Certaining Cybersecurity Leader

Exam Code- CCYL™

Table of Contents

Introduction

CCYL certification exhibits technical and strategic knowledge in the cybersecurity domain. Among other things, it prepares professionals for the secure design and operation of infrastructures spanning cloud, hybrid, and on-premises systems.

IT professionals validate the skills necessary to effectively use Zero Trust technology, automate, and make the system resilient against attackers. Moreover, they practice compliance, governance, and risk management at a very high level, as in global corporations.

The CCYL is up to date with the industry trends such as AI-driven threats, supply-chain vulnerabilities, and complex compliance mandates.

Core Competencies

- Create enterprise security designs based on Zero Trust and hybrid cloud concepts.
- Govern risk, compliance, and enterprise-wide governance programs.
- Protect an organization from advanced threats by using threat intelligence and proactive hunting.
- Combine detection engineering, automation, and incident response functionalities to achieve integration.
- Incident forensic analysis should be done with the knowledge of legal standards.
- DevOps pipelines should be secured, and data protection measures need to be enforced.
- Use security methods to secure OT, IoT, and AI-based infrastructures.

Suitable Professionals for the CCYL Certification

- **Cybersecurity Architects** securing enterprise frameworks.
- **Senior SOC Leaders** guiding operations and automation.
- **CISOs** and **Security Program Managers** leading governance efforts.
- **Incident Response Leaders** coordinating forensic investigations.
- **Red Team Leads** and **Threat Hunters** handling advanced adversaries.

Exam Information

Field	Details
Exam Code	CCYL
Delivery Mode	Online proctored exam/ authorized test center
Exam Format	MCQ and MR
No. of Questions	150
Duration	180 minutes
Passing Score	70%
Language	English
Validity	Lifetime

EXAMINATION DOMAINS & WEIGHTAGE

Domain	Domain Name	Weightage
1	Security Leadership and Governance	20%
2	Risk Management and Compliance	25%
3	Security Program Management	25%
4	Business and Financial Management	15%
5	Communication and Stakeholder Management	15%

1. SECURITY LEADERSHIP AND GOVERNANCE

This domain covers the foundational aspects of security leadership including strategic planning, governance frameworks, policy development, organizational design, and change management. Candidates should demonstrate ability to establish security governance structures, develop security strategies aligned with business objectives, create organizational policies, design security team structures, and lead organizational change initiatives.

1.1. **Security Leadership Principles**
1.2. Strategic Security Planning
1.3. Security Governance Frameworks
1.4. Governance Structures and Committees
1.5. Board and Executive Reporting
1.6. Policy Development and Management
1.7. Organizational Design for Security Teams
1.8. Change Management in Security
1.9. Security Culture Development
1.10. Zero Trust Architecture Governance
1.11. AI Security Governance
1.12. Cloud Governance

2. RISK MANAGEMENT AND COMPLIANCE

This domain focuses on enterprise risk management, regulatory compliance, third-party vendor risk, and audit management. Candidates should demonstrate ability to implement risk management frameworks, conduct enterprise risk assessments, manage compliance across multiple regulatory frameworks, assess and monitor third-party risks, and coordinate internal and external audits.

2.1. **Enterprise Risk Management Frameworks**
2.2. Risk Identification and Analysis
2.3. Risk Assessment Methodologies
2.4. Risk Treatment Strategies
2.5. Risk Appetite and Tolerance
2.6. Risk Reporting
2.7. Third-Party Vendor Risk Management
2.8. Supply Chain Risk Management
2.9. Regulatory Compliance Management
2.10. Audit Management
2.11. Controls Mapping and Documentation
2.12. Emerging Risk Management

3. SECURITY PROGRAM MANAGEMENT

This domain addresses the design, implementation, and oversight of security programs including SOC operations, incident response, vulnerability management, awareness and training, application security, cloud security, and data protection. Candidates should demonstrate ability to design security programs, select technologies, define program metrics, oversee program operations, and continuously improve security programs.

- 3.1. **Security Program Lifecycle**
- **3.2. Program Development Methodologies**
- **3.3. Security Operations Center (SOC) Program**
- **3.4. Incident Response Program Management**
- **3.5. Vulnerability Management Program**
- **3.6. Security Awareness and Training Programs**
- **3.7. Identity and Access Management (IAM) Program**
- **3.8. Application Security (AppSec) Program Management**
- **3.9. Cloud Security Program Design**
- **3.10. Data Protection Program**
- **3.11. Technology Evaluation and Selection**
- **3.12. Security Metrics and KPIs**

4. BUSINESS AND FINANCIAL MANAGEMENT

This domain focuses on the business and financial aspects of security leadership including budget planning, ROI demonstration, procurement, vendor management, and resource optimization. Candidates should demonstrate ability to develop security budgets, justify security investments with ROI and cost-benefit analysis, manage procurement processes, negotiate contracts, and optimize security spending.

- 4.1. **Security Budget Development**
- **4.2. Financial Justification and ROI**
- **4.3. Procurement and Vendor Management**
- **4.4. Contract Negotiation and Management**
- **4.5. Vendor Relationship Management**
- **4.6. Resource Optimization**
- **4.7. Financial Reporting**

5. COMMUNICATION AND STAKEHOLDER MANAGEMENT

This domain covers communication, influence, and stakeholder management skills essential for security leaders. Candidates should demonstrate ability to communicate effectively with executives and boards, translate technical concepts to business terms, influence stakeholders without direct authority, manage crisis communications, and lead change initiatives through effective communication.

5.1. **Executive and Board Communication**
5.2. Stakeholder Management
5.3. Influence and Persuasion
5.4. Crisis Communication
5.5. Technical-to-Business Translation
5.6. Change Management and Communication
5.7. Cross-Functional Collaboration
5.8. Presentation and Public Speaking
5.9. Emotional Intelligence
5.10. Negotiation Skills