



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

CIRCULAR NO. 1232 Series of 2026

Subject : **Cybersecurity Maturity Framework (CMF) and the Cybersecurity Controls Self-Assessment (CCSA) Requirement**

The Monetary Board, in its Resolution No. 269 dated 31 March 2026, approved the amendments to Section 148 and Appendix 7 of the Manual of Regulations for Banks (MORB), Sections 147-Q/145-S/126-N and Appendices Q-3, S-2, and N-1 of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI), to strengthen information and cybersecurity off-site surveillance and risk assessment activities. These amendments are designed to reinforce the existing regulatory framework and enhance the cyber resilience of the banking and financial sector.

Section 1. Section 148 of the MORB and Sections 147-Q/145-S/126-N of the MORNBFI (Information Technology Risk Management) as amended by Circular No. 1213 dated 30 May 2025, are hereby further amended to replace the IT Rating System with the Supervisory Assessment Framework (SAFr) used in assessing BSFIs and to incorporate the Cybersecurity Maturity Framework and Cybersecurity Control Self-Assessment (CCSA), and shall now read as follows:

148/147-Q/145-S/126-N. INFORMATION TECHNOLOGY RISK MANAGEMENT

xxx

IT Profile Classification. xxx

xxx

xxx. All BSFIs are required to have periodic and rigorous self-assessment exercises using more robust data sets and variables as part of their information security risk management system.

Bangko Sentral Cybersecurity Maturity Framework (CMF). The Bangko Sentral establishes the **Cybersecurity Maturity Framework (CMF)** to support BSFIs in strengthening both institutional and sector-wide cyber resilience in light of increasing digitalization and the evolving threat landscape. Aligned with global standards, the CMF provides a structured approach for assessing and enhancing cybersecurity practices and capabilities across key control areas.

Cybersecurity is a critical component of the broader Information Security Risk Management (ISRM) framework, which focuses specifically on protecting digital systems, networks, and data from cyber threats.

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

The Bangko Sentral shall evaluate the BSFI's cybersecurity maturity based on the CCSA and other supervisory activities, and assess the results according to the following maturity levels or tiers:

Tiers/Levels	Brief Description
Foundational	The BSFI demonstrates minimal adoption of control requirements. Information security and cybersecurity risk assessments are ad hoc, inconsistently performed, or not yet integrated into business decisions. Governance structures are informal, and information security and cybersecurity priorities do not reflect the BSFI's risk appetite. The BSFI lacks awareness of its role in the financial ecosystem and does not routinely participate and collaborate in cyber information sharing activities.
Established	The BSFI establishes policies and procedures or guidelines appropriate to its IT risk profile and approved by the Board or relevant committee. Information security and cybersecurity controls address identified risks and provide baseline protection for customer information, systems, and operations. While implementation covers key business functions, integration is not yet fully consistent across all business units, strategic decisions, and third-party engagements. Information security and cybersecurity priorities are guided by the BSFI's risk appetite, risk environment, and business objectives. The BSFI recognizes its role in the financial ecosystem and participates in information-sharing forums but may not consistently share information with other participants.
Managed	The BSFI demonstrates full adoption of relevant applicable requirements and conducts regular assessments of control effectiveness. Information security and cybersecurity considerations are consistently integrated across the business units, and critical risk management processes are mostly automated and subject to continuous improvement. Senior Management systematically incorporates information security and cybersecurity risks in decision making. Information security and cybersecurity priorities are reassessed when there are changes in business objectives, threats, or the technology landscape. The BSFI actively collaborates with sector participants and routinely shares relevant information within the financial ecosystem.
Optimized	The BSFI fully adopts requirements and continuously enhances its risk management framework using lessons learned and a comprehensive set of leading, lagging, and predictive risk indicators. Advanced security tools, technologies, and adaptive capabilities are used to proactively identify and respond to emerging threats. Information security and cybersecurity risks are fully embedded in strategic planning and enterprise decision-making, with the Board and Senior Management overseeing cyber risks alongside financial and other organizational risks. The BSFI demonstrates mature financial ecosystem awareness and contributes thought leadership to information-sharing communities. The BSFI maintains a robust threat intelligence capability and proactively shares actionable intelligence with relevant domestic and international stakeholders.

Consistent with a risk-based approach to controls implementation, BSFIs are expected to achieve the maturity tiers in line with their risk profile, as outlined below. BSFIs are encouraged to continuously enhance their cybersecurity capabilities and implement more advanced controls.

IT Profile Classification	Cyber Maturity Tiers/Levels
Simple	Foundational to Established
Moderate	Established to Managed
Complex	Managed to Optimized

Definition of Terms. xxx

xxx

Reporting and notification standards. xxx

a. Reporting requirement. Xxx

- (1) Periodic Reports. BSFIs shall electronically submit the following reports, as listed in *Appendix 7/Q-3/S-2/N-1*, to the appropriate supervising department of the Bangko Sentral:
 - (i) Annual IT Profile – within twenty-five (25) calendar days after the end of reference year.
 - (ii) Cybersecurity Control Self-Assessment (CCSA) – on or before the 31 March following the end of the reference year, for BSFIs notified by the Bangko Sentral as having a moderate and complex IT Profile and other BSFIs specifically identified by the Bangko Sentral.

Section 2. Appendix 7 of the MORB, as amended, on the Reports Required of Banks, and Appendices Q-3/S-2/N-1 of the MORNBF, as amended, on the List of Reports Required of Quasi-Banks/NSSLAs/NBFIs, are further amended as shown in **Annex A** of this Circular to reflect the submission of the cybersecurity control self-assessment.

Section 3. Reporting Guidelines. Detailed procedures and guidelines on the submission of the CCSA through the Advanced SupTech Engine for Risk-based Compliance (ASTERisC*) platform, as well as the maturity assessment, shall be covered in a separate regulatory issuance.

To prepare and familiarize BSFIs with the new requirement, the submission of the initial CCSA shall be due sixty (60) calendar days from the release of the reporting guidelines.¹

Section 4. Effectivity Clause. This circular shall take effect fifteen (15) calendar days following its publication in any newspaper of general circulation.

FOR THE MONETARY BOARD:



ELI M. REMOLONA, JR.
Governor

27 April 2026

¹ To be incorporated as a footnote to Appendix 7 of the MORB/Appendices Q-3, S-2, and N-1 of the MORNBF in relation to the Cybersecurity Control Self-Assessment

a. Appendix 7 of the MORB (REPORTS REQUIRED OF BANKS)

UBs/KBs/ Digital Bank/TBs/RBs/					
Form No.	MOR Ref.	Report Title	Frequency	Submission Deadline	Submission Procedure/e-mail Address
xxx	xxx	xxx	xxx	xxx	xxx
	Section 148	Cybersecurity Control Self-Assessment	Annually	31st of March after end of reference year	Via ASTERisC*
xxx	xxx	xxx	xxx	xxx	xxx

b. Appendix Q-3/S-2/N-1 of the MORNBFi (LIST OF REPORTS REQUIRED OF QUASI-BANKS/NSSLAs/NBFIs)

Category	Form No.	MOR Ref.	Report Title	Frequency	Submission Deadline	Submission Procedure/e-mail address
xxx	xxx	xxx	xxx	xxx	xxx	xxx
	Unnumbered	Section 147-Q/145-S/126-N	Cybersecurity Control Self-Assessment	Annually	31st of March after end of reference year	Via ASTERisC*
xxx	xxx	xxx	xxx	xxx	xxx	xxx