



For banks and financial institutions

CMF publishes regulation on Information Security Management and Cybersecurity

- *The regulation, which will come into force on December 1, 2020, establishes guidelines and best practices to be followed by entities in the management of information security and cybersecurity.*
- *Among them is the responsibility that Boards of Directors will have in approving cybersecurity strategies for their institutions.*

July 7, 2020 – After the conclusion of a public consultation process, the Financial Market Commission (CMF) published a regulation on Information Security Management and Cybersecurity. It will apply to Banks, Banking Subsidiaries, Support Companies of Banking Activities, and Issuers and Operators of Payment Cards.

Financial institutions have increasingly migrated to the digital realm. Although this situation offers several opportunities for supervised institutions and their customers, it also implies greater operational risks that must be properly managed to achieve a balance between the use of information technology and the control of underlying risks. To contribute to this objective, said regulation establishes a series of guidelines and best practices to be considered by entities in their information security and cybersecurity management process.

The Commission expects that this regulation will be a reference framework for future changes in this area for other institutions, such as savings and credit cooperatives and entities operating in the securities and insurance markets.

The new [Chapter 20-10 of the Updated Compilation of Rules for Banks](#) (RAN, for its Spanish acronym) contains several provisions based on the best international practices that should be considered for information security management and cybersecurity. The adoption of this new regulation will allow entities to be better prepared to prevent and respond to operational events related to information security and cybersecurity.

The main elements addressed by the new regulations are summarized below:

- Specific guidelines are given regarding the role that Boards of Directors should have for an adequate management of both information security and cybersecurity, giving them the responsibility of approving institutional strategies in this field. In addition, the Boards shall ensure that the entity maintains an information security management and cybersecurity system that provides for specific management of these risks in consideration of existing international best practices, among other aspects.
- Banks and financial institutions to which these provisions apply shall define the minimum stages of an information security and cybersecurity risk management process. Said process must consider at least the identification, analysis, evaluation, treatment, and acceptance of the risks to which information assets are exposed, as well as their monitoring and ongoing review.
- It establishes the need for entities to define their critical assets, as well as their protection functions, detection of threats and vulnerabilities, response to incidents, and recovery of the entity's normal operation.
- Entities must also have policies and procedures for the identification of assets that make up the critical infrastructure of the financial industry and the payment system, and for the appropriate exchange of technical information on incidents that affect or could affect the entity's cybersecurity.

This new Chapter of the RAN complements the provisions of various CMF regulations, such as those set out in Chapter 1-13 on operational risk management assessment; Chapter 20-7 on the risks that entities assume in outsourcing services; Chapter 20-8 on operational incident reporting; and Chapter 20-9 on business continuity management.

The regulation will come into force on December 1, 2020. Until then, banks must continue to comply with the provisions of the current Chapter 1-13 in the area of operational risk and regarding information security and cybersecurity, including the provisions of Annex No. 3.

Along with the details of the [regulation](#), the Commission makes available to interested parties [a Presentation and a Frequently Asked Questions document](#) that summarize the scope of the regulatory amendment.

Area of Communications, Education, and Image – Financial Market Commission (CMF)

Contact: prensa@cmfchile.cl | [Press Room](#)

[@CMFChile](#)

[@CMF Educa](#)

[@CMF HEsenciales](#)

[CMF on LinkedIn](#)