

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

Annexure II: Test Objectives

UNIT 1: FUNDAMENTALS OF CYBER SECURITY

- 1.1. Define cyber security and understanding its importance
- 1.2. Describe the core principles of cyber security
- 1.3. Understand cyber security risk terminology
- 1.4. Define threat and threat modelling
- 1.5. Introduction to cyber security frameworks
 - 1.5.1. NIST CSF 2.0
 - 1.5.2. ISO 27001:2022
 - 1.5.3. IOSCO – Guidance on cyber resilience for FMIs
 - 1.5.4. PCI-DSS
- 1.6. Identify common threats and threat actors
- 1.7. Explain the concept of defence in depth and layered security

UNIT 2: CYBER SECURITY GOVERNANCE AND RISK MANAGEMENT

- 2.1 Understand the purpose of Cyber security governance
- 2.2 Define governance structures
 - 2.2.1 Roles, responsibilities, and accountability
 - 2.2.2 Three lines of defence
 - 2.2.3 Committees and the CISO
- 2.3 Explain the cyber security risk governance C management tiers outlined in NIST CSF 2.0
- 2.4 Explain how cyber security objectives are set in alignment with business goals and regulatory requirements
- 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 and review
- 2.7 Explain the cyber risk management framework, including risk appetite, risk tolerance and risk registers
 - 2.7.1 Explain control objectives and effectiveness
- 2.8 Explain the use of metrics, KRIs, KPIs, the CPMI-IOSCO mechanisms for mitigating insider threats in FMIs, and the purpose and phases of cyber security audits
- 2.9 Explain insider threats and the CPMI-IOSCO mechanisms for mitigating them in Financial Market Infrastructures (FMIs)
- 2.10 Define the purpose and scope of cybersecurity assessments and audits
- 2.11 Describe the role of cyber security culture in fostering secure organisational behaviour
- 2.12 Explain cyber insurance as a risk transfer mechanism and the types of losses it may cover

UNIT 3: CYBER SECURITY DESIGN AND ARCHITECTURE

- 3.1 Define Cyber security design and architecture
- 3.2 Understand Threat Modelling
- 3.3 Explain the principles of network security architecture, including segmentation, defence in depth, perimeter and edge security, and secure connectivity
- 3.4 Describe Identity Security
 - 3.4.1 Recognize the purpose of identity lifecycle management
 - 3.4.2 Describe various Authentication methods
 - Password based
 - Multi-factor
 - Biometric
 - 3.4.3 Explain the principle of least privilege, Role Based Access Control (RBAC) and AAA model (authentication, authorization and accounting)
 - 3.4.4 Identify governance and threat controls
- 3.5 Cloud Security
 - 3.5.1 Define cloud computing and its key service models
 - IaaS
 - PaaS
 - SaaS
 - 3.5.2 Describe core cloud security controls
 - Encryption
 - Network Segmentation
 - Identity Management
 - 3.5.3 Recognize the importance of securing APIs and cloud management interfaces
 - 3.5.4 Understand deployment models, key management, and workloads
- 3.6 Explain the purpose of a cyber security baseline and the role of secure configuration standards such as the CIS Benchmarks
- 3.7 Describe data security measures, including encryption, data localisation, the protection of PII, and the DPDP Act
- 3.8 Explain the Zero Trust model and the cyber resilience principles for financial market infrastructures set out by CPMI-IOSCO
- 3.9 Explain the fundamental cryptographic techniques used to protect data confidentiality, integrity, authenticity, and non-repudiation
- 3.10 Describe key email and web security controls used to protect against phishing, spoofing, malware, and other cyber threats

UNIT 4: ASSET MANAGEMENT

- 4.1 Define asset management
- 4.2 Identify the main types of IT assets and explain why asset management is foundational to cyber security
- 4.3 Explain the purpose and contents of an asset inventory and register, and the role of an asset management policy
- 4.4 Describe the asset management lifecycle from procurement to secure disposal
- 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 Describe the risks posed by shadow assets
- 4.9 Explain the purpose of asset discovery and the techniques used to identify and maintain an accurate asset inventory
- 4.10 Explain the risks associated with legacy and end-of-life systems and the controls used to manage them

UNIT 5: ACCESS MANAGEMENT AND PHYSICAL SECURITY

- 5.1 Define Access Management
- 5.2 Identify key components of an access management framework – Identification, Authentication, Authorisation 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 Describe the key phases of the access lifecycle
 - 5.4.1 Access provisioning
 - 5.4.2 Authorization,
 - 5.4.3 Review and recertification
 - 5.4.4 Revocation
- 5.5 Single sign-on and Federated Identity management
 - 5.5.1 Single Sign-On (SSO)
 - 5.5.2 Federated Identity Management (FIM)
- 5.6 Describe the controls for privileged access, including PIM and PAM, and the risks of weak, shared, and orphaned accounts
- 5.7 Describe how multi-factor authentication (MFA) enhances secure access
- 5.8 Recognize risks associated with weak, shared, or orphaned accounts
- 5.9 Assess the role of encryption, authentication, and biometrics in achieving secure mobile access for regulated entities
- 5.10 Explain the role of physical security in protecting information assets
- 5.11 Identify the components of a physical security framework
- 5.12 Describe physical security threats
- 5.13 Explain the controls for securing facility access
- 5.14 Describe the environmental and safety controls used to protect IT infrastructure
- 5.15 Recognize procedures for managing and revoking physical access rights
- 5.16 Explain password-related risks and controls, including password managers and passwordless authentication
- 5.17 Describe the physical security controls used to protect data centres and server rooms

UNIT 6: THIRD PARTY RISK MANAGEMENT (TPRM)

- 6.1 Define third-party risk
- 6.2 Identify the different types of third parties and the cyber security risks associated with them
- 6.3 Explain the governance and oversight of third-party risks
- 6.4 Explain the purpose of third-party risk assessments and the risk-based approach used to evaluate and manage them
- 6.5 Describe the key contractual, governance, and compliance requirements for third parties
- 6.6 Recognize the need for assessing concentration risk of suppliers
- 6.7 Recognize the importance of including third party service providers during the testing of

- response and recovery plans
- 6.8 Explain the purpose of obtaining Software Bill of Material (SBOM) from software suppliers and escrow arrangements for continues support
 - 6.9 Explain the process of onboarding and offboarding Third party and their employees including knowledge transfer
 - 6.10 Describe the risk-based due diligence process for evaluating a vendor's security, financial, and operational fitness
 - 6.11 Describe fourth-party risk and the role of contractual controls in managing sub-outsourcing arrangements

UNIT 7: APPLICATION SECURITY

- 7.1 Define application security
- 7.2 Understand the relevance of application security across the software development lifecycle (SSDLC)
- 7.3 Identify common application-layer threats
 - OWASP Top 10
- 7.4 Explain secure coding principles, threat modelling, and secure design reviews
- 7.5 Describe how static and dynamic application security testing (SAST/DAST) detect vulnerabilities
- 7.6 Identify controls to secure APIs and microservices
- 7.7 Explain DevOps and DevSecOps, including how security is built into CI/CD pipelines and shared across teams
- 7.8 Explain the role of Web-Application Firewalls (WAFs) and runtime protection mechanisms in defending web applications against attacks
- 7.9 Describe the importance of secure code review and developer security training in identifying and preventing application security vulnerabilities

UNIT 8: DATA SECURITY

- 8.1 Define data security
- 8.2 Explain the data lifecycle and why data must be protected at every stage, from collection to destruction
- 8.3 Classify data by sensitivity and criticality, and explain why classification drives the level of protection
- 8.4 Describe how data is secured in its three states: at rest, in transit, and in use
- 8.5 Recognize the role of Data Loss Prevention (DLP) solutions in preventing exfiltration
- 8.6 Explain key management and cryptographic hygiene best practices
- 8.7 Describe the controls for protecting personal data, including masking, tokenisation, and minimisation
- 8.8 Explain secure backup, retention, archival, and destruction, including the risk of data remanence
- 8.9 Explain the need for segregating development, test environment and production environment
- 8.10 Recognize regulatory and compliance requirements related to data security- DPDP Act
- 8.11 Explain the controls used to secure databases and storage systems,
- 8.12 Describe the principles of privacy by design and how they are incorporated into system development

UNIT 9: VULNERABILITY MANAGEMENT

- 9.1 Define vulnerability management and its importance in reducing organizational risk exposure
- 9.2 Identify the stages of the vulnerability management lifecycle- Assessment, Prioritization, Remediation and Verification
- 9.3 Explain the difference between vulnerabilities, threats, and exploits
- 9.4 Identify the common sources of vulnerabilities, including software defects, misconfigurations, and the human factor
- 9.5 Describe the role of vulnerability scanning tools
- 9.6 Describe patch management and change control procedures for addressing vulnerabilities
- 9.7 Explain how configuration baselines and hardening standards prevent recurring weaknesses
- 9.8 Describe the particular risks of mobile devices and Bring Your Own Device (BYOD) arrangements
- 9.9 Describe how to document and track remediation progress and exceptions
- 9.10 Explain the role of penetration testing and red team exercises in assessing cyber security resilience
- 9.11 Describe vulnerability metrics and their use in management reporting

UNIT 10: SECURITY AWARENESS AND TRAININGS (CYBER HYGIENE)

- 10.1 Explain why people are central to security
- 10.2 Define the purpose of cybersecurity awareness training in reducing risks
- 10.3 Describe what a security awareness programme should cover and the design points that make it effective
- 10.4 Recognize the importance of role-based training for employees, IT staff, and management
- 10.5 Describe the main delivery methods, including e-learning, simulations, phishing drills and workshops
- 10.6 Identify metrics for measuring training effectiveness
- 10.7 Explain how awareness programs align with regulatory requirements
- 10.8 Identify need and methods for customer awareness program to prevent frauds
- 10.9 Describe common social engineering pressure techniques and how to recognise their red flags
- 10.10 Explain the role of security champions in strengthening security awareness

UNIT 11: INCIDENT RESPONSE AND CYBER RESILIENCE

- 11.1 Define incident management and response
- 11.2 Distinguish between a security event and a security incident
- 11.3 Define cyber incident detection, triage and response
- 11.4 Explain stages of the incident response lifecycle from preparation through to recovery and post-incident review
- 11.5 Explain the role of a Security Operations Center (SOC) in continuous monitoring and detection
- 11.6 Describe methods for detecting incidents using SIEM, XDR and SOAR
- 11.7 Recognize threat intelligence, indicators of compromise (IoCs) and their usage in detecting cyber incidents
- 11.8 Describe threat hunting
- 11.9 Understand how KPIs such as MTTD (Mean Time to Detect) and MTTR (Mean Time to

- Respond) measure response effectiveness
- 11.10 Understand how cyber incidents are reported
 - 11.11 Explain cyber resilience and its four pillars
 - 11.12 Define a Cyber Crisis Management Plan (CCMP)
 - 11.13 Describe the importance of Business Impact Analysis (BIA) in setting recovery priorities
 - 11.14 Describe the key principles and steps involved in safe recovery from a cyber-incident, including the role of CPMI-IOSCO cyber resilience guidance
 - 11.15 Understand the role of effective communication and stakeholder coordination during recovery
 - 11.16 Explain how resilience is tested
 - 11.17 Understand how recovery effectiveness is measured
 - 11.18 Describe the purpose of post-incident analysis and the role of corrective actions in improving cyber resilience
 - 11.19 Identify components of an organization's attack surface
 - 11.20 Describe resilience by design, and the IFSCA requirements for resilience
 - 11.21 Explain the key principles of digital forensics and evidence handling during cyber incidents
 - 11.22 Explain the role of tabletop exercises and recovery simulations in preparedness

UNIT 12: REGULATORY REQUIREMENTS (IFSCA)

- 12.1 Explain IFSCA's cyber security and cyber resilience framework, including the principle of proportionality and its key requirements for Regulated Entities
- 12.2 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
- 12.3 Explain the principles of the cyber security and cyber resilience framework
 - 12.3.1 Asset classification
 - 12.3.2 Risk Assessment
 - 12.3.3 Access Control
 - 12.3.4 Physical Security
 - 12.3.5 Vulnerability assessment and penetration testing
 - 12.3.6 Recovery
 - 12.3.7 Incident Management
 - 12.3.8 Audit Trail
- 12.4 Recognize the third-party risk management obligations under IFSCA guidelines
- 12.5 Describe the audit and reporting obligations and incident reporting requirements mandated by IFSCA
- 12.6 Understand the exemptions provided by IFSCA
- 12.7 Understand the additional, more prescriptive requirements for Market Infrastructure Institutions

UNIT 13: EMERGING CHALLENGES IN CYBER SECURITY

- 13.1 Recognise emerging technologies and threats that influence the cyber security landscape
- 13.2 Explain how AI changes the economics, quality, and scale of cyberattacks, including deepfakes, phishing automation, and AI-powered malware
- 13.3 Describe the structural risk that quantum computing poses to public-key cryptography, and

the harvest-now-decrypt-later threat

13.3.1 Understand fundamentals of quantum computing

13.3.2 Understand the need for cryptographic algorithms and protocols

13.3.3 Recognize data and systems requiring quantum-resistant protection

13.4 Describe the security challenges introduced by IoT devices and 5G networks, and the controls that address them

13.5 Explain cyber warfare and geopolitical cyber risk, including espionage, sabotage, critical-infrastructure attacks, and the attribution problem

13.6 Describe the governance challenges in the organisational use of AI, including accountability, bias, data privacy, and shadow AI
