

EBA publishes its final Guidelines on the management of third-party risk

Simplifying the regulatory framework and focusing on critical or important functions

ISSUING AUTHORITY

EBA

PUBLISHED

18 September 2026

APPLIES FROM

Two-year transitional period

In brief

On **18 September 2026**, the European Banking Authority (EBA) published its **final Guidelines** on the sound management of third-party risk regarding non-ICT services (EBA/GL/2026/09). The Guidelines establish a harmonised framework for **identifying, assessing, monitoring and mitigating risks arising from arrangements with third-party service providers (TPSPs)**, particularly where these arrangements support critical or important functions.

The Guidelines complement the Digital Operational Resilience Act (DORA), which applies to ICT services, by establishing **a dedicated framework for managing third-party risk related to non-ICT services**. They introduce **requirements relating to governance, risk assessment and due diligence**, contractual arrangements, subcontracting, audit and access rights, business continuity, concentration risk, conflicts of interest, record-keeping and exit strategies.

Background

The increasing use of third-party service providers by financial entities, combined with an evolving regulatory landscape, has created a need for a broader and more consistent approach to third-party risk management across the EU.

The new Guidelines respond to this need by extending the focus beyond traditional outsourcing to third-party arrangements more generally. They build on and **will replace the EBA's 2019 Guidelines** on outsourcing arrangements, while reflecting the introduction of DORA as the separate EU framework for ICT third-party risk.

Key enhancements

The main enhancements introduced by the Guidelines can be grouped as follows:

- **Broader scope:** The framework moves beyond traditional outsourcing and applies to third-party arrangements more generally, covering non-ICT services provided by external and intra-group service providers.

- **Focus on critical or important functions:** Enhanced requirements apply to arrangements supporting critical or important functions (CIFs), where disruption, discontinuity, defect or failure could materially impair the financial entity’s operations, financial performance or compliance with legal obligations.
- **Proportionate and risk-based approach:** The application and intensity of the requirements should reflect the nature, scale, complexity and risk profile of the financial entity and the relevant third-party arrangement.
- **Strengthened governance and accountability:** Management bodies remain responsible for third-party arrangements and the associated risks, supported by appropriate policies, internal controls, reporting and oversight.
- **Full lifecycle management:** The Guidelines cover the full lifecycle of third-party arrangements, including risk assessment and due diligence, contractual arrangements, subcontracting, ongoing monitoring, documentation, termination and exit strategies.
- **Enhanced resilience and oversight:** The framework strengthens requirements relating to business continuity, concentration risk, audit and access rights, third-country providers and supervisory access, while complementing DORA’s framework for ICT third-party risk.

What this means for institutions

- Review the third-party risk framework: Institutions should assess whether their policies, governance arrangements and risk-management processes cover all relevant non-ICT third-party arrangements, not only traditional outsourcing.
- Review and classify the third-party inventory: Institutions should maintain an up-to-date register and identify arrangements supporting critical or important functions, which require enhanced risk assessment and oversight.
- Strengthen governance and contractual safeguards: Management bodies should ensure clear accountability, while institutions should review contracts, subcontracting arrangements, audit and access rights, business continuity provisions and termination rights.
- Enhance monitoring and resilience: Institutions should monitor material third-party arrangements on an ongoing basis, manage concentration and third-country risks, and maintain credible contingency and exit strategies.
- Coordinate with DORA: Institutions should align their non-ICT third-party risk framework with DORA implementation, while maintaining the distinction between non-ICT services covered by the Guidelines and ICT services covered by DORA.

Timeline

Date	Milestone
18 September 2026	EBA publishes the final Guidelines.
Transitional period	A two-year transitional period will support smooth and proportionate implementation.

How Deloitte can help

The new Guidelines make third-party risk management a broader governance and operational-resilience priority. Deloitte's Advisory team can help institutions focus on the areas most relevant to implementation:

Governance and accountability

Clarify management-body responsibility, ownership and escalation processes, and strengthen the evidence supporting oversight by risk management, compliance and internal audit.

Critical or important functions

Identify and classify third-party services that support critical or important functions and assess the associated risks.

Contracts and subcontracting

Review contractual arrangements and subcontracting chains, including service levels, information and reporting obligations, business continuity, termination rights and exit provisions.

Operational resilience and exit planning

Assess dependencies on third-party providers, concentration risks and business continuity arrangements, and develop contingency and exit strategies for material third-party services.

Contacts



Andrada Tanase

FSI Risk & Regulatory Advisory

Partner, Deloitte Romania

Tel: +40 751 096 946

Email: atanase@deloittece.com



Andrei Evi

FSI Risk & Regulatory Advisory

Senior Manager, Deloitte Romania

Tel: +40 722 385 169

Email: aevi@deloittece.com

Source: [EBA press release, 18 September 2026 – EBA final third-party risk Guidelines](#)

This alert is provided for general information only and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

© 2026 Deloitte. All rights reserved.