Consultation Paper on the Guidelines on the sound management of third-party risk (non-ICT related services)

Public hearing: Friday, 5 Sept. 2025

Djamel Bouzemarene, Senior Policy Expert
Regulation

Public hearing structure and functioning

Public hearing structure

Introduction: Isabelle Vaillant (EBA, PRSP Director) and Francesco Mauro (EBA Head of Unit)

Guidelines (GLs) on the sound management of third-party risk ICT - Update

Next steps

Q&A sessions

Suggestions for an efficient session

Should you need assistance or would like to intervene:

- **write on Teams chat to any of the hosts or publicly;**
- **raise your hand on Teams.**

To avoid background noise, please stay muted unless you take the floor.

To increase audio quality please turn off video streaming.

Please identify yourself (if you don't use full name on Teams).

Public hearing : Agenda

9:00-11:00	GLs on sound management of third-party risk
11:00-11:30	*Coffee break*
11:30-13:00	GLs on internal governance

Objective of the update of the Gls on outsourcing

Establish **a <u>comprehensive framework on third party risk management for non-ICT related services</u>**, in particular by:

- Broadening the scope to capture most of the financial entities in the banking sector
- Aligning with Basel /FSB work (to the extent possible)
- Consolidate to guarantee a homogenous and coherent application of third-party risk management (ICT services non-ICT related services)

The Guidelines raises the level of harmonisation taking into account proportionality

DORA and the update of EBA GL on Outsourcing

Holistic framework for the management of third-party risk

DORA (L1+L2)	EBA GLs on third-party risk
Scope: contractual arrangements for ICT services **Aim:** sound management of ICT third-party risk	**Scope:** contractual arrangements for *other than* ICT services **Aim:** sound management of non-ICT third-party risk ***(to replace EBA GL on Outsourcing)***

- **Scope:** To be extended to a more general approach on the management of third-party risk (excluding ICT third-party risk which will be covered fully by DORA) where outsourcing arrangements will solely be a subset of third-party arrangements
- **Addressees**: **all together referred to as "financial entities"**
  - Financial institutions (CIs and IFs under CRD), PIs and EMIs (within the scope of PSD2/EMD2), Class 1 minus and Class 2 IFs, ART issuers (if not under CRD) and creditors under MCD that are financial institutions, (M)FH and TCBs

Content of the GLs on third-party risk management

Definitions

- Outsourcing: maintained as a subset of **Third-party arrangements** (TPA);
- New definitions introduced: **TPA and third-party risk**, third-party service provider (TPSP) and intra-group TPSP, subcontracting, concentration risk, operational resilience;
- Cloud services and cloud definitions have been deleted (as they are within DORA's scope).

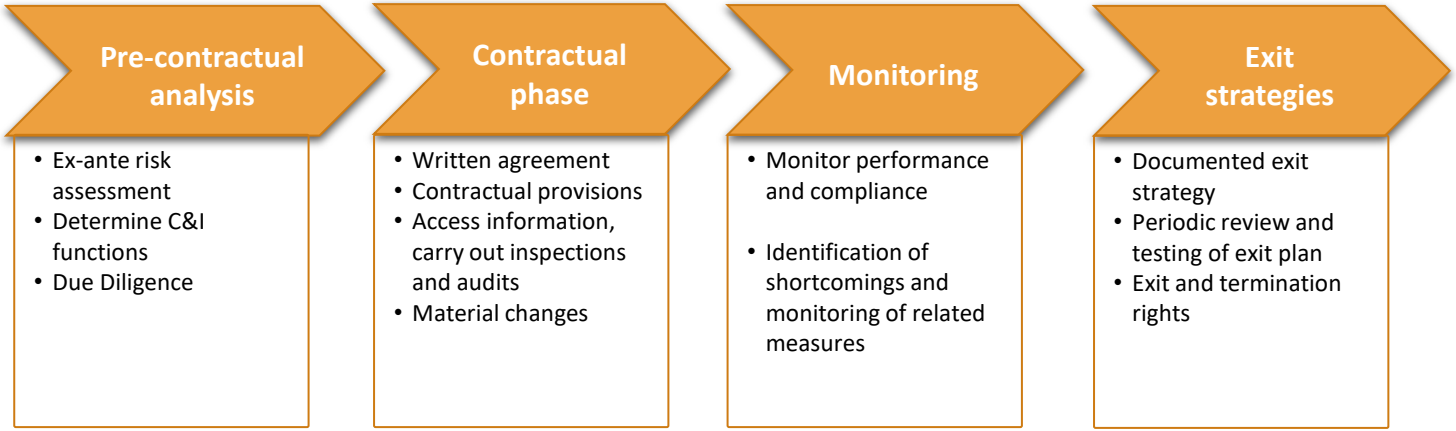
Transitional period

= 2 years from the application date

- To ensure that Financial entities can:
  - **review and amend accordingly existing TPA,** and also **update the assessment of the criticality or importance** functions related to; and
  - update the **register of non-ICT TPA**.

=> More **flexibility provided** and to ensure the effective supervision of TPA.

GLs on third-party risk management – Life-cycle of third-party arrangements



Governance arrangements

- Clear assignment of internal responsibilities and effective oversight of relevant contractual arrangements
- Policy in place (consistent with DORA)
- Conflict of interest
- Clear identification of a role or designate a senior management responsible for monitoring and cooperation with control functions

Main updates of the GLs on third-party risk management

Business continuity plans

- **Adapted and aligned with DORA/ updated GL IG,** taking into account lessons learnt from practical cases.
- Clarification made requiring financial entities to set out clear procedures to manage internal and external crisis communications when BCP is activated, and to involve TPSPs in periodical tests.

Internal audit functions

- Adapted to ensure that financial entities within the GL's scope establish **a formal follow-up process**, including rules for the timely verification and remediation of critical audit findings.

Subcontracting of C&I functions

- Aligned with DORA requirements for the information to be provided in the written agreement.

Register for TPA (non-ICT services)

- **Adapted to align with DORA's Register for ICT services, with a proportionate approach**).
- One single register can be developed distinguishing ICT/non-ICT services, where relevant and under the Financial entities' discretion**.**

Annex 1 (TBC)

- Description of the **different category to be used for classification of function by Financial entities**.
- It shall be considered as a **non-exhaustive list of examples:** if a service or function provided by TPSP is not covered, Financial entities shall use their own internal categorisation.

Next steps


Public consultation end date:
8 October 2025
Please send your comments to: Consultation on draft Guidelines on the sound management of third-party risk
Final version to be published by April 2026

GLs on third-party risk management: Consultation questions

Question n. 1: Are subject matter, scope of application, definitions and transitional arrangements appropriate and sufficiently clear?
Question n. 2: Is Title II appropriate and sufficiently clear?
Question n. 3: Are Sections 5 to 10 (Title III) of the Guidelines sufficiently clear and appropriate?
Question n. 4: Is Title IV appropriate and sufficiently clear?
Question n. 5: Is Annex I, provided as a list of non-exhaustive examples, appropriate and sufficiently clear?

ANY QUESTIONS?

European Banking Authority

Floor 24-27, Tour Europlaza
20 Avenue André Prothin
92400 Courbevoie, France

Tel: +33 1 86 52 70 00
E-mail: info@eba.europa.eu

https://eba.europa.eu/