



EIOPA finalises Guidelines on Information and Communication Technology Security and Governance

NEWS

DATE:

12 Oct 2020

Today, the European Insurance and Occupational Pensions Authority (EIOPA) finalised the Guidelines on Information and Communication Technology (ICT) Security and Governance.

These guidelines shall provide guidance to national supervisory authorities and market participants on how regulation regarding operational risks set forth in Directive 2009/138/EC and in the Commission's Delegated Regulation 2015/35 is applied in the case of ICT security and governance, considering as well EIOPA's Guidelines on System of Governance.

The objective of the guidelines is to promote the increase of the operational resilience of the digital operations of insurance and reinsurance undertakings against the risks they face. Operational resilience is key to protect insurance and

reinsurance undertakings' digital assets, including their systems and data from policyholders and beneficiaries. In particular, the guidelines:

- provide clarification and transparency to market participants on the minimum expected information and cyber security capabilities, i.e. security baseline;
- avoid potential regulatory arbitrage;
- foster supervisory convergence regarding the expectations and processes applicable in relation to ICT security and governance as a key to proper ICT and security risk management.

EIOPA consulted on the guidelines between December 2019 and March 2020 and took into account the views of stakeholders wherever possible.

National supervisory authorities are expected to apply these guidelines from 1 July 2021.

[Go to the Guidelines and the resolution of comments](#)

Legal basis

These guidelines have been developed according to Article 16 of the Regulation (EU) 1094/2010. Under this Article EIOPA may issue Guidelines and Recommendations addressed to competent authorities and financial institutions with a view to establish consistent, efficient and effective supervisory practices and ensuring the common, uniform and consistent application of Union law.

In accordance with Article 16(3) of that Regulation, competent authorities and financial institutions are required to make every effort to comply with those Guidelines and Recommendations.

[Contact Us](#)
