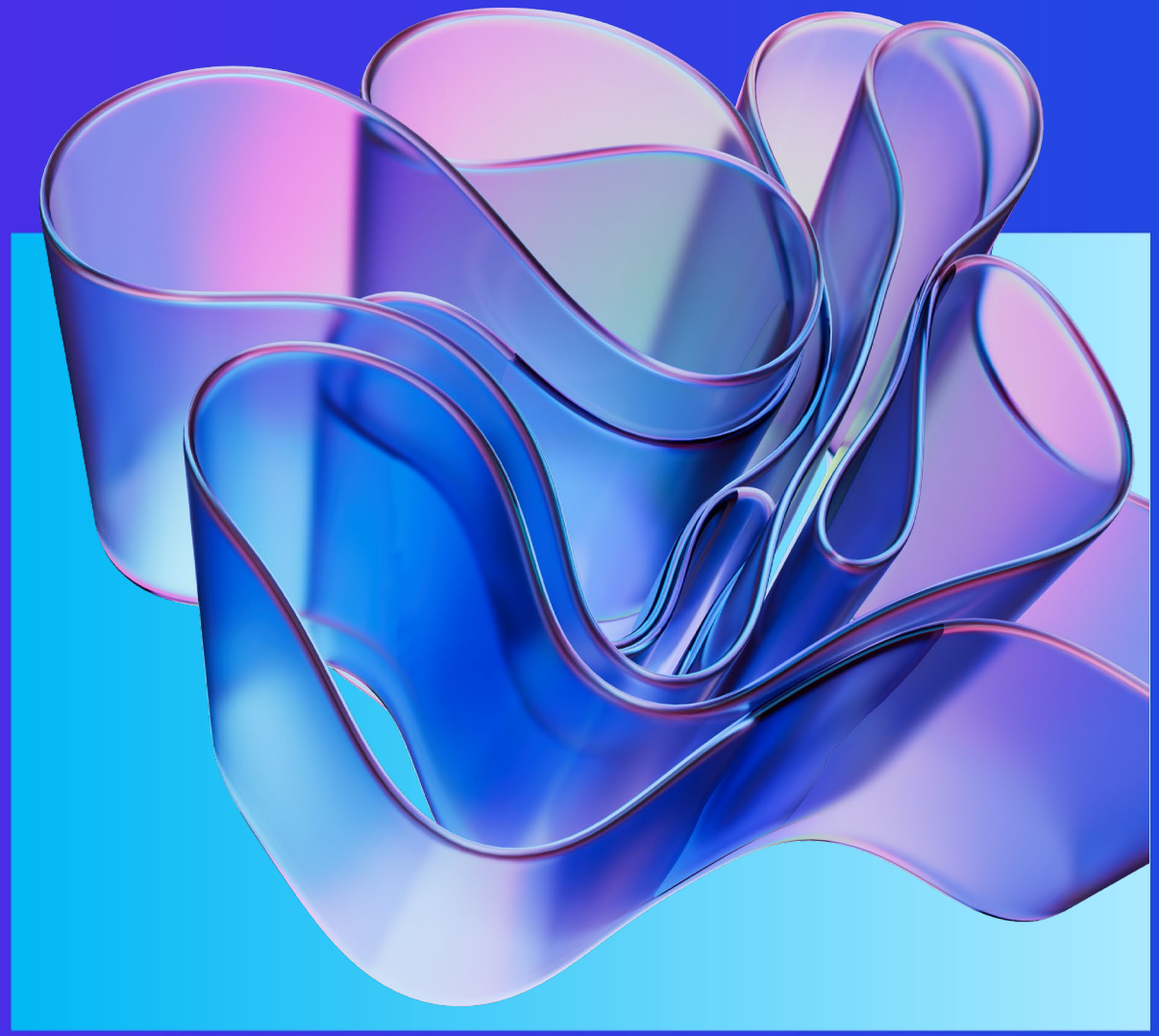
KPMG

From Compliance to Capability



A Benchmark Analysis of DORA integration into Business-as-usual Operating Models

—

July 2026

Table of contents

01	Introduction	3
02	Executive summary	6
03	ICT risk management	10
04	ICT-related incident management	18
05	Third-party risk management	22
06	DOR testing and audit	29



© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Introduction

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

From compliance to capability – Background and objective



Context

- The **Digital Operational Resilience Act** (Regulation (EU) 2022/2554 – DORA), applicable from 17 January 2025, **requires financial entities to establish a comprehensive framework** aimed at **strengthening their digital operational resilience,** by defining and integrating processes related to **ICT risk management, incident management, security testing,** and **third-party risk oversight.**



Purpose

- Within this evolving context, the **KPMG DORA EMA Working Group** has completed a **benchmarking exercise,** the results of which are reported within this document, to assess **how leading financial institutions** operating in the European market **are embedding DORA requirements into their business-as-usual digital resilience frameworks,** with a specific focus on the **operationalisation of compliance within day-to-day processes and governance,** in order to capture current practices, identify common challenges, and highlight emerging trends.



Scope

- The **survey was conducted between February and March 2026,** involving **leading financial entities** operating across the **European market,** ranging from **small and medium-sized enterprises to large institutions.** Responses were provided by multiple business functions, ensuring a comprehensive and cross-functional perspective. In particular, participants included professionals from risk management, information security, and control functions, among others, reflecting the multidisciplinary nature of DORA implementation and its impact across different areas of the organisation.



Structure

- The survey **primarily consisted of closed-ended questions,** including both single-choice and multiple-choice formats, but **respondents were provided with the opportunity to include supplementary qualitative input through optional open-text fields.** Questions covered the following topics: ICT risk management, ICT-related incident management, third-party risk management, digital operational resilience (DOR), DOR testing and audit.

Focus: Scope – Next slides

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Focus: survey scope

>70 financial institutions

17 participating countries

4 peer groups

42 questions

Peer groups are defined based on size in terms of **turn-over/balance sheet** (BS) or gross written premiums:

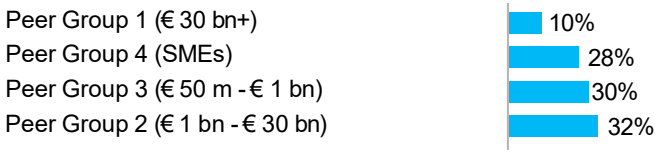
1. **Peer group 1:** Very large financial entities with turnover/BS total of **€ 30 bn or more** (≈10% of respondents);
2. **Peer group 2:** Large financial entities with turnover/BS total **over € 1 bn up to € 30 bn** (≈32% of respondents);
3. **Peer group 3:** Financial entities with turnover/BS total **over € 50 m up to € 1 bn** (≈30% of respondents);
4. **Peer group 4:** Financial entities classified as micro, small or medium enterprises (**SMEs**) (≈29% of respondents).

Participating countries

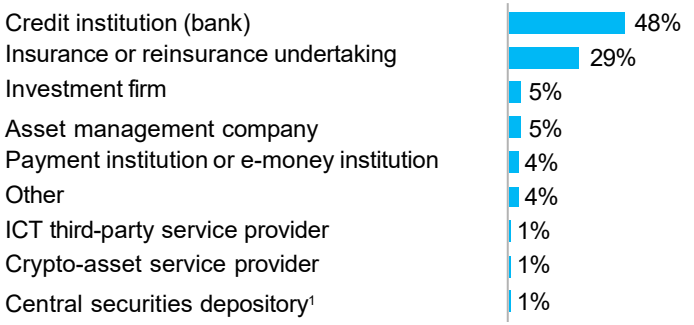
- Austria
- Belgium
- Cyprus
- Finland
- France
- Germany
- Greece
- Ireland
- Italy
- Lithuania
- Netherlands
- Portugal
- Romania
- Spain
- Sweden
- Switzerland
- UK



Peer group distribution (ascending order)

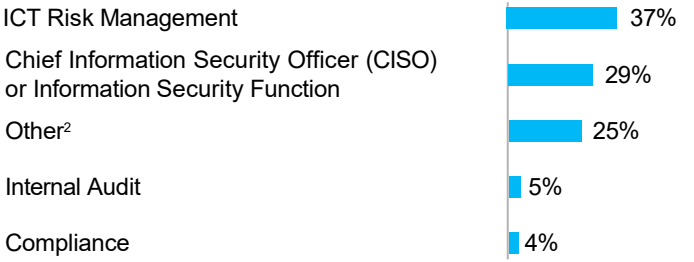


Types of organisations involved



[1] Central securities depository or central counterparty

Respondents' role



[2] e.g., management, operations...

Respondents' geographical scope



Across the entire presentation, percentages are displayed without decimal places. Consequently, minor rounding differences may occur, leading to totals that do not sum exactly to 100%.

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Executive summary

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Executive summary – Key benchmark messages

Reading the benchmark

The integration of **DORA requirements into business-as-usual digital resilience frameworks** does not follow a uniform path: the benchmark shows uneven maturity levels across the investigated domains[1], with **significant differences in operational evidence.**

Key takeaway

The benchmark points to one clear next step: execution quality and operational evidence across all domains – not another round of governance redesign.

01

Governance is integrated, but evidence of implementation still lags

Governance models have been built into business-as-usual frameworks across most domains. Roles, policies, and documented artefacts are largely in place, but the benchmark consistently shows that formal design is more mature than the operational evidence that those arrangements work under stress.

02

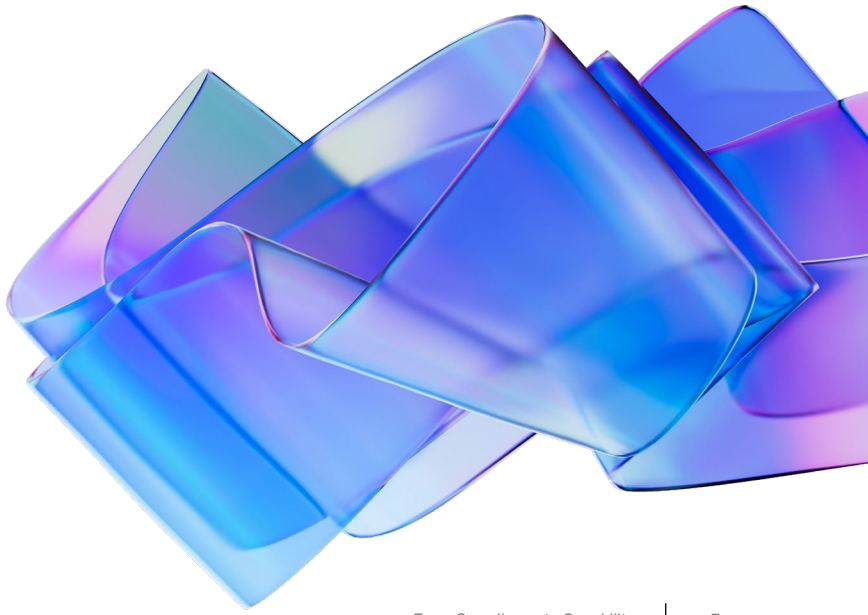
Implementation priority is risk-weighted, not uniform

Institutions are sequencing efforts with a risk-based approach, in line with legislative requirements, focusing on CIF-supporting providers and assets and TLPT-designated testing, while consciously accepting maturity asymmetries elsewhere in the perimeter.

03

Maturity is shaped by methodology, not only by investment

CIF identification approach, asset derivation method, and impact-metric choices produce materially different outcomes under identical governance structures, confirming that the manner of implementation matters as much as the amounts invested.

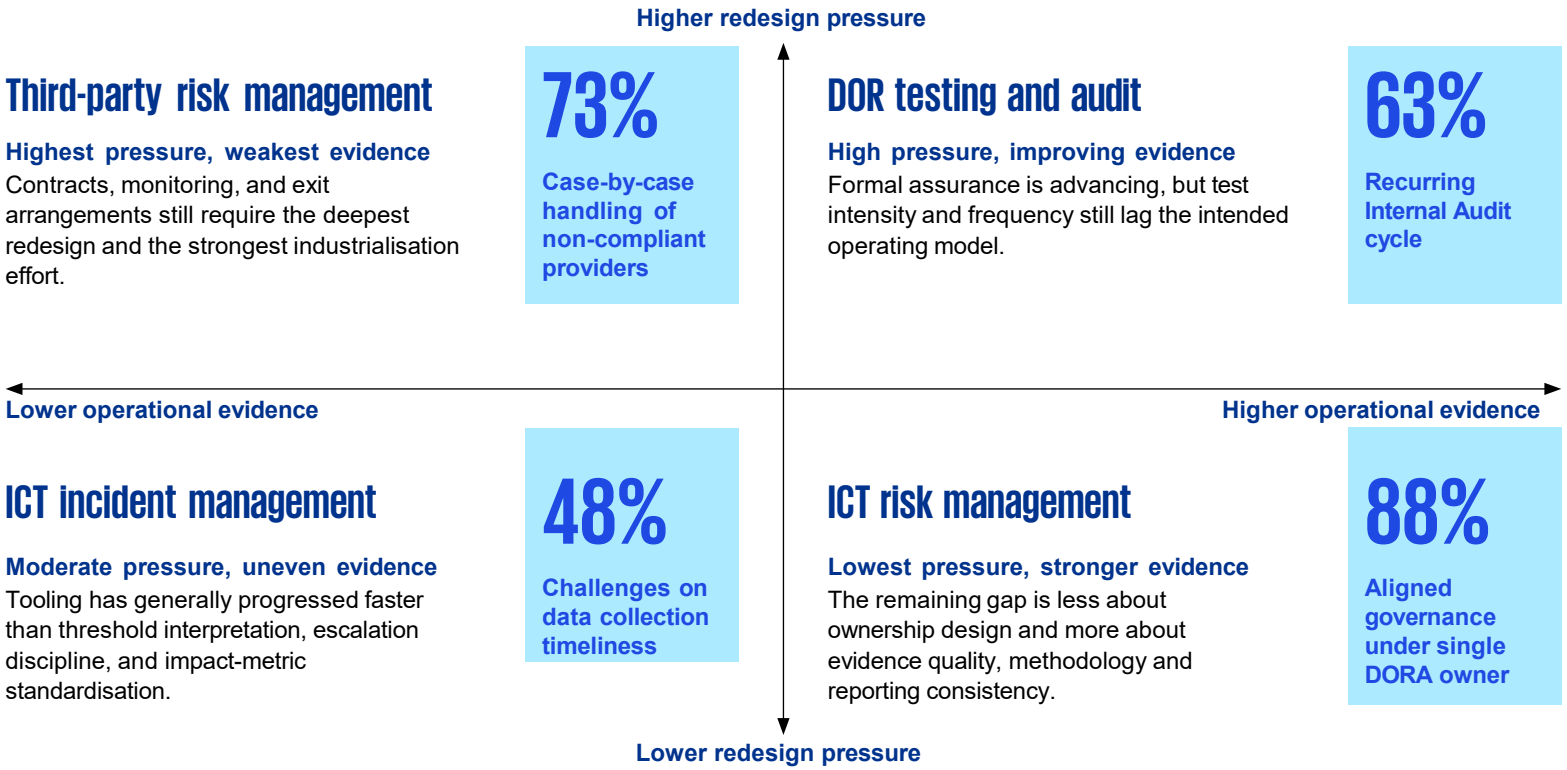


[1] ICT risk management, ICT-related incident management, third-party risk management, DOR testing and audit

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Executive summary – How the four domains compare

The benchmark assessed the extent to which the **safeguards related to the four pillars** illustrated below have been **embedded into business-as-usual operations and governance processes.** The analysis highlighted domains where **further integration and operationalisation efforts are still required,** as well as areas where redesign actions are needed to achieve a more sustainable and effective business-as-usual resilience framework.



Positioning rationale

The four DORA domains do not sit at the same point in the journey: they combine different levels of redesign pressure and operational evidence.

Key takeaway

The positioning shows that TPRM and testing face the highest redesign pressure, while ICT Risk Management and incident management more often build on existing foundations and need better operational evidence rather than another structural redesign.

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Executive summary – State of play across the four DORA pillars

ICT risk management

66% **assign DORA accountability to a single named executive (CRO, CIO, COO or CEO).**

Among these, 88% have established a formalised ICT RM control function, confirming that clear ownership translates directly into structured governance.

ICT incident management

56% **enhanced an existing SIEM rather than replacing it.**

Tooling investment is broadly complete; the remaining DORA gaps in incident management are concentrated in classification thresholds and escalation protocols.

Third-party risk management

51% **have renegotiated more than 75% of their CIF-supporting contracts.**

Progress is risk-led: CIF relationships are being remediated ahead of non-critical providers, reflecting a deliberate sequencing by criticality rather than uniform coverage.

DOR testing and audit

33% **operate an annual CIF-focused testing calendar, the most common testing pattern observed.**

The testing calendar remains less mature than the assurance framework around it: audit formalisation has advanced faster than the intensity and frequency of operational testing.

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

ICT risk management



© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

ICT risk management – Executive summary

ICT risk management (hereinafter also “RM”) is the **most structurally advanced domain** in the benchmark. **Governance ownership** is already largely defined, **CIF and asset-classification approaches** are converging, and **reporting capabilities** are progressing. The remaining maturity gap is not **basic design,** but the consistency with which **classification choices, tooling, and metrics** translate into a **robust resilience evidence base.**

ICT governance and responsibilities

Among institutions assigning **DOR accountability** to a **single executive owner, 88%** have established a **formalised ICT risk management control function.** Hence **institutions enter DORA with a solid governance foundation,** leaving the main challenge less in redesigning accountability and **more in embedding DOR requirements into day-to-day execution.**

CIFs and asset mapping

Methodological choices remain a primary driver of the **effective digital resilience perimeter.** Institutions adopting a **DORA-based CIF identification approach** report materially **broader CIF scopes,** while **scope of asset** supporting CIFs **varies significantly depending on whether filter logic or full inheritance method is applied.**

Tooling and reporting

The adoption of **GRC tooling** enhances **reporting maturity** on **Digital Operational Resilience**, enabling more consistent **board-level oversight** through **structured reporting cadences** across most institutions. However, while **reporting governance** has progressed, the underlying **KPI/KRI framework** often **lags,** remaining **under development** or **insufficiently granular.**



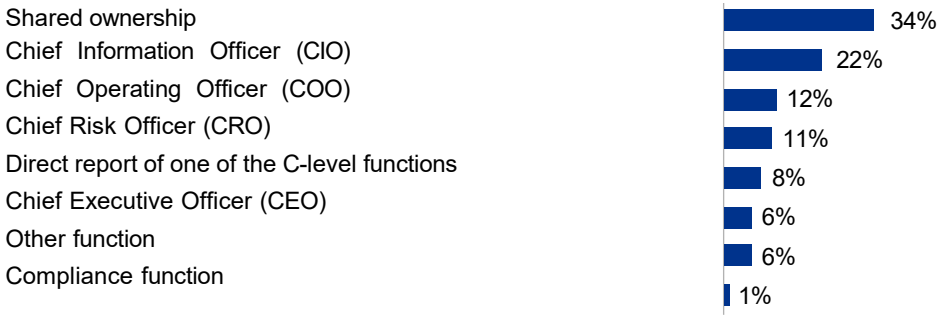
Executive takeaway

ICT risk management is no longer a **design problem** for most institutions; it is an **evidence-quality problem,** where **methodology and metric choices** still shape how **resilience** is actually demonstrated.

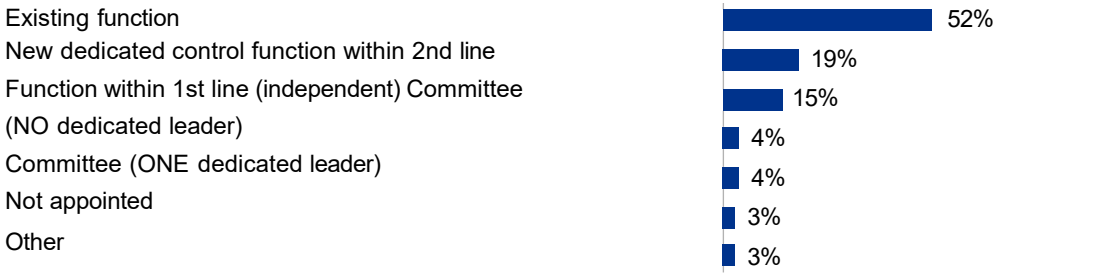
© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

ICT RM – Ownership aligns with structured control setup

Assignment of overall responsibility for DOR



Assignment of responsibilities for ICT RM control function



Percentages are shown as whole numbers; totals do not sum to exactly 100% due to rounding.

Insights

88% governance alignment

The **clear assignment of DOR-related responsibilities** is closely linked to the **allocation of ICT risk management** responsibilities to **a single organisational function.** Among the **43** institutions where **DORA accountability** is assigned **to a single named executive** (CRO, CIO, COO, CEO, or a direct report), **88%** have established a **formalised ICT risk management control function,** as an existing function, an independent first-line function, or a newly dedicated second-line function.

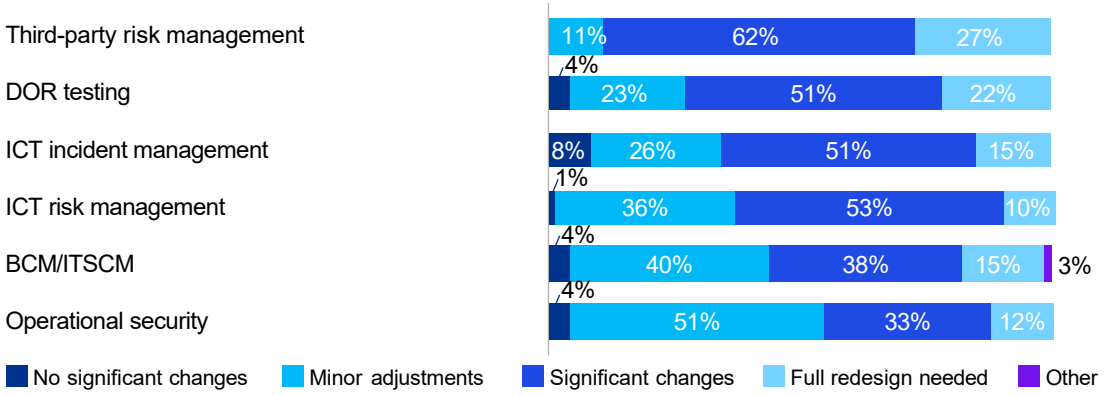
Key takeaway

In order to integrate digital operational resilience into business-as-usual processes, the majority of respondents have allocated risk management responsibilities to already existing corporate functions. Furthermore, 43 of 73 respondents favour the assignment of overall DORA responsibility to a single designated role.

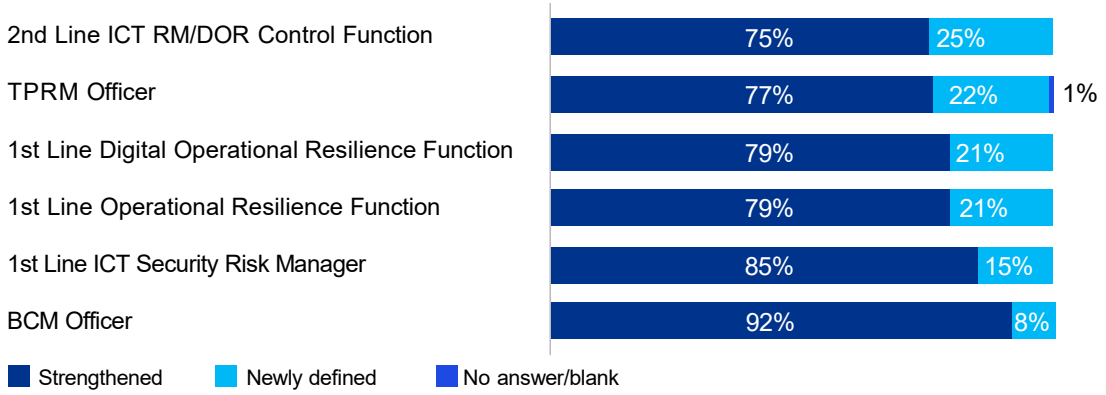
© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

ICT RM – DORA impact drives targeted role creation

DORA impact by domain



Roles evolution in response to DORA



Insights

89% **institutions – TPRM requires new or redesigned processes**

The implementation of **DORA requirements** within **third-party risk management** required **89% of institutions** to implement **significant changes or a full redesign**, the **highest rate of any domain**. **DOR Testing** follows at **73%**. The **organisational response** mirrors the disruption: the roles with the **highest new-creation rate** are the 2nd-line **ICT RM Control function** (**25%**) and the **TPRM Officer** (**22%**). The main exception is **BCM/ITSCM**: despite **53% of institutions reporting significant impact or full redesign**, only **8% created a new BCM Officer**, indicating that the function was **already well-established before DORA**.

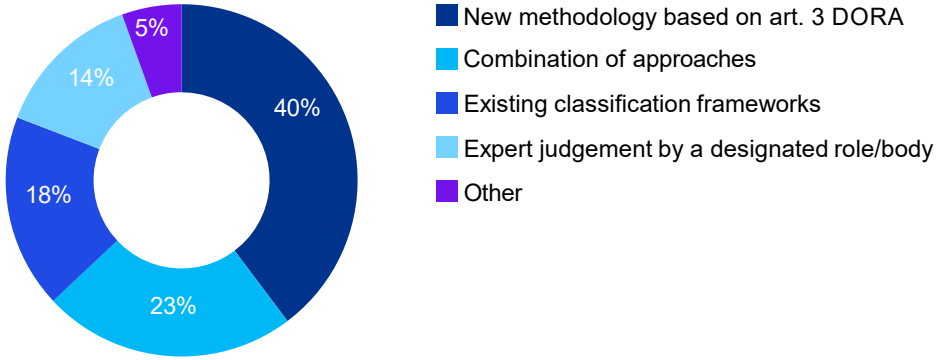
Key takeaway

DORA reshapes organisational structures selectively. Domains that required the deepest rethinking are also those driving the creation of dedicated new roles. Where functions such as BCM were already mature, institutions have opted to strengthen existing roles rather than create new ones, confirming that the degree of pre-DORA maturity is the primary predictor of role creation vs. role enhancement.

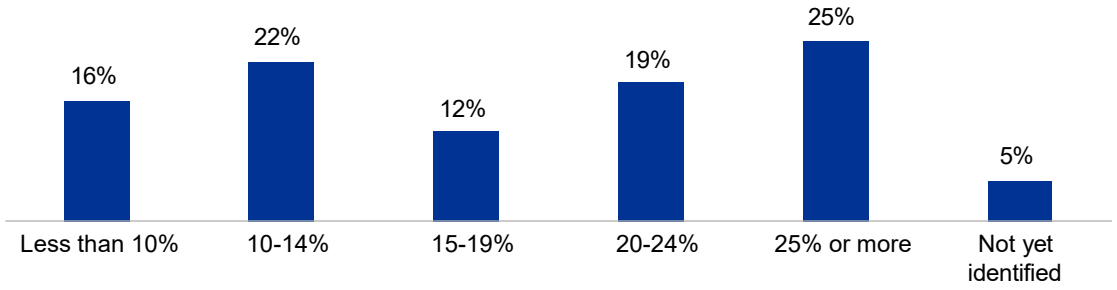
© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

ICT RM – Formal CIF methodology expands identified scope

CIF identification method



Share of processes classified as CIFs



Percentages are shown as whole numbers; totals do not sum to exactly 100% due to rounding.

Insights

34% **DORA method users ≥25% CIFs**

The **DORA-based method,** adopted by **40% of institutions,** making it the **most widely used approach,** is strongly associated with a **broader CIF scope.** Among the **29 institutions adopting the DORA method, 34% classify 25% or more** of their processes as **CIFs,** compared to **25% across the full benchmark sample.** This suggests that grounding the **identification methodology** directly in the **regulatory definition** tends to surface a **wider set of critical functions.**

Key takeaway

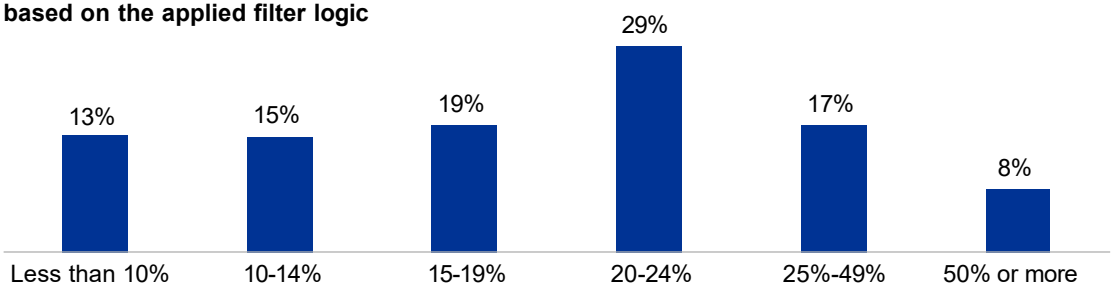
The methodology adopted to identify CIFs has a direct impact on the reported CIF scope. The DORA-based approach is the most widely adopted and is typically associated with a broader CIF identification.

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

ICT RM – Asset criticality depends on derivation method

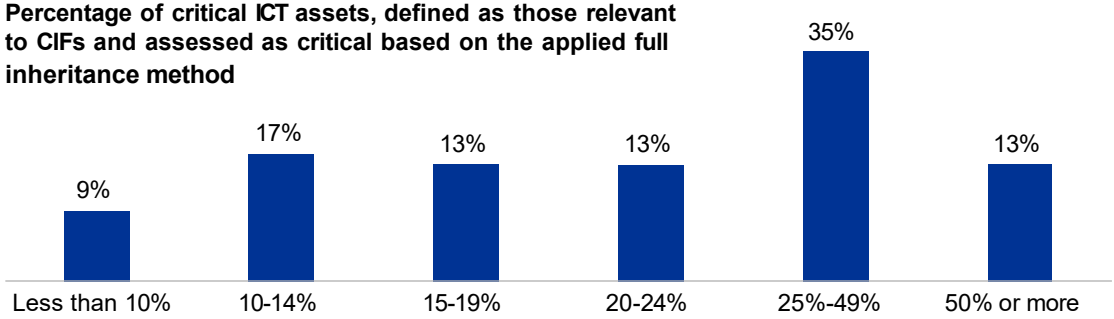
Filter logic approach[1]

Percentage of critical ICT assets, defined as those relevant to CIFs and assessed as critical based on the applied filter logic



Full inheritance approach[2]

Percentage of critical ICT assets, defined as those relevant to CIFs and assessed as critical based on the applied full inheritance method



Percentages are shown as whole numbers; totals do not sum to exactly 100% due to rounding.

Insights

66% of institutions apply **filter logic** to derive **critical ICT assets,** the most widely adopted approach, used by **48 of 73 respondents.** Among these, the **critical asset share** is concentrated in the **20-24% range,** with only **4 institutions exceeding 50%.**

32% of institutions applying **full inheritance,** used by **23 of 73 respondents.** There is a shift toward **higher critical-asset shares** compared to **filter logic users:** the **modal group** falls in the **25-49% range,** and the proportion reporting **above 25%** is greater than among **filter logic adopters.**

Key takeaway

The approach used to map assets supporting CIFs directly influences the proportion of identified supporting assets. Among respondents, the filter logic approach is the most commonly adopted and leads to the identification of a broader set of CIF-supporting assets compared to the full inheritance approach.

[1] Filter logic approach: not all ICT assets supporting a CIF are automatically classified as critical; specific criteria are applied to determine that.
[2] Full inheritance approach: all ICT assets supporting a CIF are automatically classified as critical.

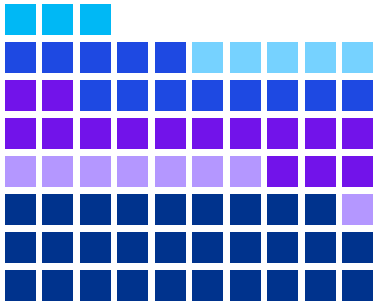
© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

ICT RM – GRC tooling drives reporting maturity

GRC tool selection

GRC solution models adopted to support integrated ICT risk management

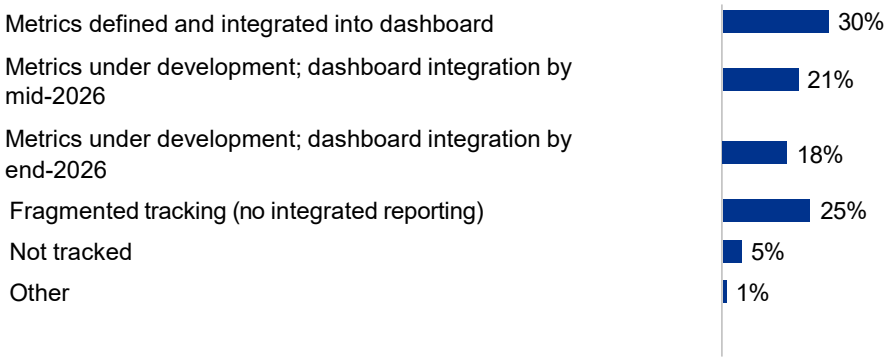
Other	4%
Internally developed tool	7%
Planned (not yet implemented)	18%
third-party solution	32%
Dashboard-integrated metrics within 3rd-party solution	**35%**
Plurality of specific solutions	40%



Percentages are shown as whole numbers; totals do not sum to exactly 100% due to rounding.

Reporting maturity level

Status of DORA-specific resilience metrics definition and dashboard integration



Insights

35% 3rd-party → full dashboard

Third-party GRC solutions, adopted by **32%** of institutions, making them the **second most common approach,** show a meaningful association with **higher reporting maturity.** Among the **23 institutions using GRC tools, 35%** already report **fully dashboard-integrated ICT RM metrics,** compared to **23%** across the full benchmark sample. This suggests that institutions relying on a **dedicated third-party platform** are more likely to have reached the **highest level of reporting integration.**

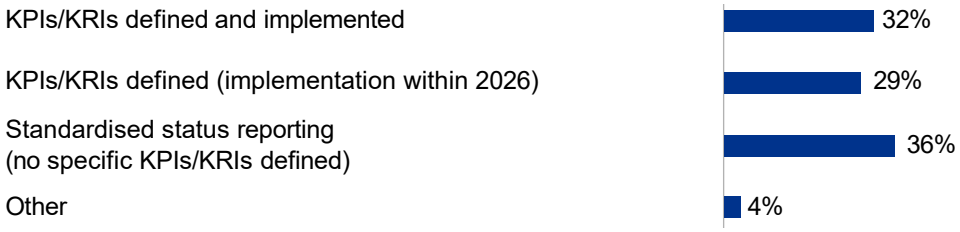
Key takeaway

Tooling alone does not guarantee reporting maturity. Third-party solutions show a stronger association with fully integrated reporting than fragmented multi-tool setups, but the advantage is narrow and should not be overstated.

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

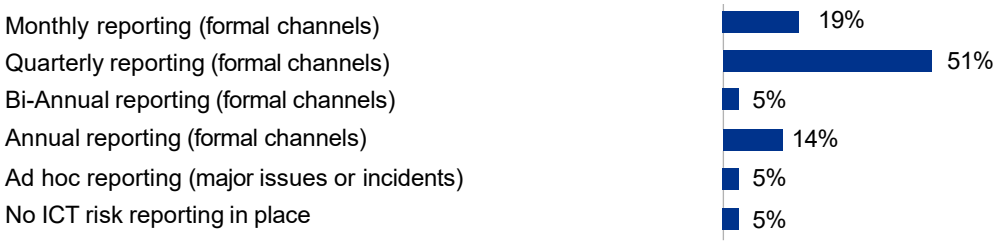
ICT RM – Board reporting cadence outpaces KPI/KRI maturity

KPI/KRI implementation for DOR strategy



Multiple answers allowed; percentages refer to respondents selecting each option, so totals may exceed 100%.

Board digital resilience reporting frequency



Percentages are shown as whole numbers; totals do not sum to exactly 100% due to rounding.

Insights

70% **Monthly or quarterly report to the board**

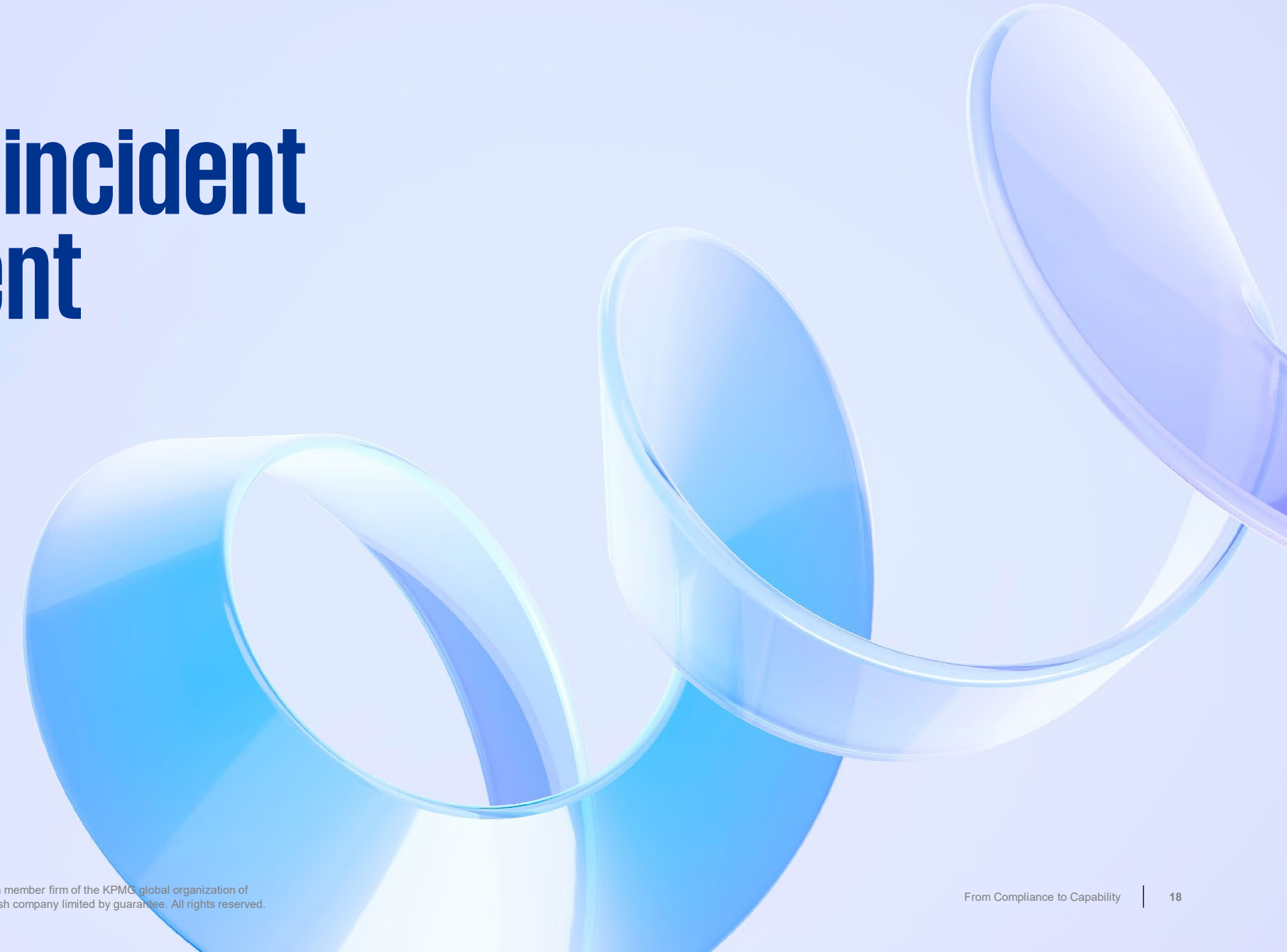
Board oversight of **digital resilience** is already structured across the market, **with 51%** of institutions **reporting quarterly** and a further **19% reporting monthly** through **formal channels**. However, **measurement maturity** is less advanced: only **32%** of institutions **have KPIs/KRIs** already **defined and implemented**, while **29% are still targeting implementation by 2026**, and **36% still rely on standardised status reporting** without specific KPIs/KRIs. Overall, **reporting routines** appear to be **maturing faster** than the underlying **performance measurement framework.**

Key takeaway

Board oversight of digital resilience is supported by a relatively structured reporting cadence across most institutions. However, reporting governance has advanced faster than the underlying KPI/KRI framework, which often remains under development or not yet sufficiently specific.

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

ICT-related incident management



© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Incident management – Executive summary

Incident management appears **more mature** in its **monitoring backbone** than in its **reporting and measurement layer.** Most institutions are building on an **existing SIEM foundation,** but the benchmark still points to **residual weaknesses** in **threshold interpretation, escalation discipline,** and **impact-metric standardisation.**

Monitoring foundation

The **tooling base is broadly in place. 56%** of institutions already had a SIEM solution and **enhanced it for DORA** rather than replacing it entirely. This suggests that DORA has mainly **accelerated capability uplift** instead of driving a **wholesale redesign** of the **monitoring stack.**

Governance frictions

Even where SIEM capabilities are well established, **the most persistent DORA gaps lie outside the platform layer, particularly in threshold classification and escalation design.** Even institutions with an **enhanced SIEM base** cite **DORA threshold classification** and **escalation streamlining** as key lessons learned that have to be addressed.

Classification metric standardisation

Institutions are applying the Regulatory Technical Standards requirements[1] on **the classification** of ICT-related incidents **through different operational approaches** when determining the comparable reference period and the transaction-time reference used to assess impact. **These approaches are not always clearly defined or systematically applied.**

Executive takeaway

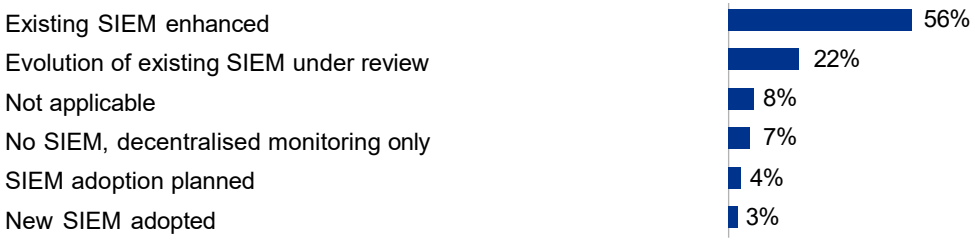
Incident management appears operationally more mature than analytically mature: the monitoring base is largely in place, but classification logic, escalation discipline, and impact metrics remain less standardised.

[1] Regulatory Technical Standards on criteria for the classification of ICT-related incidents

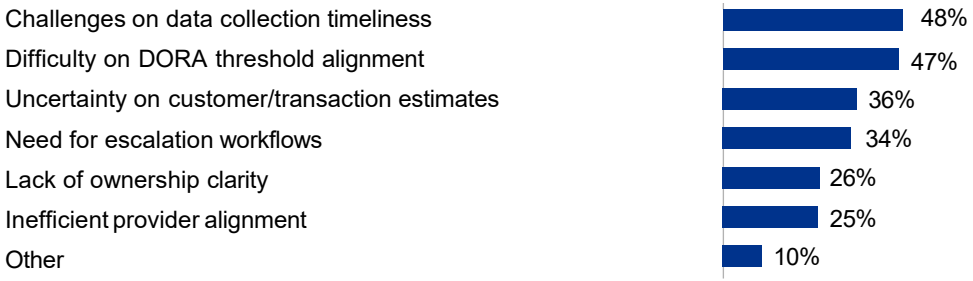
© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Incident management – Tools maturity and lessons learned

SIEM[1] implementation status for DORA compliance



Incident reporting lessons learned



Multiple answers allowed; percentages refer to respondents selecting each option, so totals may exceed 100%.

Insights

56% enhanced SIEM base

Most institutions entered **DORA** with a **SIEM foundation: 56%** of the benchmark sample retained an existing solution and enhanced it for **DORA.** Yet **tooling does not remove reporting complexity.** Within that subgroup of **41 institutions**, **51%** still cite **DORA threshold classification** as a **key lesson learned** and **37%** cite **escalation streamlining needs,** indicating that **incident reporting readiness** depends on **governance and data interpretation** as much as on **monitoring technology.**

Key takeaway

SIEM maturity supports DORA implementation, but it is not sufficient on its own. The hardest residual issues still sit in classification, escalation, and reporting-data quality rather than in the selection of a monitoring platform.

[1] Security Information and Event Management solution

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Incident management – Impact metrics remain non-standardised

Comparable reference periods



Transaction time reference



Percentages are shown as whole numbers; totals do not sum to exactly 100% due to rounding.

Insights

52% **non-standard timing basis**

Institutions are applying the **EBA RTS on the classification of ICT-related incidents**[1] through different operational approaches when determining the **comparable reference period** (ref. Article 1) and the **transaction time reference** (ref. Article 9) used to assess impact. For the comparable reference period, **35%** rely on **BAU-like periods,** while **38%** either report **no formal methodology** or **do not know** how the reference period is selected. For transaction-time reference, approaches are similarly mixed: **30%** base the metric on the **type of service,** while **22%** do not know which reference is used. This shows that RTS-based classification is being implemented, but not yet through a consistent **measurement logic**.

Key takeaway

EBA RTS requirements are being adopted, but incident impact classification is still driven by heterogeneous and often weakly defined reference-period methodologies.

[1] Regulatory Technical Standards on criteria for the classification of ICT-related incidents

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Third-party risk management

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Third-party risk management – Executive summary

Third-party risk management (hereinafter also “TPRM”) **is progressing most visibly on critical ICT service providers**. Institutions are prioritising **contract remediation** and **exit strategy** definition on **CIF-supporting providers**, but the benchmark still shows **reactive execution patterns** in **assurance and exit testing.**

Contract remediation

Contract remediation is being **prioritised where exposure to risk is highest. CIF-supporting providers** are **ahead** of non-CIF relationships in **contract renegotiation progress,** showing that institutions are sequencing implementation around **critical dependency** rather than applying the same pace across the **full estate.**

Monitoring and assurance

Assurance practices largely rely on **third-party certifications** and **external audits.** However, among institutions disclosing **audit frequency,** only **31%** conduct **annual audits on CIF-supporting providers,** with the rest using **less frequent** or **ad hoc reviews.** This indicates that **external assurance** often substitutes rather than complements **structured, recurring internal oversight.**

Exit readiness

Exit planning is advancing **faster than exit testing.** Many institutions have documented or are developing **exit strategies** for **CIF-supporting providers,** but a majority still lack **structured exit-plan testing. Exit resilience** is therefore increasingly **defined on paper,** but not yet consistently **demonstrated operationally.**



Executive takeaway

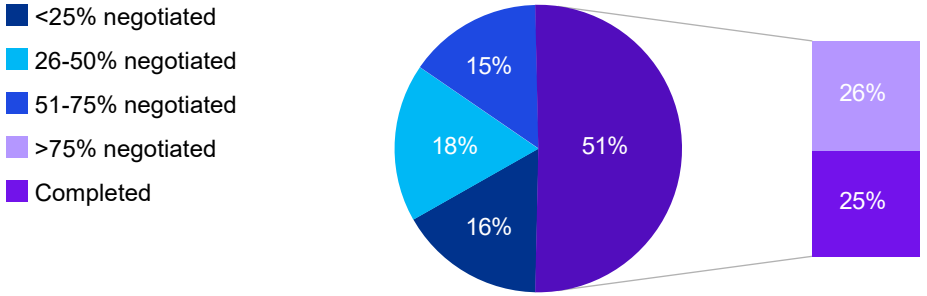
TPRM progress is **clearest** in **prioritisation** and **governance design,** but the benchmark still points to a **delivery model** that remains **partly reactive** in **negotiation, assurance,** and **exit validation.**

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

TPRM – Contract renegotiation is prioritised on CIF providers

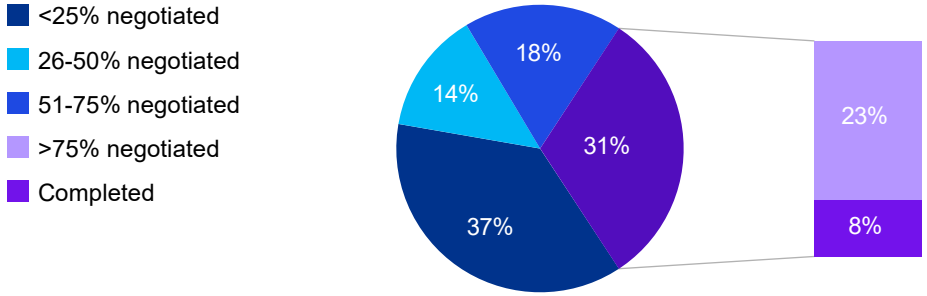
CIF-supporting contracts

Status of renegotiation of ICT service provider contracts to comply with DOR



Non-CIF-supporting contracts

Status of renegotiation of ICT service provider contracts to comply with DORA



Insights

51% **advanced CIF-supporting ICT providers contract renegotiation**

Contract integration is clearly prioritised on **CIF-supporting ICT providers. 51% of institutions** report that **more than 75% of CIF-supporting contracts** are already **renegotiated or the renegotiation has been fully completed,** compared with only **32% for non-CIF-supporting contracts.**

Key takeaway

The benchmark highlights a two-speed approach to ICT contract remediation to ensure DORA compliance. Institutions are prioritising the integration of regulatory requirements into contracts with CIF-supporting ICT providers, while the alignment of non-CIF contracts is progressing more gradually.

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

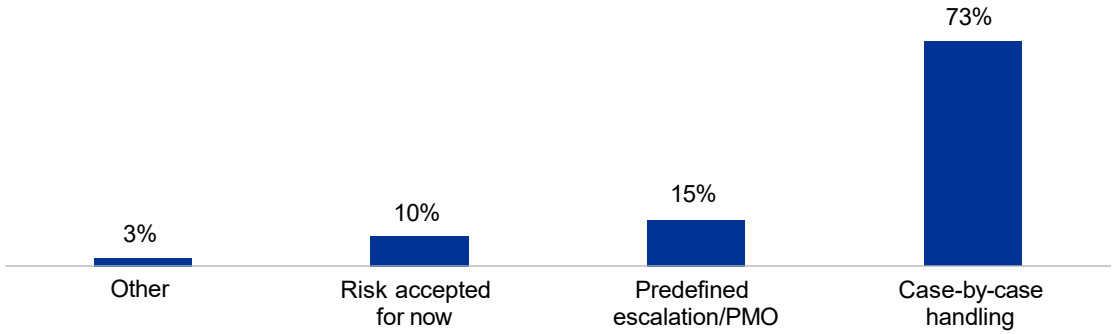
TPRM – Contract frictions still trigger reactive handling

Main negotiation challenges



Multiple answers allowed; percentages refer to respondents selecting each option, so totals may exceed 100%.

Approach for handling non-compliant providers



Percentages are shown as whole numbers; totals do not sum to exactly 100% due to rounding.

Insights

73% case-by-case handling

ICT contract re-negotiation pressure is concentrated on **provider-side frictions.** Long negotiation timelines (cited by **71% of institutions**) and resistance to **DORA-specific clauses** (cited by **70%**) are the main challenges to address in the compliance process. There is a lack of structured processes to manage these challenges: **73% of institutions** handle them **case by case,** while only **15%** report having a **predefined escalation and risk assessment process.**

Key takeaway

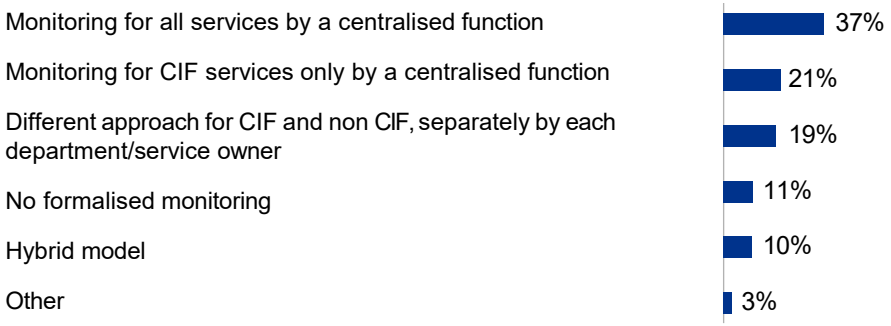
Challenges related to the evolution of contractual clauses with ICT service providers to ensure DORA compliance are still more often absorbed reactively than through a standardised remediation approach.

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

TPRM – Monitoring maturity shapes audit strategy

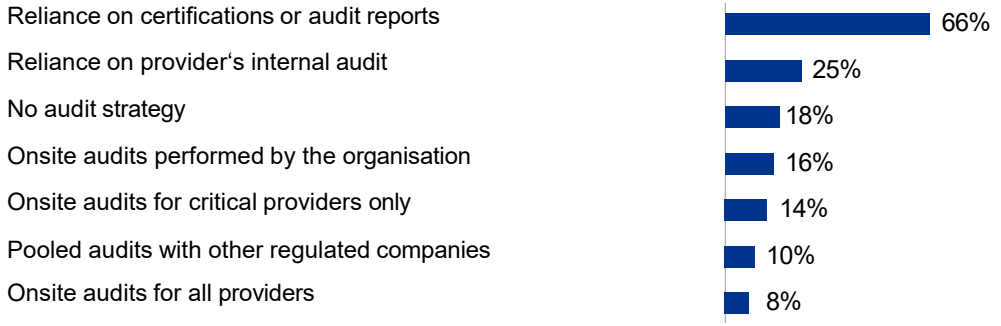
Monitoring of ICT service providers approach

Status of implementation and monitoring of providers (CIF and non-CIF supporting)



Percentages are shown as whole numbers; totals do not sum to exactly 100% due to rounding.

Audit strategy for providers supporting CIFs



Multiple answers allowed; percentages refer to respondents selecting each option, so totals may exceed 100%.

Insights

85% certification reliance

ICT third parties monitoring maturity is closely linked to **audit discipline.** Among the **27 institutions** with **centralised monitoring** across both CIF and non-CIF services, **85%** rely on **third-party certifications** or **audit reports** as a **core oversight mechanism** and only **4%** report that **no audit strategy** is in place. Moreover, among the **8 institutions** without a **formalised monitoring process, 63%** also report having **no audit strategy for providers supporting CIFs,** indicating that **weak monitoring design** translates directly into **weaker assurance coverage.**

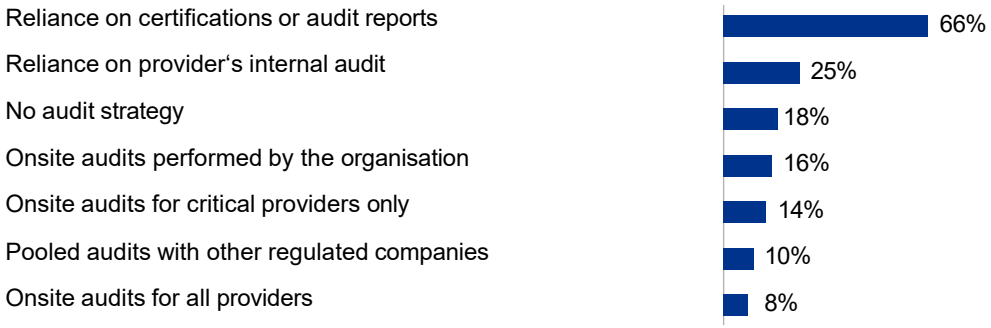
Key takeaway

A mature third-party monitoring model creates the conditions for a credible third-party assurance strategy. Where monitoring is centralised, institutions are better able to structure audit evidence; where monitoring is not formalised, assurance tends to remain reactive or undefined.

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

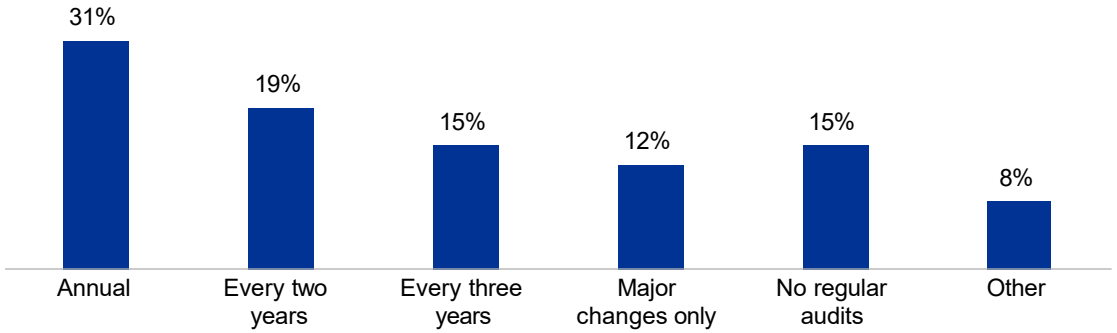
TPRM – Audit execution remains certification-led

Audit strategy for providers supporting CIFs



Multiple answers allowed; percentages refer to respondents selecting each option, so totals may exceed 100%.

Audit frequency on ICT providers supporting CIFs



Insights

66% certification-led oversight

Third-party certifications and **audit reports** form the **primary assurance foundation,** used by **66% of institutions.** Yet this strategy masks a **critical execution gap:** among institutions that specified **audit frequency,** only **31% conduct annual audits** on **CIF-supporting providers,** while the rest **audit less regularly** or have **no systematic schedule.** This disconnect suggests that many organisations default to **external certifications** precisely because they lack the **resources** or **governance cadence** for **structured internal oversight.**

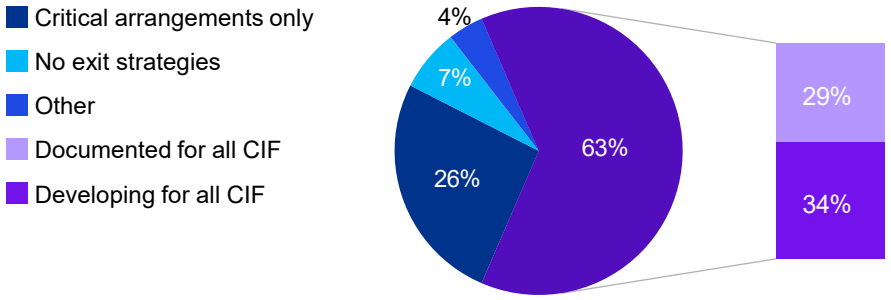
Key takeaway

The benchmark points to an assurance model that leans heavily on external evidence. Direct audit execution exists, but it is still not consistently translated into an annual inspection rhythm for CIF-supporting providers.

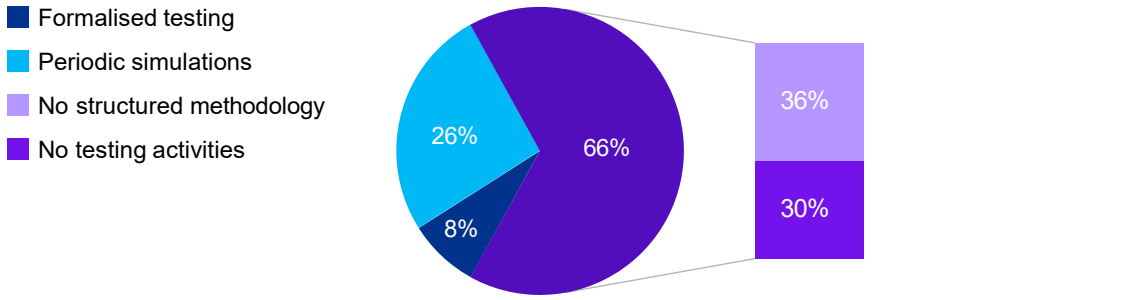
© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

TPRM – Exit planning outpaces exit test maturity

Implementation status of exit strategy



Exit plan testing method



Insights

66% **Immature exit plan testing**

Exit strategy planning for ICT providers supporting CIFs is materially **ahead** of **exit testing. 63% of institutions** report that **exit strategies** are either **already documented** for all **CIF-supporting providers** or are being developed toward that state. Yet **66%** either have **no structured testing methodology** or **no exit plan testing activities** at all. This suggests that governance frameworks are evolving more rapidly than the corresponding operational validation of their effectiveness under stress.

Key takeaway

Most institutions have recognised the need for formal exit planning, but testing still lags far behind documentation. The benchmark indicates that exit resilience is often evidenced on paper before it is demonstrated operationally.

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

DOR testing and audit



© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

DOR testing and audit – Executive summary

DOR testing and audit point to a **formalised** but **still conservative operating model.** Institutions have generally brought DORA into **recurring assurance cycles,** and **TLPT designation** reinforces **testing calendar discipline,** yet the **broader testing rhythm** still remains **annual-first** rather than fully **risk-intensified.**

Internal assurance baseline

Formal assurance routines are **already established. 63%** of institutions place DORA within an **annual or multi-year internal audit cycle,** showing that the topic has entered the **normal oversight perimeter** rather than remaining a **one-off compliance exercise.**

DOR testing cadence

The **testing calendar is less mature** than the **assurance framework** around it. The benchmark remains centered on **annual CIF-focused testing,** with limited evidence of **higher-frequency or broader-scope patterns. Audit formalisation** has advanced faster than **operational testing intensity.**

TLPT readiness

TLPT expectations reinforce DOR testing calendar discipline where concrete. Among **officially designated institutions, 85%** report at least **annual or more frequent** CIF-focused testing, with none on an **unplanned basis.**

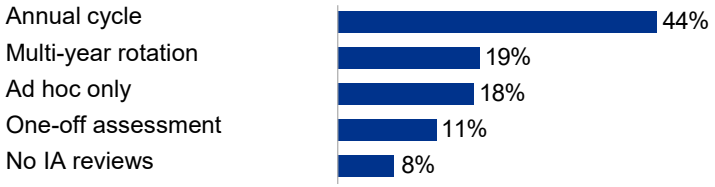
Executive takeaway

DOR **testing model** has entered **recurring oversight,** but institutions still need to translate that **governance baseline** into a **broader** and **more intensive operational testing cadence.**

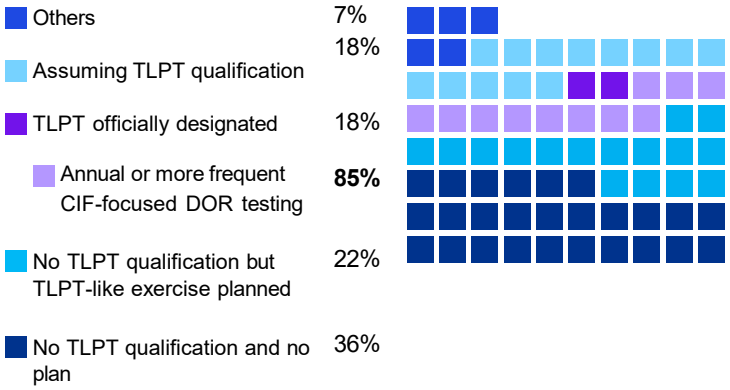
© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

DOR testing and audit – TLPT drives structured assurance

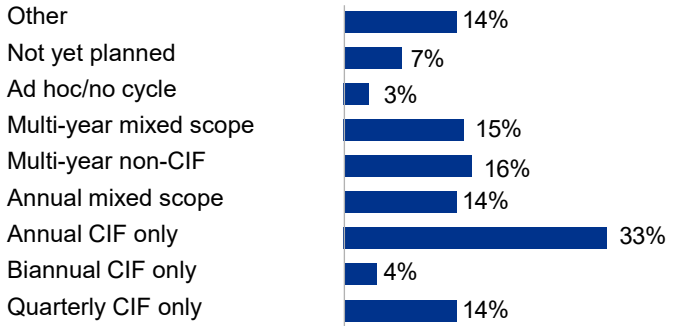
Internal Audit assessment of DORA compliance



TLPT[1] qualification status and planning



DOR testing[2] calendar



Multiple answers allowed; percentages refer to respondents selecting each option, so totals may exceed 100%.

Insights

63% **Recurring Internal Audit cycle**

Formal **internal assurance** on DORA compliance is usually **recurring** (**63%** using annual or multi-year **Internal Audit cycles**), yet the overall **DOR testing calendar remains conservatively concentrated around annual CIF-focused testing.** However, **TLPT readiness** actively reinforces structure: among institutions designated for TLPT, **85%** report at least an annual CIF-focused testing cadence. This suggests that the combination of **structured oversight** and **advanced testing requirements (TLPT)** eliminates ad hoc approaches and drives calendar discipline.

Key takeaway

DORA internal audit assurance is formalised across institutions, but baseline testing cadence remains conservative. Direct regulatory expectations serve as the primary driver for strict calendar discipline, ensuring continuous oversight and reducing deferred or ad hoc testing.

[1] Threat-Led Penetration Testing
[2] Digital Operational Resilience Testing as defined by Article 25 DORA Regulation (e.g. vulnerability scans, network security assessments, penetration tests, performance tests)

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Contacts

KPMG in Italy
KPMG Advisory S.p.A.



Luca Boselli
Partner, Head of
Cyber & Tech Risk
lboselli@kpmg.it



Valerio Ghislandi
Associate Partner
Cyber & Tech Risk
vghislandi@kpmg.it

KPMG in Germany
KPMG AG Wirtschaftsprüfungsgesellschaft



Vaike Metzger
Partner
Financial Services
vmetzger@kpmg.com



Peter Hertlein
Partner
Financial Services
phertlein@kpmg.com

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG Advisory S.p.A., an Italian limited liability share capital company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.