



11 July 2025

New EBA Guidelines Managing Third-Party Risk in Financial Institutions

Source: European Banking Authority, Consultation Paper on the Draft Guidelines on the Sound Management of Third-Party Risk, EBA/CP/2025/12, 8 July 2025.

The European Banking Authority (EBA) has released a consultation paper on the **Draft Guidelines for the Sound Management of Third-Party Risk (EBA/CP/2025/12)**. This long-anticipated update aims to expand and replace the 2019 outsourcing guidelines, adapting to the fast-evolving regulatory environment. The guidelines are open for public comment until **October 8, 2025**.



The governance of third-party arrangements is increasingly regulated under various EU legislative acts. Directive 2013/36/EU (CRD) mandates the EBA to issue governance guidelines for institutions, including third-party risk. Directive 2019/2034/EU (IFD) and Regulation (EU) 2023/1114 (MiCAR) extend similar governance obligations to investment firms and issuers of asset-referenced tokens, respectively. Directive 2014/65/EU (MiFID II) and Directive 2015/2366/EU (PSD2) regulate outsourcing in investment and payment services. With Regulation (EU) 2022/2554 (DORA) (effective January 2023) covering information and communication technology (“**ICT**”) related services,

The EBA’s new Guidelines address non-ICT third-party arrangements, aiming to harmonise rules and ensure consistent risk management across financial sectors while avoiding regulatory fragmentation.

Key Takeaways for Greek Financial Institutions

1. Expanded Scope

The new Guidelines apply to a broader range of entities, including:

- a) Institutions subject to Directive 2013/36/EU (CRD);



- b) Investment firms (non-small, non-interconnected under Article 12(1) of Regulation (EU) 2019/2033 (IFR));
- c) Payment and electronic money institutions;
- d) Issuers of asset-referenced tokens (ARTs) subject to MICAR; and
- e) creditors as defined in point (2) of Article 4 of Directive 2014/17/EU (MCD) which are financial institutions.

2. Beyond Outsourcing

The Guidelines now cover **all third-party arrangements**, not just outsourcing. This includes intragroup services and non-ICT providers. Outsourcing is now seen as a *subset* of third-party risk.

3. Critical or Important Functions

Enhanced rules apply to third-party arrangements considered “critical or important.” These are defined as functions whose disruption could materially impair:

- a) Regulatory compliance
- b) Financial performance
- c) Operational continuity

4. Governance Obligations

- a) Institutions must maintain **robust internal governance** and a clear **third-party risk policy**.
- b) The **management body** remains fully accountable.
- c) Pre-contractual due diligence, ongoing monitoring, audit rights, and clear termination clauses are mandatory.

Implications for the Greek Financial Sector

Greek banks, fintechs, and payment firms must now:

- a) Map all third-party relationships—ICT and non-ICT alike;
- b) Re-assess contracts and service-level agreements for alignment;
- c) Establish or update third-party risk registers;
- d) Prepare for new documentation and reporting duties to regulatory authorities.



EBA's Strategic Objectives

The EBA aims to:

- a) Harmonise oversight of the provision of third party services across the EU.
- b) Avoid regulatory arbitrage, especially with third-country providers.
- c) Prevent overreliance on a handful of providers and mitigate concentration risk.

This comes amid growing systemic reliance on cloud providers, cross-border tech vendors, and central group service hubs.



Sonia Saranti

ss@saranti-partners.com

T: +302120216569

*This publication is provided for general informational purposes only
and does not constitute legal or other professional advice.*