



# EU RegCORE Client Alert

## Financial Services

October 2026



**Dr. Michael Huertas**

Tel: +49 160 97375760

[michael.huertas@pwc.com](mailto:michael.huertas@pwc.com)

**EU RegCORE Team**

[de\\_regcore@pwc.com](mailto:de_regcore@pwc.com)

## EBA's new non-ICT third-party risk Guidelines: implications for operating models and transactions

### QuickTake

On 18 September 2026, the European Banking Authority (**EBA**) published its final Guidelines on the sound management of third-party risk related to non-ICT services (EBA/GL/2026/09) (the **2026 Guidelines**). The 2026 Guidelines address services other than information and communication technology (**ICT**). Once applicable, they will replace the 2019 outsourcing Guidelines and extend the detailed framework to recurring or ongoing third-party support beyond arrangements meeting the outsourcing definition.<sup>1</sup>

Our central reading is that in-scope firms should consider classifying their service dependencies before commissioning contract remediation. The decisions affect which arrangements need enhanced controls, whether a group service model leaves local management with usable evidence, and whether an acquired

---

<sup>1</sup> EBA, Final report on Guidelines on the sound management of third-party risk related to non-ICT services, EBA/GL/2026/09, 18 September 2026 (**2026 Guidelines**), operative paras 5–7, 17–22 and 31–33, pp 16–17, 19–21 and 24–26; EBA, Guidelines on third party risk management, product page, accessed 13 October 2026. The product page records the Guidelines as final and awaiting translation and the final report as not yet applicable.

business can separate from its seller on the agreed timetable. A programme based only on the existing outsourcing register may miss relevant arrangements; imposing the full package for critical or important functions on every supplier could sit uneasily with proportionality and the exclusions.

The EBA aligns the framework with the Digital Operational Resilience Act (**DORA**), but a completed DORA programme is unlikely to settle the non-ICT work on its own. Mixed services, group service centres and non-ICT providers using ICT subcontractors are likely to need a documented classification and a coherent view of the dependencies behind the direct contract.<sup>2</sup>

As at 13 October 2026, the Guidelines are final and awaiting translation, and the final report is not yet applicable. The published text leaves application and repeal dates open. Paragraph 20 sets a point two years after the eventual application date at which unfinished review and documentation of arrangements supporting critical or important functions should be reported to the competent authority, together with planned completion measures or a possible exit strategy. Other arrangements may be reviewed and documented at renewal under paragraph 21, subject to paragraph 18's application to arrangements entered into, reviewed or amended from the application date. In our view, publication therefore does not itself start the implementation clock.<sup>3</sup>

For boards and deal teams, the immediate priority is to identify decisions that could commit the firm to an unworkable service model: centralising a control function, renewing a material service, changing a provider or acquiring a business dependent on seller infrastructure. The analysis below links those decisions to service classification, contractual rights, retained capacity and a resourced continuity or separation plan.

## Key takeaways

| Change or decision           | What it means for firms                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Perimeter before repapering  | Classify recurring non-ICT support and apply exclusions before deciding which contracts need remediation.                   |
| Operating model decisions    | Test retained capacity, local oversight evidence and the service model before centralisation or acquisition.                |
| DORA and hidden dependencies | Assess mixed services and underpinning ICT dependencies; direct supplier diversification may conceal shared infrastructure. |
| Risk-based contract controls | Apply the broader baseline and the enhanced layer for critical or important functions to the relevant arrangements.         |
| Continuity and separation    | Match contractual rights and transition periods to the resources, capacity and time needed to execute the plan.             |
| Implementation events        | Track entry, review, amendment and renewal alongside the eventual application date and transition deadline.                 |

*PwC Legal analysis based on EBA/GL/2026/09 and EBA/GL/2019/02.*

---

<sup>2</sup> 2026 Guidelines, operative paras 5–7, 23–25, 31–33 and 38–49, pp 16–17, 22, 24–25 and 27–32. EBA, final-Guidelines press release on third-party risk, 18 September 2026, [EBA press release](#); 2026 Guidelines, operative para 58, p 34.

<sup>3</sup> 2026 Guidelines, operative paras 18–22, p 21; EBA product page cited in footnote 1; EBA, final-Guidelines press release, 18 September 2026, [EBA press release](#).

## The new requirements in detail

### Acquisitions and changes to the operating model

For a buyer of an in-scope financial entity, third-party dependencies belong in transaction diligence and integration planning. The buyer should identify seller-group services, documentation gaps, provider-consent requirements, concentration created by integration and the people and resources needed to operate independently. Contract remediation and migration costs can affect the integration budget and timetable. The recipient entity and services determine the regulatory assessment; a purchaser or sponsor is not brought within these Guidelines merely by making the acquisition.

Transition service agreements may require particular care. A temporary agreement can provide recurring support while it operates. Where it supports a critical or important function, the receiving entity should align service scope, oversight information, subcontractor change controls, data access and exit assistance with its obligations. The end date should be tested against a resourced separation plan. An extension option provides contingency only if continued service is available on workable terms; it will not of itself create the capacity needed to separate.

For example, assume an acquired bank needs eighteen months to migrate a critical reporting service from its seller, but its transition service agreement lasts twelve months. The parties should resolve that evidenced timing gap through the service period, migration scope and committed resources. An extension option is useful only if continued service is available and the receiving entity can oversee it.

These are PwC Legal's transaction implications of the Guidelines, rather than new EBA requirements for purchase-price adjustments, warranties or closing conditions. Depending on the risk, parties may need consent, remediation or service-documentation milestones in the transaction documents. A useful diligence output identifies each material dependency, its responsible owner, the rights or resources still needed, and the decision required before signing, completion or service expiry. The same analysis supports proposed changes to an existing group service model.<sup>4</sup>

## The legal status and implementation sequence

### A final framework with an application date still to follow

These are Guidelines issued under Article 16 of the EBA Regulation. Competent authorities and financial institutions must make every effort to comply; authorities notify whether they “comply” or “intend to comply”, or explain non-compliance. They are not a new directly applicable regulation. Their practical effect runs through sectoral governance obligations, supervisory practice and the relevant national implementation mechanisms.<sup>5</sup>

The EBA's earlier compliance table with the 2019 Guidelines illustrates that transmission. It records Bafin's affirmative compliance response and documents how other authorities incorporated the old Guidelines, sometimes through national circulars and with local extensions. The table was last updated on 22 October

---

<sup>4</sup> 2026 Guidelines, operative paras 17–21, pp 19–21; paras 68, 83–95 and 109–116, pp 37, 42–46 and 49–52. The acquisition and transition-service implications are PwC Legal analysis of these requirements. For the entity and group perimeter, see operative paras 9–15 and 26–30, pp 17–18 and 22–24.

<sup>5</sup> 2026 Guidelines, operative paras 1–6, pp 15–16; Regulation (EU) No 1093/2010, Article 16(3).

2024. It is evidence of the 2019 framework's implementation, not confirmation that any authority has adopted the 2026 Guidelines or that a particular national requirement has already been repealed.<sup>6</sup>

Existing applicable requirements continue to govern, including DORA for ICT services. Groups should track the completed dates and national supervisory implementation in a jurisdiction-specific record; a single group policy update may not complete every local step.

### **Review and amendment can bring an arrangement into the new cycle**

Paragraph 18 applies the Guidelines to arrangements entered into, reviewed or amended on or after the eventual application date. Paragraph 19 requires existing arrangements to be reviewed and amended accordingly. Paragraph 20 provides the two-year escalation point: where review and documentation of arrangements supporting critical or important functions remain incomplete, the entity should inform its authority and explain the completion measures or possible exit strategy. Paragraph 21 permits review and documentation of other arrangements at renewal.<sup>7</sup>

In our view, firms should distinguish those tracks in their implementation plan. A scheduled contract change, operating-model review or acquisition-related amendment after application deserves an assessment of the paragraph 18 trigger; the transition should not be treated as an automatic exemption for every legacy agreement. Conversely, the text supports a more proportionate renewal approach for non-critical arrangements. It does not specify which routine monitoring activities count as a review, so the treatment of borderline cases should be documented and, where material, discussed with the supervisor.

For evergreen arrangements, identify automatic renewal, substantive review and amendment events rather than wait for an unspecified renewal date. The eventual application date should remain a controlled programme input. Existing deficiencies still require attention under current obligations.

## **Reassessing the perimeter of third-party support**

### **Which financial entities are addressed**

The addressees include institutions within Article 4(1)(3) of the Capital Requirements Regulation (**CRR**) and third-country branches within Article 47(3)(1) of the Capital Requirements Directive (**CRD**); investment firms other than small and non-interconnected firms under Article 12(1) of the Investment Firms Regulation (**IFR**); payment and electronic money institutions; issuers of asset-referenced tokens (**ARTs**); and creditors under Article 4(2) of the Mortgage Credit Directive which meet the financial-institution condition specified in paragraph 9.

Financial holding companies and mixed financial holding companies approved under Article 21a(1) CRD are also addressed. Account information service providers offering only the account information service in point 8 of Annex I to Directive (EU) 2015/2366 are excluded.<sup>8</sup>

That list matters for financial groups. A standalone insurer, management company for undertakings for collective investment in transferable securities (**UCITS**), alternative investment fund manager (**AIFM**) or crypto-asset service provider is not brought directly within these Guidelines merely because DORA applies to it or because it belongs to a financial group. Banking and investment-group consolidation requirements can

---

<sup>6</sup> EBA, Guidelines compliance table, EBA/GL/2019/02, last update 22 October 2024, pp 1–4, including Belgium and Germany. EBA, Final Report on Guidelines on outsourcing arrangements, EBA/GL/2019/02, 25 February 2019 (**2019 Guidelines**), operative paras 13–16, p 22.

<sup>7</sup> 2026 Guidelines, operative paras 18–22, p 21. The final report supplies no completed calendar date for application, the two-year deadline or repeal.

<sup>8</sup> 2026 Guidelines, operative paras 5 and 8–15, pp 16–18.

nevertheless require consistent group governance across relevant subsidiaries within the applicable prudential scope. The report's explanation of this point preserves the UCITS and Alternative Investment Fund Managers Directive (**AIFMD**) delegation frameworks.

Similarly, ART issuers should not be conflated with all businesses regulated under the Markets in Crypto-Assets Regulation (**MiCAR**); an e-money-token issuer needs its treatment assessed by reference to its credit-institution or electronic-money-institution status.<sup>9</sup>

For investment firms, Class 1 institutions, Class 1 minus firms and Class 2 firms require careful classification. The exclusion for small and non-interconnected firms does not remove their obligations under the second Markets in Financial Instruments Directive (**MiFID II**) or any applicable DORA requirements. A group should therefore map legal entity, prudential category and service regime together before assigning a standard remediation package.

### **The service and the function determine the analysis**

The 2019 definition centred on a provider performing a function that would otherwise be undertaken by the institution itself. The new third-party-arrangement definition covers recurring or ongoing support for one or more functions and expressly includes outsourcing as a subset. The relevant unit of analysis is consequently the service and the function it supports, rather than whether procurement previously selected an outsourcing label.<sup>10</sup>

The distinction should not be overstated. The 2019 Guidelines already required firms to identify and manage risks from all third-party arrangements, regardless of whether they constituted outsourcing. The 2026 change is the extension and systematisation of the register, pre-contractual, contractual and monitoring framework beyond arrangements meeting the outsourcing definition. Existing governance duties are the starting point, rather than a reason to defer action until the new text applies.<sup>11</sup>

A sensible assessment begins with whether there is recurring or ongoing support; whether the service is ICT or non-ICT; whether an exclusion applies; and whether disruption would materially impair financial performance, service continuity or compliance with authorisation and financial-services obligations. Operational tasks of internal control functions should be treated as critical or important unless the assessment establishes that failure would not adversely affect the effectiveness of those functions. Where a provider performs banking, payment-service or ART-issuance functions to an extent that would require authorisation by a competent authority, paragraph 36 states that the financial entity should automatically consider the function critical or important.<sup>12</sup>

For example, recurring support for prudential reporting, customer operations or operational compliance controls may warrant reassessment even where an old procurement file concluded that the arrangement was not outsourcing. Those examples are illustrations, not automatic classifications. Firms should document the actual service, the affected function, the materiality assessment and any applicable exclusion. The same supplier may provide services with different regulatory treatment; where one arrangement covers multiple functions, the entity should assess all aspects together, as paragraph 32 states.

---

<sup>9</sup> 2026 Guidelines, operative paras 13–15 and 26–30, pp 18 and 22–24; background para 14, p 9; consultation feedback on UCITS and AIFMs and group application, pp 72–74. The feedback explains consolidated treatment and does not create a separate standalone addressee category. See also 2026 Guidelines, operative para 9, p 17; Regulation (EU) 2023/1114 (MiCAR), Article 48(1)(a).

<sup>10</sup> 2026 Guidelines, operative para 17, pp 19–20, and paras 31–32, pp 24–25; 2019 Guidelines, operative paras 12 and 26, pp 19–20 and 25.

<sup>11</sup> 2019 Guidelines, operative paras 32–33, p 30; 2026 Guidelines, operative paras 17, 58–67, 68–82, 83–109 and 110–113, pp 19–20 and 34–50.

<sup>12</sup> 2026 Guidelines, operative paras 31–37, pp 24–27.

## **Exclusions require a reasoned assessment**

The final text excludes, as a general principle, services legally required to be performed by a third party, including statutory audit, and regulated financial services legally required to be performed by another financial entity regulated under Union law. It also lists market information services, specified financial transactions, payment network infrastructure, clearing and settlement arrangements with members, overseen global financial messaging infrastructure and correspondent banking.<sup>13</sup>

The regulated-financial-service exclusion is narrower than a general exemption for buying services from a licensed firm. A provider's regulated status does not make every back-office or support service it supplies a legally required regulated financial service. A financial entity purchasing both an excluded custody service and separate operational support should assess each service on its merits. Equally, the non-ICT exclusions do not settle whether a distinct ICT service falls within DORA.

The exclusion for services without material impact on risk exposures or operational resilience includes examples such as legal opinions, tax opinions, representation before courts and administrative bodies, and various ordinary business services. An advisory engagement should be distinguished from the ongoing performance of operational control tasks. The listed examples do not justify treating a materially different managed service as excluded solely because the provider is an adviser. Exclusion from these Guidelines also does not remove the need to manage the risks of the arrangement.<sup>14</sup>

As a general principle, paragraph 33 also excludes the acquisition of goods and utilities. Those exclusions do not remove the need to manage the associated risks appropriately; any distinct ICT service remains subject to a separate DORA scope assessment.<sup>15</sup>

## **DORA and the dependencies behind non-ICT services**

### **Mixed services need a documented classification**

The Guidelines exclude ICT risk management and ICT services within DORA, while requiring a holistic approach to ICT and non-ICT third-party risk. For mixed arrangements, paragraph 32 states that the financial entity should determine whether the use of an ICT service is material to service provision and therefore triggers DORA. This assessment should be read alongside DORA's ICT-service definition and Chapter V scope; it does not create a general exemption for directly supplied ICT services merely because they are assessed as non-material. The final report does not supply a universal numerical threshold for that judgment.

For a technology-enabled managed service, we would examine the contracted output, operational tasks, data and digital services supplied, and their dependencies. Paragraph 32 requires the financial entity to assess all functions covered by one arrangement together. Separate schedules can clarify distinct services but should preserve that combined assessment. A provider's use of computers does not itself resolve classification, and a business-process description should not obscure a material ICT service.<sup>16</sup>

---

<sup>13</sup> 2026 Guidelines, operative para 33, pp 25–26. The lettering in the published list repeats after the clearing-and-settlement entry; the paragraph reference is used here to avoid ambiguity.

<sup>14</sup> 2026 Guidelines, operative para 33 and footnote 41, pp 25–26, and para 35, p 26. The distinction between advisory opinions and operational control performance is an application of those provisions to the service supplied.

<sup>15</sup> 2026 Guidelines, operative para 33 and footnote 41, pp 25–26, read with paras 5–7 and 32, pp 16–17 and 25.

<sup>16</sup> 2026 Guidelines, operative paras 5–7 and 31–32, pp 16–17 and 24–25; consultation feedback on ICT/non-ICT services, pp 71–72. Paragraph 7 should be read with paras 5 and 32 on services and mixed arrangements. DORA, Regulation (EU) 2022/2554, Article 3(21) and Chapter V. DORA, Articles 28(3) and 30(2); European Commission, Q&A DORA030–2999 on the definition of ICT services, published in the EIOPA Q&A database.

An illustrative reporting arrangement shows the distinction. One provider might prepare regulatory returns using its own systems; another might supply a platform on which the financial entity performs the reporting. A third might supply both. The legal and operational facts determine the analysis. Creating separate schedules can make those facts clearer, but drafting labels are unlikely to change the substance of the service.

## **The non-ICT register closes a dependency visibility gap**

The European Supervisory Authorities (**ESAs**), through their joint Q&A 2024\_7089, explain that, where the direct provider does not provide an ICT service, its use of ICT subcontractors is generally outside the DORA register. It also preserves a risk-assessment route to requalification where the underlying ICT service supports a critical or important function, or material parts thereof, to an extent equivalent to direct provision, bringing DORA Chapter V into play. That qualification should be retained in any classification methodology.<sup>17</sup>

Paragraph 58 states that the non-ICT register should document ICT subcontractors effectively underpinning a direct provider's non-ICT service supporting critical or important functions, expressly referring to those functions as defined under DORA. This creates a practical means of seeing dependencies that may not appear in the DORA register. It does not automatically reclassify every non-ICT provider or every ICT subcontractor as a direct DORA arrangement.<sup>18</sup>

In our view, this is especially consequential for concentration analysis. Several business-service providers may appear independent at contract level while relying on the same underlying cloud provider, processing centre or specialist subcontractor. Procurement diversification may then provide less resilience than the supplier list suggests. Firms should link material dependency information across the ICT and non-ICT views and test correlated failure scenarios, with the level of detail proportionate to the service and risk.

## **One register is an option with distinct legal boundaries**

The EBA permits a combined register and encourages consistency with the DORA register. It does not require identical reporting populations or every DORA field for every non-ICT arrangement. Baseline fields include, among others, arrangement references and types, relevant dates, service descriptions and categories, criticality, group or institutional protection scheme status, provider identifiers and ultimate-parent information. Additional fields for services supporting critical or important functions include governing law, latest audit dates, where applicable subcontractors of material parts and their chain rank, substitutability and reintegration or discontinuation assessments and their dates, recovery objectives, the existence of an exit plan, possible alternative providers, and the estimated annual budget cost for the past year and its currency. Paragraphs 61–62 contain the complete field list.<sup>19</sup>

Information on ended arrangements should remain in the register, with supporting documentation retained for an appropriate period. The final Guidelines do not prescribe a universal five-year retention period, so the retention policy should reflect applicable obligations and the evidence needed for effective oversight.<sup>20</sup>

The useful implementation is a common data model with separately identifiable legal populations. Each entity should be able to explain why a service is included, excluded or classified under DORA; reproduce its own register; and reconcile the record with the contractual rights and risk assessment. Combining

---

<sup>17</sup> Joint ESAs, Q&A 2024\_7089, Identification of ICT Service Providers, final answer published 8 August 2025, [Joint ESAs Q&A webpage](#). The answer expressly preserves requalification based on the financial entity's risk assessment.

<sup>18</sup> 2026 Guidelines, operative para 58, p 34, and paras 87–88, pp 44–45.

<sup>19</sup> 2026 Guidelines, operative paras 58–64, pp 34–36, and para 28(d), p 24. DORA, Article 28(3).

<sup>20</sup> 2026 Guidelines, operative para 59, p 34; consultation feedback on retention, p 90. The final text calls for an appropriate period rather than the fixed period proposed in consultation.

spreadsheets without reconciling identifiers, functions and legal entities is likely to preserve the underlying inconsistency. Equally, combining registers should not inadvertently expand a statutory reporting submission beyond its applicable requirements.

## **Group operating models and third country branches**

### **Shared oversight must produce evidence for each entity**

Intragroup arrangements remain subject to the framework and do not transfer management-body responsibility to the group centre. Centralised monitoring, pre-contractual assessment, registers and exit planning are possible, subject to the applicable group and waiver provisions.

Where paragraph 28 applies, centralised monitoring of services supporting critical or important functions should preserve independent monitoring of the provider and appropriate oversight by each financial entity. Each entity should receive risk-assessment and performance-monitoring reports at least annually and on request, summaries of relevant audit reports and the full reports on request. Its management body should be informed of relevant planned provider changes and their potential impact, with a summary of the risk analysis, including legal risks, regulatory compliance and effects on service levels.

An entity relying on central pre-contractual assessment should receive a summary and consider its own structure and risks. Each relevant entity and its competent authority should be able to obtain the entity's register without undue delay. An entity relying on a group exit plan should receive a summary and satisfy itself that the plan can be effectively executed for its business.<sup>21</sup>

Effective oversight by each entity depends on local management being able to understand and challenge assessments performed centrally. A group report should identify the entity's services, risks, contractual rights and continuity options; otherwise it may not evidence the dependencies relevant to that entity's customers and authorisation.

The pricing analysis also has an operational dimension. For intragroup services supporting critical or important functions, the Guidelines permit service synergies to be reflected in financial conditions, provided the provider remains viable on a standalone basis, irrespective of the failure of another group entity. For shared service centres, firms should therefore examine whether the funding model and continuity assumptions survive stress elsewhere in the group. Transfer-pricing compliance alone is unlikely to answer that resilience question.<sup>22</sup>

### **Head undertaking support requires documentation suited to a branch**

The final text expressly addresses EU branches of third-country credit institutions. Since a branch has no legal personality separate from its head undertaking, they cannot contract with each other. Paragraph 10 instead requires another formal arrangement, such as a service-level arrangement or policies, to document the services required by the branch and performed by the head undertaking, using a proportionate approach and reading the Guidelines with the relevant internal-governance framework.<sup>23</sup>

A branch should map the head-undertaking services it receives, responsible people, escalation and continuity arrangements, and access to information needed to meet its obligations. That documentation should

---

<sup>21</sup> 2026 Guidelines, operative paras 26–30, pp 22–24. These requirements continue key features of 2019 Guidelines, operative paras 21–25, pp 23–25.

<sup>22</sup> 2026 Guidelines, operative paras 51–53, pp 32–33; 2019 Guidelines, operative paras 45–47, p 35.

<sup>23</sup> 2026 Guidelines, operative paras 9–10, p 17; consultation feedback on branch arrangements, pp 73–74.

distinguish services from a separate group company, where an intragroup contract is possible. Treating both relationships identically risks either an ineffective purported contract or an undocumented dependency.

When revisiting a European booking and service model, assess head-undertaking support, separate affiliates and external providers together, while preserving their different legal mechanics. The Guidelines do not themselves permit regulated business or replace branch authorisation requirements.

## Third-country providers require more than contractual promises

Paragraph 69 concerns functions of banking activities, payment services, issuance of ARTs and investment services whose performance requires authorisation or registration in the Member State where the financial entity is authorised. The provider should be authorised or registered to perform those activities or services, or otherwise permitted to do so under the relevant national legal framework.

For provision of the specified banking, payment or ART-issuance functions by a provider in a third country, paragraph 70 adds third-country authorisation or registration and supervision, together with an appropriate supervisory cooperation agreement. That agreement should secure the information exchange, access and enforcement cooperation specified in paragraph 70(c). These conditions are not a blanket cooperation-agreement requirement for every provider located in a third country. Investment services remain subject to their separate rules, including Article 32 of Delegated Regulation (EU) 2017/565 for outsourcing functions related to client portfolio management to a provider in a third country.<sup>24</sup>

The broader risk assessment nevertheless needs to address jurisdiction, political and security conditions, data protection, enforcement and insolvency-related impediments to urgent recovery of a function. For a material offshore service centre, contractual access rights should be assessed against whether they can actually be exercised. Data-transfer documentation, governing law and a termination right may not by themselves demonstrate continued service when local insolvency or other legal restrictions intervene.<sup>25</sup>

### Provider suitability and enhanced due diligence

Due diligence should assess the prospective provider's business model, ownership and organisational structure, financial soundness, operational and technical capability, relevant track record, group relationships and supervisory status. Its depth should be proportionate to the function's criticality or importance. For services supporting critical or important functions, the assessment should also address reputation, capacity and resources, internal controls, supply-chain and geographic risks, continuity arrangements, required permissions where applicable and practical access for audits.

Where personal or confidential data are processed, the entity should be satisfied that appropriate technical and organisational safeguards are implemented. Providers should also act consistently with the entity's values and code of conduct. For third-country providers and, where applicable, their subcontractors, the assessment should take account of environmental, social and governance (**ESG**) risks and international human-rights and environmental standards.<sup>26</sup>

---

<sup>24</sup> 2026 Guidelines, operative paras 69–70, pp 37–38; Commission Delegated Regulation (EU) 2017/565, Article 32, preserved by para 70.

<sup>25</sup> 2026 Guidelines, operative paras 72(g), 75–82 and 86, pp 39–42 and 44.

<sup>26</sup> 2026 Guidelines, operative paras 77–82, pp 41–42. Paragraph 79 sets out the enhanced critical-or-important-function checks; paras 81–82 address data safeguards, values and third-country conduct considerations.

## Ongoing monitoring and reassessment

Financial entities should monitor providers using a risk-based approach and monitor arrangements supporting critical or important functions on an ongoing basis. They should regularly update risk assessments and periodically report the risks of those critical or important arrangements to the management body. Material changes in a function's risk, nature or scale should trigger reassessment of criticality.

Provider reports, performance measures and continuity-testing information should inform corrective or remedial action, including termination where appropriate. A formal follow-up process should cover internal-audit findings, including timely verification and remediation of material findings that may affect proper execution of an arrangement.<sup>27</sup>

## Contracts and the control of subcontracting

### A broader baseline with an additional criticality layer

The final text requires written allocation of rights and obligations and minimum terms across in-scope arrangements. Paragraph 84 covers the services, service and data locations, governing law, data protection and recovery, service levels, supervisory cooperation and termination. For CRD institutions, it also addresses resolution powers and substantive obligations. Paragraph 85 adds the critical-or-important-function layer, including measurable performance targets, material-development reporting, contingency planning, enhanced audit rights and an adequate transition period.<sup>28</sup>

The contractual baseline is broader than in the 2019 Guidelines, whose detailed minimum list in paragraph 75 addressed outsourcing of critical or important functions. Paragraph 84 now sets minimum terms for all in-scope third-party arrangements, while paragraph 85 retains an enhanced package for services supporting critical or important functions. For services that do not support those functions, paragraph 99 calls on financial entities to consider including access and audit rights on a risk-based basis; paragraph 88 of the 2019 Guidelines had called for those rights to be ensured on a risk-based basis. The final text therefore does not invariably require unrestricted individual audit rights for every supplier.<sup>29</sup>

A remediation programme should therefore use a baseline module, a critical-or-important-function module and any relevant sectoral or geographic additions. That approach allows the firm to negotiate obligations that correspond to the actual regulatory classification. It also helps avoid unnecessary provider resistance caused by importing every DORA clause into every non-ICT contract, without considering whether the obligation applies or serves the same purpose.

### Subcontracting control must operate through the chain

For critical or important functions, the contract should specify whether subcontracting is permitted and the relevant conditions. The final text requires advance notification of new subcontracting and intended material changes, a reasonable approval or objection period, and implementation only after approval or the expiry of that period without objection. A firm that considers the change outside its risk tolerance should object and request modifications before the period ends.

---

<sup>27</sup> 2026 Guidelines, operative paras 56–57, pp 33–34, and paras 110–113, p 50. Monitoring of critical or important support is ongoing, and material changes call for reassessment.

<sup>28</sup> 2026 Guidelines, operative paras 83–86, pp 42–44. For supervisory information-gathering and investigatory powers applicable to CRD institutions regardless of criticality, see also para 97, p 47.

<sup>29</sup> 2019 Guidelines, operative paras 74–75, pp 44–45, and paras 87–88, pp 47–48; 2026 Guidelines, operative paras 83–85 and 98–99, pp 42–44 and 47.

For the relevant critical or important-function delivery chain, the provider should identify all subcontractors. Continuous monitoring should focus on those supporting critical or important functions or material parts thereof, particularly those effectively underpinning the service; focused monitoring should not be mistaken for permission to omit other subcontractors from identification.<sup>30</sup>

The legal mechanics deserve attention. Paragraph 95 requires the direct agreement to ensure that the agreement between the provider and its subcontractor may be terminated in specified cases of unauthorised or improperly implemented subcontracting. That is distinct from the financial entity's own termination rights under paragraph 108. A clause allowing the financial entity to terminate its direct contract does not necessarily deliver control over the provider's subcontract.<sup>31</sup>

Firms should test how the provider implements those obligations downstream, including reporting, service continuity and equivalent access, inspection and audit rights for the financial entity and relevant authorities. Evidence of the relevant flow-down clauses or an appropriately scoped legal assurance may be more useful than a generic undertaking to use reasonable efforts. The Guidelines do not require a direct contract between the financial entity and every subcontractor, but the agreed chain must support effective oversight.

### **Audit rights and exit assistance need to be usable**

Pooled audits and third-party certifications remain permitted, subject to safeguards. For services supporting critical or important functions, financial entities should not rely solely on certifications and reports over time, and their pooled-audit involvement and information should be sufficient. The contract should preserve unrestricted inspection and audit rights; paragraph 104(h) expressly confirms retained individual-audit rights where the entity relies on certifications or reports. Confidentiality and multi-client concerns can be addressed through proportionate assurance arrangements without neutralising effective rights.<sup>32</sup>

Exit provisions should correspond to the operational plan. Contracts supporting critical or important functions need an adequate transition period, continued service and assistance with an orderly transfer. As a practical drafting matter, firms should settle transition charges, access to relevant data and process documentation, necessary licences, assistance responsibilities and capacity assumptions before disruption. These are implementation considerations drawn from the exit requirements, rather than an EBA-prescribed list of mandatory commercial clauses.<sup>33</sup>

## **Concentration continuity and exit feasibility**

### **An exit plan must expose rather than conceal difficult dependencies**

Concentration, substitutability and exit planning were already important in 2019. The new perimeter extends the population to which that analysis is applied and strengthens its connection to ICT dependencies. Firms should assess multiple arrangements with the same or closely connected providers, group-wide aggregation, subcontractor concentration and, for significant institutions, step-in risk. Authorities also consider

---

<sup>30</sup> 2026 Guidelines, operative paras 87–94, pp 44–46.

<sup>31</sup> 2026 Guidelines, operative para 95, p 46, and paras 108–109, pp 49–50. Paragraph 95 concerns the provider/subcontractor agreement; paragraph 108 concerns termination of the financial entity's third-party arrangement.

<sup>32</sup> 2026 Guidelines, operative paras 98–107, pp 47–49. In particular, paras 103–104 address assurance sufficiency and retained individual audit rights.

<sup>33</sup> 2026 Guidelines, operative paras 85(f), 109 and 114–116, pp 44, 49–52. The suggested commercial terms are implementation analysis, not a quotation of mandatory clauses.

sector-level concentration and can require restriction or exit where governance or supervisory access is inadequate.<sup>34</sup>

The Guidelines do not create a non-ICT provider designation or direct oversight regime equivalent to DORA's framework for critical ICT third-party providers. The supervisory route remains principally through the regulated financial entities and cooperation between their authorities. Providers may nevertheless face substantial contractual and evidence demands from clients, including where several financial entities depend on the same service infrastructure.

The register explicitly permits a substitutability assessment of impossible, alongside easier categories. For services supporting critical or important functions, an impossible-substitutability assessment does not dis-apply the exit expectations. Paragraph 46(f) calls for the ability, within an appropriate timeframe, to transfer the function, reintegrate it or discontinue the dependent business activities.

Paragraph 115 also calls for exit without undue disruption to business activities, impairment of regulatory compliance or detriment to the continuity and quality of services to clients. The firm should demonstrate how its continuity measures and proposed route satisfy those conditions.<sup>35</sup>

For arrangements supporting critical or important functions, the Guidelines call for realistic, feasible exit plans, based on plausible scenarios and reasonable assumptions, with sufficient testing where appropriate. In our view, firms should compare the time needed for migration with the contractual transition period, and separately test whether continuity measures can maintain service within the relevant recovery objectives throughout that transition. A plan can fail even where every document exists: the receiving provider may lack capacity, the necessary licence may not transfer, the data may be incomplete or the retained team may be too small to supervise the migration.<sup>36</sup>

### **Continuity testing and exit testing**

For services supporting critical or important functions, financial entities should maintain and periodically test appropriate business continuity plans, involving the provider as appropriate. Taking account of proportionality, the business impact analysis should assess severe disruptions using quantitative and qualitative criteria, with internal and external data and scenario analysis as appropriate, and consider mapped business functions, support processes, third-party dependencies and substitutability. This periodic continuity-testing expectation is distinct from the requirement that exit plans be sufficiently tested where appropriate.<sup>37</sup>

### **Recovery and resolution use related but different classifications**

The Guidelines distinguish their critical or important functions from critical functions under the Bank Recovery and Resolution Directive (**BRRD**). The former concern the impact on the financial entity and its compliance or continuity; the latter have a separate recovery and resolution definition. For entities subject to the BRRD, functions necessary to perform the activities of core business lines or BRRD critical functions should be treated as critical or important under these Guidelines, unless the assessment establishes that failure or

---

<sup>34</sup> 2026 Guidelines, operative paras 74–75, 111 and 124–128, pp 39–40, 50 and 53–54; 2019 Guidelines, operative paras 66, 106–108 and 116–119, pp 41–42, 51–52 and 54–55. These Guidelines do not establish a direct non-ICT provider designation or oversight regime; compare DORA, Chapter V, Section II.

<sup>35</sup> 2026 Guidelines, operative paras 46(f) and 62(d)–(g), pp 30 and 36, and paras 114–116, pp 51–52.

<sup>36</sup> 2026 Guidelines, operative paras 54–55, 85(f), 109 and 114–116, pp 33, 44 and 49–52. Exit feasibility and testing are qualified as stated in para 115(a).

<sup>37</sup> 2026 Guidelines, operative paras 54–55, p 33, and para 115(a), p 51. Business continuity testing is periodic; sufficient testing of exit plans is qualified by where appropriate.

inappropriate provision would not materially affect the operational continuity of those business lines or critical functions.<sup>38</sup>

For banks and relevant investment firms, the service map should therefore be capable of supporting both ordinary third-party governance and recovery or resolution analysis. Firms should test whether the services, data access and funding assumptions needed through financial distress remain available, and whether any required contractual recognition or resolution-related terms are effective under the applicable law. An ordinary supplier-failure scenario is unlikely to substitute fully for analysing the institution's own stress.

# Practical considerations for firms

## What firms should prioritise now

- 1. **Confirm the perimeter.** Reconcile procurement and payment records with outsourcing and DORA inventories. Produce a service-level classification recording inclusion, exclusion, criticality and the applicable entity and framework.
- 2. **Sequence implementation.** Record entry, review, amendment and renewal events, the eventual application date and transition work for critical or important functions. Prioritise material dependencies and decisions already planned.
- 3. **Establish local evidence.** Confirm access to entity-specific registers, risk assessments, monitoring and audit information, with clear owners and escalation of gaps.
- 4. **Link dependencies.** Establish the required subcontractor identification and focus detailed monitoring on material and effectively underpinning dependencies, including relevant ICT services. Reconcile provider and parent identifiers and test shared dependencies that could cause correlated failures.
- 5. **Prioritise contracts.** Match baseline, critical or important-function and sectoral requirements to classification. Produce a clause-gap and negotiation list covering downstream controls, supervisory access, data recovery and transition assistance.
- 6. **Challenge continuity and separation.** Compare migration time with contractual support, staffing, receiving-provider capacity, data and licence availability, funding and third-country constraints. Escalate assumptions that lack evidence.

### A practical allocation of the work

| Workstream                | Principal owner                    | Evidence to produce                                                               |
|---------------------------|------------------------------------|-----------------------------------------------------------------------------------|
| Perimeter and criticality | Legal and risk with service owners | Service and entity classification with reasons and unresolved perimeter questions |

<sup>38</sup> 2026 Guidelines, operative para 17 and footnote 35, p 19, and para 37, pp 26–27; background paras 13 and 27, pp 9 and 11–12; BRRD, Directive 2014/59/EU, Article 2(1)(35)–(36).

| Workstream                 | Principal owner                       | Evidence to produce                                                                      |
|----------------------------|---------------------------------------|------------------------------------------------------------------------------------------|
| Inventory and dependencies | Procurement and data owners           | Reconciled entity register with material dependency links and documented data gaps       |
| Contract remediation       | Legal with procurement                | Prioritised clause gaps and negotiation requirements matched to classification           |
| Local and group governance | Entity management and group oversight | Entity-specific reports, decision owners and evidence of review and challenge            |
| Continuity and exit        | Operations and service owners         | Resourced plans with migration assumptions and contractual support assessed together     |
| Transaction integration    | Deal team and receiving entity        | Consent and separation milestones with dependencies, owners, cost and timing assumptions |

*Illustrative allocation proposed by PwC Legal; firms should adapt ownership to their governance structure.*

## Updating contractual arrangements and policy documentation

The policy may be combined with the DORA policy, but should distinguish ICT services subject to DORA from non-ICT services; non-ICT services supporting critical or important functions supplied by providers authorised by a competent authority from those supplied by providers that are not; intragroup and institutional-protection-scheme arrangements from external arrangements; and providers located in a Member State from providers located in third countries. The management body should review the policy on non-ICT services supporting critical or important functions at least annually. Roles, approval processes, monitoring, record-keeping and exit responsibilities should match how decisions are actually taken.<sup>39</sup>

The Guidelines expect financial entities to retain sufficient substance and avoid becoming empty shells or letter-box entities. The retained organisation needs sufficient knowledge, resources and capacity to meet its regulatory obligations and oversee providers. A cost-reduction or managed-service proposal should specify which capabilities remain with the financial entity and how management will decide, challenge and respond throughout the arrangement.<sup>40</sup>

Supervisory engagement should be integrated into the programme. The final text calls for timely notification and, where appropriate, supervisory dialogue about planned contractual arrangements supporting critical or important functions and functions that become critical or important, providing at least the information specified in paragraphs 61 and 62. It also calls for timely notification of material changes and/or severe events concerning those arrangements that could materially affect the continuing provision of the financial entity's business activities. It also allows authorities to request detailed information on other arrangements. These provisions should not be presented as a universal prior-approval requirement, but firms should separately check applicable sectoral and national notification or approval rules.<sup>41</sup>

<sup>39</sup> 2026 Guidelines, operative paras 38, 44 and 47–50, pp 27–32.

<sup>40</sup> 2026 Guidelines, operative paras 41–46, pp 27–30, and para 123, p 53.

<sup>41</sup> 2026 Guidelines, operative paras 65–67, p 36, and paras 117–122, pp 52–53.

# Outlook

The final framework makes recurring non-ICT support a more explicit part of third-party governance, with differentiated controls and substantive exclusions. The useful first step is a defensible service and entity assessment that directs remediation to the arrangements and decisions that matter.

That assessment should expose unresolved dependencies before a renewal, operating-model change or acquisition fixes them into the business. Contract rights, local oversight evidence and transition capacity should be assessed together, so that a documented arrangement also supports continuity in practice.



## About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from relevant related developments. We have assembled a multi-disciplinary and multi-jurisdictional team of sector experts to support clients navigate challenges and seize opportunities as well as to proactively engage with their market stakeholders and regulators.

Moreover, we have developed a number of RegTech and SupTech tools for supervised firms, including PwC Legal's Rule Scanner tool, backed by a trusted set of managed solutions from PwC Legal Business Solutions, allowing for horizon scanning and risk mapping of all legislative and regulatory developments as well as sanctions and fines from multiple thousands of legislative and regulatory policymakers and other industry voices in over 170 jurisdictions impacting financial services firms and their business.

Equally, in leveraging our Rule Scanner technology, we offer a further solution for clients to digitise financial services firms' relevant internal policies and procedures, create a comprehensive documentation inventory with an established documentation hierarchy and embedded glossary that has version control over a defined backward plus forward looking timeline to be able to ensure changes in one policy are carried through over to other policy and procedure documents, critical path dependencies are mapped and legislative and regulatory developments are flagged where these may require actions to be taken in such policies and procedures.

The PwC Legal Team behind Rule Scanner are proud recipients of ALM Law.com's coveted "2024 Disruptive Technology of the Year Award" and the "2025 Regulatory, Governance and Compliance Technology Award in 2025".

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via [de\\_regcore@pwc.com](mailto:de_regcore@pwc.com) or our [website](#).



### Contact

**Dr. Michael Huertas**  
Tel: +49 160 97375760  
[michael.huertas@pwc.com](mailto:michael.huertas@pwc.com)

**EU RegCORE Team**  
[de\\_regcore@pwc.com](mailto:de_regcore@pwc.com)

