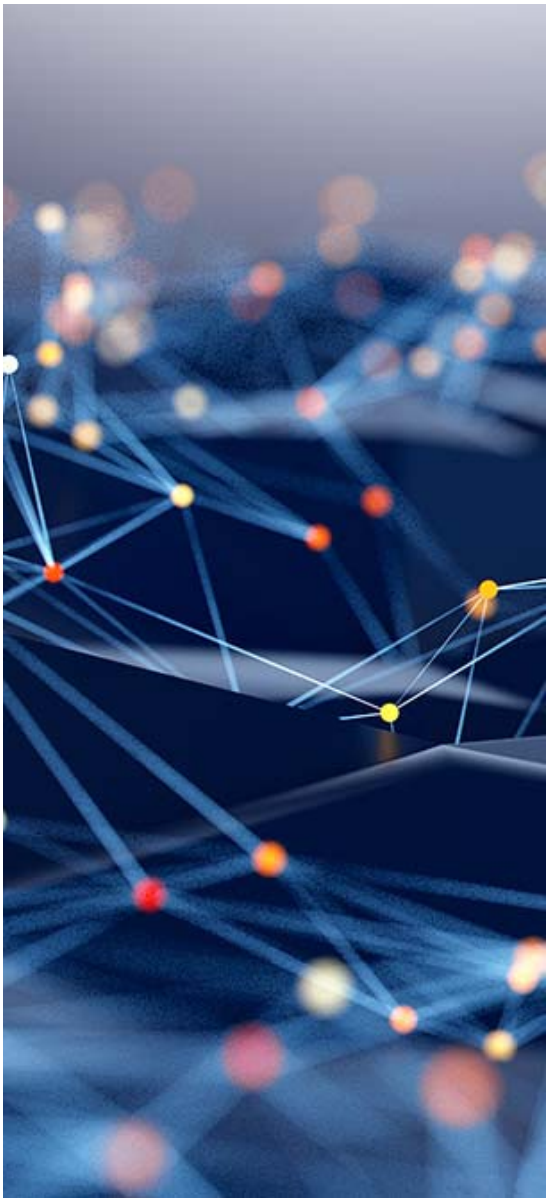
CUATRECASAS

ASF regulatory standard on ICT security and governance

ASF Regulatory Standard 6/2022-R of June 30

Legal flash – Banking, Finance and Capital Markets
June 30, 2022



Key aspects

- Establishes general requirements and principles on the security and governance of information and communications technology, including cybersecurity
- Establishes specific requirements on outsourcing to cloud computing service providers by insurance and reinsurance companies on an individual and group basis

ASF Regulatory Standard 6/2022-R – ICT security and governance, and outsourcing to cloud computing service providers

Published in the Official Gazette of the Republic of Portugal on June 30, Regulatory Standard 6/2022-R of June 30 of the Portugueses Insurance and Pension Funds Supervisory Authority ("**ASF**") regulates the security and governance of information and communications technology ("**ICT**"), as well as outsourcing to cloud computing service providers.

The main changes are summarized below.

Scope of application

The new regulatory standard applies to:

- insurance and reinsurance companies with their head office in Portugal;
- branch offices of foreign insurance and reinsurance companies operating in Portugal;
- insurance and reinsurance groups, when the ASF is the group supervisor; and
- sub-groups, when the head insurance or reinsurance parent company, head insurance holding company or head domestic mixed financial company is subject to group supervision by the ASF.

ICT governance system and data security

- Under the new standard, the board of directors is responsible for establishing an **effective system for managing ICT and security risks** as part of the insurance or reinsurance company's overall risk management system. This system must enable companies to identify the risks and assess the requirements for protecting business processes and activities, business functions, tasks, and assets, including information and ICT assets, considering any known vulnerabilities and previous incidents.

- The new standard defines the need for an **ICT strategy**.

- It also establishes the obligation for **periodic auditing** of company systems and processes for risks associated with ICT and security and the responsibilities and characteristics of the **information security function**, which must be independent and objective.

- Insurance and reinsurance companies must approve an **information security policy** that includes rules to protect the confidentiality, integrity and availability of information.

- It regulates the duty to create processes for **monitoring activities** that affect information security—imposing the duty to carry out information reviews, assessments and security tests to identity vulnerabilities—and the relevant systems and services. It also establishes the duty to document and implement logical and physical **security measures**.

- The new standard also raises awareness of the duty to provide training in this area.

- In ICT operations management, companies must (i) document how they operate; (ii) tailor the frequency of safety backups to the risk assessment carried out; (iii) test security and recovery procedures regularly; (iv) ensure the data is stored in one or more locations; (v) implement a problem and incident management process; and (vi) approve an **ICT continuity policy** that includes a **business impact analysis** and the relevant **response and recovery plans** as part of the company's overall business continuity management policy.

Outsourcing to cloud computing service providers

- Before entering into any agreements with cloud computing service providers, companies must assess whether a **core** or important **function or activity** is involved and carry out a **comprehensive risk assessment**.

- When the outsourced services are related to core or important functions, companies must establish **specific information security requirements**, monitor compliance with these requirements, and have an **exit strategy** that ensures the possibility of terminating the agreement if necessary.

- The new standard imposes on insurance and reinsurance companies a **duty to monitor and supervise the activities of their service providers on an ongoing basis**, especially as regards core operating functions. Insurance and reinsurance companies must exercise their **access and auditing rights** to ensure their cloud computing service providers comply with applicable European and Portuguese legislation, as well as with the appropriate ICT security standards.

- It also regulates the **duty to inform the ASF in advance** if core or important functions and activities are outsourced to cloud service providers, and it establishes a minimum set of items to be included in this information.

- Lastly, it imposes the obligation to (i) enter into **written** agreements (while also establishing their minimum content); (ii) **keep an up-to-date record** of these agreements; and (iii) provide the ASF with all the requested information, including a copy of the agreements.

Entry into force

Regulatory Standard 6/2022-R enters into force on July 30, 2022.

For additional information on the contents of this document, please contact Cuatrecasas.