STANDARD SUMMARY · CERT.GT

SIB regulations on technology risk

Version 1.0 · Reviewed Oct 11, 2026 · TLP:CLEAR · For: Banks, sociedades financieras (finance companies) and other supervised institutions, and their technology providers.

The Junta Monetaria (Monetary Board) issued the Reglamento para la Administración del Riesgo Tecnológico (Regulation for Technology Risk Management, Resolution JM-102-2011), which the Superintendencia de Bancos (SIB, the banking regulator) supervises. It sets out the minimum that financial institutions must do to manage the risks of their technology. In 2021 it was amended (Resolution JM-104-2021) to incorporate cybersecurity.

Who it applies to

- To the institutions supervised by the Superintendencia de Bancos that the regulation lists, among them banks and sociedades financieras.
- Indirectly, to their providers: the institution remains responsible for the technology services it contracts.

What it asks for, in general terms

Organization	Defined responsibilities for the board of directors, the risk management committee and the risk management unit.
Policies and manual	Policies and procedures approved by the board and brought together in a technology risk management manual.
Infrastructure and systems	Inventory, planning and management of the IT infrastructure, the information systems and the databases.
IT security	Information security management: access, classification, logs, backups and physical security.
Cybersecurity	Since the 2021 amendment: specific functions and people in charge, monitoring, and the capacity to respond to cyber incidents.
Continuity	IT operations continuity plan, alternate site and periodic tests.
Third-party services	Conditions for contracting services and for processing information outside the premises or outside the country.

How to prepare for a review

- Keep the current manual at hand, with the date of board approval.
- Keep evidence that the controls operate: logs, committee minutes, test results.
- Document the tests of the continuity plan and what was corrected afterwards.
- Keep the inventory of technology providers and their contracts up to date.
- Record incidents, their analysis and the actions taken.

How it relates to other frameworks

- ISO 27001 covers a good part of what the regulation asks for in IT security and provides the structure of the management system.
- NIST CSF is useful for organizing the cybersecurity capabilities that the amendment incorporated.
- PCI DSS also applies to institutions that issue or process cards.

Disclaimer

- This is a summary for guidance and does not cite articles. The exact obligations, deadlines and institutions covered are in the text of the resolutions.
- Check whether there have been amendments after the review date of this document.
- For compliance decisions, consult your legal department or the SIB directly.

Official text

Resolutions JM-102-2011 and JM-104-2021 of the Junta Monetaria. Always check the text currently in force at sib.gob.gt.

cert.gt is a private, community-driven initiative of Devel Group.

cert.gt · devel.group · Report an incident at cert.gt/en/reportar or email incidentes@cert.gt

Summary prepared by cert.gt for educational purposes; it is not the official text of the standard and does not replace legal or compliance advice. This is not a document from a government entity. You may copy and adapt it with attribution (CC BY 4.0).