

NISM-IFSCA-02B: Certification Course on Cyber Security and Cyber Resilience in the GIFT IFSC (Advanced)

Annexure II: Test Objectives

UNIT 1: FUNDAMENTALS OF CYBER SECURITY

- 1.1. Define cyber security and explain its importance
- 1.2. Describe the core principles of cyber security, including the CIA triad, and the information attributes that shape security design
- 1.3. Describe cyber security risk terminology precisely, from threat and vulnerability through inherent and residual risk to appetite and tolerance
- 1.4. Explain how threat modelling can be conducted using structured frameworks such as STRIDE and MITRE ATT&CK
- 1.5. Explain the different risk response strategies and the role of security controls in reducing identified risks to an acceptable level
- 1.6. Compare the major cyber security frameworks
 - 1.6.1. ISO 27001:2022
 - 1.6.2. NIST CSF 2.0
 - 1.6.3. PCI-DSS
- 1.7. Understand how security ownership and accountability can be embedded across an organisation as a shared responsibility for protecting information assets
- 1.8. Explain the impact of emerging technologies and evolving threats
 - 1.9.1 Increase in sophisticated attacks
 - 1.9.2 Cyber frauds
- 1.9. Case Study

UNIT 2: CYBER SECURITY GOVERNANCE AND RISK MANAGEMENT

- 2.1 Explain the purpose and benefits of cyber security governance, including the responsibilities of the board and senior management
- 2.2 Define governance structures
 - 2.2.1 Roles, responsibilities
 - 2.2.2 Accountability
 - 2.2.3 Three lines of defence
- 2.3 Explain how cyber security objectives are aligned with business goals, and regulatory requirements.
- 2.4 Know the role of stakeholders
 - 2.4.1 Organizational Leadership
 - 2.4.2 Oversight committees
 - 2.4.3 CISO and the Reporting line
- 2.5 Explain the role of security policies, standards, guidelines, procedures, and the handling of exceptions
- 2.6 Understand Risk Management Lifecycle
 - 2.6.1 Identify
 - 2.6.2 Assess

- 2.6.3 Respond and mitigate
- 2.6.4 Monitor, review and report
- 2.7 Explain the cyber risk management framework, including risk appetite, risk tolerance and regulatory requirements.
 - 2.7.1 Risk Register
- 2.8 Explain how control objectives are defined, implemented, measured, and improved to manage identified risks and ensure control effectiveness.
 - 2.8.1 Control Effectiveness
 - 2.8.2 Types of Controls
- 2.9 Know the importance of Metrics, Dashboards and Reports
 - 2.9.1 Understand Key Risk Indicators (KRI)
 - 2.9.2 Understand Key Performance Indicators (KPI) and Key control Indicators (KCI) and Compliance Indicators
 - 2.9.3 Explain the purpose of security reporting and how security information is tailored to different audiences.
- 2.10 Explain the mechanisms recommended by IOSCO for mitigating insider threats in their guidance on cyber resilience for financial market infrastructures (FMIs)
- 2.11 Understand Assessments and Audits
 - 2.11.1 Identify key phases of an audit process and how to document audit findings.
 - 2.11.2 Explain how Governance, Risk, and Compliance (GRC) platforms streamline audit workflows
- 2.12 Case Study

UNIT 3: CYBER SECURITY DESIGN AND ARCHITECTURE

- 3.1 Understand threat modelling through its five analytical lenses: threat actors, attack vectors, targets, asset criticality, and emerging threats
- 3.2 Describe network security architecture using segmentation and zoning, defence in depth, perimeter and edge security, and secure encrypted connectivity
- 3.3 Understand Cloud Security
 - 3.3.1 Define cloud computing and its key service models
 - 3.3.2 Describe core cloud security controls
 - 3.3.3 Recognize the importance of securing APIs and cloud management interfaces
 - 3.3.4 Explain cloud deployment models, key management practices, and security measures for protecting cloud workloads.
- 3.4 Explain how to establish and enforce a cybersecurity baseline using secure configuration management, vulnerability remediation, and CIS Benchmarks.
- 3.5 Define the Zero Trust security model and its core principles
 - 3.5.1 Identify key components of a Zero Trust architecture
 - 3.5.2 Describe how Zero Trust differs from traditional perimeter-based security
- 3.6 Explain the key Principles recommended by IOSCO for enhancing cyber resilience of Financial Market Infrastructures (PFMIs)
- 3.7 Understand the importance of situational awareness in pre-empting cyber events outlined by IOSCO

3.8 Case Study

UNIT 4: ASSET MANAGEMENT

- 4.1 Define asset management, its policy foundation, and its scope across the asset lifecycle.
- 4.2 Identify the types of assets to be managed
 - 4.2.1 Hardware assets
 - 4.2.2 Software assets
 - 4.2.3 Data assets
 - 4.2.4 Networks assets
 - 4.2.5 Cloud assets
- 4.3 Explain the importance of maintaining an accurate and up-to-date asset inventory
 - 4.3.1 Asset Management Policy
 - 4.3.2 Asset Register
 - 4.3.3 Asset Discovery
 - 4.3.4 Asset Management Lifecycle
- 4.4 Explain how unauthorized or “shadow” assets increase the attack surface
- 4.5 Explain how asset ownership and accountability are defined within an organization.
- 4.6 Recognize how asset classification supports risk prioritization and control implementation.
- 4.7 Analyze how asset visibility supports vulnerability management and incident response
- 4.8 Case Study

UNIT 5: ACCESS MANAGEMENT

- 5.1 Define Access Management
- 5.2 Identify key components of an access management framework- Identification, Authentication, Authorization and Accountability
- 5.3 Recognize importance of principles of least privilege, Need to know basis and segregation of duties in reducing unauthorized access risk
- 5.4 Identify the stages of access lifecycle
 - 5.4.1 Access Provisioning
 - 5.4.2 Authorization in the Lifecycle
 - 5.4.3 Access Review
 - 5.4.4 Access Revocation
- 5.5 Explain Single Sign-On and Federated Identity Management, including the trust model, token flow, benefits, and risks
- 5.6 Identify key controls for privileged user access
 - 5.6.1 Privileged Identity Management (PIM)/ Privileged Access Management (PAM)
- 5.7 Describe how multi-factor authentication (MFA) enhances secure access
- 5.8 Recognize risks associated with weak, shared, or orphaned accounts
- 5.9 Describe periodic access reviews and recertification processes
- 5.10 Case Study

UNIT 6: PHYSICAL SECURITY

- 6.1 Define physical security and explain its role in protecting information assets
- 6.2 Describe the key components of a physical security framework
 - 6.2.1 People

- 6.2.2 Premises
- 6.2.3 Equipment
- 6.2.4 Processes

- 6.3 Identify the physical security threats that affect facilities, equipment, and personnel
- 6.4 Explain the controls that secure access to facilities, including perimeter, entry, and surveillance controls
- 6.5 Explain how environmental and safety controls protect equipment and continuity of operations
- 6.6 Recognize procedures for managing and revoking physical access rights
- 6.7 Case Study

UNIT 7: THIRD PARTY RISK MANAGEMENT (TPRM)

- 7.1 Define third-party risk and identify the types of third parties
- 7.2 Explain third-party policy framework and lifecycle
- 7.3 Understand centralised governance of third-parties
- 7.4 Categorise suppliers by business impact and supply risk
- 7.5 Explain the purpose of risk assessment of third parties.
- 7.6 Recognize the importance of updating key clauses in third-party contracts related to data protection and cyber security.
- 7.7 Recognize the importance of NDAs, SLAs, and right-to-audit provisions
- 7.8 Describe how to evaluate compliance with organizational and regulatory requirements by third parties
- 7.9 Recognize the importance of including third party service providers during the testing of response and recovery plans
- 7.10 Explain the purpose of obtaining Software Bill of Material (SBOM) from software suppliers and escrow arrangements for continues support.
- 7.11 Recognize the need for assessing concentration risk of suppliers
- 7.12 Explain the process of onboarding and offboarding third-party and their employees including knowledge transfer.
- 7.13 Case Study

UNIT 8: APPLICATION SECURITY

- 8.1 Explain application security and the security activities at every phase of the Secure Software Development Lifecycle, including the elements that implement it
- 8.2 Recognise common application-layer threats through the OWASP Top 10
- 8.3 Describe secure coding principles and enforce them through published standards, code review, and training
- 8.4 Describe how static and dynamic application security testing (SAST/DAST) detect vulnerabilities.
- 8.5 Identify controls to secure APIs and microservices.
- 8.6 Explain runtime protection through Web Application Firewalls, virtual patching, and Runtime Application Self-Protection (RASP)
- 8.7 Recognize the importance of performing security assessment of applications prior to deployment in production
- 8.8 Explain the core principles of DevOps

- 8.9 Describe the evolution from DevOps to DevSecOps
- 8.10 Explain how shared security ownership across development, operations, and security teams strengthens DevSecOps practices and accountability
- 8.11 Case Study

UNIT 9: DATA SECURITY

- 9.1 Explain the data lifecycle, the risks and controls at each stage, and the enablers and challenges of lifecycle security
- 9.2 Classify data based on sensitivity, criticality, and business impact, and operate a workable classification process including data sets, labelling, and periodic review.
- 9.3 Perform data flow analysis using Data Flow Diagrams to locate risks and enforce controls.
- 9.4 Secure data in its three states, at rest, in transit, and in use, including database and storage hardening.
- 9.5 Deploy Data Loss Prevention within a layered stack alongside DAM, DRM, encryption, and access control
- 9.6 Explain key management and cryptographic hygiene best practices, including HSMs, key separation, and rotation.
- 9.7 Understand the guidelines for handling Privacy and PII data
- 9.8 Describe data masking, anonymization, and tokenization techniques for protecting Privacy data and PII.
- 9.9 Explain the data security requirements in the DPDP Act and Rules
- 9.10 Explain the principles of data archival, retention, and secure destruction based on business, legal, regulatory, and security requirements.
- 9.11 Explain the need for segregating development, test environment and production environment
- 9.12 Explain secure data backup, retention, and restoration practices
- 9.13 Case Study

UNIT 10: VULNERABILITY MANAGEMENT

- 10.1 Define vulnerability management and its importance in reducing organizational risk exposure
- 10.2 Identify the stages of the vulnerability management lifecycle
 - 10.2.1. Assessment
 - 10.2.2. Prioritization
 - 10.2.3. Remediation
 - 10.2.4. Verification
- 10.3 Explain the difference between vulnerabilities, threats, and exploits.
- 10.4 Recognize common sources of vulnerabilities
 - 10.4.1 Unpatched systems
 - 10.4.2 Misconfigurations
 - 10.4.3 Outdated software
 - 10.4.4 Application Vulnerabilities, Weak Authentication, and the Human Factor
- 10.5 Describe the role of vulnerability scanning tools
- 10.6 Describe patch management and change control procedures for addressing vulnerabilities
- 10.7 Explain how configuration baselines and hardening standards prevent recurring weaknesses

- 10.8 Identify key threats and vulnerabilities specific to mobile platforms, including insecure data storage, weak authentication, and insecure APIs
- 10.9 Evaluate risks introduced by bring-your-own-device (BYOD) environments and recommend compensating controls
- 10.10 Describe how to document and track remediation progress and exceptions.
- 10.11 Case Study

UNIT 11: SECURITY AWARENESS AND TRAININGS (CYBER HYGIENE)

- 11.1 Define the purpose of cybersecurity awareness training in reducing risks.
- 11.2 Explain how employee or contractor behaviour impacts an organization's overall security posture.
- 11.3 Identify key topics that must be covered in awareness programs
- 11.4 Recognize the importance of role-based training for employees, IT staff, and management.
- 11.5 Describe methods for delivering effective training, including e-learning, simulations, phishing drills and workshops
- 11.6 Recognise social engineering pressure techniques and email, call, and message red flags
- 11.7 Identify metrics for measuring training effectiveness
- 11.8 Explain how awareness programs align with regulatory requirements and identify the methods for customer awareness program to prevent frauds.
- 11.9 Case Study

UNIT 12: INCIDENT RESPONSE AND CYBER RESILIENCE

- 12.1 Distinguish security events from security incidents
- 12.2 Explain how detection, triage and response work as an integrated capability.
- 12.3 Explain the stages of the incident response lifecycle
 - 12.3.1 Preparation
 - 12.3.2 Identification
 - 12.3.3 Containment
 - 12.3.4 Eradication
 - 12.3.5 Recovery
 - 12.3.6 Lessons Learned
- 12.4 Explain the role of a Security Operations Center (SOC) in continuous monitoring and detection
- 12.5 Recognize threat intelligence, indicators of compromise (IoCs) and their usage in detecting cyber incidents
- 12.6 Explain how SIEM, XDR, SOAR, and threat intelligence feeds work together to detect incidents
- 12.7 Understand the approach for adverse event analysis outlined in NIST CSF 2.0
- 12.8 Identify processes for triaging, classifying, and prioritizing security incidents.
- 12.9 Understand eradication and recovery procedures to restore systems to normal operations
- 12.10 Recognize the importance of post-incident review and root cause analysis
- 12.11 Explain how automated response and playbooks improve response time
- 12.12 Analyze how KPIs such as MTTD (Mean Time to Detect) and MTTR (Mean Time to Respond) measure response effectiveness
- 12.13 Describe the threat hunting process
- 12.14 Define a process for contact with authorities and special interest groups

- 12.15 Define cyber resilience and its role in ensuring business continuity during and after a cyber incident
- 12.16 Identify the key pillars of cyber resilience
- 12.17 Define a Cyber Crisis Management Plan (CCMP)
- 12.18 Describe the importance of Business Impact Analysis (BIA) in setting recovery priorities (RTO/RPO/SDO).
- 12.19 Explain the design elements recommended by IOSCO for recovering from a cyber attack
- 12.20 Identify the steps for restoring affected systems after a cyber attack.
- 12.21 Explain the role of tabletop exercises, drills and recovery simulations in preparedness.
- 12.22 Explain the Testing methodologies and practices outlined by IOSCO to validate the effectiveness of an organization's cyber resilience framework
- 12.23 Recognize the importance of communication plans and stakeholder coordination during recovery.
- 12.24 Identify metrics to measure recovery effectiveness
- 12.25 Analyze and recommend corrective actions to address identified gaps and strengthen the organization's overall cyber resilience posture
- 12.26 Explain the concept of resilience by design outlined by IOSCO in their guidance on cyber resilience for financial market infrastructures (FMIs)
- 12.27 Case Study

UNIT 13: IFSCA'S REGULATORY FRAMEWORK ON CYBER SECURITY

- 13.1 Explain IFSCA's cyber security and cyber resilience framework, including the principle of proportionality and its key requirements for Regulated Entities
- 13.2 Describe the governance requirements mandated by IFSCA, including responsibilities of the Oversight Body, senior management, Governing Board, and the role of a CISO/designated officer
- 13.3 Explain the principles of the cyber security and cyber resilience framework
 - 13.1.1 Asset classification
 - 13.1.2 Risk Assessment
 - 13.1.3 Access Control
 - 13.1.4 Physical Security
 - 13.1.5 Vulnerability assessment and penetration testing
 - 13.1.6 Recovery
 - 13.1.7 Incident Management
 - 13.1.8 Audit Trail
- 13.4 Recognize the third-party risk management obligations under IFSCA guidelines
- 13.5 Describe the audit and reporting obligations and incident reporting requirements mandated by IFSCA
- 13.6 Identify the exemption categories and the conditions attached to them under the March 2026 amendment.
- 13.7 Describe the additional, more prescriptive requirements for Market Infrastructure Institutions under the April 2026 MII circular
- 13.8 Explain the measures advised in the June 2026 advisory on heightened cyber security risks arising from frontier Artificial Intelligence models

UNIT 14: EMERGING CHALLENGES IN CYBER SECURITY

- 14.1 AI-enabled cyberattacks
 - 14.1.1 Deepfakes
 - 14.1.2 Phishing Automation
 - 14.1.3 AI-Powered Malware and Frontier Models
- 14.2 Describe the structural risk quantum computing poses to public-key cryptography
 - 14.2.1 Understand fundamentals of quantum computing
 - 14.2.2 Understand the need for cryptographic algorithms and protocols
 - 14.2.3 Identifying What Requires Quantum-Resistant Protection
- 14.3 Describe the security challenges of IoT devices and 5G networks and the controls that address them
- 14.4 Explain cyber warfare and geopolitical cyber risk, including espionage, sabotage, critical infrastructure attacks, supply chain compromise, and the attribution problem
- 14.5 Understand Governance challenges in usage of AI
- 14.6 Case Study
