BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR I FINANCIAL SUPERVISION SECTOR

MEMORANDUM NO. M-2026-047

To : **ALL BANGKO SENTRAL-SUPERVISED INSTITUTIONS (BSIs)**

Subject : **Guidelines on the Submission of the Cybersecurity Controls Self-Assessment (CCSA) through the Advanced SupTech Engine for Risk-based Compliance (ASTERisC*) Platform**

The increasing reliance on digital financial services and the rapid evolution of cyber threats necessitate a robust approach to cybersecurity risk management across Bangko Sentral-Supervised Institutions (BSIs). To aid BSIs in enhancing cyber capabilities, the Bangko Sentral ng Pilipinas (BSP) is implementing a Cybersecurity Maturity Framework (CMF) designed to strengthen sector-wide resilience and align with global standards and leading practices.

The CMF shall be complemented by the Cybersecurity Controls Self-Assessment (CCSA) for benchmarking BSIs' current activities, processes, and guidelines, and planning for their target maturity. The assessment tool contains activity/capability-based questions intended to reflect the BSI's maturity in a particular control area and to gather cyber trends and practices.

In line with the **Cybersecurity Controls Self-Assessment (CCSA)** requirement under BSP Circular No. 1232, covered BSIs shall accomplish and submit the CCSA through the Advanced SupTech Engine for Risk-based Compliance (ASTERisC*).

Accordingly, the following guidelines shall be observed by all covered BSIs:

1. Submission of CCSA through the ASTERisC* platform:

    a. The CCSA questionnaire shall be deployed in ASTERisC* and shall be made available to covered BSIs upon issuance of this memorandum. ASTERisC* is accessible through https://asterisc.bsp.gov.ph.

    b. The ASTERisC* user manual, instructional videos, field guides, and User Account Form (UAF) for the CCSA are accessible in the BSP website (www.bsp.gov.ph/ses/reporting_templates). New and existing ASTERisC* users are required to review the instructional videos and user manual prior to submission of the CCSA through ASTERisC*.

    c. The CCSA requirement will be accessible in the "My Cybersecurity Controls Self-Assessment (CCSA)" section of the BSI dashboard.

    d. The BSI Single Point of Contact (SPOC) designated in ASTERisC* shall be responsible for accomplishing and submitting the CCSA through the platform. The BSI is expected to establish adequate processes to gather and consolidate data and information from the relevant units to ensure accurate and complete responses.

    e. An email notification shall automatically be sent to the ASTERisC* authorized user upon successful submission of the accomplished CCSA questionnaire.

2. The CCSA Questionnaire, attached as **Annex A**, is composed of six sections:

a. Sections I to IV contain the control questionnaire, which serves as the primary basis for assessing the maturity of a BSI's information security and cybersecurity risk management practices. The assessment shall cover four major domains and their corresponding sub-domains, namely: (i) Information Security Governance; (ii) Information Security Risk Management; (iii) Security Control Implementation; and (iv) Cyber Threat Intelligence and Collaboration.
b. Section V contains survey questions, which the BSP may use to gather additional information needed to understand the technology landscape.
c. Section VI consists of required documentation that facilitates a deeper understanding of the control environment.

3. In responding to the questions, please take into account that cybersecurity forms part of information security. Accordingly, cybersecurity considerations should be included in responses to information security-related questions, where applicable. Regardless of how controls and processes are designed and documented, BSIs may select the control statements that best corresponds to their current practices. Further, the non-implementation of a specific control or the selection of a negative control statement in the CCSA does not automatically result in a lower maturity score, as controls will be assessed holistically. After submission, the CCSA will undergo a validation process and results will be made available to the respective BSIs through the ASTERisC*.

4. The initial submission of the CCSA shall be due **sixty (60) calendar days** from the issuance of this memorandum. The CCSA requirement shall be activated in ASTERisC* and made accessible only to covered entities.

5. Covered BSIs shall submit the CCSA annually, on or before **31 March** following the end of the reference year.

For purposes of this requirement, covered BSIs are those classified by the Bangko Sentral as having a **Moderate** or **Complex** IT Profile, as well as other BSIs that the Bangko Sentral may specifically designate. To facilitate compliance, the BSP shall notify covered BSIs and inform them of the corresponding CCSA submission requirement. Any BSI subsequently reclassified from a Simple IT Profile to a Moderate or Complex IT Profile shall be informed of the reclassification and the applicable CCSA requirement.

For inquiries regarding the CCSA requirements and related guidelines, as well as technical issues related to the ASTERisC* platform, BSIs may coordinate with the Technology Risk and Innovation Supervision Department (TRISD) at trisd@bsp.gov.ph.

For compliance.

Digitally signed by
Arifa A. Ala
Date: 2026.10.01
19:32:09 +08'00'

ARIFA A. ALA
Sector-In-Charge

01 October 2026

CYBERSECURITY CONTROLS SELF-ASSESSMENT QUESTIONNAIRE

I. Information Security Governance

1. Which of the following statements describes your institution's Information Security Program (ISP) and Information Security Strategic Plan (ISSP)? (Select all that apply)

    a. The ISP and ISSP have not yet been established.

    b. The ISP and ISSP have been established, and the Board has designated an accountable member of Management to oversee their implementation.

    c. The Board or its designated committee formally reviews and approves the ISP and ISSP at least annually. The effectiveness and overall status of the program are presented to the Board through a formal written report on a defined schedule.

    d. Board-level reporting moves beyond basic metrics to include insights on threat intelligence trends and the institution's security posture. The Board actively holds business units accountable for implementing appropriate security controls.

    e. The Board's oversight includes evaluating the impact of the organization's security posture on the broader financial ecosystem. Governance discussions focus on strategic improvements and contributing to the security of the financial sector.

2. Which of the following statements describes how information security awareness is promoted within the institution? (Select all that apply)

    a. The employee handbook clearly states the employee's responsibility and accountability in information security and the formal disciplinary process for non-compliance.

    b. Cyber risks are considered and discussed in business unit meetings and initiatives.

    c. Employees are conscious of cyber risks, capable of identifying cyber threats and incidents, and know how to appropriately escalate potential cybersecurity issues.

    d. Accountability for compliance with information security policy and procedures are embedded in performance evaluations.

    e. Cyber risks are embedded in the institution's risk culture and considered in relevant business decisions.

    f. Cyber risks are reported and discussed at appropriate Board and management committee meetings

    g. The Board, Senior Management, and employees are part of the mandatory information security and cybersecurity awareness programs and the promotion of a cyber-aware culture is continually reviewed and enhanced.

    h. The institution leads efforts that promote cyber security culture across the financial sector and influence other sectors.

i. The internal audit provides independent assurance on the effectiveness of the institution's information security and cybersecurity awareness programs.

3. Which of the following statements describes how information security accountabilities and responsibilities are established in the institution? (Select all that apply)

   a. The Board or its designated committee formally designates an accountable member of Management to implement and manage the ISP.

   b. The Board is kept informed of the effectiveness and status of the ISP, including the accountable and responsible personnel, through a formal written report submitted at least annually.

   c. The Board holds business unit leaders accountable for implementing and managing security controls within their respective processes.

   d. Board-level reporting includes metrics that assess the effectiveness of security initiatives throughout the institution.

   e. Board oversight evolves to include evaluating management's effectiveness in anticipating and responding to emerging threats.

   f. Accountability extends to the institution's role and potential impact on the security of the broader financial ecosystem.

4. Which of the following statements describes the institution's information security-related resource plans and strategies? (Select all that apply)

   a. Information and cybersecurity roles and responsibilities are not formally delegated. Qualifications and accountabilities are not yet defined and documented.

   b. Information and cybersecurity personnel roles and responsibilities are clearly identified, with security functions anchored on defined and appropriate qualifications.

   c. Management possesses appropriate skills and knowledge to lead the institution's ISP and ISSP.

   d. A formal process exists to identify cybersecurity tools and expertise consistent with short and long-term goals.

   e. The institution evaluates the current workforce and designs interventions to address identified capabilities and expertise gaps.

   f. The institution has established a talent recruitment, retention, and succession program for information/cyber security personnel.

   g. The institution has designated the responsibility to develop, contribute, and integrate enterprise-wide security and cyber defense strategies.

   h. The institution benchmark information and cybersecurity functions against peers, including recruitment, retention, and succession planning strategies.

   i. The Institution forges a partnership with industry associations and the academe to source talent.

5. Which of the following statements describes the institution's board committee meetings relative to information and cybersecurity concerns or issues? (Select all that apply)

    a. Information and cybersecurity issues are discussed in committee meetings when there is a highly publicized cyber-related event or a regulatory alert.

    b. The Board or appointed Board-level Committee member/s has information security expertise or engages an expert to aid with oversight capabilities.

    c. Management established a policy and process to identify the root cause(s) when an information and cybersecurity incident resulted in a material loss.

    d. The Board or appointed Board-level Committee holds business units accountable to implement effectively appropriate information and cybersecurity controls in their respective processes.

    e. The Board or appointed Board-level Committee evaluates Management's actions and possible cybersecurity impact on the financial ecosystem and other critical infrastructure.

    f. The Board or appointed Board-level Committee discusses information and cybersecurity improvements and shares its possible contribution to the financial ecosystem.

II. Information Security Risk Management

6. Which of the following statements describes the institution's information security risk management process (select all that apply)

    a. An Information Security Risk Management (ISRM) process is not yet established or integrated in the institution's risk management framework.

    b. The institution follows informal or ad-hoc activities for risk identification, assessment, and mitigation.

    c. Policies, procedures, standards, or guidelines for identifying, assessing, mitigating, responding, managing, and monitoring risks are defined and established.

    d. Roles and responsibilities for risk management activities are clearly defined.

    e. The institution uses Key Risk Indicators (KRIs) to measure its security posture and track risk levels over time.

    f. ISRM outputs are used to inform strategic decisions and resource allocation, and a formal process exists for escalating significant risks to senior management and the Board.

    g. The institution has clearly defined and Board-approved risk appetite and tolerance for cybersecurity-related risks, consistent with the institution's overall risk management strategy.

    h. The risk management process incorporates leading and lagging indicators in measuring risk and automated tools are utilized to facilitate early risk detection and management.

III. Security Control Implementation

A. Identification

7. Which of the following statements describes the integration of information security-related expectations within your institution? (Select all that apply)

    a. Business processes are informally defined and not linked to cybersecurity.

    b. Processes are documented and mapped to critical systems.

    c. Cybersecurity controls are integrated into business process workflows.

    d. Business processes are continuously improved through the use of cyber risk metrics and automated security controls.

8. Which of the following statements describes how the institution manages its information asset inventory? (select all that apply)

    a. The institution maintains an inventory of technology hardware assets.

    b. The institution maintains a comprehensive inventory of information assets (e.g., hardware, software, data, systems).

    c. Information assets are protected according to defined data classification and their business value.

    d. Management has designated the responsible business unit to maintain the information asset inventory.

    e. Information asset inventory is updated to identify new, relocated, re-purposed, and disposed assets, at least annually.

    f. Supply chain risks are evaluated prior to the acquisition of mission-critical information systems and components.

    g. The institution uses automated asset discovery tools at defined intervals.

    h. The institution uses automated tools to discover, track, manage, and update assets in real-time.

9. Which of the following statements describes how the institution manages threats and vulnerabilities? (Select all that apply)

    a. Anti-malware/anti-virus solution is deployed and used to detect attacks, but no formal procedure exists regarding deployment, management, and monitoring. Email system blocks/filters commonly known cyber threats.

    b. Policies, procedures, and standards are in place for deployment, management, maintenance, and monitoring anti-malware/anti-virus solution.

    c. Anti-malware/anti-virus solution is automatically updated. Email attachments are automatically scanned for malware and are quarantined, as necessary.

    d. A centralized monitoring tool is utilized for the deployment and updating of the anti-malware/anti-virus tool/software.

e. Anti-malware/anti-virus software performance indicators are defined and regularly reported to management and the appropriate committee.

f. Automated security tools detect and alert on suspicious user behavior indicative of potential insider threats.

g. Malware/virus scanning is conducted in all environments in real-time or near real-time. User tasks and content are securely stored and isolated to prevent malware from accessing critical data, operating systems, servers, or applications.

10. Which of the following statements describes how interconnections between the institution and external parties are managed? (Select all that apply)

    a. External connectivity that supports critical business processes is identified.

    b. The institution ensures all third-party connections are authorized.

    c. Critical business processes are mapped to the supporting external connections/parties.

    d. A process is in place to review network diagrams and external connections at least annually.

    e. Connection monitoring covers all external parties (e.g., third parties, business partners, service providers, customers).

    f. Controls in the primary and backup third-party connections are monitored and evaluated regularly.

    g. The institution uses automated tools to monitor the volume of information flow, network connections (new or modified), and risk alerts in real time.

    h. The institution can segment, isolate, or drop connections with external parties to limit cyberattack damage.

    i. Not applicable – please explain

11. Which of the following statements describes the institution's cloud security governance and risk management practices? (Select all that apply)

    a. Cloud adoption is ad hoc. Roles and responsibilities between the institution and the cloud service provider are not clearly defined.

    b. Policies and procedures governing the use of cloud services are documented, including responsibilities under the shared responsibility model.

    c. Cloud services are subject to risk assessments prior to adoption. Security requirements for identity and access management, data protection, logging, and monitoring are incorporated into cloud service arrangements.

    d. Cloud configurations and assets are periodically reviewed using defined procedures or automated tools to identify misconfigurations and security weaknesses.

    e. The institution implements Infrastructure as Code (IaC) for provisioning and managing cloud infrastructure to ensure secure, consistent, and auditable configurations, thereby reducing the risk of misconfigurations and unauthorized changes.

f. The institution implements a Cloud Access Security Broker (CASB), or similar solutions, to monitor, control, and enforce security policies for the use of cloud services, including visibility of cloud activities, data protection, and detection of unauthorized or risky cloud usage.

g. The institution implements Cloud Security Posture Management (CSPM) to continuously monitor cloud environments for security misconfigurations, policy violations, and compliance risks.

h. Cloud security risks are integrated into the institution's enterprise risk management framework. Multi-cloud or hybrid cloud environments are assessed for operational and security risks.

i. Security monitoring extends to cloud environments, including centralized logging, threat detection, and incident response integration.

j. Cloud service provider security posture and compliance with contractual and regulatory requirements are periodically evaluated.

k. Not applicable – please explain.

12. Which of the following statements describes the institution's security architecture process? (Select all that apply)

a. A network diagram is available for internal connections.

b. A data flow diagram is available and documents the information flow to connected parties.

c. Network and system diagrams illustrate information flow, including protection mechanisms. The document is controlled, secured from unauthorized access, and reviewed regularly.

d. Security controls are in place to detect and prevent intrusions from third-party connections.

e. New or changes in network, data flow, or interconnections are validated against network and security architecture before implementation.

f. Architecture is continuously optimized using threat modeling and automated validation tools.

B. Prevention

13. Which of the following statements describes the institution's current state in information and cyber security policies, standards, and procedures? (Select all that apply)

a. No formal security policies, standards, or procedures in place.

b. ISSP and ISP are formalized. Security policies, standards, and procedures are in place (password rules, access control, encryption, etc.), and no identified gaps with BSP regulations (Appendix 75 of the MORB and Q-62 of the MORNBFI).

c. Compliance with security policies, standards, and procedures is strictly monitored. Policy review is done regularly and is updated as necessary.

d. Implementation of automated tools to monitor, implement, and manage the policy framework (e.g. GRC software)

14. Which of the following statements describes the institution's baseline security standards? (Select all that apply)

    a. Default (off-the-shelf) security baselines are applied to critical systems but are not formally documented or consistently enforced across the enterprise.

    b. The institution has established baselines and formal deployment processes, ensuring assets have appropriate safeguards.

    c. Baseline configurations are protected, and changes undergo a security impact assessment and appropriate approval.

    d. The institution employs automated tools to detect and prevent unauthorized software, hardware, or system configuration changes on critical assets.

    e. The institution implements a comprehensive automated tool to detect and prevent unauthorized software, hardware, or system configuration changes across all assets in real-time.

15. Which of the following statements describes the institution's security training and awareness program? (Select all that apply)

    a. Cybersecurity awareness is informal or ad hoc. There are no structured training programs in place, and any awareness efforts are typically initiated only after a security incident occurs or are reliant on industry association offerings.

    b. The institution has established a formal cybersecurity training program that is scheduled regularly.

    c. Training content is tailored to specific roles within the institution, ensuring that employees receive relevant information based on their job functions.

    d. Cybersecurity training is actively managed, and its effectiveness is measured through various methods such as post-training assessments, employee feedback, and performance metrics.

    e. The institution conducts phishing simulations and scenario-based exercises to evaluate employee responses to real-world threats.

    f. The institution employs advanced, adaptive training platforms that personalize cybersecurity education based on individual behavior, risk profile, and learning progress.

    g. Artificial intelligence and analytics are used to deliver dynamic content that evolves with emerging threats and employee needs.

    h. Continuous learning is encouraged through interactive modules, gamified experiences, and real-time alerts.

16. Which of the following statements describes the institution's security screening standards in the hiring process? (Select all that apply)

    a. The institution's screening process is currently limited to pre-employment requirements and follows standard assessment requirements.

b. Policies and procedures for employees, hiring candidates, contractors, and outsourced/third parties are defined, covering pre-employment, during employment, and considering background verification consistent with business and data security requirements.

c. The institution has defined performance indicators, and security screening activities are closely monitored for compliance and relevance to the function being sourced or performed. Results are reported to Management and the appropriate committee.

d. Quality assurance process is in place where screening activities and scope are reviewed, updated regularly, and compliance with the set security screening standards is evaluated for relevance.

17. Which of the following statements describes the institution's current manpower resources for the information security (IS) and cybersecurity functions? (Select all that apply)

a. The CISO is a senior-level executive who possesses relevant certifications and substantial experience, as defined in internal qualification standards, in the field of IS.
b. IS and cybersecurity responsibilities are assigned on an ad hoc basis, and personnel may not have formal training, certifications, or clearly defined competencies related to cybersecurity.
c. Designated personnel are responsible for IS and cybersecurity functions, and some staff have relevant training or certifications, although competency requirements and role qualifications are not consistently defined or enforced.
d. The institution has defined qualification requirements for IS and cybersecurity roles, and personnel responsible for these functions possess relevant education, training, and/or professional certifications (e.g., CISSP, CISM, etc.).
e. The institution maintains a structured competency framework for IS and cybersecurity personnel, with continuous professional development, and periodic assessments to ensure personnel remain capable of addressing evolving cyber threats.

18. Which of the following statements describes the institution's physical and environmental control standards? (Select all that apply)

a. Physical access to information systems and communication assets is controlled and restricted to prevent unauthorized access.

b. Physical access to mission-critical, high-risk, and confidential systems is restricted and logged, and unauthorized access is prevented.

c. Physical access controls are integrated with logical access systems, in accordance with the institution's defined access privileges.

d. Automated physical access systems are integrated with real-time monitoring and alerting. Environmental controls are optimized using predictive analytics.

e. Sector-leading practices are adopted for physical and environmental security.

f. Not applicable – please explain

19. Which of the following statements BEST describes the institution's technology design standards?

a. Minimal layering of defenses; flat network; product development is functionality-focused; and no defined standards for infrastructure security.

b. Baseline security standards are documented for networks, servers, software, and end-user devices; secure coding guidelines are in place; and product design standards address security and privacy.

c. Independent groups such as information security, compliance, and internal audit validate security integration in infrastructure and product design.

d. Implementation of advanced security frameworks like zero trust infrastructure, and DevSecOps, among others; and the use of automated configuration compliance tools to evaluate the current state against the desired information security maturity level.

20. Which of the following statements describes the institution's identity and access management standards? (Select all that apply)

a. Employees are granted access to data, information, and systems only as necessary for their specific job roles and responsibilities, in accordance with the "least privilege" principle.

b. Employee access to data, information, and systems are regularly assessed to maintain appropriate separation of duties. Privileged user accounts are limited and subject to stringent controls, including dedicated credentials and enhanced authentication.

c. Access control policy clearly defines password complexity, reuse, and failed attempts requirements.

d. Access to systems, applications, hardware, and other resources requires identification and authentication.

e. Access to services, products, and channels require authentication control commensurate with its risk levels.

f. User access reviews on all systems are regularly performed and proportionate to the system's risk level, and changes/revocation of logical and physical access undergo a formal approval process.

g. Administrators are assigned separate access credentials for non-administrative and administrative tasks.

h. Physical and logical access revocation is immediate upon involuntary termination and within 24 hours of an employee's end of service.

i. Access policy requires that default accounts and passwords be changed, and unnecessary default accounts are removed before system implementation.

j. Employees accessing high-risk or mission-critical applications and systems require multi-factor authentication.

k. Third parties or outsourced service providers require multi-factor authentication or layered controls when accessing the BSI's network, systems, or applications.

l. Automated tools are in place that perform real-time user credential risk scoring and mitigation.

m. Automated tools/controls are in place to revoke or isolate access to mitigate potential damage when suspicious behavior is detected.

21. Which of the following statements describes the institution's remote access standards? (Select all that apply)

    a. No formal policy for remote access. Remote sessions are not encrypted or monitored and use single-factor authentication.

    b. Documented policies for remote access and multi-factor authentication (MFA) are required for critical users, functions, and roles.

    c. A Virtual Private Network (VPN) or equivalent is used for remote connections. Logs are collected for remote sessions.

    d. Vendor access is authorized and approved prior to provisioning and is revoked upon completion of the approved activity.

    e. Identity and access management solutions are implemented. MFA is required for all remote connections.

    f. Remote access reviews are conducted regularly.

    g. Hardened endpoints and jump servers are enforced.

    h. Centralized monitoring for remote sessions, including vendors/third parties.

    i. Automated monitoring of remote sessions is integrated into Security Operations Center (SOC) dashboards, proactive notification for anomalous activity, and automated deprovisioning of access or isolation.

    j. Not applicable. The institution does not allow remote access.

22. Which of the following statements describes the institution's network security standards? (Select all that apply)

    a. No network segmentation or zoning (flat network), minimal perimeter defenses, firewall rules are not managed. Devices and network appliances use vendor defaults. An ad hoc baseline configuration exists.

    b. Firewall and network segmentation policies, baseline configurations, and network hardening guidelines are documented and implemented. Perimeter defenses are established and centralized monitoring is performed via log collection from network devices.

    c. Enterprise network is segmented into multiple trust or security zones with risk-based, defense-in-depth strategies to mitigate cyberattacks.

    d. Servers are dedicated to a single service or purpose to prevent functions requiring different security controls from co-existing.

    e. Anti-spoofing controls are in place to detect and prevent spoofed source IP addresses from entering the internal network. Wireless networks use a firewall configured to restrict unauthorized traffic.

    f. Network zones, including virtual instances, are designed and configured to restrict and monitor traffic between trust and untrusted zones.

g. The wireless network broadcast range is within the physical boundaries of the institution.

h. Public-facing servers are routinely rotated and restored to a known clean state or version to limit exposure to potential known threats.

i. Implementation of advanced technologies such as Security Orchestration, Automation, and Response (SOAR), automated configuration management, and compliance scanning, among others.

23. Which of the following statements describes the institution's virtualization standards? (Select all that apply)

a. No formal policy for virtualization exists. Virtual machines (VMs) are deployed on an ad-hoc basis, and security configurations for hypervisors and VMs are not standard.

b. A formal virtualization policy is documented, covering the VM lifecycle (provisioning, patching, decommissioning) and access control.

c. Security baselines and hardening standards are defined and enforced for hypervisors and new VM builds.

d. The hypervisor management interface is secured, and access is tightly restricted and monitored.

e. Network controls (e.g., virtual firewalls) are implemented to inspect and restrict traffic between VMs on the same host (east-west traffic).

f. A repository of hardened "golden images" is maintained for all new VM deployments and is regularly evaluated using the latest security patches and vulnerability bulletins.

g. The virtual environment is managed through automated orchestration tools that enforce security policies throughout the VM lifecycle.

h. Advanced security capabilities are implemented to establish and maintain zero-trust environments.

i. Automated tools continuously scan for and remediate insecure configurations and VM sprawl.

j. Not applicable – please explain.

24. Which of the following statements describes the institution's application security standards? (Select all that apply)

a. Application security requirements are dependent on the business units.

b. Basic secure coding guidelines are available to developers, but their application is either inconsistent or not formally enforced or tested.

c. Policies and procedures exist for all application security requirements, such as access and authentication controls, audit trails and logs, and business/compliance logic controls.

d. Application and business logic security are measured and evaluated through regular conduct of static and dynamic application security testing, vulnerability assessments, and penetration tests.

e. Security testing is risk-based, with more rigorous vulnerability assessments and penetration tests applied to high-risk and internet-facing applications.

f. Identified vulnerabilities are formally tracked, prioritized, remediated, and reported to Management and the appropriate committee.

g. The institution uses static and dynamic security testing tools integrated into the development pipeline (CI/CD) or application development lifecycle to identify or detect security requirements non-compliance and known vulnerabilities before deployment.

h. The institution established a centralized repository for application security policies, processes, and procedures and has established mechanisms to measure security risk and compliance level with security standards of specific applications.

i. Not applicable – please explain.

25. Which of the following statements describes the institution's data security standards? (Select all that apply)

a. Ad hoc data security requirements are followed and are dependent on vendor recommendations/requirements.

b. Data security requirements are defined throughout the data lifecycle (i.e., creation/collection, processing/use, storage, transmission/sharing, archiving, and destruction/disposal).

c. Production and non-production environments require separation to prevent unauthorized access and modification to information assets.

d. Use of customer personal information and production data in non-production is not allowed without masking, cleansing, or removing sensitive data elements consistent with legal and regulatory requirements and industry standards.

e. Controls are defined and implemented to detect and prevent unauthorized access to collaboration tools, devices, applications, or storage, including detection and prevention of exfiltration of confidential data.

f. Structured and unstructured confidential data are protected against unauthorized internal and external access, with continuous monitoring of access and changes based on defined access rights and privileges, regardless of platform or storage location.

26. Which of the following statements BEST describes the institution's data-at-rest security standards?

a. Data-at-rest is stored without encryption or not by default.

b. Encryption requirements are documented but not consistently applied across all systems.

c. The institution has defined and implemented data-at-rest encryption standards aligned with its data classification scheme and applied on a risk-based basis.

d. The institution implements tokenization to substitute unique values for confidential or sensitive information.

27. Which of the following statements describes the institution's database security standards? (Select all that apply)

    a. Database access is controlled using basic user accounts and password-based authentication; however, access permissions are broad, inconsistently applied, and granted based on ad hoc or informal requests.

    b. Database security controls are defined, documented, and implemented to enforce the principle of least privilege, preventing unauthorized data access and use by both standard and privileged users.

    c. Database access and activity for production databases are logged and monitored. Audit logs are reviewed at defined intervals using documented procedures to detect and investigate suspicious or unauthorized access, changes, or queries.

    d. A documented and formal process is implemented for the periodic review and recertification of user access rights, privileges, and permissions, with reviews conducted by designated system or data owners and inappropriate access promptly revoked or adjusted.

    e. Automated, near real-time monitoring of database activity is in place to detect anomalous behavior and trigger predefined response actions.

28. Which of the following statements describes the institution's data-in-transit standards? (Select all that apply)

    a. Encryption requirements are not clearly defined.

    b. Encryption policies are defined for internal and external data transmission.

    c. Data transmission requires encryption when transmitted publicly or to an untrusted or external network.

    d. Confidential data requires encryption when transmitted across private connections and within trusted zones.

    e. The institution implements tokenization to substitute unique values for confidential or sensitive information.

29. Which of the following statements describes the institution's asset removal, transfer, and disposal standards? (Select all that apply)

    a. Asset removal, transfers, or disposal are informal or ad hoc.

    b. Asset removal, transfers, and disposal follow documented procedures and timelines.

    c. Data and assets are destroyed according to the BSI's asset disposal policies and requirements and within a specified period.

    d. Asset removal or transfers are documented and logged.

e. Automated tools are used to track and verify asset disposal, and disposal logs are periodically reviewed.

30. Which of the following statements describes the institution's malware protection standards? (Select all that apply)

    a. Malware protection requirements are informal and not centrally managed.

    b. Malware protection requirements are defined and documented.

    c. Anti-virus/anti-malware is installed on devices, endpoints, and servers prior to deployment.

    d. Mobile devices are centrally managed for anti-virus and patch deployment.

    e. Malware protection is centrally monitored, with automated detection and response for known threats; logs are regularly reviewed; and incidents are tracked and analyzed.

    f. Advanced endpoint detection tools are deployed with behavioral analysis and AI-driven malware detection capabilities.

    g. Endpoint protection is integrated with threat intelligence and real-time response, and is regularly improved based on the results of threat analysis.

31. Which of the following statements describes the institution's encryption standards? (Select all that apply)

    a. Encryption requirements are ad hoc and not yet established.

    b. Encryption policies are established for communication, endpoint, data, and other information assets and are enforced across all systems.

    c. Key management is centralized and reviewed.

    d. Encryption and cryptographic standards are evaluated and updated, considering the evolving threat landscape and industry standards.

32. Which of the following statements describes the institution's security standards relative to systems development and acquisition? (Select all that apply)

    a. Security requirements and considerations for software development or acquisition are ad hoc.

    b. A secure program coding policies, procedures, or standards are established as part of the BSI's software development life cycle (SDLC) process and are benchmarked against globally recognized standards or leading practices.

    c. Access segregation requirements for dev, UAT, and prod environments are defined, and access privileges are periodically reviewed and monitored.

    d. Developed and acquired software and applications are evaluated for baseline security compliance, with comprehensive testing of scenarios and Interdependencies.

    e. Secure development standards require static code analysis to identify vulnerabilities before deployment.

f. A risk-based independent assurance function is in place that evaluates application or software security. Results are reported to Management and appropriate committees.

g. Automated tools are used to scan software code under development to identify vulnerabilities early in the design phase.

h. Independent code reviews are performed for internally developed or acquired software to ensure no known security weaknesses or gaps exist before deployment.

i. Interconnection security is assessed as part of the organization's overall security assessment process.

33. Which of the following statements describes the institution's Change management standards?

    a. Information security requirements are not consistently considered in the change management process, with security reviews being ad hoc, undocumented, or performed only after changes are implemented.

    b. Information security requirements for change management are documented and applied to selected changes, but security risk assessments are inconsistent across systems or teams.

    c. Information security requirements are consistently integrated into the change management lifecycle, with all changes subject to risk-based security assessment, approval, and post-implementation review.

    d. The change management process is fully integrated with information security and risk management, using risk-driven, automated, and continuously improved controls to address emerging threats.

34. Which of the following statements describes the institution's security patch management standards? (Select all that apply)

    a. Information security considerations are not yet embedded in the patch management policies and procedures.

    b. Security patching requirements are defined and documented, with clear prioritization and deployment targets.

    c. Unpatched systems are monitored for security incidents, and compensating controls are reviewed to manage residual risk.

    d. Patch management performance and compliance are tracked and reported to management and relevant committees.

    e. Automated tools are used to deploy security patches and monitor compliance with defined security baselines.

35. Which of the following statements describes the institution's security standards for vendor management and outsourcing? (Select all that apply)

    a. Vendor and service provider due diligence is minimal, and contracts do not consistently include cybersecurity requirements.

b. Vendor management policies are documented, with due diligence performed prior to onboarding and contracts and SLA including minimum cybersecurity requirements.

c. Vendors and service providers are required to comply with the BSIs cybersecurity policies and standards.

d. Vendor and service provider performance and compliance with cybersecurity requirements are regularly monitored. Risk assessments are conducted periodically, and corrective actions are tracked.

e. Vendor risk management is integrated into enterprise risk frameworks. Continuous monitoring tools are used to assess vendor security posture. The institution collaborates with vendors to improve cybersecurity maturity and resilience.

C. Detection

36. Which of the following statements describes the institution's security detection tools? (Select all that apply)

    a. An informal process is in place to monitor basic threats, such as unauthorized devices or software.

    b. Basic detection and prevention controls, such as anti-virus software and firewalls, are deployed to protect systems and networks against common threats.

    c. A formal event detection process is documented and implemented. Normal network and system behavior is baselined to serve as a consistent standard for identifying deviations.

    d. The effectiveness of detection and prevention controls are reviewed periodically.

    e. Security monitoring tools are strategically deployed on critical assets and infrastructure based on risk assessment results.

    f. Network and system logs from various sources are centrally collected, correlated, and enriched with business context to improve detection accuracy.

    g. The institution uses automated, real-time correlation of event data to design predictive analytics.

    h. Analytics are used to anticipate attack activity and detection of threats early.

37. Which of the following statements describes the institution's log management standards? (Select all that apply)

    a. Logs are decentralized and are reviewed only during incident investigation.

    b. Logs from critical systems are centrally collected into a secure repository (e.g., SIEM) where they are protected from unauthorized access or alteration.

    c. Automated tools are used to correlate event information from various sources in near-real time and investigate alerts to identify potential security events.

    d. The institution has a program to create and continuously refine custom detection rules and advanced analytics based on threat intelligence and lessons learned, including proactive threat hunting activities.

38. Which of the following statements describes the institution's layered detection capabilities? (Select all that apply)

    a. Foundational detection layers are in place, including monitoring of the physical environment for unauthorized access and basic network perimeter monitoring (e.g., reviewing firewall logs).

    b. Detection capabilities include network intrusion detection/prevention systems (IDS/IPS). A formal process is documented for reviewing alerts from all established layers (physical, network, and host).

    c. Advanced detection layers are implemented, such as file integrity monitoring (FIM) for critical system files and configuration monitoring for security devices. Real-time alerts are generated for unauthorized changes, access, or hardware.

    d. Alerts from all detection layers (physical, network, host, application) are centrally correlated and analyzed to provide a holistic view of complex security events. The institution employs advanced techniques, such as deception technology (e.g., honeypots), to detect and analyze adversary behavior proactively.

D. Response

39. Which of the following statements describes the institution's technology and cybersecurity incident response plan and procedures? (Select all that apply)

    a. Incident response plan and procedures are not formally established, and incident response actions are ad hoc.

    b. The Institution has documented response plans and procedures to cyber threats (e.g., playbook). A process or facility is available where employees can escalate and report information and cybersecurity incidents.

    c. The BSI incident response plan is integrated with its business continuity and disaster recovery plan.

    d. The response/resilience procedures contain detailed actions, resource requirements, and timing.

    e. Critical business processes are identified and correlated in the incident response/resilience plans, and continuity processes are in place in the institution's business continuity plan.

    f. Business impact analyses include cyberattack scenarios.

    g. The incident response plan is regularly tested to identify gaps and improve the plan.

    h. Lessons learned from cyber incidents experienced by the BSI and other applicable cybersecurity incidents are used to improve the incident response plan.

    i. System logging capabilities and log retention periods are evaluated against applicable laws and regulations to support of forensic and legal investigations.

    j. Automated response mechanisms are implemented to execute predefined actions when security alerts or triggers are generated.

40. Which of the following statements describes the institution's incident analysis and triage assessment standards? (Select all that apply)

    a. Incident triage process and prioritization are not yet established.

    b. Incident analysis and triage policies and procedures are defined and clearly delineate prioritization criteria for handling incidents.

    c. Incident response plan prioritization is risk-based and supports rapid response to significant cyberattacks affecting critical services and resources.

    d. Incident analysis is performed at the initial stages of the intrusion, and incident response metrics are monitored to facilitate continuous improvement.

    e. Lessons learned from incident analysis and triage are used to improve processes, protocols, standards, or guidelines.

41. Which of the following statements describes the institution's impact mitigation and containment standards? (Select all that apply)

    a. Incident impact mitigation and containment measures are ad hoc and not yet defined in existing policies, procedures, and guidelines.

    b. Responsibilities of third-parties on incident impact mitigation and containment measures are and not yet defined in existing policies, procedures, and guidelines.

    c. Incident mitigation and containment policies, procedures, and guidelines cover responsibilities, accountability, documentary, and reportorial requirements for internal and external parties.

    d. Notification requirements are established for affected third parties and business partners.

    e. Third-party incident response service providers are engaged based on defined escalation or severity criteria.

    f. The technology infrastructure is designed to limit disruption to the production environment during a cyberattack.

    g. Processes are in place to evaluate the effectiveness of mitigation and containment on affected assets.

    h. Assets affected by an incident are baselined, evaluated, or tested thoroughly before redeployment.

    i. Investigation and mitigation actions are documented to support continuous improvement.

    j. The performance of third parties, business partners, and internal units in incident containment and mitigation is measured, evaluated, and reported to management and relevant committees.

    k. Threat intelligence and incident data are analyzed in the context of the institution's environment to develop proactive response measures.

    l. Technical tools are used to analyze network traffic, application and system logs, and deep-packet inspections, to timely respond to outgoing or incoming attacks.

m. Containment and mitigation strategies and procedures are designed to manage multiple incidents occurring simultaneously.

42. Which of the following statements describes the testing standard for incident response? (Select all that apply)

    a. Incident response plans or playbook testing is not yet tested.

    b. Incident response plans or playbook testing is ad hoc or not regularly tested.

    c. The incident response plan is periodically tested, and results are used to drive continuous improvement

    d. The incident response plan for third parties or business partners is periodically tested, and results are used to drive continuous improvement

43. Which of the following statements describes the institution's incident response team development? (Select all that apply)

    a. Key technical staff are assigned to respond to incidents on an ad-hoc basis.

    b. Roles are not formally documented, and the response depends on the availability of specific individuals.

    c. A formal incident response team is established, composed of representatives from key business and technical units (e.g., IT, security, legal, communications).

    d. Roles and responsibilities for all team members are clearly defined and documented.

    e. The incident response team participates in regular training and tabletop exercises to maintain and improve their skills.

    f. The team has access to pre-approved resources and third-party specialists (e.g., forensic investigators) to assist during a significant incident.

    g. The team's performance is measured using defined metrics (e.g., Mean Time to Detect, Mean Time to Respond).

    h. Lessons learned from incidents and exercises are formally documented and used to continuously improve response playbooks, tools, and team skills.

44. Which of the following statements describes the institution's crisis communication and notification standards? (Select all that apply)

    a. Communications during an incident are handled reactively and on an ad hoc basis. There are no pre-defined templates, stakeholder contact lists, or protocols.

    b. A formal crisis communication plan and notification protocol are documented. The plan identifies key internal and external stakeholders (e.g., employees, customers, regulators) and defines the criteria and process for notification.

    c. Pre-approved communication templates are developed for various incident scenarios to ensure clear, consistent, and accurate messaging. The communication plan is regularly tested as part of incident response tabletop exercises.

d. The organization uses an automated notification system to rapidly and reliably disseminate information to stakeholders across multiple channels. The effectiveness of communications is reviewed after each incident to continuously refine messaging and delivery methods.

E. Recovery

45. Which of the following statements describes the institution's incident response recovery standards? (Select all that apply)

    a. Incident recovery is reactive and handled on an ad-hoc basis. Formal recovery plans, Recovery Time Objectives (RTOs), and Recovery Point Objectives (RPOs) are not defined or documented yet.

    b. A formal incident recovery plan is documented for critical systems. RTOs and RPOs are defined and approved by management. The plan outlines key roles, responsibilities, and procedures for recovery.

    c. The documented recovery plan is tested on a regular schedule to validate its effectiveness and identify gaps.

    d. Test results are formally documented, and any issues found are tracked until full remediation. Recovery metrics are measured and reported to management.

    e. The recovery process is continuously improved based on test results, lessons learned from incidents, and threat intelligence.

    f. The institution uses advanced testing, such as full-scale simulations, including third-party dependencies, to confirm its ability to meet RTOs/RPOs.

46. Which of the following statements describes the institution's information security standards in business continuity management? (Select all that apply)

    a. No formal information security-related requirements in Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).

    b. BCP/DRP information security requirements are documented and aligned with business as usual (BAU) requirements.

    c. BCP/DRP information security processes/technology are regularly tested and measured through defined metrics and reported to oversight committees.

    d. BCP/DRP continuously updated based on lessons learned, threat intelligence, peer practices, and benchmarking activities against industry standards.

47. Which of the following statements describes the institution's business impact analysis (BIA) /risk assessments (RA)? (Select all that apply)

    a. No formal BIA process in place. Critical functions are dependencies are not identified.

    b. BIA and risk assessment are conducted regularly to determine critical functions, including dependencies and interconnections.

    c. RTOs and RPOs are defined and aligned with business priorities. Third-party dependencies are assessed.

    d. BIA and RA are revisited, considering technology changes, threat intelligence, and reported industry incidents.

48. Which of the following statements describes the institution's communication plan? (Select all that apply)

    a. No formal communications plan, roles and responsibilities relative to communications during the incident response process are not defined, and a stakeholder contact list is not maintained.

    b. A communications plan is documented and outlines key roles and responsibilities. A stakeholder list is maintained.

    c. The communications plan is tested on a regular/consistent basis and updated based on the test results.

    d. The stakeholder list is updated regularly, and communication updates are provided to stakeholders during incidents/test simulations.

    e. Post-incident/test communication reviews are conducted.

    f. The communication plan includes scenario-based communications (e.g., ransomware, supply chain breach, etc.). Stakeholders are updated using automated notification systems.

    g. Communication plan is improved based on test results and lessons learned and post incident communication reviews.

F. Assurance and Testing

49. Which of the following statements describes the institution's information security assurance and testing standards? (Select all that apply)

    a. Assurance and testing plans are not formally established to regularly assess the effectiveness of controls across the prevent, detect, respond, and recover phases.

    b. The organization conducts annual business continuity and disaster recovery plan tests on critical systems, applications, and data.

    c. The formal and comprehensive testing program is defined to include specific cyberattack scenarios, such as ransomware attacks, to validate data recovery capabilities.

    d. Documented Information backups test expectations are regularly verified for completeness, accessibility, and integrity.

    e. Assurance and testing programs involve critical third-party service providers and interconnections.

    f. Identified issues from tests are subjected to root cause analysis, and corrective action plans are integrated to update the plans and formally tracked until their completion.

    g. Tests are comprehensive, involving multiple business units to evaluate the institution's ability to maintain critical operations' resilience during cyber or disruptive events, and results are reported to management and appropriate committees.

    h. Lessons learned from advanced simulations are used to continuously optimize security controls, response playbooks, and overall cyber resilience strategy.

50. What are the cybersecurity test and evaluations conducted to validate the overall effectiveness of the information security program? (Select all that apply)

    a. Self-assessment

    b. Security audit/review and compliance check

    c. Vulnerability assessment (VA)

    d. Penetration testing (PT)

    e. Scenario-based testing

    f. Compromise/breach assessment

    g. Red-teaming exercise

51. Which of the following statements describes the institution's vulnerability assessment and penetration test standards? (Select all that apply)

    a. The institution has yet to define policies and procedures for vulnerability assessment and management, including testing criteria, scope, and frequency.

    b. The institution established formal policies and procedures for vulnerability assessment, management, and monitoring, including criteria for scope and frequency.

    c. Independent vulnerability assessment and penetration tests of internet-facing applications and internal networks are prioritized according to the institution's risk assessment results, and results are reported to Management and the appropriate committee.

    d. Independent penetration tests of network perimeter boundaries and critical customer-facing web applications are regularly performed to evaluate security gaps and mitigations' effectiveness.

    e. Vulnerability assessment and penetration tests of internet-facing applications before they are deployed, when significant changes occur, or whenever a plausible threat intelligence feed is received.

    f. Penetrations threats involve simulation of cyber-attacks (red/blue teaming) to detect control gaps in employee behavior, security environment, resources, and response playbooks.

    g. The institution defined a criterion to change independent VAPT providers and test scope, and complexity regularly.

IV. Cyber Threat Intelligence and Collaboration

52. Which of the following statements describes the institution's situational awareness and threat monitoring standards/practices? (Select all that apply)

    a. The institution has not yet defined policies or procedures regarding threat intelligence gathering and monitoring.

    b. Policies, procedures, and protocols are defined and formalized for collecting threat information and monitoring from the financial sector.

The institution uses a defined cyber intelligence framework to collect and analyze threat information.

c. The institution subscribes to or belongs to a cyber threat and vulnerability-sharing source/s.

d. Received/gathered threat information is analyzed to learn about the tactics, techniques, procedures (TTP), and existing risk mitigation is evaluated and updated, as necessary.

e. A threat intelligence program is implemented and monitored.

f. Threat information is used to monitor threats and vulnerabilities and to strengthen internal risk management and controls.

g. Threat intelligence is gathered automatically and in real-time, using automated tools to correlate threat data to BSI-specific risks, and management is alerted when a defined risk threshold is met.

h. The institution has defined automated ways to report/share threat analysis results to Regulators and other relevant agencies and actively shares in the financial sector's central intelligence repository.

53. Which of the following statements describes the institution's Security Operations Center (SOC)? (Select all that apply)

    a. No SOC. Monitoring is done across different tools/systems, not correlated, and ad hoc.

    b. Security processes and technology are centralized and coordinated in a SOC or equivalent.

    c. Monitoring systems operate continuously with sufficient resources, including comprehensive log ingestion and correlation with threat intelligence, to support effective incident management.

    d. Detection, containment, isolation, and recovery metrics (mean time to detect, mean time to repair/recover, etc.) are measured and monitored.

    e. Artificial Intelligence (AI)/Machine Learning (ML)-driven analytics and automation tools are in place.

54. Which of the following statements describes the institution's governance and risk management practices for artificial intelligence (AI) and machine learning (ML) technologies in relation to cybersecurity? (Select all that apply)

    a. Cybersecurity risks arising from the use of AI or ML technologies have not yet been formally identified or assessed.

    b. AI/ML technologies used within the institution are documented, and associated security and operational risks are considered within existing risk management processes.

    c. Policies and procedures define governance requirements for the development, acquisition, or use of AI/ML solutions, including security, data protection, and model lifecycle management.

d. AI-enabled security tools are subject to validation, testing, and periodic review to ensure reliability and alignment with the institution's risk appetite.

e. Risk assessments consider AI-related threats, including adversarial manipulation, model misuse, or AI-enabled cyberattacks.

f. AI/ML systems are integrated into cybersecurity monitoring and risk management processes with appropriate governance oversight.

g. Governance and control mechanisms for AI/ML technologies are periodically reviewed and enhanced based on emerging risks and industry practices.

h. Not applicable – please explain.

55. Which of the following statements describes the institution's information-sharing and collaboration standards? (Select all that apply)

a. No policy or formal agreement for information sharing and collaboration.

b. No structured monitoring of logs or subscription to cyber threat intelligence (CTI) feeds.

c. Documented policies are in place for information sharing and incident reporting through relevant industry platforms.

d. Designated contact points are formally identified for incident reporting and external coordination.

e. Subscription to CTI feeds provides necessary intelligence to the institution.

f. Proactive participation in sharing information with the financial sector, law enforcement agencies, BSP, and other information-sharing community forums.

g. Enterprise-wide continuous monitoring is implemented across networks, endpoints, cloud, and vendors, supported by a SOC integrated with cyber threat intelligence feeds.

h. Automated and intelligence-driven threat information sharing platforms are implemented to support timely exchange of threat intelligence.

i. Sector-wide collaboration strategy approved and driven by the Board.

j. Proactive situational awareness and threat monitoring are communicated to executives and shared to the industry information sharing platform or forums.

56. Which of the following statements describes the institution's standards for information security continuous improvement? (Select all that apply)

a. No structured improvement process. Incident reviews and lessons learned are not consistently captured.

b. A formal policy for continuous improvement exists in information security strategies and plans covering people, processes, and technologies.

c. Metrics to measure current security posture, target maturity, and identified gaps are monitored and reported to relevant committees.

d. Incident reviews and lessons learned sessions provide inputs to the continuous improvement program.

e. The institution uses benchmarking against peers and industry best practices.

V. Other Relevant Information

57. Following the guidance on the CMF and the maturity tiers/levels, what is your institution's self-assessed maturity level with respect to its Information Security and Cybersecurity risk management?

Domains	Maturity Level	Assessment Rationale
1. Information Security Governance		
2. Information Security Risk Management		
3. Security Control Implementation		
a. Identification		
b. Prevention		
c. Detection		
d. Response		
e. Recovery		
f. Assurance and Testing		
4. Cyber Threat Intelligence and Collaboration		

58. Provide an inventory of information security and cybersecurity related policies and cyber incident response playbooks with the following information:

Document Title	Purpose/Description	Date Created	Last Updated

59. Provide the relevant information on the following IT and cybersecurity risk monitoring indicators:

Area	Description	Indicators / Metrics	Computation
A. IT Governance			
Leadership and key positions turnover	Measures the extent of turnover among key leadership position[1] during the covered period.	% of key leadership positions that were vacated by personnel with at least three (3) years of tenure during the covered period for the following functions: • IT • Cybersecurity	$\frac{\text{No. of key leadership positions with ≥3 years tenure who resigned or separated during the covered period}}{\text{Total no. of approved key leadership positions}} \times 100$ *Note: The computation shall be performed separately for IT and cybersecurity functions.*

[1] Refers to position deemed essential to the effective operation of IT and cybersecurity functions. Example: CISO, SOC Lead, Security Architect, IT Operations Head, among others.

Area	Description	Indicators / Metrics	Computation
	Measures the proportion of key leadership positions that have remained unfilled for an extended period.	% key leadership positions vacant for more than 90 days for the following functions: • IT • IS • Cybersecurity	$\frac{\text{No. of key leadership positions vacant for more than 90 days}}{\text{Total no. of approved key leadership positions}} \times 100$ *Note: The computation shall be performed separately for IT, IS, and cybersecurity functions.*
B. IT Operations Management			
System Availability	Measures the availability of applications supporting the Bank's operations and customer services.	Monthly system availability (%) of the following applications during the covered period: • Core banking system (e.g., CASA, Loans, Tellering, General Ledger) • Treasury • Trust • Remittance • AML • Card Management System • Fraud Management System	$\frac{\text{Total uptime during the month}}{\text{Total scheduled operating time during the month}} \times 100$ *Note: The computation shall be performed separately for each application.*
Change Management	Measures the proportion of critical and high-priority change requests related to critical applications[2] that remain unresolved beyond the approved implementation timeline.	% of critical and high priority[3] change requests related to critical applications that remain unresolved beyond the approved implementation timeline	$\frac{\text{No. of critical and high-priority change requests related to critical applications that remain unresolved beyond the approved implementation timeline}}{\text{Total no. of critical and high-priority change requests related to critical applications}} \times 100$
Incident Management	Measures the proportion of critical and high-priority IT incidents related to critical applications that remain unresolved beyond the approved turnaround time (TAT).	% of critical and high-priority IT incident tickets related to critical applications that are outstanding and beyond the approved turnaround time (TAT)	$\frac{\text{No. of critical and high-priority IT incident tickets related to critical applications that are outstanding and beyond TAT}}{\text{Total no. of critical and high IT incident tickets related to critical applications}} \times 100$
Incident Management (*Service*	Measures the extent to which service disruptions, incidents,	% of critical and high-priority IT incidents attributed to critical	$\frac{\text{No. of critical and high-priority IT incident tickets}}{} \times 100$

[2] **Critical applications** are systems that support critical business functions, where failure, unavailability, or compromise could result in significant operational, financial, regulatory, customer, or reputational impact to the institution. Such identification should be based on the **results of the business impact analysis**.

[3] Critical and high-priority change request, IT incident tickets, or IT problem tickets refer to items or events classified by the BSI as having the highest severity based on their actual or potential impact on critical applications, business operations, customers, regulatory compliance, or information assets.

Area	Description	Indicators / Metrics	Computation
Provider-related)	or security events are attributable to critical third-party service providers.	third-party service provider	caused by critical third-party service provider / Total no. of critical and high IT incident tickets
Problem Management	Measures the proportion of critical and high-priority IT problems related to critical applications that remain unresolved and beyond the approved turnaround time (TAT).	% of critical and high-priority IT problem tickets related to critical applications that are outstanding and beyond the approved turnaround time (TAT)	No. of critical and high-priority IT problem tickets related to critical applications that are outstanding and beyond TAT / Total no. of critical and high-priority IT problem tickets related to critical applications x 100
IT Asset Management	Measures the proportion of critical IT assets[4] that have reached end-of-life, end-of-support, or obsolescence status.	% of critical obsolete IT assets	No. of critical obsolete IT assets / Total no. of critical IT assets x 100
Vendor Management / Outsourcing	Measures the proportion of critical third-party service providers that meet their contractual service level commitments.	% of critical third-party service providers meeting service level agreement (SLA) requirements	No. of critical third-party service providers meeting agreed SLA targets / Total no. of critical third-party service providers x 100
C. Information and Cybersecurity Management			
Privileged Access Management	Measures the extent to which privileged accounts are protected through multi-factor authentication and credential vaulting.	% of privileged accounts protected by multi-factor authentication (MFA) and vaulting[5]	No. of privileged accounts with MFA and vaulting / Total no. of privileged accounts (Admin, Root Access, etc.) x 100
Patch Management	Measures the proportion of critical servers that have not been patched within the approved remediation timeline.	% of unpatched critical servers	No. of unpatched critical servers / Total no. of critical servers x 100
Endpoint Security	Measures the extent to which critical servers are protected by host-based intrusion detection and malware protection solutions.	% of critical servers (internal / internet facing) with Host-based Intrusion Detection System (IDS) and Malware Protection Solutions	No. of critical servers (internal / internet facing) with Host-based IDS and Malware Protection Solutions / Total no. of critical servers x 100
D. Development and Acquisition			
Project Timeline	Measures the proportion of critical or major[6] IT and cybersecurity projects that experienced	% of critical or major projects with delayed timeline and adverse impact in the following areas:	No. of critical or major projects with delayed timeline

[4] Critical IT assets = Servers, Hardware, Applications and other devices supporting critical functions
[5] Vaulting refers to the process of securely storing privileged accounts in a centralized, encrypted repository known as vault.
[6] Critical or major projects refer to high-priority initiatives with significant strategic, operational, regulatory or risk management implications for the Bank.

Area	Description	Indicators / Metrics	Computation
	delays against committed timelines and resulted in adverse[7] impacts to operations, regulatory commitments, or business objectives.	• IT • Cybersecurity	No. of projects with delays and adverse impact[8] / Total no. of critical or major projects x 100 *Note: The computation shall be performed **separately** for IT and cybersecurity.*
E. Technology Recovery and Resilience			
Disaster Recovery (DR) Environment	Measures the extent to which critical applications and security tools are supported by a functioning disaster recovery environment capable of supporting recovery operations.	% of critical applications and security tools covered by a functioning DR environment	No. of critical applications and security tools with a functioning DR environment / Total no. of critical applications and security tools x 100
Disaster Recovery Testing	Measures the extent to which critical applications have undergone disaster recovery testing to validate recovery capabilities	% of critical applications tested within the last 12 months	No. of critical applications tested for disaster recovery within the last 12 months / Total no. of critical applications x 100
Disaster Recovery Testing Effectiveness	Measures the extent to which critical applications successfully met recovery requirements during disaster recovery testing.	% of critical applications that successfully passed DR testing within the last 12 months	No. of critical applications that successfully passed disaster recovery testing within the last 12 months / Total no. of critical applications tested x 100
F. Electronic Payment and Financial Services			
Fraud Management	Measures the effectiveness of fraud management system in detecting and preventing fraudulent activities.	Monthly % of fraud **attempts or incidents** detected and prevented by the fraud management system during the covered period	No. of fraud incidents detected and prevented / Total no. of fraud attempts x 100

60. How many IS-related major projects have been approved in the last 2 years? (Please indicate the number of planned projects)

61. How many IS-related major projects have been completed/implemented in the last 2 years? (Please indicate the number of projects completed)

62. To whom does the Chief Information Security Officer (CISO) or equivalent report: (Select one)
    a. Board of Directors
    b. President
    c. Chief Risk Officer or Risk Management
    d. IT Head
    e. Others (please specify)

[7] Adverse impact is present if the delays resulted to significant operational disruption, financial impact or loss, regulatory concerns, security risks, or failure to meet critical business objectives.
[8] Projects that underwent approved timeline re-baselining shall not be excluded from the computation if the project experienced schedule slippage relative to the originally approved timeline and such delay resulted in an adverse impact.

63. Kindly list the security tests, assessments and/or independent review conducted for the year and corresponding results

Type of Test	Date Conducted	Results (i.e. Strong, Acceptable or Weak)*
Independent vulnerability assessment and penetration testing		
Security audits/reviews		
Compliance checks		
Scenario-based testing		
Compromise/breach assessment		
Red team tests		
Cyber Maturity Assessments		
Others, please specify		

* *You may indicate actual rating used as specified in your reporting standard.*

64. What are the top five IT and cybersecurity risks identified in the latest risk assessment exercise?
    a.
    b.
    c.
    d.
    e.

65. How many vulnerabilities were detected in the previous year? Please indicate the severity of vulnerabilities identified with the corresponding remediation timeline.

Severity	Status of Remediation			
	No Action/ Deferred	Not Started	Ongoing	Completed
High				
Moderate				
Low				

66. When was the last update to the information security awareness training program? (ddMMMyyy)

67. Do you have a corresponding process for enhanced screening procedures, as well as periodic monitoring and evaluation of employees holding critical and/or sensitive functions?

68. What are the top five (5) primary challenges encountered in retaining personnel occupying key IT and cybersecurity leadership positions?
    a.
    b.
    c.
    d.
    e.

69. Are there unpatched information assets in your environment?
    a. If yes, kindly provide statistics on unpatched information assets.
    b. None

70. Which of the following are currently outsourced? (Select all that apply)
    a. Security operations center

b. Vulnerability assessment
c. Application security testing (SAST, DAST, and other procedures not mentioned)
d. Network monitoring
e. Fraud management
f. Data center operations
g. Incident response
h. IT Service Desk
i. Others: (Please specify)
j. None

71. List down the security solutions/tools that the institution is planning to implement in the next 12 months.

Security Tool and brief description	Target date of implementation

72. Based on your recent assessment, what is the average time to detect potential malware, threats and or attacks?
    a. Real-time
    b. 1-3 days
    c. 4-10 days
    d. More than 10 days
    e. We don't measure/monitor.

73. Relative to the question above, is it within the target detection timeline?
    a. Yes
    b. No

74. When was the Institution's incident response plan last tested? ddMMMyyyy

75. Which of the following cybersecurity threats are you most concerned about? Rank from 1 to 10, 1 is the highest concern.

Cyber Threat	Rank (1-10)
Advanced Persistent Threats (APT)	
API Exploit	
ATM Jackpotting	
Business Email Compromise	
Business Logic Exploit	
Card Not Present Fraud	
Data Leakage/Breach	
DoS/DDoS	
Identity Theft	
Insider Threat	
Malware	
Ransomware	
Social Engineering (phishing/vishing/smishing/etc.)	
Supply Chain Attack	
Web Application Targeting	
Others - please specify	

76. Please identify the capabilities and services available in your SOC.

Capabilities	Description	No, Partial, Yes
SIEM Integration	The automation & orchestration tool receives events from the SIEM system	
Threat intelligence integration	Contextualize potential incidents using threat intelligence	
Asset management integration	Contextualize potential incidents using asset information	
User management integration	Contextualize potential incidents using user information	
Vulnerability management integration	Contextualize potential incidents using vulnerability management information	
Historical event matching	Contextualize potential incidents using similar historical events	
Knowledge base integration	Automatically update the knowledge base using event information	
Risk-based event prioritization	Risk-based prioritization of security events using contextualized information	
Firewall integration	Automated remediation by blocking attackers on the firewall	
IDPS integration	Automated remediation by blocking attackers in the network	
Email protection integration	Automated remediation by blocking email senders	
Malware protection integration	Automated remediation by quarantining malware and scanning endpoints for malware threats	
Sandbox integration	Automated delivery of malware samples to sandbox environments for extensive analysis	
Active Directory / IAM integration	Automated locking and suspension of user accounts or revocation of access rights based on event outcome	
Granular access control	Allows to apply the principle of least privilege to configuration of user accounts	
Controlled and monitored maintenance / support Security automation and response (SOAR)	Only trusted tools used for maintenance, remote maintenance / support monitored and controlled Integrates security tools and automates incident response workflows.	

77. Kindly provide/share your institution's IT and cybersecurity-related budget in the table below:

    For consistency, the following guidelines shall apply:
    a. Enterprise-wide budget covers the whole institution, which is distinct and separate from its parent and subsidiaries;
    b. IT budget covers all projects and initiatives pertaining to applications, systems, IT infrastructure, and the IT department; and
    c. The budget for multi-phase projects or capital expenditures may be spread over the applicable years, consistent with how it is accounted for by the institution.

BUDGET (PHP)	2026	2025	2024	Remarks
TOTAL ENTERPRISE-WIDE BUDGET				
CAPEX				
OPEX				

Others				
TOTAL ENTERPRISE-WIDE BUDGET (calculated)				
TOTAL IT BUDGET (PHP)				
CAPEX				
OPEX				
Others				
TOTAL IT BUDGET (calculated)				
BREAKDOWN OF IT BUDGET (PHP)				
Core Systems and Applications[9]				
Infrastructure and Operations[10]				
Cybersecurity Operations [11]				
Staff and Compensation[12]				
Training and Development[13]				
Cloud Services[14]				
Outsourcing and Managed Services[15]				
Others, pls. specify[16]				
ACTUAL IT EXPENDITURE (PHP)				
Core Systems and Applications	[redacted]			
Infrastructure and Operations				
Cybersecurity Operations				
Staff and Compensation				
Training and Development				
Cloud Services				
Outsourcing and Managed Services				
Others, pls. specify				
TOTAL ACTUAL IT EXPENDITURE (calculated)				

CYBERSECURITY BUDGET (PHP)	2026	2025	2024	Remarks
TOTAL CYBERSECURITY BUDGET				
CAPEX				
OPEX				
Others				
TOTAL CYBERSECURITY BUDGET (calculated)				
BREAKDOWN OF CYBERSECURITY BUDGET				
Security Tools (SIEM, IDS/IPS, IAM, EDR, DLP, etc.)[17]				
Vulnerability Mgt., PenTest and Cyber Testing[18]				
Security Operations Center (SOC)[19]				
Staff and Compensation[20]				
Training and Development[21]				

[9] Development, enhancement, maintenance, and support of core business systems and applications
[10] IT infrastructure, operations, and technology tools used to support day-to-day IT services, including security tools managed by the IT function
[11] Cybersecurity-related activities performed and managed by IT function as part of operating technology infrastructure and services
[12] Salaries, benefits, and other personnel-related costs of IT personnel
[13] Training, certifications, and professional development activities for IT and cybersecurity personnel
[14] Cloud-based infrastructure, platforms, software, and related services.
[15] Third-party IT service providers, managed services, and outsourced technology functions
[16] Other IT-related activities not otherwise classified under the identified categories
[17] Cybersecurity tools and technologies managed by the cybersecurity /information security function
[18] Vulnerability assessments, penetration testing, red teaming, cyber exercises, and related security testing activities.
[19] Security monitoring, threat detection, incident analysis, and SOC operations
[20] Salaries, benefits, and other personnel-related costs of cybersecurity personnel
[21] Cybersecurity training, certifications, awareness programs, and professional development activities of cybersecurity personnel

Cloud Services[22]				
Outsourcing and Managed Services[23]				
Compliance and Risk Management[24]				
Others, pls. specify[25]				
ACTUAL CYBERSECURITY EXPENDITURES				
Security Tools (SIEM, IDS/IPS, IAM, EDR, DLP, etc.)				
Vulnerability Mgt., PenTest and Cyber Testing				
Security Operations Center (SOC)				
Staff and Compensation				
Training and Development				
Cloud Services				
Outsourcing and Managed Services				
Compliance and Risk Management				
Others, pls. specify				
TOTAL ACTUAL CYBERSECURITY EXPENDITURE (PHP)				

78. Is the cybersecurity budget included in the Total IT Budget? Yes / No

79. For BSIs using APIs, please check appropriate responses to the following control areas:

(Regardless of the number of APIs and systems that use APIs, please indicate whether such controls are utilized for connections to internal and external systems. A specific control may be marked as both "used" and "not used" if the control is not implemented consistently across all APIs.)

Control Area	Security Control	Used		Not Used		Remarks
		Internal	External	Internal	External	
Authentication & Authorization	Strong authentication (OAuth 2.0, OIDC) enforced					
	Access tokens validated securely					
	Role-based access control (RBAC/ABAC) implemented					
	No use of shared or hardcoded credentials					
API Gateway & Traffic Management	API gateway in place for all external APIs					
	Rate limiting / throttling configured					
	IP whitelisting/blacklisting enforced where applicable					
Input Validation & Data Protection	Input validation to prevent injection attacks					
	Output encoding to avoid data leakage					
	Sensitive data masked or encrypted in transit					
	TLS 1.2+ enforced for all API communications					

[22] Cloud-based infrastructure, platforms, software, and related services.
[23] Third-party cybersecurity service providers and managed security services
[24] Cybersecurity governance, risk management, compliance, control assessments, and audit-related activities
[25] Other cybersecurity activities not otherwise classified under the identified categories

Logging & Monitoring	Centralized logging of all API calls					
	Alerts for abnormal or high-risk activities					
	API logs protected from tampering					
Threat & Vulnerability Management	Regular API security testing (SAST/DAST/API pentesting)					
	Security patches applied promptly					
	Known vulnerabilities documented and tracked					
API Design & Lifecycle Security	APIs use secure design principles (least privilege, fail secure)					
	Deprecated APIs removed or properly versioned					
	Documentation updated and access controlled					
Third-Party & Internal Integrations	Security due diligence for third-party APIs					
	Contracts include security and compliance requirements					
	External API keys stored securely (vault, HSM)					
Incident Response & Recovery	API-specific incident response procedures established					
	Automated containment measures for API abuse					
	Backup and recovery procedures tested					

80. For BSIs with Advanced EPFS, please check features and functionalities available in your Fraud Management System:

_____a. Geolocation blocking
_____b. Velocity checks
_____c. Blacklist screening
_____d. Behavioral anomalies
_____e. Mobile and account change tracking

81. For BSIs with mobile applications, please check security controls implemented:

_____ a. 24-hour Transaction Pause Period
_____ b. Blocking app installs on unsecured or jailbroken devices
_____ c. Prohibition of unauthorized scripts and automation tools
_____ d. Authentication and integrity checks
_____ e. Device fingerprinting
_____ f. Restricting interceptable authentication, (i.e. OTPs via SMS and email)
_____ g. Biometric authentication
_____ h. Behavioral biometrics
_____ i. Passwordless authentication (FIDO)
_____ j. Adaptive authentication
_____k. Descriptive customer notification/alerts
_____ l. Killswitch facility
_____ m. Customer-managed permissions
_____ n. Money lock feature

_____ o. Customizable transaction limits
_____ p. Transaction and audit logs enabled

82. Indicate the data center tier (as guided by the Uptime Institute Tier Classification System) of current production environment of core systems, and, where applicable, of any datacenter provided by third-party or cloud service providers:

    a. **Tier 1 (Basic Capacity)**: A Tier 1 data center provides basic infrastructure to support IT systems with a single path for power and cooling and no redundant components. Planned or unplanned maintenance may require shutdown of IT operations.
    b. **Tier 2 (Redundant Capacity Components)**: A Tier 2 data center includes redundant capacity components (e.g., UPS, cooling equipment) but still has a single distribution path for power and cooling. Maintenance activities may still require service interruptions.
    c. **Tier 3 (Concurrently Maintainable)**: A Tier 3 data center is designed to allow maintenance of power and cooling components without shutting down IT operations. It has multiple distribution paths, with only one active at a time, and includes redundant components to support continuous operations.
    d. **Tier 4 (Fault Tolerant)**: A Tier 4 data center is designed to be fault tolerant, meaning it can sustain operations even if a component fails. It has multiple active power and cooling distribution paths and redundant capacity components to prevent service interruption from single failures.

83. Select recovery strategies implemented:
    a. Fully Equipped and Mirrored Environment (Hot site)
    b. Synchronous replication: ensures zero data loss, ideal for critical data, but can impact performance.
    c. Asynchronous replication: offers better performance but with minimal data loss.
    d. Automated Failover Mechanisms
    e. Automated failover systems automatically redirect user traffic and workloads to the secondary site when the primary site fails, providing near-instantaneous and seamless transition.
    f. Cloud Backup
    g. Warm Site
    h. Cold Site

84. Does your institution maintain cyber insurance as part of its cyber risk management strategy? If yes, please provide the following details:
    a. Insurer,
    b. Coverage amount, and
    c. Policy scope and covered cyber incidents

VI. Required attachments

(Provide information and the latest available reports as of the CCSA cut-off period.)

1. IT, Information Security, and Security Operations, organizational chart
2. Information security and cybersecurity KRI Monitoring Report
3. Latest vulnerability assessment and penetration testing report for Electronic Payment and Financial Services (EPFS) applications, systems, and infrastructure.
4. Maturity assessment report, if any.
5. Red team/purple team report, if any.
6. Monitoring report for outstanding audit issues on Information Security and Cybersecurity, with date issue raised and resolution timeline.
7. Monitoring report for outstanding vulnerabilities involving critical applications, systems, and infrastructure, with date issue raised and resolution timeline.
8. Aging report of outstanding vulnerabilities per criticality/severity

9. Cyber incident statistics for the previous year showing incident classification, severity count of incidents, and total amount involved, as available.

------ Nothing Follows -------