Just in Time

EBA Guidelines on the Sound Management of Third-Party Risk Regarding Non-ICT Services

November 2026



iason ESSENTIAL SERVICES FOR FINANCIAL INSTITUTIONS

Executive Summary

- The EBA updates the regulatory framework for third-party risk management in response to financial entities' increasing reliance on **third-party service providers (TPSPs)**. Financial entities use external providers to obtain specialised expertise, reduce costs, improve scalability and efficiency, and concentrate internal resources on core activities. At the same time, increasing dependency on third parties can generate operational, compliance, reputational, concentration and other risks capable of affecting financial entities, their customers and, potentially, the wider financial system.
- The Guidelines therefore move beyond the traditional concept of **outsourcing** towards the broader concept of a **third-party arrangement**. Outsourcing remains relevant but is explicitly treated as a subset of third-party arrangements. This broader perspective reflects the fact that material dependencies on external providers may arise even where the contractual relationship does not meet the traditional definition of outsourcing.
- A central reason for the revision is the introduction of **Regulation (EU) 2022/2554 – DORA**. DORA establishes an EU framework for managing risks arising from ICT services provided by third parties. The EBA Guidelines complement this regime by establishing corresponding expectations for **non-ICT services**. The objective is therefore not to duplicate DORA, but to close the regulatory gap between ICT and non-ICT third-party dependencies and enable financial entities to establish a holistic third-party risk management framework.

Copyright © 2026 - All rights reserved

At a Glance

01	Framework Overview and Principles	4
02	Assessment of Third-party Arrangements and Criticality	8
03	Governance Framework	10
04	Third-Party Arrangements Assessment, Documentation and Register	12
05	Monitoring of Third-party Arrangements	16
06	Exit Strategies	18
07	Supervisory Expectations	20
08	Conclusion & Take-aways	22

Keywords: Third-Party risk; DORA

Copyright © 2026 - All rights reserved

01

Framework Overview and Principles

Copyright © 2026 - All rights reserved

Framework Overview and Principles 1/3

Background and Rationale

The EBA starts from the premise that confidence in the reliability of the financial system depends upon **robust governance** and **operational resilience**. Increasing reliance on **TPSPs** can generate efficiency gains but simultaneously represents an important source of operational risk.

The revised approach responds particularly to the interaction with DORA. While DORA governs ICT third-party risks, the EBA considers that financial entities require comparable governance principles for non-ICT services. Otherwise, similar operational dependencies could be treated differently solely because of the technological or non-technological nature of the service.

A key regulatory concern is that third-party arrangements must not undermine the conditions under which an entity is authorised. They must therefore not:

- result in the delegation of the management body's responsibility;
- alter the financial entity's obligations towards customers;
- undermine the conditions of authorisation;
- impair the independence or quality of internal control functions;
- restrict the ability of the entity or competent authorities to supervise compliance; or
- create obstacles to recovery and resolution.

Financial entities are expected to retain sufficient expertise to **control and challenge TPSPs**. Compliance cannot therefore consist merely of formal or documentary assessments. The entity must possess sufficient knowledge and operational capability to evaluate the provider's performance, identify weaknesses and take corrective action.

The EBA also stresses that **intragroup arrangements are not inherently less risky** than external arrangements. The same regulatory framework generally applies to services obtained from affiliated entities. Although group membership may give a financial entity greater influence or control over the provider, objective selection, risk assessment, conflict-of-interest management and effective oversight remain necessary.

Similarly, centralised arrangements within an **institutional protection scheme (IPS)** remain subject to the Guidelines. Centralisation can create efficiencies but cannot remove the individual entity's regulatory responsibilities.

The Guidelines also link third-party risk management with **recovery and resolution planning**. Arrangements supporting functions relevant to critical functions or core business lines must not prevent operational continuity during financial distress, restructuring or resolution.

Copyright © 2026 - All rights reserved

Framework Overview and Principles 2/3

Scope, Application and Key Definitions

The Guidelines apply to a broad population of financial entities, including institutions subject to the CRD, relevant investment firms, payment institutions and electronic money institutions, issuers of asset-referenced tokens, certain financial-institution creditors under the Mortgage Credit Directive, and third-country branches. Small and non-interconnected investment firms meeting the conditions of Article 12(1) IFR are excluded.



The framework applies specifically to **non-ICT services**.
ICT services within DORA's scope are excluded because they are governed by DORA. Nevertheless, the EBA explicitly expects financial entities to adopt a **holistic approach** covering both ICT and non-ICT third-party risks.



A **third-party arrangement** is broadly defined as an arrangement of any form between a financial entity and a TPSP—including an intragroup TPSP—for supporting one or more functions on a recurrent or ongoing basis.

An **outsourcing arrangement** is a narrower category: it exists where the TPSP performs, recurrently or continuously, a function that would otherwise be undertaken by the financial entity itself. Thus:

"All outsourcing arrangements covered by the definition are third-party arrangements, but not every third-party arrangement is outsourcing".



The Guidelines also define **third-party risk** broadly as risk arising from the use of services supporting functions provided by TPSPs or their subcontractors.

The concept of **concentration risk** is particularly important.
It refers to dependency on an individual provider or multiple related providers where their failure, unavailability or inadequate performance could jeopardise the financial entity's critical or important functions, produce substantial losses or potentially endanger financial stability.



Finally, **operational resilience** is defined as the ability of the financial entity to deliver critical or important functions through disruption.

Copyright © 2026 - All rights reserved

Framework Overview and Principles 3/3

Implementation and Proportionality

The Guidelines will apply to third-party arrangements entered into, reviewed or amended after their application date.
Existing arrangements must subsequently be reviewed and amended to achieve compliance.

A **differentiated transitional regime** is provided.
For third-party arrangements supporting critical or important functions, entities are expected to complete the review and documentation process within the transitional period. If this has not been completed within **two years from the application date**, the entity should inform its competent authority and explain the measures planned to complete the review or, where relevant, its potential exit strategy.

For arrangements supporting functions that are **not critical or important**, review and documentation can occur upon renewal of the arrangement.

The 2019 EBA Guidelines on outsourcing will be repealed when the new framework becomes applicable.

The **principle of proportionality** applies throughout the Guidelines. The appropriate governance and risk management framework should reflect the financial entity's risk profile, nature, business model, scale and complexity.

Relevant considerations include the complexity of the function supported by the TPSP, the risks generated by the arrangement, whether the supported function is critical or important, and the potential impact on continuity of activities.

Proportionality therefore does not eliminate the obligation to manage third-party risk; rather, it **determines** the **intensity** and **sophistication** of the **arrangements required.**

Copyright © 2026 - All rights reserved

02

Assessment of Third-party Arrangements and Criticality

Copyright © 2026 - All rights reserved

Assessment of Third-party Arrangements and Criticality

Financial entities should establish a holistic risk management framework covering all business lines and internal units.
For each relevant relationship, they must determine whether the service is non-ICT, whether it supports a function on a recurrent or ongoing basis, and whether that function is **critical or important**.

Where an arrangement covers several functions, the financial entity should assess the arrangement as a whole rather than artificially separating its components.

Certain categories are generally excluded from the Guidelines, including legally mandated services such as statutory audit; certain regulated financial services; market information services; financial transactions between financial institutions acting as counterparties; central-bank transactions; payment network infrastructures; clearing and settlement arrangements; supervised global financial messaging infrastructures; correspondent banking; and various ancillary services or acquisitions without material impact on risk exposures or operational resilience.

The exclusion does not imply that the risks of those relationships can be ignored; appropriate risk management remains necessary.

Criticality is assessed according to the potential consequences of **disruption**.

A function should be regarded as critical or important where disruption, defective performance or failure would materially impair compliance with authorisation requirements, financial performance, or the soundness and continuity of services and activities.

Operational tasks belonging to **internal control functions** are generally expected to be considered critical or important unless the entity demonstrates that failure would not adversely affect the effectiveness of those control functions.

Particular attention is also required where third-party arrangements support functions relevant to **BRRD critical functions or core business lines**.

Copyright © 2026 - All rights reserved

03

Governance Framework

Copyright © 2026 - All rights reserved

Governance Framework

Just in Time

The management body must define, approve and regularly review a **strategy** for sound **third-party risk management**. This strategy should complement the financial entity's operational risk management framework and support operational resilience.

Entities may maintain integrated ICT/non-ICT strategies or separate frameworks, but the overall approach must remain holistic.

The management body retains ultimate responsibility and must ensure adequate internal resources. Third-party arrangements cannot be used to transfer management responsibilities to external providers or eliminate the entity's internal capacity to understand, monitor and control the outsourced or supported activity.

The framework should ensure that risks associated with TPSPs are **identified, assessed, monitored, managed, reported and mitigated**. Relevant risks extend beyond operational risk and include legal, compliance, reputational, concentration, business continuity and other material risks.

For arrangements supporting critical or important functions, financial entities should establish a written policy defining the lifecycle of the relationship, including responsibilities, approval processes, risk assessment, due diligence, contractual requirements, monitoring and exit.

Potential **conflicts of interest** must also be identified and managed. This is particularly relevant for intragroup arrangements, where commercial or organisational relationships could affect objective decision-making.

Business continuity arrangements must account for third-party dependencies, while the internal audit function should independently assess whether the governance framework and third-party risk controls are appropriately designed and implemented.

Copyright © 2026 - All rights reserved

04

Third-Party Arrangements Assessment, Documentation and Register

Copyright © 2026 - All rights reserved

Third-Party Arrangements Assessment, Documentation and Register 1/3

Documentation and Register of Third-party Arrangements

Documentation represents a core element of the framework. Financial entities must maintain appropriate information concerning their third-party arrangements and must be capable of providing it to competent authorities.

The register enables both financial entities and supervisors to understand the overall dependency structure, identify critical or important relationships and analyse concentration risk.

For groups and IPS structures, the register may be maintained centrally, provided individual financial entities and competent authorities can obtain the relevant entity-specific information **without undue delay**.

The EBA allows some flexibility in coordinating this documentation with DORA. Financial entities may combine the non-ICT register with the DORA register or maintain a proportionate separate register, provided consistency is maintained.

Copyright © 2026 - All rights reserved

Third-Party Arrangements Assessment, Documentation and Register 2/3

Pre-contractual Analysis, Risk Assessment and Due Diligence

Before entering into an arrangement, a financial entity should conduct an appropriate **pre-contractual analysis**.
The intensity of this assessment increases when the arrangement supports a critical or important function.



The entity must first ensure that entering into the arrangement will not breach regulatory or supervisory conditions. Third-party arrangements must not impair the entity's authorisation, governance, internal controls or the ability of competent authorities to supervise it.



A The risk assessment should cover relevant risks arising from the provider, the service, geographical location, subcontracting structure and overall dependency created by the arrangement. Particular attention is required for **concentration risk** and potentially complex subcontracting chains.



Due diligence should establish whether the TPSP has appropriate capabilities, resources, organisational structure and, where relevant, financial capacity to perform the service reliably and in compliance with applicable requirements.
For critical or important functions, due diligence must be sufficiently robust to provide the financial entity with a sound basis for concluding that the provider can meet the required service, control, resilience and regulatory standards.



Third-country arrangements require particular scrutiny because differences in legal systems, data protection, professional secrecy, enforcement and supervisory access may affect the financial entity's ability to comply with EU requirements.

Copyright © 2026 - All rights reserved

Third-Party Arrangements Assessment, Documentation and Register 3/3

Just in Time

Contractual Requirements

Third-party arrangements should be documented through appropriate written agreements clearly establishing the rights and obligations of both parties.

For services supporting critical or important functions, the contractual framework becomes significantly more detailed. Agreements should allow the financial entity to manage performance, risk, regulatory compliance, business continuity and termination effectively.

One important area concerns **subcontracting**. The agreement should specify whether the TPSP may subcontract a critical or important function, or material parts of it. The financial entity needs sufficient visibility over subcontracting and must be able to assess material changes in the subcontracting structure.

The Guidelines are designed to prevent subcontracting chains from making risk opaque or rendering effective oversight impossible. The financial entity remains responsible for ensuring that the overall arrangement continues to satisfy applicable requirements.

Financial entities must retain appropriate rights where changes to subcontracting materially increase risk or adversely affect the supported critical or important function, including the ability to terminate the arrangement where necessary.

Access and audit rights	For critical or important functions, **access, information and audit rights** are fundamental. Financial entities must be able to obtain sufficient assurance that TPSPs are performing services in accordance with contractual and regulatory requirements. Competent authorities must likewise retain the ability to obtain information and conduct effective supervision. Audit arrangements may be implemented on a risk-sensitive basis, recognising practical issues concerning security, confidentiality and the organisational burden of multiple individual audits. The Guidelines permit approaches such as pooled audits where appropriate, while maintaining the underlying principle that the entity cannot surrender effective audit and access rights.
Termination rights	Contracts should provide appropriate termination rights where continuation of the relationship would create unacceptable regulatory or operational risks. Termination is particularly **relevant** where the TPSP materially breaches applicable law or contractual obligations, significant deficiencies remain unresolved, changes materially affect the arrangement, supervisory access is impaired, or the service can no longer be provided within the entity's risk tolerance.

Copyright © 2026 - All rights reserved

05

Monitoring of Third-party Arrangements

Copyright © 2026 - All rights reserved

Monitoring of Third-party Arrangements

Just in Time

Third-party risk management does not end when the contract is signed. Financial entities must continuously monitor relevant arrangements and periodically reassess their risks. For arrangements supporting critical or important functions, monitoring should ensure that services continue to satisfy appropriate **performance and quality standards**.

The Guidelines identify several possible monitoring instruments, including:

- reports received from the TPSP;
- key performance indicators;
- key control indicators;
- service-delivery reports;
- self-certifications;
- independent reviews; and
- information concerning business continuity arrangements and testing.

Financial entities must also monitor their internal **concentration risk**, including concentration arising from subcontractors.

Risk assessments should be regularly updated. If the nature, scale or risk profile of a function changes materially, the financial entity should reconsider whether its classification as critical or important remains appropriate.

Where actual or potential shortcomings are identified, financial entities must take appropriate corrective or remedial action. Where deficiencies cannot be satisfactorily addressed, **termination of the arrangement** may be required.

Copyright © 2026 - All rights reserved

06

Exit Strategies

Copyright © 2026 - All rights reserved

Exit Strategies

A particularly significant requirement concerns **exit planning** for third-party arrangements supporting critical or important functions.

Financial entities should maintain documented exit strategies aligned with their third-party risk strategy and business continuity arrangements.

Exit scenarios should contemplate, among other things, termination of the agreement, TPSP failure, excessive concentration or difficulty in exiting the relationship, deterioration in service quality, business disruption, material risks affecting continuous performance and significant breaches of applicable law, regulation or contractual provisions.

The central objective is to ensure that an entity can exit a critical third-party relationship **without undue disruption**, without compromising regulatory compliance and without damaging the continuity and quality of services provided to customers.

Exit plans must therefore be **realistic, feasible and based on plausible scenarios and reasonable assumptions**. Appropriate testing should be undertaken where relevant.

Entities should evaluate the costs, operational impact, resources and time required to transfer the service to another provider or bring the activity back in-house.

Alternative solutions should be identified in advance. Transition plans should address the transfer of functions and relevant data to alternative providers or back to the financial entity itself while maintaining business continuity.

The exit strategy should establish clear objectives, responsibilities, resources and success criteria. Monitoring indicators should also identify circumstances - including unacceptable service levels - that trigger exit or other corrective action.

Copyright © 2026 - All rights reserved

07

Supervisory Expectations

Copyright © 2026 - All rights reserved

Supervisory Expectations

The Guidelines establish detailed expectations for **competent authorities**.

Supervisors should assess whether third-party arrangements materially alter the conditions under which a financial entity was originally authorised and whether they remain capable of effectively supervising the entity.

Third-party risk should be assessed through the **SREP** or, for relevant payment institutions, through corresponding supervisory processes, including information requests and onsite inspections.

Competent authorities may request detailed information concerning critical or important arrangements, including risk assessments, TPSP business continuity plans, exit strategies and the resources dedicated to monitoring the provider.

Supervisory assessment should consider whether entities properly monitor and manage their third-party arrangements, possess sufficient resources, identify relevant risks and appropriately manage conflicts of interest.

A particularly important supervisory objective is preventing EU/EEA financial entities from becoming **"empty shells"**. Supervisors should therefore assess whether extensive reliance on third-country or intragroup arrangements leaves the EU entity with sufficient substance, governance and risk management capabilities.

The risks considered should include operational risk, reputational risk, step-in risk where relevant, entity-level concentration risk, **sector-wide concentration risk**, the level of control over the TPSP and conflicts of interest.

Where concentration risk is identified, competent authorities should monitor its development and assess its potential implications for other financial entities and the stability of the financial system.

Where governance arrangements are inadequate or regulatory requirements are breached, supervisory measures may include restricting the scope of non-ICT services supporting critical or important functions or requiring the entity to **exit one or more third-party arrangements**.

Copyright © 2026 - All rights reserved

08

Conclusion & Take-aways

Copyright © 2026 - All rights reserved

Conclusion & Take-aways 1/2

From outsourcing risk to comprehensive third-party risk management.	The Guidelines mark a significant evolution from the traditional outsourcing framework towards a broader approach covering recurrent or ongoing arrangements with third-party service providers. Outsourcing remains relevant but becomes a subset of the wider third-party risk framework.
Non-ICT third-party risk becomes the complement to DORA.	While DORA governs ICT third-party risk, the new EBA Guidelines address non-ICT services. Financial entities are expected to adopt a **holistic third-party risk management approach** covering both ICT and non-ICT dependencies.
Critical or important functions drive regulatory intensity.	The classification of functions is fundamental because arrangements supporting critical or important functions are subject to significantly enhanced requirements concerning risk assessment, due diligence, contractual clauses, monitoring, audit rights, subcontracting and exit strategies.
Accountability remains with the financial entity.	The use of a TPSP does not transfer regulatory responsibility. The **management body remains ultimately responsible** for the financial entity's activities and must ensure adequate governance, resources, expertise and oversight capabilities.
Financial entities must retain sufficient substance.	Third-party arrangements must not result in an **"empty shell"** structure. Financial entities must preserve sufficient internal resources and capabilities to manage risks, challenge providers and continue meeting the conditions of their authorisation.
The entire third-party lifecycle needs to be governed.	Compliance cannot be limited to contract negotiation. The Guidelines establish expectations covering the complete lifecycle: identification and classification → pre-contractual risk assessment → due diligence → contracting → monitoring → subcontracting oversight → business continuity → termination and exit.
Intragroup arrangements are not automatically lower risk.	Services provided by entities belonging to the same group remain within the third-party risk framework. Group membership may provide greater control over the provider, but it does not eliminate the need for risk assessment, monitoring and management of conflicts of interest.
Concentration risk becomes a major prudential concern.	Financial entities must assess dependencies on individual or related TPSPs. Competent authorities are also expected to consider **sector-wide concentration**, particularly where several financial entities depend on the same provider for critical or important functions.
Subcontracting chains require greater transparency and control.	Financial entities must understand material subcontracting arrangements supporting critical or important functions and retain sufficient contractual rights to assess and respond to material changes in the service chain.
Third-country providers require additional safeguards.	Arrangements involving TPSPs located outside the EU require particular attention to regulatory compliance, professional secrecy, data protection, legal enforceability, access to information and the ability of competent authorities to exercise effective supervision.

Copyright © 2026 - All rights reserved

Conclusion & Take-aways 2/2

Audit and access rights are essential.	Financial entities and competent authorities must retain appropriate rights to information, inspection and audit, particularly for arrangements supporting critical or important functions. Contractual structures must not prevent effective supervisory access.
Ongoing monitoring must be substantive rather than formal.	Financial entities are expected to continuously assess provider performance and risk using appropriate mechanisms such as KPIs, control indicators, service reports, independent reviews and business continuity information.
Exit strategies become a key operational-resilience requirement.	For critical or important functions, entities need credible and documented exit strategies. These should allow services to be transferred to another TPSP or reintegrated internally **without undue disruption to business activities, regulatory compliance or customer services**.
Documentation and registers will become central supervisory evidence.	Financial entities must maintain sufficient information on their third-party arrangements to allow both internal oversight and effective supervision. Coordination with the DORA register is possible, reducing unnecessary duplication.
Proportionality does not mean exemption.	Requirements should reflect the entity's size, complexity, business model, risk profile and the criticality of the service. The regulatory burden is therefore differentiated, but all relevant third-party risks still need to be appropriately managed.
The Guidelines have direct implications across multiple functions.	Implementation is not solely a Procurement or Outsourcing exercise: it requires coordination between the **management body, Risk Management, Compliance, Legal, Procurement/Vendor Management, Business Continuity and Internal Audit**.
Existing third-party inventories and classifications will need to be reassessed.	The broader concept of third-party arrangements means that relationships historically classified as “non-outsourcing” may need to be reconsidered to determine whether they fall within the new framework.
Contractual frameworks will require a gap analysis.	Existing templates and agreements - particularly those supporting critical or important functions - should be assessed against the new requirements concerning audit/access rights, subcontracting, monitoring, termination, business continuity and exit.
Alignment between DORA and non-ICT third-party governance will be strategically important.	Although the legal frameworks are distinct, the EBA explicitly promotes a holistic approach. Financial entities can therefore benefit from developing a **single third-party risk management architecture** with differentiated requirements for ICT and non-ICT services.

Copyright © 2026 - All rights reserved

ESSENTIAL SERVICES FOR FINANCIAL INSTITUTIONS

iason is an international consulting firm that has been supporting both financial institutions and regulators in topics related to Risk Management, Finance and ICT since 2008

Strategy

Strategic advisory on the **design** of **advanced frameworks** and **solutions** to fulfil both **business** and **regulatory needs** in Risk Management and IT departments

Methodology & Governance

Implementation of the designed **solutions** in bank departments **Methodological support** to both **systemically important financial institutions** and **supervisory entities**

Solution

Advanced **software solutions** for **modelling, forecasting, calculating** metrics and **integrating** risks, all on cloud and distributed in Software-as-a-Service (**SaaS**)

KEEP IN TOUCH

iason

Company Profile

iason is an international firm that consults Financial Institutions on Risk Management. **iason** integrates deep industry knowledge with specialised expertise in Market, Liquidity, Funding, Credit and Counterparty Risk, in Organisational Set-Up and in Strategic Planning.

Dario Esposito

Lorena Corna

This is an **iason creation**.
The ideas and the model frameworks described in this presentation are the fruit of the intellectual efforts and of the skills of the people working in iason. You may not reproduce or transmit any part of this document in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of iason.

www.iasonltd.com

Copyright © 2026 - All rights reserved