Managing Difficult Conversations
- Building Team Loyalty and Commitment
- Team Motivation Strategies
- Mentoring and Coaching Practices
- Leading with Empathy
- Ethical Leadership Development

## • Organization leadership

- Board Relationship Management
- Building Board Trust and Credibility
- Board Communication Strategies
- Securing Funding and Sponsorship
- Organizational Leadership at Scale and Scope
- Organizational Leadership at Scale and Scope - Cont.
- T-Shaped Leadership Approach
- Strategic vs Tactical Leadership
- Organizational Change Leadership
- Strategic Analysis Framework
- Understanding Organizational Internal Context
- Understanding Organizational External Context
- SWOT Analysis Implementation
- Change Planning and Execution
- Change Communication Strategies
- Building Sustainable Competitive Advantage
- Information Security Group Branding
- Security Brand Communication
- Education and Awareness Leadership
- Stakeholder Management Strategies
- Regulatory Compliance Leadership
- Crisis and Disaster Management
- Crisis and Disaster Management – Cont.
- Crisis and Disaster Management – Cont.
- Business Intelligence Applications
- Leading Innovative Projects
- Industry-

## Specific Leadership Challenges

- Considerations of Various Industries

## • Responsible and Ethical AI Leadership

- Role of CISO in AI Ethics and Governance Boards
- Key Responsibilities in AI Ethics Governance
- Embedding AI Ethical Principles into Cybersecurity
- Privacy Risks in Large Language Models (LLMs) and Generative AI
- Why Leadership Matters: Core Constituents
- Mitigating Privacy Risks in Large Language Models and Generative AI
- Embedding Fairness, Accountability, and Transparency in AI Development
- Embedding Fairness, Accountability, and Transparency in AI Development (Cont'd)
- Ethical Frameworks: OECD AI Principles
- Ethical Frameworks: UNESCO AI Ethics

## • Cross-Functional AI Innovation Leadership

- Role of CISO in Cross-Functional AI Initiatives
- Strategic Collaboration Activities in AI Initiatives
- Cross-Functional AI Governance
- Responsibilities of the CISO in AI Governance Bodies
- AI Awareness and Training Across Departments
- Role of CISO in AI Awareness and Training Across Departments
- Managing AI Talent Development Within Cybersecurity

## • Strategic AI Alignment and Innovation Management

- Role of CISO in Aligning AI Innovation with Enterprise Strategy
- Aligning AI Innovation to Business and Security Strategy
- Balancing AI Experimentation with Compliance and Control
- Communicating AI Risk Posture to the Board and Executive Leadership
- Investment Planning for AI Innovation and Risk Management
- Vendor Evaluation and Third-Party AI Risk Considerations

- Summary
- Practice Questions

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

## • Introduction and Program Management Fundamentals

- CISO Evolution: From Tech to Strategy
- Evolution of CISO's Role
- Evolution of CISO's Role (Cont'd)
- Leadership Misconception

- Knowledge Prerequisites for Information Security Management
- Core Security Program Execution Principles
- CISO's Mind Map
- Business Objective Alignment Strategies
- Information Security Program Definition Process
- Program Development Framework
- Effective Program Management Techniques
- Program Monitoring and Assessment
- Key Accounting Concepts in Security
- Asset Management Fundamentals
- Asset Lifecycle Management
- Cost-Benefit Analysis Methods
- Understanding Security Program Liabilities
- Net Present Value in Security Investments
- NPV vs IRR
- Profit and Loss Statement Analysis
- ROI Calculation in Security Programs
- Strategic Cost Avoidance
- Security Program Revenue Considerations
- Expense Management Framework
- Security Budget Planning
- Financial Resource Allocation

## • Financial and Resource Management

- Budget Development Strategies
- Understanding CapEx in Security
- Understanding CapEx in Security (Cont'd)
- OpEx Management Principles
- CAPEX vs OPEX
- Budgeting Methodologies Comparison
- Security Program Cash Flow
- Burn Rate Monitoring Techniques
- Strategic Staffing Analysis
- Administrative Resource Planning
- Security Delivery Team Structure
- Technical Competency Requirements
- Operations Staff Development
- Digital Forensics Capabilities
- Cross-Functional Skill Development
- Team Management Excellence
- Professional Development Planning

- Career Advancement Frameworks
- Security Awareness Strategy
- Awareness Program Implementation
- Role-Based Security Education

## • Program Architecture and Operations

- Security Architecture Principles
- Program Roadmap Development
- Project Management Fundamentals
- Project Initiation Best Practices
- Strategic Project Planning
- Execution Phase Management
- Monitoring Framework Implementation
- Project Closure Procedures
- Operations Management Strategy
- Conflict Resolution Techniques
- Time Management in Disputes
- Cost Impact Analysis
- Quality Assurance in Operations
- Vendor Management Fundamentals
- Strategic Vendor Selection
- Negotiation Best Practices
- Contract Management Principles
- Long-term Vendor Relations
- Vendor Community Building

## • Stakeholder Management and Project Assessment

- Enhanced Project Management
- Performance Measurement Systems
- Technical Performance Indicators
- Business Alignment Metrics
- Project Success Metrics
- Data Collection Frameworks
- Analysis and Reporting
- Continuous Improvement Process
- Internal Stakeholder Engagement
- External Stakeholder Management
- Communication Strategy Development
- Expectation Management
- Process Enhancement Methods
- Change Management Framework
- Impact Assessment Techniques

- Resource Optimization
- Stakeholder Collaboration
- Testing Strategy Development
- Implementation Planning
- Post-Deployment Review

## • Security Controls and Risk Management

- Operational Process Evaluation
- Control Design Methodology
- Risk Appetite Framework
- Risk Assessment ISO vs NIST
- Control Testing Protocols
- Control Type Classification
- Control Type Classification (Cont'd)
- Preventive Control Implementation
- Detective Control Strategy
- Corrective Control Framework
- Deterrent Control Design
- Recovery Control Design
- Compensating Control Design
- Resource Requirement Analysis
- Human Capital Planning
- Infrastructure Requirements
- Architectural Considerations
- Risk Mitigation Planning
- Performance Metrics Design
- Control Monitoring Systems
- Documentation Standards
- Testing Program Implementation
- Deficiency Management
- Problem Resolution Framework

## • Cloud Security and Program Wrap-up

- Cloud Security Fundamentals
- Shared Responsibility Framework
- Cloud Shared Responsibility Model
- IaaS Security Management
- PaaS Security Framework
- SaaS Security Governance
- Program Management Review
- Financial Management Summary
- Operational Excellence Review

- Security Control Overview
- Future Program Direction
- **Secure AI/ML System Architecture**
  - AI and ML System Architecture Security
  - Architecture Security for ML Pipelines
  - Ensuring Secure Model Deployment and Access Control
  - Zero Trust Application to ML/AI Models
  - Securing APIs and ML Endpoints
- **AI in Cybersecurity Operations**
  - AI in Cybersecurity Operations
  - Integrating AI into Cybersecurity Operations
  - Role of AI in SOC Operations
  - AI Integration in SIEM and SOAR with Automated Playbooks
  - Threat Hunting using ML-based Tools
  - AI and the CISO's Role in Secure Operations
- **Roadmap for CISOs to Implement AI in Security Programs**
  - Roadmap for CISOs to Implement AI in Security Programs
  - Assessing Organizational Readiness
  - Building AI Skillsets in the Security Team
  - Budgeting and Risk Appetite Alignment for AI Adoption
- Summary
- Practice Questions

## Domain 4: Information Security Core Competencies

- **Identity and Access Management (IAM) Fundamentals**
  - Introduction to Information Security Core Competencies
  - Identity and Access Management Overview
  - Authentication, Authorization, and Accounting Framework
  - Identity Management Lifecycle
  - Authentication Mechanisms and Factors
  - Password-Based Authentication
  - Biometric Authentication Methods
  - Certificate-Based and Multi-Factor Authentication
  - Authorization Models and Access Control
  - Role-Based Access Control Implementation
  - Rule-Based and Attribute-Based Access Control
  - Authorization Controls and Mitigation Strategies
  - Access Accounting and Monitoring

- IAM Plan Development
- Identity Theft Prevention
- Social Engineering Attack Lifecycle
- Business Email Compromise Attacks

## • Physical Security and Business Continuity

- Physical Security Fundamentals
- Facility Construction and Location Factors
- Data Center Tier Classifications
- Physical Security Risk Assessment
- Physical Security Plans and Design Elements
- Access Control Implementation
- Data Backup Fundamentals
- Backup Technologies and Approaches
- ISO BCM Standards Overview
- ISO 22301 Requirements
- ISO/IEC 27031 Guidelines
- Business Continuity Management Implementation
- Disaster Recovery Planning Basics
- Alternate Recovery Site Options
- BCP Testing Methodologies
- DRP Testing Approaches

## • Network Security and Infrastructure

- Network Security Fundamentals
- Network Security Technology Planning
- Firewall Implementation Strategies
- Intrusion Detection Systems Architecture
- Intrusion Prevention Systems Design
- Secure Web Gateway Implementation
- Virtual Private Network Solutions
- Network Data Loss Prevention
- Network Access Control Systems
- Network Security Design Elements
- Network Address Translation Implementation
- Virtual Private Cloud Architecture
- Network Segmentation Strategies
- Zero Trust Network Access Framework
- Software-Defined WAN Implementation
- Network Security Management Challenges
- ISO Network Security Standards
- Network Protocols Overview

- OSI Model Layers and Security
- Wireless Network Security Fundamentals
- Wireless Security Controls

## • Cloud and Endpoint Security

- Cloud Computing Security Overview
- Cloud Service Models
- Cloud Security Alliance Threats
- Data Breach Prevention in Cloud
- Cloud Access Security Management
- Cloud Control Matrix Implementation
- Cloud Control Matrix Implementation (Cont'd)
- Endpoint Security Fundamentals
- Antivirus Technology Implementation
- Endpoint Detection and Response
- Extended Detection and Response
- Endpoint Encryption Strategies
- Endpoint Device Hardening
- Configuration Management Practices
- Patch Management Lifecycle
- Mobile Device Security Framework
- IoT Security Challenges
- Endpoint Threats
- Endpoint Vulnerabilities

## • Application Security and Development

- Secure SDLC Model Overview
- Secure Code Training Programs
- Security Requirements Gathering
- Planning and Design Security Integration
- Implementation Security Controls
- Testing and Validation Approaches
- Secure Deployment Strategies
- Waterfall Methodology Security
- Agile Security Implementation
- Threat Modeling and STRIDE Framework
- Application Security Testing Tools
- Static Application Security Testing
- Dynamic Application Security Testing
- Interactive Application Security Testing
- Development Environment Separation
- Secure Coding Best Practices

- DevSecOps Implementation
- Database Security Controls
- Database Hardening Strategies
- **AI System Lifecycle Security**
  - AI System Lifecycle Security
  - Securing the AI System Development Process (AI/ML-SDLC)
  - Data Ingestion Pipelines: Securing Training, Validation, and Production Data
- **Encryption and Incident Response**
  - Cryptography Fundamentals
  - Encryption Algorithms Overview
  - Symmetric vs. Asymmetric Encryption
  - Blockchain Technology Implementation
  - Digital Signatures and Certificates
  - Public Key Infrastructure Design
  - Encryption Strategy Development
  - Determining Critical Data Location and Type
  - Deciding What to Encrypt
  - Selecting, Integrating, and Managing Encryption
  - Vulnerability Management and Penetration Testing
  - Vulnerability Assessments
  - Risk Assessments
  - Patching and Remediation
  - Vulnerability Management in Practice
  - Penetration Testing
  - Security Testing Teams
  - Threat Management
  - Technological Threats
  - Threat Intelligence
  - Incident Response Model Framework
  - Incident Response Communications
  - Incident Analysis Methodology
  - Incident Analysis
  - Incident Response
  - Incident Containment
  - Incident Eradication
  - Incident Recovery
  - Incident Postmortem
  - Incident Response Scenarios
  - Incident Response Plan Testing

- Digital Forensics Framework
- Evidence Collection Procedures
- Evidence Analysis Techniques
- Investigation Reporting Standards
- **AI- Driven Incident and Threat Response Strategies**
  - AI-Driven Threat Intelligence
  - Threat Intelligence Key Responsibilities
  - AI-Driven Threat Intelligence
  - AI-Driven Incident Response and Forensic Investigations
  - Logging, Monitoring, and Incident Response for AI Systems
  - Incident Response for AI Systems
  - Incident Response Best Practices for AI Systems
  - AI Threat Response Strategy
  - AI Threat Response Strategy (Cont'd)
- Summary
- Practice Questions

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

- Introduction
- Key Challenges for CISOs
- **Strategic Planning**
  - Strategic Planning in Cybersecurity
  - Key Components of a Strategic Security Plan
  - From Vision to Execution
  - Organic Strategic Planning: A Flexible, Adaptive Approach
  - Issues-Based Strategic Planning Approach
  - Risk-Based Strategic Planning
  - Goal-Based Strategic Planning
  - Strategic Planning Assessment Phase
  - Strategic Planning Formulation Phase
  - Strategic Planning Execution Phase
  - Strategic Planning Evaluation Methods
  - Factors Impacting Strategic Planning Success
  - How CISOs Can Engage with Leadership Effectively?
- **Understanding the Organization**
  - General Corporation
  - Close Corporation: Security & Risk Considerations
  - Subchapter Corporation & Security Considerations

- Limited Liability Company (LLC) Structure
- Support Pyramid in Security Programs
- Identifying Key Program Sponsors & Their Security Impact
- Understanding Stakeholder Dynamics
- Role of Influencers in Security Programs

## • Information Security Strategic Planning & Execution

- Information Security Strategy Foundation
- Strategic Plan Component Framework
- Mission Statement Development Guidelines
- Vision Statement Creation Process
- Values Statement Integration
- SWOT Analysis in Security Programs
- AI-powered SWOT Analysis
- AI-powered SWOT Analysis Tools
- Strategic Objectives Development
- Security Program Roadmap Design
- Performance Scorecard Implementation
- Key Performance Indicators Selection
- Key Risk Indicators (KRIs) Framework
- AI-driven KPI and KRI Dashboards
- Financial Accounting in Security Programs
- Strategy Communication Planning
- Communication Goals Development
- Communication Schedule Design
- Media Selection for Strategy Communication
- Message Development Framework
- Security Awareness Communication
- Crisis Communication Planning
- Security Training Program Design
- AI-Powered Personalized Security Awareness Campaigns
- AI-Powered Personalized Security Awareness Campaign Tools
- Security Testing Strategy
- Creating Security Culture Framework
- Influencing Organizational Behavior
- Security Culture Assessment Methods

## • Enterprise Security Program Management

- Enterprise Security Program Design
- Blueprint Development Methodology
- Security Program Foundation Elements
- Architectural Views Introduction

- Business View Framework
- Functional View Implementation
- Technical View Design
- Implementation View Strategy
- Security Metrics Development
- Performance Measurement Implementation
- Balanced Scorecard Design
- Continuous Monitoring Framework
- **Enterprise Architecture and Frameworks**
  - ITIL Continual Service Improvement Model
  - Enterprise Architecture Introduction
  - Zachman Framework Analysis
  - TOGAF Implementation Strategy
  - TOGAF Implementation Strategy
  - SABSA Framework Components
  - SABSA Framework Components (Cont'd)
  - FEAF Design Elements
  - FEAF Design Elements (Cont'd)
  - AI-Driven Traceability and Impact Analysis in TOGAF, FEAF, and SABSA Frameworks
- **Finance & Budgeting**
  - Financial Statement Analysis for Security Leaders
  - Understanding Organizational Assets & Security Implications
  - Business Liabilities
  - Shareholder Equity
  - Operating Activities Analysis
  - Investment Activities Evaluation
  - Financing Activities Assessment
  - Financial Performance Metrics
  - Security Program Funding Fundamentals
  - Budget Analysis Methodology
  - Security Program Forecasting
  - Resource Requirements Planning
  - Financial Metrics Framework
  - Technology Refresh Strategy
  - New Project Funding Approaches
  - Contingency Funding Planning
  - Cryptocurrency Wallet Management
  - Disaster Declaration Funding
  - License Management Strategy
  - Budget Management Principles

- Financial Resource Allocation
- Budget Monitoring Methods
- Financial Reporting Framework
- Cost Per Seat Analysis
- Service Cost Comparison
- Budget Balancing Techniques
- Financial Resource Optimization
- Economic Principles in Security
- AI-Powered Predictive Budgeting and Forecasting for Cybersecurity
- AI-Driven Dashboards for Real-Time ROI Tracking of Cybersecurity Investments

## • Procurement & Vendor Management

- Procurement Program Fundamentals
- Statement of Work Development
- Total Cost of Ownership Analysis
- RFP Development Strategy
- Master Service Agreement (MSA) Design
- Service Level Agreement (SLA) Framework
- Terms and Conditions (T&C) Development
- Procurement Requirements Analysis
- Regulatory Compliance in Procurement
- Global Procurement Requirements
- Local Procurement Requirements
- Procurement Risk Management
- Standard Contract Language Design
- Breach Language Requirements
- Vendor Management Framework
- Vendor Procurement Lifecycle
- Contract Negotiation Process
- Performance Management Strategy
- Cost-Benefit Analysis Methods
- Vendor Management Policies
- Contract Administration Framework
- Service Delivery Metrics
- Contract Reporting Requirements
- Change Management Process
- Contract Renewal Strategy
- Contract Closure Procedures
- Contract Closure Procedures - continue
- Delivery Assurance
- Streamlined Procurement Lifecycle Using AI

- Leveraging Natural Language Processing (NLP) Tools to Analyze Legal Agreements
- NLP Tools to Analyze Legal Agreements
- AI-driven Vendor Scoring
- AI-driven Vendor Scoring Tools
- AI-driven Automated Alerts for SLA Breaches

- **Delivery Assurance Framework**

- Delivery Assurance Framework
- Third-Party Attestation Services
- Summary
- Practice Questions