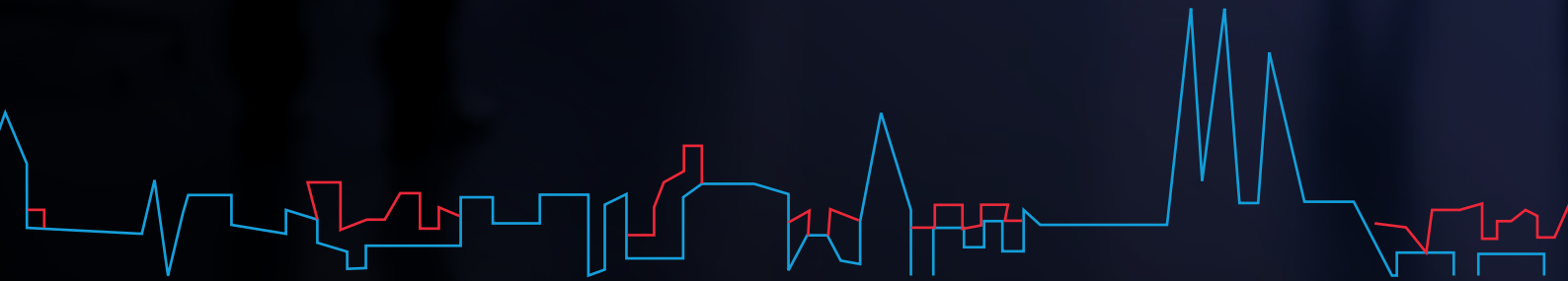
LUXEMBOURG
ALTERNATIVE
ADMINISTRATORS
ASSOCIATION

# DORA

## L3A WORKING GROUP

August 2026



# TABLE OF CONTENTS

LUXEMBOURG ALTERNATIVE ADMINISTRATORS ASSOCIATION

# About L3A

The Luxembourg Alternative Administrators Association ("L3A") is the leading representative body for fund and corporate administrators of alternative assets in Luxembourg.

Since its founding in 2004, the association has been dedicated to promoting the interests of alternative service providers and contributing to the development of Luxembourg as the investment hub and operations centre of choice for global alternative investment managers.

Our members deliver our mission through their work on our 5 permanent committees, being Operations, Tax, Regulatory, HR and Events & Communications, with output delivered to industry players, regulators and government bodies amongst others, and published through our website and social media channels, in particular LinkedIn.
As the recognised voice of our profession, we engage with authorities through participation in commissions and working groups, and maintain strong ties with government bodies, professional organisations, and Chambers of Commerce.

Our membership is made up of over 60 members, including Full Members, being Luxembourg administration firms predominantly providing services to foreign investment managers of funds and related entities in the alternative management industry and Associate Members, being Luxembourg professional firms operating in the real asset environment and offering services to Full Members and/or their clients.

Together, we form a trusted network committed to excellence.

# Contributors

### Working Group Members

- Elena Nalon- AIS
- Daphne Mandel- AIS
- Francesco Giarrusso- CITCO
- Raneisha Leacock- CITCO
- Mohammed Saadi- IRACE Digital Bank
- Amaury Saive- Alter Domus
- Adrian Ross Frando – Vistra
- Johann Lobo - EY

### Coordinators

- Johannes Höring - Waystone
- Norman Finster - EY
- Marta Bawor – L3A

# 1 INTRODUCTION

# DORA

The Digital Operational Resilience Act (DORA) was conceived to enable financial entities across the European Union to manage ICT risk at large, ICT incident response, operational resilience and third-party dependencies. It introduced a harmonized and comprehensive framework that elevates digital resilience from a technical discipline to a core governance priority for management and a regulatory priority.

Against this backdrop, the L3A Working Group has developed this paper to provide practical, industry-driven guidance on key areas of interpretation and implementation of DORA, particularly in the context of the Luxembourg alternative investment ecosystem. While the regulation sets out high-level principles and requirements, it also raises a number of operational, contractual, and interpretative challenges, especially given the complexity of service delivery models, ICT dependencies, and multi-layered third-party arrangements. This document is structured around a series of priority topics identified by industry participants, including what entities fall under the scope of ICT service providers, proportionality and ICT risk management, governance, & reporting. It also addresses issues of extreme relevance such as ICT asset management, the Register of Information, incident management, resilience testing, and the oversight of ICT third-party providers. For each topic, the paper combines regulatory interpretation with pragmatic implementation guidance, reflecting the operational realities observed across the Luxembourg market.

This paper does not seek to replace regulatory texts or supervisory guidance, but rather to support consistent interpretation of DORA requirements, facilitate dialogue between industry participants and competent authorities, and contribute to the development of proportionate, effective, and sustainable implementation practices. Through this contribution, the L3A Working Group aims to support financial entities in strengthening their digital operational resilience, while ensuring alignment with both the letter and spirit of DORA.

# 2 TOPIC 1: SCOPE OF DORA & DEFINITION OF ICT PROVIDERS

## 2.1. CONTEXT

DORA establishes a framework governing the ICT risk management obligations of financial entities and their third-party ICT service providers across the European Union. Since its full application on 17 January 2025, one of the most practically significant interpretive challenges has been determining the precise scope of the notions of "ICT services" and "ICT third-party service providers", given that the mere use of IT tools to support the delivery of a business process service does not, in itself, transform that service into an ICT service.

The following section sets out practical guidance to assist in determining whether services received from financial and non-financial entities constitute ICT services within the meaning of DORA, and whether the providing entity falls within the definition of an ICT third-party service provider.

## 2.2. PRACTICAL GUIDELINES – DETERMINING WHETHER A SERVICE IS AN ICT SERVICE WITHIN THE MEANING OF DORA

In assessing whether a service qualifies as an ICT service under DORA, particular regard must be given to a number of key concepts:

### A. ICT SERVICES & ICT SERVICE PROVIDERS

Under Art. 3(21) of DORA, "ICT services" are defined as: "digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services."

Instead, art. 3(19) defines an "ICT third-party service provider" as "an undertaking providing ICT services."

CSSF clarified that financial services provided by professionals of the financial sector other than those covered by Articles 29-3 to 29-6 of the Law of the Financial Sector ("LFS") of 5 April 1993 are not to be considered an ICT service within the meaning of DORA . On the contrary, services offered by professionals of the financial sector which are covered by Articles 29-3 to 29-6 of the LFS, considering the nature of these services, must be considered as an ICT service in the meaning of DORA Article 3(21) in all cases, even though they are provided by a regulated financial entity.

Moreover, in January 2025, the European Commission published its authoritative answer to Q&A DORA030 (submitted via EIOPA), addressing the precise question of what types of services should be considered ICT services under Article 3(21).

Where financial entities provide ICT services to other financial entities in connection with their financial services, the

receiving financial entities should assess:
i. whether the services constitute an ICT service under DORA; and

whether the providing financial entities and the financial services they provide are regulated under Union law or any national legislation of a Member State or of a third country.

If both points are met, then the related ICT service should be considered to predominantly be a financial service and should not be treated as an ICT service within the meaning of DORA Article 3(21) .

Whilst this test was formulated for regulated financial entities providing services to one another, its underlying logic, that the predominant character of the service governs its classification, is applicable by analogy and sets the overarching interpretive framework.

## B. KEY PRINCIPLE: PREDOMINANCE

The European Commission stated that if a regulated financial entity provides ICT services to other financial entities in connection with their regulated financial services, the related ICT services predominantly constitute financial services and should not be treated as an ICT service within the meaning of DORA Article 3(21).

The legal classification of a service should reflect what the service is at its core, not merely what tools are used in its delivery. Therefore, **where an ICT element is merely a tool supporting a broader business process service, and is inseparable from, preparatory to, or necessary for that broader service, it should not be stripped out and classified independently as an ICT service triggering DORA.**

Building on the concepts outlined above, the following guidelines serve to determine whether a given service would qualify as an "ICT Service" within the meaning of DORA:

### Identify the Predominant Service the Client is Receiving

What is the substance of the service contracted for?

- Is the client receiving digital or data output delivered through ICT systems, e.g., access to a platform, data feed, software functionality, or system?
- Or is the client receiving a business process output, e.g., a completed process, a human decision, a professional recommendation, a report, or an operational result?
- If the output is a business process result (not a digital or data service as such), the service is not an ICT service merely because IT tools were used to produce it.

### Identify whether there is a “prevailing ICT component”

Business processes without a prevailing ICT component should not be considered within the scope of ICT services under Article 3(21) of DORA.

- Is the ICT element the primary object of what is being provided, or is it merely an internal tool used to support delivery?
- Is the client exposed to any ICT risk arising from your service, or does that risk sit entirely within your entity's own

operations?

Where the IT tools are used entirely within your own operational sphere, and the client receives a finished business process output rather than access to, or dependence upon, your IT systems, the prevailing character is that of a business process service.

## ASSESS THE SEPARABILITY OF THE ICT ELEMENT

Consider whether the IT tools used could be extracted and offered on a standalone basis to the client. If the IT component is:

- embedded in your internal operations;
- not separately contracted for or invoiced;
- not directly accessed by the client; and
- not provided independently of the business process service,

then it is not a standalone ICT service and does not trigger DORA classification.

## CONSIDER WHETHER YOUR ENTITY IS "PROVIDING ICT SERVICES"

It depends on whether ICT services are being provided, i.e., made available to the client. If the client does not receive ICT services (because what they receive is a business process output), then the entity is not an ICT third-party service provider in respect of that service relationship.

Considering the above, the following approach should be followed in negotiations with clients:

1. **Document the nature of the service:** produce a brief written analysis applying the framework above to the specific service in question, demonstrating that the output provided is a business process output and that there is no prevailing ICT component provided to the client.

2. **Distinguish between your position as a business process provider and that of your own sub-contractors:** if third-party IT platforms or cloud services are used internally, those arrangements may independently be ICT service relationships. This is an internal matter which does not transform client-facing services into ICT services.

## 2.3. PRACTICAL GUIDELINES – DETERMINING WHETHER DATA FEED PROVIDERS (E.G. BLOOMBERG) SHOULD BE INCLUDED IN THE REGISTER OF INFORMATION

DORA's definitions for what classify as an "ICT Service" and "ICT Service Provider" are broader than traditional outsourcing definitions.

As such, **any ICT service provided by a third party falls within the Register of Information scope, even though said (data feed) service would not be classified as "outsourcing" under prior frameworks** (please refer to Circular CSSF 22/806, as amended).

Data providers such as Bloomberg provide data feeds, analytics services, and software platforms, all of which fall within the DORA concept of "ICT services". A Bloomberg terminal subscription, for example, delivers real-time market data, analytics, and news via an ICT infrastructure, and is therefore an ICT service within the meaning of the regulation.

Bloomberg has itself published dedicated operational resilience documentation, which is consistent with the understanding that data feed providers are within scope of DORA obligations.

## 2.4. PRACTICAL GUIDELINES – DEFINING WHAT TYPES OF PROVIDERS SHOULD BE INCLUDED IN THE REGISTER OF INFORMATION

In line with the guidance and explanations provided in Sections I and II above, the Register of Information must include all providers delivering any form of digital, data, software, hardware, cloud, security, or infrastructure service on an ongoing basis. This covers both external vendors and intragroup service providers, ensuring comprehensive visibility over ICT dependencies and supporting regulatory compliance and effective risk management.

## 2.5. INTRAGROUP & CRITICAL ICT SERVICE PROVIDERS

### INTRAGROUP ICT SERVICE PROVIDERS

DORA requires intragroup ICT providers to undergo the same due diligence and oversight as external vendors, regardless of corporate relationships. Entities must perform thorough risk assessments, monitor performance, and establish robust contractual arrangements such as service level agreements and incident response procedures to ensure accountability. All group-level ICT dependencies should be documented and periodically reviewed for potential risks or changes.

Engaging group entities for ICT services does not exempt DORA-subject entities from compliance. All regulatory obligations, including risk management, contractual standards, and ongoing oversight, apply equally to intragroup arrangements, which must be treated with the same scrutiny as third-party vendors.

**Note: if the financial service entity receives an ICT service from its intragroup ICT service provider, it does not automatically mean the entity is providing a DORA ICT service to its clients. The above criteria for identifying a DORA ICT service should be applied to the local financial entity with whom the licensed services are contracted.**

### CRITICAL ICT THIRD-PARTY SERVICE PROVIDERS (CTPPS)

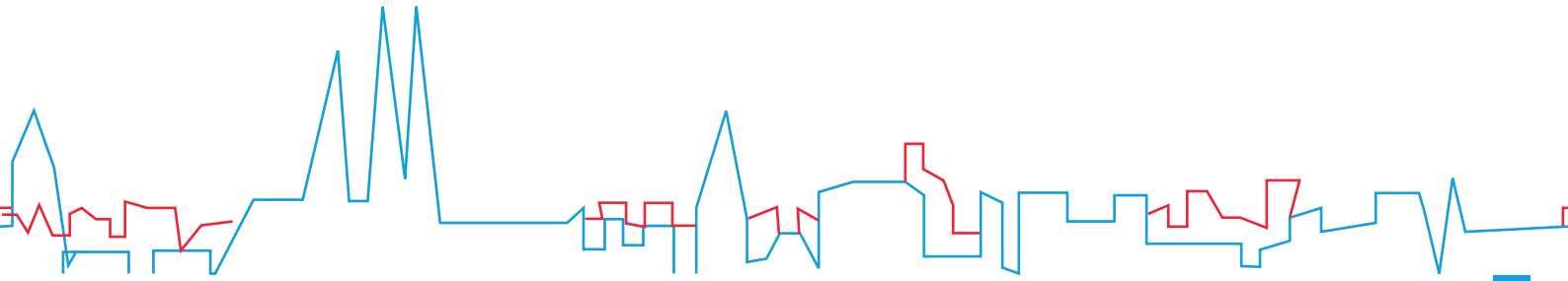
Under Article 31 of DORA, a critical ICT third-pary service provider (CTPP) is an ICT provider that has been formally designated as "critical". **The identification and designation of CTPPs is not left to individual financial entities; it is the exclusive responsibility of the European Supervisory Authorities (ESAs) – the EBA, EIOPA and ESMA.** These CTPPs are essential tech vendors whose failure could impact EU financial stability and are therefore critical to the financial system as a whole, not to individual entities.

Thus, while each DORA-subject entity must maintain and submit a register of its ICT providers, financial service entities should ensure that a clear distinction is made within internal assessments (where necessary) between ICT providers that are critical to the entity and CTPPs.

Moreover, although CTPPs face direct ESA oversight and stringent compliance obligations, financial service entities maintain responsibility for thorough due diligence, oversight and risk management in their engagements with designated CTPPs.

## 2.6. CONCLUSION

The classification of whether a service classifies as an "ICT service" under DORA ultimately relies on its predominant character, meaning what the client is actually receiving as a service, rather than the mere fact that IT tools were used in the service's delivery. If the output is a business process result, the service falls outside DORA's scope. Instead, services delivering digital or data outputs through ICT systems on an ongoing basis will trigger the full scope of DORA's applicability, including inclusion in the Register of Information. Entities should therefore apply a documented assessment to each service relationship, considering the predominance, separability, and nature of the ICT component in order to determine their obligations and ensure regulatory compliance.



# 3 TOPIC 2: PROPORTIONALITY & IMPLEMENTATION PRACTICALITIES

## 3.1. CONTEXT

Article 4 of Regulation (EU) 2022/2554(DORA) requires financial services entities to implement DORA requirements in accordance with the principle of proportionality, taking into account:

- the size of the entity,
- its overall risk profile, and
- the nature, scale and complexity of its services, activities and operations.

This requirement applies:

- to all ICT risk management requirements under Chapter II, and
- in a proportionate manner also to ICT incident management (Chapter III), digital operational resilience testing (Chapter IV), and ICT third-party risk management (Chapter V, Section I), where explicitly foreseen.

Competent authorities are explicitly mandated to assess and challenge the application of proportionality when reviewing the entity's ICT risk management framework under Articles 6(5) and 16(2) of DORA.

As part of this process, authorities may request detailed evidence and supporting documentation that demonstrates how proportionality has been interpreted and applied in the entity's controls, procedures, and risk assessments. This scrutiny ensures that the proportionality principle is not used to justify insufficient risk management measures, but instead reflects a thoughtful, transparent, and justifiable approach aligned with the entity's risk profile and operational complexity.

### Supervisory Expectation

Supervisory practice under DORA makes clear that proportionality does not permit non-compliance, selective implementation, or informal exemptions. Instead, proportionality:

- determines how deeply and rigorously requirements are implemented, not whether they are implemented; and
- must be explicitly defined, documented, and defensible against the entity's actual ICT risk exposure and criticality of services.

Authorities will expect a clear, evidence-based rationale demonstrating that the selected level of control sophistication is appropriate in light of the entity's role in the financial system and its operational dependencies. Such evidence may include risk assessments and ICT incident data, internal reports and board-approved policies.

## 3.2. PRACTICAL GUIDELINES – APPLICATION OF PROPORTIONALITY

It is recommended that financial services entity apply the DORA proportionality principle through a structured and documented approach including the following elements:

### Define proportionality criteria ex-ante

The entity should formally define the criteria used to assess proportionality, at a minimum covering:

- size (e.g. based on staff, balance sheet, assets under management),
- overall ICT and operational risk profile,
- number and criticality of services and functions,
- ICT architecture complexity and outsourcing model,
- systemic relevance and substitutability of services.

These criteria should be approved by senior management and reviewed periodically.

### Establish proportionality tiers

Based on the defined criteria, the entity should map its activities and ICT systems to clearly defined proportionality tiers (e.g. basic / enhanced / advanced), which determine:

- depth of documentation,
- frequency and sophistication of testing,
- level of automation and monitoring,
- granularity of incident classification and reporting.

This approach facilitates supervisory review. By establishing clear proportionality tiers based on well-defined criteria, organizations ensure that their digital operational resilience measures are tailored to the actual risks and needs of their activities. Mapping activities and ICT systems into proportionality tiers (e.g., basic, enhanced, advanced) allows for differentiated requirements regarding documentation, testing, automation, and incident reporting. As a result, the entity is better positioned to justify its approach during supervisory assessments and audits.

### Apply proportionality consistently across DORA pillars

Once the tier is decided, proportionality should be applied consistently across all DORA pillars, in particular:

- **ICT risk management (Chapter II):** Scope, detail, and formality of policies, controls, backup strategies, and governance may be lighter for less complex entities, while still covering all required risk domains.
- **ICT incident management (Chapter III):** Incident escalation, staffing, tooling, and classification methodologies may be scaled, provided that detection, response, and regulatory reporting obligations are fully met.
- **Digital operational resilience testing (Chapter IV):** The nature and frequency of tests (including exclusion of threat level penetration testing (TLPT) where applicable) should reflect the entity's complexity and criticality, as expressly permitted by DORA.
- **ICT third-party risk management (Chapter V):** Due diligence, contract provisions, and monitoring intensity should correlate with the materiality and criticality of outsourced ICT services.

### Document proportionality decisions

All proportionality decisions should be:

- formally documented,
- linked to specific DORA requirements, supported by risk assessments and impact analyses, and
- retained as supervisory evidence.

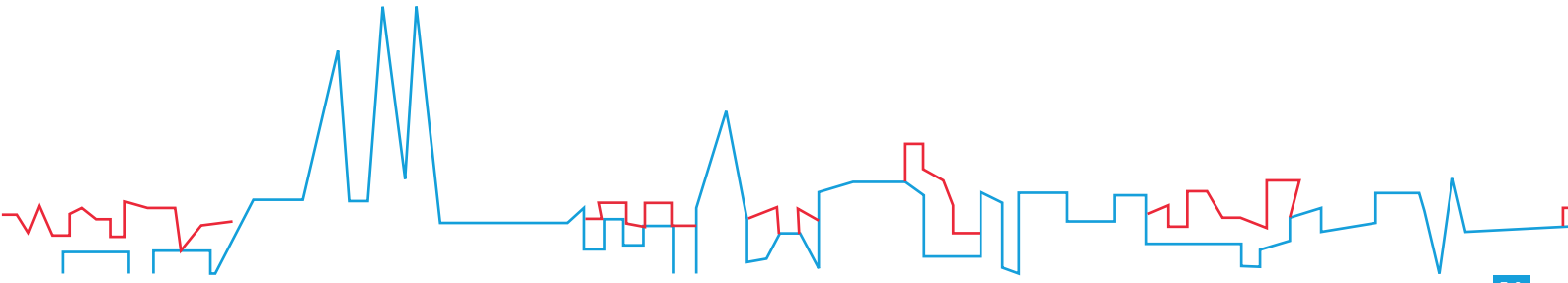
This documentation should clearly demonstrate that the applied approach results from risk-based decisions, not from resource constraints.

In practice, this means that organizations should be able to provide evidence that their proportionality decisions are grounded in a deliberate, methodical approach to tailoring policies, processes and controls to the actual risks identified within the ICT environment.

### Document proportionality decisions

To ensure that a proportional approach is appropriately determined, implemented and documented by the financial services entity, it is recommended that:

- the management body retains ultimate accountability for proportionality choices under DORA, in line with Article 5;
- proportionality assumptions are reviewed at least annually, or upon material changes to the business or ICT environment;



- internal audit and compliance functions explicitly assess whether proportionality is applied consistently and defensibly;
- documentation supporting proportionality decisions is regularly updated and made readily available for supervisory review.

## 3.3. CONCLUSION

**The proportionality principle under DORA should be treated as a design and scoping mechanism, not as a compliance reducer.**

Organizations should actively embed their proportionality framework into planning, implementing, and reviewing digital resilience measures. Instead of reducing compliance requirements, proportionality ensures policies, processes and controls match the entity's scale and exposure to ICT risks, enabling robust yet appropriate solutions.

A well-documented, risk-based proportionality framework is essential to demonstrate compliance with DORA and to withstand supervisory scrutiny. Documentation must clearly show that the framework and its implementation appropriate, are regularly reviewed and approved by the relevant internal governance bodies.

# 4 TOPIC 3: ICT RISK MANAGEMENT, GOVERNANCE & REPORTING

## 4.1. CONTEXT

DORA introduces strengthened requirements for ICT risk management, governance and reporting, placing clear accountability on the management body to ensure that ICT risks are effectively identified, managed, monitored and reported.

These requirements go beyond technical controls, emphasising the need for structured governance, formalised documentation and clear reporting lines enabling informed decision making and supervisory review. Financial entities must be able to demonstrate that their ICT risk management framework is comprehensive, proportionate to their risk profile, and subject to regular review and continuous improvement.

In practice, this raises several operational and organisational challenges, including how to consolidate ICT risk information into a coherent reporting framework, how to ensure meaningful oversight by the management body, and how to embed ICT risk awareness across the organisation.

This section addresses these challenges by outlining pragmatic approaches to:

- structuring ICT risk reporting at both supervisory and Board levels,
- formalising governance and oversight through consistent reporting practices,
- and ensuring that staff and management maintain an appropriate level of awareness and expertise in ICT risk management.
- This section is drafted as practical guidelines for applying DORA regulatory requirements.

## 4.2. PRACTICAL GUIDELINES – REPORT ON THE REVIEW OF THE ICT RISK MANAGEMENT FRAMEWORK

The Report on the Review of the ICT Risk Management Framework provides a consolidated view of the effectiveness, proportionality and maturity of the entity's ICT risk management practices, supporting management oversight, decision-making and supervisory assessment, while ensuring identified risks and weaknesses are addressed through a structured continuous improvement process, in line with Article 6(5) (documentation and reporting) and Article 16(2) (review of the ICT risk management framework).

- While DORA does not require systematic submission, competent authorities may request this report on an ad-hoc basis to assess the consistency, completeness and effectiveness of the ICT risk management framework.
- The report should follow the structure set out in Article 27 of Commission Delegated Regulation (EU) 2024/1774 supplementing DORA.
- The below is NOT a substitute to the structure mandated by the regulation but just provide insight and guidance on potential inputs and considerations for key sections of the report.

### Executive Summary

The report requires an "Introduction" section. This section can potentially be expanded to become an "Executive Summary" providing a clear high level overview of the report for the supervisory authorities, the senior management and the Board. The section would include:

- Business context: brief overview of the entity's core activities, services and strategy, including its position within the group (if applicable) and identification of critical or important functions (CIFs) supported by ICT.

- Operational context: summary of the nature, scale and complexity of operations, including organisational structure, key processes, and any major business initiatives or transformations impacting ICT risk.
- IT context: high-level description of the ICT landscape, including key systems, architecture (e.g. cloud, legacy), and the role of ICT in supporting business operations and critical functions.
- Third party dependencies: overview of reliance on ICT third-party providers, including critical services, concentration risks, and the potential impact of disruption or failure on operations and CIFs
- Major changes in the ICT risk management framework: Summary of significant updates since the previous report, including changes in governance, controls, tools, policies, or organisational setup.
- Overall ICT risk profile, threat landscape and security exposure: executive view of key ICT risks, evolving threat environment, control effectiveness, and overall security posture of the entity
- Outline of remediation actions and timeline: high-level summary of key remediation initiatives, including priorities, expected timelines, and progress status for addressing identified weaknesses.

## Description of Major Changes

The report requires describing major changes in the ICT risk management framework. The following are examples of areas where such changes can occur and should be reported:

- **ICT governance and organisation:** When reviewing changes to the ICT risk management framework, it is essential to assess whether the ICT governance structure remains clearly defined, effective, and aligned with DORA expectations.

This includes verifying that reporting lines, roles and responsibilities across the three lines of defence are updated and consistently applied. Particular attention should be given to the continued involvement of the management body, ensuring it maintains appropriate oversight of ICT risk and digital operational resilience. Supporting committees should be evaluated for their effectiveness in reviewing ICT risks and changes. Escalation mechanisms must be reviewed to confirm that any new or evolving ICT risks, control deficiencies, or incidents can be promptly and effectively elevated to senior management and the board.

- **ICT risk management strategy, policies and procedures:** Changes to the framework should be assessed against the organisation's digital operational resilience strategy to ensure continued alignment with its risk appetite and regulatory obligations under DORA. This includes reviewing whether policies and procedures governing ICT risk identification, assessment and mitigation have been appropriately updated to reflect new threats, technologies, or business models. The completeness and effectiveness of controls across the resilience lifecycle (identify, protect, detect, respond, recover) should be reassessed. Additionally, it should be verified that changes are consistently implemented, communicated, and embedded in operational practices across the organisation.

- **ICT systems, protocols and tools:** The review should consider whether changes in the ICT risk management framework are adequately supported by the organisation's systems, security tools, and technical controls. This includes evaluating whether existing tools remain fit for purpose in identifying, monitoring and mitigating ICT risks, and whether any new tools or technologies have been properly integrated into the control environment. Protocols, configurations, and monitoring capabilities should be assessed to ensure they continue to provide sufficient coverage, accuracy, and timeliness in detecting vulnerabilities and incidents. Dependencies between systems and potential impacts on resilience should also be examined.

- ICT third party governance: Changes should be assessed for their impact on the oversight and management of ICT third-party service providers, in line with DORA requirements. This includes reviewing whether the identification and classification of critical ICT third parties remain accurate, particularly in light of new outsourcing arrangements or changes in service delivery models. Potential concentration and dependency risks should be re-evaluated. Contractual arrangements should be reviewed to ensure continued compliance with regulatory expectations, including provisions on security, availability, audit rights, and exit strategies.

Monitoring processes should be assessed to confirm that performance, risk exposure, and compliance issues, including any material incidents or control weaknesses, are effectively tracked, reported, and addressed.

### Description of the ICT Risk Profile and Posture

The report also requires describing the overall ICT risk profile and security posture of the Bank. The following are examples of elements to be considered:

- **ICT risk assessment results:** summary of the annual ICT risk assessment, key inherent and residual risks tracked in the entity's risk register including accepted risks, impact on critical and important functions, risks of interdependencies and single points of failure.
- **ICT-related incidents and lessons learned:** list of relevant ICT related incidents in scope of the review, description of the major ICT-related incident(s) (as defined under Article 18) which potentially triggered a review of the ICT risk management framework, root cause analysis and corrective actions, lessons learned and improvements applied.
- **Audits and digital operational resilience testing:** description of audits and/or tests performed which potentially triggered the review of the ICT risk management framework, key deficiencies identified and remediation
- **Remediation plans:** remediation actions for all weaknesses and findings identified with clear ownership and timeline for identified weaknesses and findings including updates on progress where relevant, planned improvements for the next reporting period.

### Report Preparation and Governance

The preparation of the report does not necessarily require a "start from scratch" approach. It can leverage a range of existing inputs that may already be available within the organization, including for example:

- Results of the CSSF IT self-assessment questionnaire or other ICT-related regulatory deliverable.
- Internal and external IT audit findings.
- Outputs from resilience testing activities (e.g. penetration tests, BCP/DRP tests, SWIFT CSP assessments, exit strategy tests, compliance reviews), including group-level testing where applicable.
- ICT risk reporting submitted to or reviewed by the Board.
- ICT incident register and related trend analyses.
- Register of information for ICT third party providers.

The report should be:

- reviewed and prepared at least annually,
- reviewed also upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes,
- reviewed by senior management,
- made available to the CSSF upon request,
- formally acknowledged or approved by the management body.

From a CSSF standpoint, the annual ICT Risk Management Report is a key deliverable that demonstrates that ICT risks are managed in a structured manner, proportionality is consciously and consistently applied, and the management body exercises effective oversight. Incomplete, informal, or purely descriptive reporting is unlikely to meet supervisory expectations under DORA.

## 4.3. PRACTICAL GUIDELINES – BOARD REPORTING ON ICT RISK

While the report on the review of the ICT risk management framework provides a periodic, comprehensive assessment of the framework's overall effectiveness, proportionality and maturity, regular Board reporting on ICT risk posture delivers a more frequent, forward-looking view of current risks, trends and key developments to support ongoing oversight and decision-making.

- ICT risk reporting should:
- be provided at least quarterly,
- be aligned with enterprise risk reporting,
- support informed oversight by the management body.
-

Below are example of topics and content which can be covered in such reporting:

### Threat landscape and incident trends

This section explains the external cyber threat environment and internal ICT-related incidents for the reporting period. It may include:

- overview of top cyber threats relevant to the entity and how these threats are trending,
- breakdown of ICT-related incidents by severity,
- focus on higher-severity incidents,
- for major ICT-related incidents: regulatory notification status, business impact, root cause and actions taken,
- indication of whether regulatory thresholds were triggered.

### Top 5 ICT risks

Below an example of presentation of such ICT risks:

| ICT Risk | Key Controls in Place | Residual Risk Level | Trend | Mitigation Comment |
|---|---|---|---|---|
| **ICT system outage** | Availability monitoring, backup procedures, disaster recovery arrangements | Medium | Improving | Infrastructure upgrade progressing |
| **Delegation / supply chain cyber compromise** | Due diligence, third-party risk assessments, performance monitoring | Medium-High | Stable | Strengthened oversight; updated exit plan |
| **Exploitation of misconfiguration or vulnerabilities** | Patching, configuration standards, vulnerability assessments | Medium | Stable | Improved remediation timelines |
| **Malware or ransomware attack** | Malware protection, email filtering, network segmentation | Medium | Improving | Increased scan frequency and filtering |
| **Phishing or social engineering** | Awareness training, email filtering | Medium | Deteriorating | More frequent phishing simulations |

## Key Risk Indicators (KRIs)

KRIs may include:

- number of severe incidents linked to the identified ICT risk
- overdue critical findings on key mitigating controls
- relevant quantitative indicators
- defined appetite and tolerance thresholds

## Below KRI examples:

| ICT Risk | Key Risk Indicators | Risk Appetite Threshold | Risk Tolerance Threshold |
|---|---|---|---|
| **ICT system outage** | % system availability | ≥ 99.9% | ≥ 99.5% |
| **Delegation / supply chain cyber compromise** | % updated due diligence and risk assessments | 100% updated | ≥ 95% |
| **Misconfiguration / vulnerabilities** | Patch timeliness | > 95% patches on time | > 90% patches on time |
| **Malware / ransomware** | % devices with malware protection | 100% coverage | ≥ 98% coverage |
| **Phishing / social engineering** | Phishing simulation failure rate | < 5% failures | < 10% failures |

## Risk mitigation and project status

Shows progress on ICT resilience initiatives and projects, delays or blockers, and links between initiatives and ICT risk scenarios and strengthened controls.

## ICT third-party and outsourcing risk

This may include, for example:

- number of ICT services (critical vs non-critical)
- ICT services onboarded or offboarded since last reporting
- for each new critical ICT service: short description, outcome of the risk assessment, status of inclusion in the Register of Information

Particularly relevant for entities heavily dependent on ICT third party providers including intra-group services.

## Regulatory and compliance standing

This may include, for example:

- status of required ICT-related regulatory reporting (e.g. CSSF Self-Assessment Questionnaire)
- ICT-related notifications (e.g. new ICT outsourcing relationships)
- remediation of regulatory findings (e.g. CSSF on-site inspection findings)
- upcoming regulatory deadlines (e.g. EU AI Act)

## Decision points for the Board

This may include, for example:

- approval of ICT/security policies
- acceptance of residual ICT risks
- decisions regarding ICT resilience initiatives and projects

## 4.4. PRACTICAL GUIDELINES – TRAINING AND AWARENESS

Training must ensure that all staff, including senior management and Board members, understand ICT risks relevant to their roles.
Training programmes should be:

- role-based,
- regularly updated,
- aligned with the ICT risk framework.

Training programme may include, for example:

- Annual cyber-awareness training, covering phishing, social engineering, safe online behavior and the organisation's ICT risk management policies.
- Ongoing internal awareness communications and phishing simulations to reinforce secure behaviors (communicated via email or via intranet posts).
- Role-specific training, particularly for staff responsible for ICT incident assessment, escalation, or oversight of ICT third-party services.
- Training for senior management and the Board, ensuring they understand their ICT risk oversight responsibilities and can make informed decisions.
- Training on emerging technologies adopted by the organisation, such as artificial intelligence (AI), focusing on secure and responsible use.
- Technical upskilling for ICT staff, ensuring they maintain current expertise on the technologies they operate in, for example, cloud technology, virtualisation, identity management and network security.
- Confirmation of adequate training for Group ICT staff (with supporting evidence), where ICT services are performed by a group entity, ensuring equivalent skills and competencies.

Training programmes must be reviewed and updated regularly to incorporate lessons learned from incidents, audits, threat intelligence and changes in the ICT landscape.

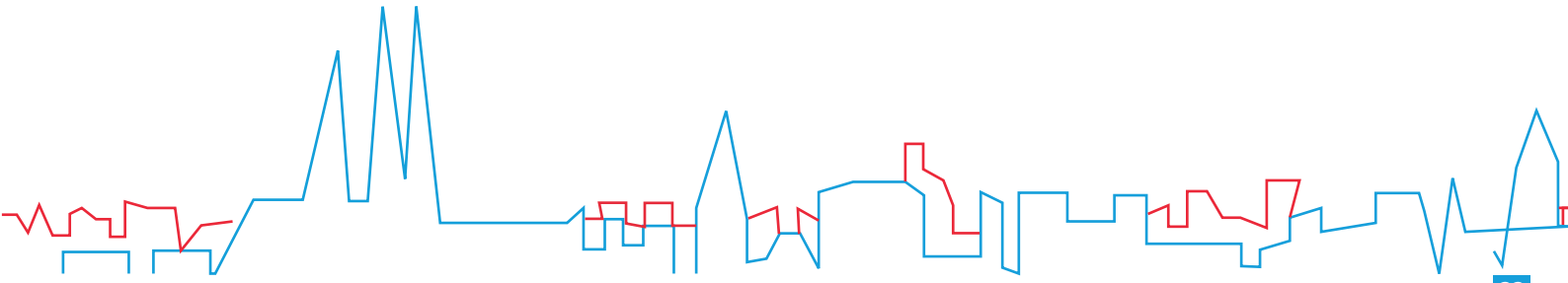
## 4.5. CONCLUSION

DORA elevates ICT risk management to a core governance priority, requiring financial entities to demonstrate not only the existence of controls but their effectiveness, proportionality and continuous improvement.

In practice, this requires a structured and coherent approach combining:

- a comprehensive review of the ICT risk management framework,
- regular, forward-looking reporting to the management body,
- and sustained investment in training and awareness across the organisation.

From a supervisory perspective, the ability to clearly evidence how ICT risks are identified, monitored, escalated and remediated is critical. Entities that implement consistent, decision-oriented reporting and strong governance practices will be best positioned to meet regulatory expectations and demonstrate operational resilience under DORA.



# 5

# TOPIC 4: ICT ASSET MANAGEMENT, CIF MAPPING & REGISTER OF INFORMATION

## 5.1. CONTEXT

DORA imposes comprehensive and granular ICT asset management obligations on financial entities, requiring a complete inventory of all ICT assets with enhanced mapping requirements for assets deemed critical.

This section addresses the key practical questions arising from those obligations: the level of granularity required for the ICT asset list, the appropriate methodologies for mapping assets to Critical or Important Functions (CIFs), the derivation and assignment of RTO and RPO requirements, and the maintenance of the Register of Information in accordance with the Implementing Technical Standards.

## 5.2. LEVEL OF GRANULARITY OF THE ICT ASSET LIST

The ICT asset list under DORA must be comprehensive and granular. Every single ICT asset (hardware, software, network resources, remote sites) must be captured with a defined set of mandatory attributes. For assets deemed critical, the level of mapping must go further still covering full configuration detail, data flows in and out, storage, and all interdependencies.

The regulation does not permit selective or high-level cataloguing. The intent is that the inventory is sufficiently granular to underpin the entire ICT risk management framework, business continuity planning, and third-party risk management obligations.

In light of the granularity and accuracy required, a practical approach would be to build upon existing inventories (such as business function inventories, application inventories, CMDB, supplier inventories) wherever possible, enriching them with any additional information necessary to meet DORA's requirements. Furthermore, given the dynamic nature of the data involved, consolidating all required information within a single inventory may not be feasible. It is therefore advisable to make use of multiple inventories and to establish clear, documented, and operational links between them, such that the inventories collectively satisfy the full range of requirements under DORA.

## 5.3. UPDATE FREQUENCY OF THE ICT ASSET LIST

The inventories must be updated periodically and at least whenever a major change in the network and information system infrastructure, in the processes or procedures affecting ICT-supported business functions, information assets or ICT assets occurs. In any event, the adequacy of the classification and documentation must be reviewed at least yearly.

## 5.4. PRACTICAL GUIDELINES - METHODOLOGIES FOR MAPPING ASSETS TO CRITICAL OR IMPORTANT FUNCTIONS (CIFS)

Under DORA, mapping assets to Critical or Important Functions (CIFs) requires financial entities to first identify and classify all business functions using materiality criteria to determine which qualify as CIFs.

### How to identify critical or important functions

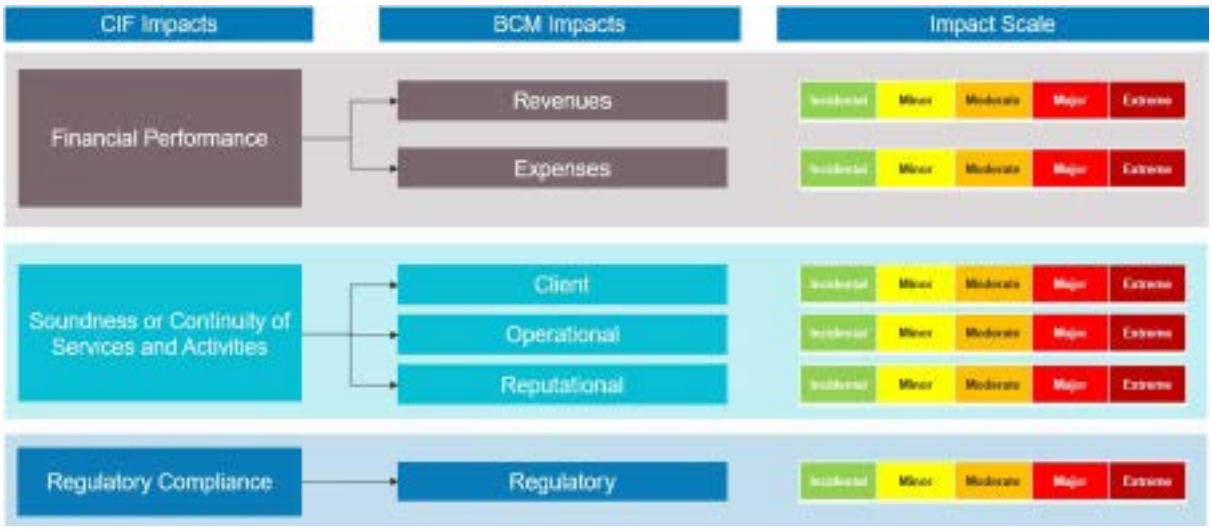
CIFs can be identified using existing outsourcing assessments or business continuity analysis. A CIF is a function whose disruption would materially affect the entity's financial performance, the soundness and continuity of its processes and operations, or its ability to meet regulatory and legal obligations.

A practical way to determine whether a function is a CIF is to start from the entity's existing BCM impact criteria and reinterpret them through the lens of CIF materiality.

BCM frameworks typically assess impacts across dimensions such as revenue, expenses or cost, operational or process disruption, client impact, reputational effects and regulatory considerations. These are examples of BCM impacts and may differ across organisations. These BCM impact categories can be mapped directly to CIF impacts. BCM revenue impacts relate to CIF impacts on financial performance. BCM expense or cost impacts also map to CIF impacts on financial performance by highlighting material unplanned costs. BCM operational or process impacts align with CIF impacts on continuity of the entity's processes and operations. BCM client impacts can indicate CIF relevance where client facing disruption becomes operationally material. BCM reputational impacts correspond to CIF impacts on soundness and stakeholder confidence. BCM regulatory impacts map directly to CIF impacts on regulatory and legal compliance.

It is also important to recognise that BCM analysis generally focuses on short term disruption, often centred around immediate recoverability within defined time windows. CIFs, however, are not limited to a strict time horizon.

Their materiality reflects whether disruption affects the entity's operations, financial performance or regulatory compliance in the short to medium term, without a fixed recovery period.




## Mapping ICT assets to Critical or Important Functions (CIFs)

Once CIFs are established and approved by Management, entities must build a comprehensive ICT Asset Register covering hardware, software, services, and data, and then construct a dependency matrix linking each asset to the CIFs it supports. This mapping must extend to ICT third-party service providers.

ICT assets should be mapped to CIFs using a structured decision tree approach:

- If disruption of the ICT asset causes the CIF to stop immediately, the ICT asset supports the CIF;
- If the ICT asset cannot remain unavailable beyond the CIF's tolerable downtime or recovery time objective (RTO), the ICT asset supports the CIF;
- If no realistic alternative system or manual workaround exists that allows the CIF to continue operating within acceptable timeframes, the ICT asset supports the CIF;
- If loss, unavailability or corruption of the data processed, stored or transmitted by the ICT asset would materially affect the CIF, the ICT asset supports the CIF;

If none of these conditions apply, the ICT asset is considered non CIF supporting or only indirectly related to the CIF.

The entire mapping exercise must be validated through scenario analysis and CMDB reconciliation, integrated into the broader ICT risk management framework (covering incident management, business continuity, and threat-led penetration testing), and reviewed on an ongoing basis, at minimum annually, under clear governance ownership.

## 5.5. Practical Guidelines - Defining RTO and RPO and assigning to ICT assets supporting CIFs

RTO and RPO must always be derived from the recovery requirements of the Critical or Important Function (CIF). For each CIF, the entity must take the CIF's RTO and RPO from the business impact analysis and cascade these requirements only to the ICT assets that effectively support that CIF, as determined by the mapping principles described above. ICT assets that do not support the CIF must not inherit the CIF's RTO or RPO.

Once the ICT assets that effectively support the CIF have been identified, their recovery capabilities must be assessed against the CIF's required RTO and RPO, and any identified gaps must be remediated. For example, if a CIF must recover within two hours with no more than ten minutes of data loss, all ICT assets supporting that CIF must meet those thresholds.

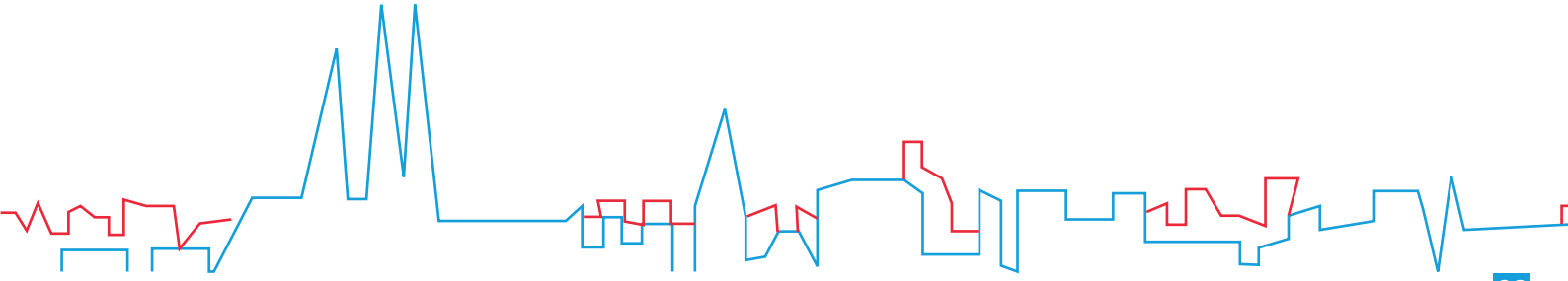
ICT assets that do not support any CIF may follow business as usual recovery expectations, such as a BAU RTO of up to seven days and a BAU RPO aligned with daily backup cycles.

## 5.6. Practical Guidelines - Maintaining the Register of Information (RoI)

Maintaining an accurate and up to date Register of Information (RoI) is a core requirement under DORA and a foundational element of ICT third party risk management. The structure, content and level of granularity of the RoI are defined by the Implementing Technical Standards (ITS) on standard templates for the Register of Information (Commission Implementing Regulation (EU) 2024/2956). Financial entities are expected to align their RoI strictly with these templates, as deviations from the prescribed data model and formats frequently result in validation errors and supervisory follow up.

Entities are encouraged to leverage both the ITS templates themselves and the practical guidance published by the CSSF on the submission of the Register of Information via the eDesk portal (https://www.cssf.lu/en/2026/02/dora-submission-timeframe-for-register-of-information-edesk-portal-open-as-of-11-february-2026/), as well as relevant clarifications issued by the European Supervisory Authorities. Experience across the industry shows that basing the RoI directly on these sources significantly reduces implementation complexity and rework. Submitting the RoI as early as possible is considered good practice, as early submission provides time to identify data quality issues, correct structural inconsistencies and resolve errors flagged during submission. Proactive exchanges with the CSSF are encouraged, as the competent authority seeks to support financial entities in addressing practical RoI related challenges. Where possible, exchanging views with industry peers can also help identify common pitfalls and pragmatic implementation approaches.

The RoI should be maintained on a continuous basis throughout the year rather than treated as a one off annual exercise. Integrating updates into existing onboarding, change management and contract lifecycle processes is more efficient and significantly reduces reconciliation effort. This approach is particularly important given that, under DORA, competent authorities may request the ROI on an ad hoc basis, in addition to the periodic submission using the ITS templates.



Where an entity is part of an EU based group, DORA allows for the submission of a consolidated Register of Information at group level, provided the requirements of the ITS are met. Aligning with a group level RoI approach is therefore often beneficial, especially where ICT services and providers are shared, as it promotes consistency and data quality. However, each regulated entity remains fully accountable for ensuring that its own ICT outsourcing arrangements, criticality and dependencies are correctly reflected in the consolidated register, with appropriate local validation and sign off in place prior to submission.

Finally, entities with a large number of ICT service providers or complex outsourcing arrangements should carefully assess whether manual maintenance via spreadsheet templates remains appropriate. At scale, spreadsheet based approaches often become difficult to manage and prone to errors. In such cases, the use of dedicated tools or structured data solutions aligned with the ITS data model can materially improve data quality, traceability and long term compliance.

## 5.7. Conclusion

Compliance with DORA's ICT asset management framework requires financial entities to build and maintain a comprehensive and granular inventory, underpinned by rigorous mapping to CIFs and supported by clearly documented RTO and RPO thresholds. Where a single consolidated inventory is not feasible, entities should establish clear and operational links between multiple inventories to collectively satisfy DORA's requirements. The Register of Information should be maintained on a continuous basis, integrated into existing onboarding, change-management and contract-lifecycle processes, rather than treated as a one-off annual exercise. Early submission, proactive engagement with the CSSF, and alignment with ITS templates remain the most effective means of reducing implementation risk and ensuring regulatory compliance.

# 6 TOPIC 5: ICT INCIDENT MANAGEMENT & OPERATIONAL RESILIENCE TESTING

## 6.1. Context

### ICT Incident Management & Operational Resilience Testing

### Incident Classification: What to Log vs. What to Report

| Requirement | Scope | Audience |
|---|---|---|
| ICT incident register | ALL ICT-related incidents | Internal only |
| Major incident reporting | Only incidents meeting Article 18 + RTS thresholds | CSSF (eDesk/API) |

Moving into DORA compliance means shifting away from purely retrospective, engineering-focused logging and moving toward real-time, impact-driven triage. To properly align with CSSF expectations and avoid administrative bottlenecks, institutions are recommended to immediately transition their classification and escalation processes toward an impact-first narrative.

RTS-Aligned Incident Classification Logic
The foundational step for the organization is to formalize an internal classification matrix that directly mirrors the guidelines laid out in the European Supervisory Authorities' Final Draft Regulatory Technical Standards (RTS) on major incident classification (JC 2023 83). Rather than waiting for infrastructure teams to trace an issue to its definitive root cause, teams are advised to trigger triage execution the moment any service degradation or data compromise hits the radar.

The evaluation hinges on a clear, top-down decision tree. The framework mandates evaluating whether a "Critical or Important Function" is impacted first, alongside evaluating the severity of quantitative thresholds—such as affected client volume, geographic spread, or data loss. Additionally, teams must be trained on incident aggregation rules, ensuring that distinct events stemming from the same root cause or attack campaign within a 24-to-72-hour window are aggregated and measured collectively against the major incident thresholds.

### Appointing the "ICT Incident Notifier"

To ensure this framework functions seamlessly under operational pressure, institutions are highly advised to formally designate an internal ICT Incident Notifier (or an equivalent dedicated crisis lead).

It is critical that this role carries an explicit operational mandate and pre-delegated authority. The notifier must be empowered to initiate regulatory reporting workflows immediately, bypassing standard, time-consuming executive committee assemblies when a major threshold is crossed.

### Operationalizing the Three-Stage Reporting Lifecycle

Having an empowered notifier is especially vital given the incredibly tight 4-hour initial notification window mandated by the CSSF via their eDesk or API channels. Operational procedures must account for the fact that these early "Warning" reports are legally intended to be directional and iterative, not exhaustive. Management should explicitly communicate to teams that accepting initial incompleteness is a necessary operational reality to hit the regulatory target.

### Three-Stage Reporting Process

| Stage | Deadline | Key Content |
|---|---|---|
| Initial notification | 4 hours | Time, nature, status, suspected cause |
| Intermediate report | 72 hours + updates | Impact assessment, remediation progress |
| Final report | 1 month after resolution | Root cause, total impact, lessons learned |

**Best Practice:** To build a reliable buffer against these deadlines, the recommended approach is twofold:

- Establish Aggressive Internal SLAs: Set internal triage and escalation limits strictly below the regulatory thresholds (for instance, a maximum 2-hour window from initial detection to notifier escalation).
- Pre-Configure Infrastructure: Proactively build and test CSSF eDesk reporting templates and API access keys for both the primary notifier and designated back-ups to eliminate technical friction during an active crisis.

## Refining the Operational Resilience

When designing a testing framework under DORA Article 25, the overarching goal is to shift away from traditional, check-the-box compliance exercises and move toward a dynamic, risk-proportionate program that maintains active Management Body oversight.

## Embedding Proportionality into the Testing Strategy

Following the core principles of Article 4, institutions are recommended to deliberately scale their testing depth to reflect the actual size, risk profile, and complexity of their business operations. Management Bodies are explicitly cautioned against over-engineering these frameworks in a way that drains operational resources or creates an unsustainable volume of tests. Instead, the recommended approach is to establish a balanced, predictable calendar that guarantees complete coverage of all identified Critical or Important Functions (CIFs).

A comprehensive testing strategy should naturally blend distinct methodologies throughout the financial year to provide a layered defense view:

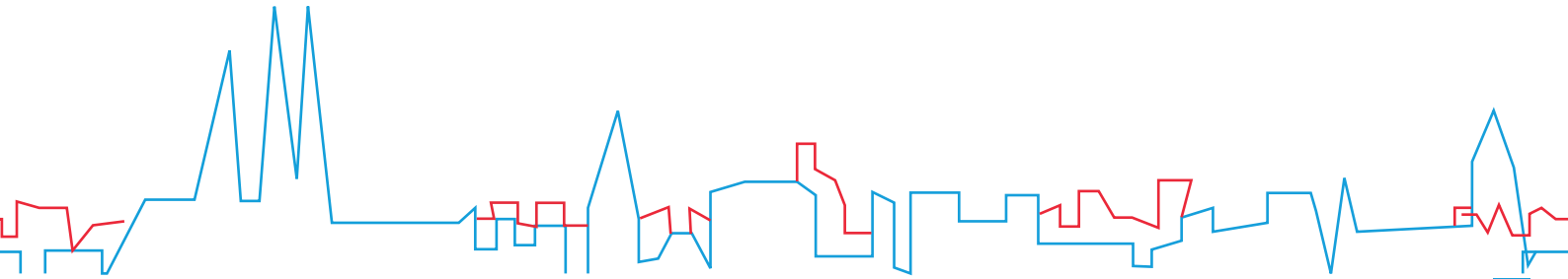
- Quarterly Vulnerability Scanning: Automated, surface-level discovery designed to catch unpatched dependencies and infrastructure exposures before they can be exploited.
- Annual Penetration Testing: Focused, manual exploitation targeting network boundaries and defensive perimeters surrounding your critical systems.
- Annual BCP & DR Testing: Full-scale failover and redundancy verifications to stress-test your business continuity plans and prove actual recovery time objectives (RTO).
- Semi-Annual Scenario Exercises: Tabletop or simulation drills involving senior leadership to specifically stress-test crisis governance, internal decision-making, and communication protocols.

The ultimate success metric of an Article 25 testing program is never the sheer volume of tests conducted; it is the transparency of the findings tracking system and the speed of downstream remediation. To ensure accountability, all testing outputs require a formalized, quarterly reporting loop back to senior management.

## Navigating Threat-Led Penetration Testing (TLPT) Governance

Because Threat-Led Penetration Testing (Articles 26–27) demands heavy operational overhead, introduces real production risk, and relies on highly advanced red-teaming methodologies, a disciplined gating process is essential.

Institutions are highly advised to pause any execution or procurement of a full TLPT cycle unless they have been explicitly and formally designated as an in-scope entity by the CSSF. If the institution's systemic footprint and risk profile do not trigger a formal regulatory notification, the recommended approach is for the Management Body to clearly document this non-applicability within its annual governance review. This allows the organization to protect its regulatory stance while confidently directing specialized security resources toward maximizing the standard Article 25 testing program.



For those institutions that are formally identified by the regulator, establishing a dedicated TLPT governance framework becomes an immediate priority. This involves early planning to engage CSSF-approved external threat intelligence and red-team providers, alongside structuring pooled testing agreements if the entity shares critical market infrastructure dependencies with other participants.

### Immediate Operational Roadmap

For the leadership team, moving from design to execution means focusing on a small handful of high-impact workstreams. On the incident side, the recommended priority is to build and publish the formalized classification framework—explicitly embedding the 7 RTS criteria and the 24-to-72-hour aggregation rules into the frontline ticketing systems. Parallel to this, the operational focus must turn to the resilience testing program.

This involves drafting a comprehensive testing strategy for formal Management Body approval and locking in an annual calendar that schedules the necessary vulnerability scans, penetration tests, and disaster recovery drills.

## 6.2. Practical Guidelines - Pitfalls to Avoid

When deploying a framework as sweeping as DORA, it is incredibly easy for teams to accidentally over-engineer processes or misinterpret the regulator's intent. To keep operations lean and effective, management is advised to treat the following scenarios as critical guardrails:

Avoid Over-Reporting: A frequent mistake is flooding the CSSF by reporting every minor ICT hitch. The reporting workflow must be strictly reserved for major incidents that explicitly breach the RTS thresholds. Non-major events should be quietly routed to the internal incident register, maintaining a clean operational boundary.

During an active disruption, waiting for engineers to discover the root cause before sending the initial notification is a major compliance failure. The 4-hour window requires an immediate commitment to transparency; sending a directional, incomplete report on time is always the correct regulatory move.

Differentiate Your Testing Boundaries: Teams should be explicitly cautioned against assuming that advanced, threat-led penetration testing (TLPT) automatically applies to everyone. Launching a complex red-team exercise without an explicit CSSF mandate risks misallocating significant capital and engineering time that would be far better spent strengthening basic remediation tracking under Article 25.

## 6.3. Practical Guidelines - Recommended Quick Decision Diagrams

Incident Triage
This flowchart provides frontline incident handlers with an immediate, binary decision-making framework to determine regulatory reporting obligations the moment a disruption is detected.

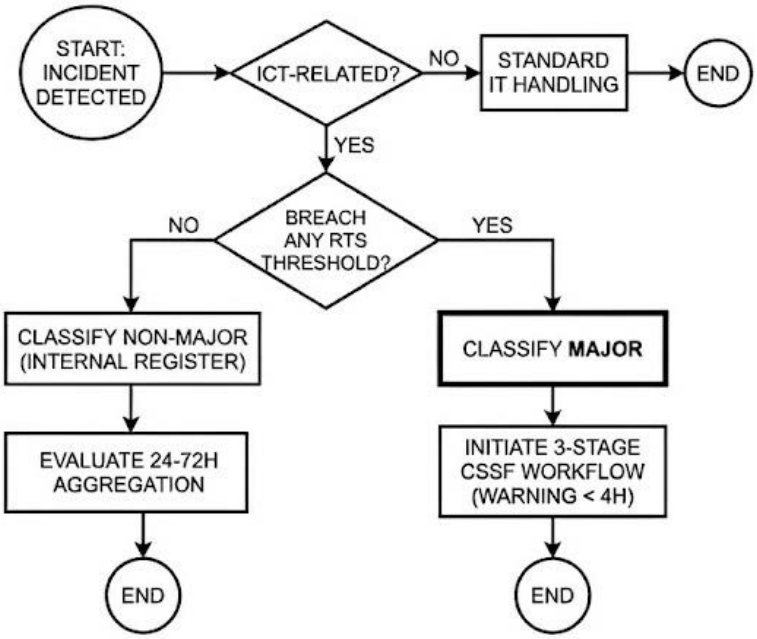
Initial Logging: Every detected event—regardless of initial perceived severity—must immediately be recorded in the internal ticketing system to maintain a comprehensive, audit-ready operational history.

The ICT Gateway: The first filter establishes whether the issue constitutes an actual ICT incident (defined as a compromise of service availability, integrity, or data confidentiality). If it does not, it is routed to standard IT service management handling.

Threshold Evaluation: If it is an ICT incident, it must immediately be cross-referenced against the 7 RTS classification criteria.

The "No" Path (Non-Major): If no thresholds are breached, the incident is classified as Non-Major and logged only in the internal register. Handlers are directed to run the 24-to-72-hour aggregation check to see if its impact combines with other parallel events to trigger a threshold retroactively.

The "Yes" Path (Major): Meeting any single threshold automatically classifies the event as a Major Incident. This bypasses normal engineering escalation loops and activates the ICT Incident Notifier to initiate the 3-stage CSSF workflow, starting with the initial notification within the strict 4-hour window.




## Testing Triage

This decision tree acts as a strategic gate for the Management Body to manage complex testing requirements without over-allocating specialized engineering resources.

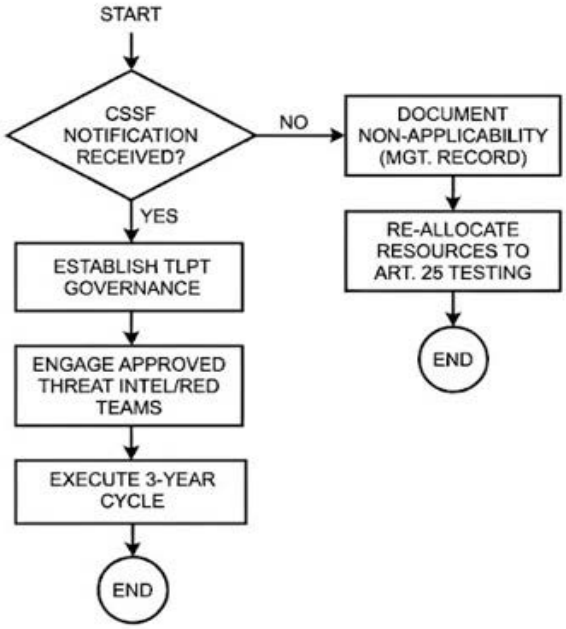
1. The Governance Trigger: During the annual corporate governance or risk profile review, the institution evaluates its current business size, systemic footprint, and complexity.

2. The Regulatory Filter: The entire process hinges on one single criterion: Has a formal, official notification been received directly from the CSSF designating the entity as in-scope for Threat-Led Penetration Testing?

3. Strategic Execution Paths:

- **The "No" Path (Standard Gating):** Without an explicit regulatory mandate, the institution must not initiate a TLPT cycle. Instead, the Management Body formally documents this non-applicability within its annual governance record to defend its regulatory stance, safely shifting 100% of those specialized security resources into maximizing the standard, proportionate Article 25 testing calendar (vulnerability scanning, penetration testing, and BCP/DR drills).

- **The "Yes" Path (Designated Entities):** If notified by the regulator, the organization immediately activates a dedicated TLPT governance framework. This safely triggers the procurement of CSSF-approved external threat intelligence and ethical red-team vendors to execute the mandatory 3-year testing cycle.




## 6.4. Conclusion

Effective DORA compliance in the areas of ICT incident management and operational resilience testing requires financial entities to implement two complementary capabilities: a structured, impact-driven incident classification and reporting framework, and a proportionate, risk-based testing programme. The practical guidance set out in this topic emphasises that success depends not on the volume of incidents reported or tests conducted, but on the quality of internal triage processes, the speed of regulatory notification, and the transparency of remediation tracking.

Entities are advised to prioritise three foundational actions: first, formalising an internal classification matrix aligned with the ESA's RTS criteria and embedding clear escalation thresholds into frontline operations; second, designating an empowered ICT Incident Notifier capable of initiating the three-stage CSSF reporting workflow within the mandated four-hour

window; and third, establishing an annual testing calendar that scales vulnerability scanning, penetration testing, and business continuity exercises to the entity's size, risk profile, and systemic importance. With respect to Threat-Led Penetration Testing, entities should refrain from initiating TLPT cycles unless formally designated by the CSSF, and should instead redirect resources toward maximising their Article 25 testing programme.

From a supervisory perspective, the CSSF will assess not only whether incidents were reported on time, but whether the entity maintains a documented, governance-approved framework that demonstrates ongoing operational resilience. Entities that adopt a disciplined, risk-proportionate approach — supported by clear internal mandates, pre-configured reporting infrastructure, and active Management Body oversight — will be best positioned to meet both the regulatory requirements and the underlying objective of DORA: ensuring the continuity and integrity of critical financial services in the face of ICT disruptions.

# 7 TOPIC 6: OVERSIGHT OF ICT THIRD PARTIES

## 7.1. CONTEXT

The Digital Operational Resilience Act (DORA) introduces a comprehensive framework for managing ICT third-party risk across the EU financial sector. The provisions governing ICT third-party oversight present operational challenges given the complex, multi-layered service arrangements that are characteristic of the alternatives industry. This paper sets out the key pain points identified by industry participants and proposes areas for active contribution to support effective and proportionate implementation.

## 7.2. DIFFICULTY AUDITING ICT PROVIDERS AND SUB-PROVIDERS

Luxembourg AIFMs rely on a broad ecosystem of ICT service providers, ranging from fund administrators and depositary banks to specialized technology vendors and cloud infrastructure providers. A core challenge identified by industry participants is the practical difficulty of conducting meaningful audits of these providers, and particularly their sub-contractors.

DORA requires financial entities to maintain robust audit rights over their ICT third-party providers. However, in practice, many large technology providers — particularly hyperscale cloud providers, operate under standardized contractual terms that significantly limit individual clients' ability to conduct bespoke audits. For smaller players, negotiating leverage required to secure meaningful audit rights is often absent. This creates a structural gap between regulatory expectation and market reality.

Furthermore, audit fatigue is a growing concern. Where multiple financial entities rely on the same ICT provider, duplicative individual audits create significant burdens on both sides without necessarily improving oversight outcomes. Industry participants have called for greater recognition of pooled or third-party audit mechanisms as a valid means of satisfying DORA's audit requirements.

## 7.3. LIMITED FEASIBILITY OF AUDIT RIGHTS ALONG SUBCONTRACTING CHAINS

The challenge is compounded when ICT services are delivered through extended subcontracting chains. A typical Luxembourg AIFM may contract with a primary ICT provider, which in turn relies on multiple sub-contractors for specific components of service delivery. DORA's requirements flow down the chain, but the practical ability of a financial entity to enforce audit rights against fourth or fifth-party providers is extremely limited.

Contractual "flow-down" clauses, while theoretically capable of preserving audit rights along the chain, are difficult to enforce in practice. Sub-providers often resist granting audit rights to entities with whom they have no direct contractual relationship. In many cases, the primary provider itself may not have unfettered audit access to its own sub-contractors, making it impossible to pass on rights that do not exist.

This creates a significant blind spot in the oversight framework. Industry participants note that without clearer regulatory guidance — or supervisory acceptance of alternative assurance mechanisms such

as SOC 2 reports, ISO 27001 certifications, or independent third-party assessments — compliance with the letter of DORA in this area will remain aspirational rather than achievable for many Luxembourg AIFMs.

## 7.4. PRACTICAL GUIDANCE: UNCERTAINTY REGARDING OBLIGATIONS WHEN AN ICT PROVIDERS BECOMES A CRITICAL THIRD-PARTY PROVIDER (CTPP)

The designation of an ICT provider as a Critical Third-Party Provider (CTPP) under DORA triggers a distinct supervisory regime, including direct oversight by a Lead Overseer. While this framework is designed to enhance systemic resilience, it creates significant uncertainty for Luxembourg AIFMs in their day-to-day contractual and risk management relationships.

### KEY UNCERTAINTIES IDENTIFIED BY INDUSTRY PARTICIPANTS INCLUDE:

- Contractual renegotiation obligations: It is unclear to what extent financial entities are required to proactively renegotiate existing contracts with newly designated CTPPs to reflect the enhanced requirements, and within what timeframe.
- Interaction between financial entity obligations and CTPP oversight: The respective responsibilities of the financial entity and the Lead Overseer in monitoring CTPP performance are not always clearly delineated, creating potential for duplicative requirements or, conversely, gaps in accountability.
- Impact on exit planning: DORA requires financial entities to maintain viable exit strategies for critical ICT providers. Where a provider is designated a CTPP, the systemic importance of that provider may itself undermine the feasibility of exit, creating a tension between regulatory expectations and market structure.

### ACTIVE INDUSTRY CONTRIBUTION

**1. Practical Oversight Frameworks for ICT Providers**

Industry participants are well-placed to contribute to the development of practical, risk-based oversight frameworks that reflect the realities of the Luxembourg alternatives market. Specifically, the working group could develop:

- Tiered oversight models that calibrate the intensity of monitoring and audit activity to the criticality and risk profile of each ICT provider, rather than applying uniform requirements across all third parties.
- Standardized due diligence questionnaires and assessment templates tailored to the alternatives sector, enabling consistent and efficient oversight without duplicative effort.
- Guidance on the use of collective audit mechanisms, including the conditions under which pooled audits or recognized third-party certifications can satisfy DORA's requirements.

**2. Guidance on Reasonable Audit Rights**

The working group should actively engage with regulators and counterparts to develop practical guidance on what constitutes reasonable audit rights under DORA, particularly in the context

Tcontext of large or dominant ICT providers. This guidance should address:

- Minimum contractual provisions that satisfy DORA's audit requirements while remaining commercially achievable.- The role of industry-recognized certifications (SOC 2, ISO 27001, ISAE 3402) as substitutes or supplements to direct audit rights.
- Mechanisms for coordinating audits across multiple financial entities to reduce duplication and improve efficiency.
- Petitioning the regulator to directly audit CTPPs, thereby reducing risk and driving greater control of CTPPs.

**3. Clarification of Expectations When a Provider Becomes a CTPP**

The working group should seek regulatory clarity on the practical implications of CTPP designation for existing contractual arrangements and ongoing risk management obligations. Priority areas for clarification include:

- Transition timelines and expectations for contract remediation following CTPP designation.
- The division of supervisory responsibility between financial entities and the Lead Overseer.
- Regulatory expectations around exit planning where concentration risk makes genuine exit impractical.

## 7.5. PRACTICAL GUIDANCE: BEST PRACTICES FOR OVERSIGHT OF ICT THIRD PARTIES

A key challenge for financial institutions in implementing DORA lies in operationalising the regulatory requirements, in a structured, scalable and sustainable manner. In practice, institutions often face fragmented third-party management practices, inconsistent documentation and limited visibility over ICT dependencies, particularly in complex, multi-vendor environments.

To address this, a phased and pragmatic approach to ICT third-party oversight is critical. A structured approach model provides an effective pathway to transition from current-state fragmentation to a fully operational, risk-based oversight framework aligned with DORA expectations.

**Establishing the Baseline:**

Begin by building a comprehensive understanding of the existing third-party landscape. Many institutions operate with partial inventories, inconsistent classification of providers and limited alignment between contractual, risk, and operational data. This lack of transparency directly undermines the ability to meet DORA requirements, particularly in relation to maintaining a complete register of ICT third-party arrangements and identifying providers supporting critical or important functions.

Structured planning enables institutions to consolidate and assess their current framework, with particular focus on multi-vendor strategy, concentration risk exposure, and the robustness of existing contractual and control mechanisms. Importantly, this assessment should not be limited to direct providers but should also consider upstream dependencies, including subcontracting chains and cloud service ecosystems.

From a regulatory standpoint, this phase supports alignment with DORA's obli-

gations, including the identification and classification of ICT services, the mapping of dependencies to critical functions, and the establishment of a reliable third-party register. More fundamentally, it provides the foundation for a risk-based prioritisation, ensuring that remediation efforts are focused on areas of highest impact.

**Designing a Consistent and Scalable Framework:**

Once visibility is established, institutions must address identified gaps through the design and implementation of a coherent and standardised third-party risk management framework. In practice, deficiencies often arise from inconsistent approaches to due diligence, incomplete contractual safeguards, and the absence of formalised exit strategies.

Remediation focuses on building the core components required under DORA, ensuring that they are both internally consistent and operationally usable. This includes the development of structured methodologies for assessing the criticality of ICT services, performing risk-based due diligence, and conducting ICT and operational risk assessments. Equally important is the establishment of a robust contractual framework, incorporating DORA-aligned clauses covering audit rights, access to data, incident reporting, subcontracting, and termination conditions.

A key success factor at this stage is the standardisation of artefacts and processes. The use of harmonised templates, checklists, and assessment criteria ensures comparability across providers and facilitates supervisory review. Furthermore, institutions should ensure that remediation efforts are closely aligned with existing regulatory frameworks, such as CSSF Circular 22/806, to avoid duplication and ensure coherence across regulatory obligations.

Another critical dimension is the incorporation of exit planning as a practical capability rather than a formal requirement. Institutions should define clear exit strategies for critical ICT providers, supported by actionable playbooks and aligned with business continuity and disaster recovery planning. This reflects DORA's emphasis on ensuring that firms can maintain operational continuity under stressed conditions, including the failure of a key third party.

**Embedding Continuous and Risk-Based Oversight:**

After baselining and designing a consistent and scalable framework, the last task is to embed the framework into day-to-day operations, to ensure that ICT third-party oversight evolves from a static compliance exercise into a dynamic, risk-driven discipline. Under DORA, institutions are expected to move beyond periodic assessments and implement continuous monitoring of third-party performance, risk, and resilience.

In practice, this requires the execution of recurring oversight activities, including periodic due diligence reviews, ongoing risk assessments, contractual compliance checks, and performance monitoring against defined service levels. Institutions must also ensure the continuous maintenance of the ICT third-party register, reflecting any changes in scope, criticality, or provider relationships.

Attention should be paid to the integration of third-party oversight with broader

operational resilience and ICT risk management frameworks. This includes linking third-party performance to incident management processes, incorporating provider dependencies into business continuity planning, and reviewing outputs from disaster recovery and security testing activities.

Additionally, institutions must ensure that their oversight framework supports regulatory reporting and regulatory engagement, including the ability to provide timely and accurate information to competent authorities, such as the CSSF, particularly in the context of material outsourcing arrangements or significant incidents.

**Addressing Concentration Risk and Systemic Dependencies:**

Across all activities, institutions must explicitly consider concentration risk and systemic exposure, which are central themes under DORA. The increasing reliance on a limited number of ICT providers, particularly global cloud service providers, introduces vulnerabilities that extend beyond individual institutions. Effective oversight therefore requires a portfolio-level perspective, assessing dependencies not only at the individual contract level but across the entire ICT ecosystem. Institutions should evaluate the potential impact of provider failure, geographic concentration, and sector-wide dependencies, and define risk appetite thresholds where appropriate.

Where diversification is not feasible, institutions must ensure that risks are formally acknowledged, monitored, and mitigated through enhanced controls, including strengthened contractual safeguards and more intensive oversight.

**Leveraging Technology to Enable Scalable Oversight:**

Given the scale and complexity of ICT third-party ecosystems, manual processes are unlikely to meet DORA expectations. Institutions should therefore invest in technology-enabled solutions, such as integrated governance, risk, and compliance (GRC) platforms, to support the automation and centralisation of third-party risk management activities. Such tools enable the maintenance of a single source of truth for third-party data, facilitate workflow management for due diligence and risk assessments, and support the generation of management and regulatory reporting. More advanced implementations may also incorporate risk indicators, automated alerts, and data analytics, enabling a more proactive approach to risk identification and mitigation.

## 7.6. CONCLUSION

The oversight of ICT third parties represents one of the most operationally complex aspects of DORA for Luxembourg-based alternative investment managers. The challenges of auditing extended service chains, securing meaningful contractual rights with dominant providers, and navigating the uncertainties of the CTPP regime require both pragmatic regulatory guidance and coordinated industry action. This working group is well-positioned to contribute concrete, practical proposals that support the objectives of DORA while reflecting the operational realities of the Luxembourg alternatives sector.

# 8 OVERALL CONCLUSION

The work of the L3A Working Group demonstrates that, while DORA provides a robust and harmonized regulatory framework, its effective implementation depends on proportional application and pragmatic operationalization based on a realistic picture of risk.

Across all topics addressed in this paper, several common themes emerge:

- Whether assessing ICT services, applying proportionality or managing third-party risk, regulatory compliance must reflect the true nature and risk profile of activities, rather than a purely formal or technical classification.
- DORA consistently requires that decisions, right from proportionality assessments to ICT risk governance and third-party oversight, must be clearly documented.
- Successful implementation relies on embedding DORA requirements into existing governance, risk management, and operational processes, rather than creating parallel or fragmented structures.
- DORA is not a one-off compliance exercise, but a framework requiring ongoing monitoring, testing, learning and improvement, supported by strong governance and management body involvement.
- Certain areas, typically, ICT third-party oversight and the treatment of complex service arrangements, require continued engagement between industry participants and regulators to practical solutions.

For Luxembourg's alternative investment sector, the complexity of operating models, reliance on specialized service providers, and globalized ICT ecosystems make DORA implementation both challenging and strategically important. Entities that adopt a structured, risk-based and proportionate approach, supported by clear governance and high-quality documentation, will be best positioned to meet supervisory expectations and demonstrate resilience.

Finally, this aims to contribute to an ongoing dialogue. The L3A Working Group remains committed to refining these perspectives as regulatory expectations evolve and implementation practices mature, with the objective of supporting a consistent and effective application of DORA across the industry.

LUXEMBOURG
ALTERNATIVE
ADMINISTRATORS
ASSOCIATION