LPEA

Experts' Insights:

Implementing DORA Register of Information

Table of Contents

Introduction

The Luxembourg Private Equity and Venture Capital Association (“LPEA”) aims at promoting and defending the interests of investors and professionals principally active in the field of Private Equity (“PE”) and Venture Capital (“VC”).

The Association is the trusted and relevant representative body of PE and VC practitioners with a presence in Luxembourg.

Created in 2010 by a leading group of PE and VC players, with more than 590 members, LPEA plays a leading role locally, actively promoting PE and VC in Luxembourg.

LPEA provides a dynamic and interactive platform, which helps investors and advisors to navigate through latest trends in the industry. International by nature, the association allows members to network, exchange experience, expand their knowledge and grow professionally attending workshops and trainings held on a regular basis.

About the document

The work presented herein has been conducted by members of the LPEA, who are professionals active in the field of digital operational resilience, risk management, regulatory compliance and information management. This document gathers members' expertise, knowledge and experience in relation to the management of the Register of Information ("RoI") under the Digital Operational Resilience Act ("DORA") and provides their pragmatic highlights in this regard. The Association maintains a neutral stance regarding the insights shared within this context. The LPEA does not provide specific advice or endorse any particular company, product, or service over another. All opinions expressed are those of the individual members and do not necessarily reflect the views of the Association as a whole.

About the authors

Christophe Buschmann - *KPMG Luxembourg, Director*

Christophe is a Director in charge of Technology Risk at KPMG Luxembourg and previously served as Commissioner for Data Protection at the Luxembourg supervisory authority CNPD

Aurélie Caillard - *Pinsent Masons Luxembourg, Associate*

Aurélie is an Associate at Pinsent Masons Luxembourg. She provides expert advice to both domestic and international clients on data protection, intellectual property and technology, media and telecommunications (IP/TMT), contract law, and emerging technologies.

Leonhard Kossmann - Fundvis, Co-Founder & CEO

Leonhard is a data-scientist and the Co-Founder and CEO of Fundvis an Agentic-AI driven process automation platform from Luxembourg.

Onur Özdemir - *KPMG Luxembourg, Partner - Information Risk Management*

Onur has more than 15 years' experience in audit, information technology, governance and risk management, with a focus on IT and third-party risk regulatory compliance.

George Ralph - *RFA, Global Managing Director & CRO*

As Global Managing Director & CRO of RFA, George is a technology and business leader with a proven track record of strategic alignment, process improvement and guidance.

Executive Summary

DORA presents a significant shift in how financial entities must manage their digital operations and third-party ICT dependencies. One of the core requirements under DORA is the creation and maintenance of a comprehensive Register of Information ("RoI"), due by 15 April 2025, which will document all contractual arrangements with ICT third-party providers across entity, sub-consolidated, and consolidated levels.

On the regulators' side, this register will be an important source of information in the supervision of the management of ICT third-party risk by in-scope entities and a key element in the designation of the Critical Third-Party Service Providers (CTPP) who will categorize as systemic entities.

Regarding the reporting format, the CSSF confirmed that this register needs to be submitted in plain CSV format. The European Supervisory Authorities (ESAs) also recently informed market participants that they will not provide an Excel converter as they did for the Dry Run Exercise. Those points place an important emphasis on accurate data input and the adoption of robust data management tools to ensure compliance.

For financial entities, this means embedding digital resilience in their existing risk management framework. The RoI indeed serves not just as a compliance tool but as a centralized resource that enables companies to better manage and monitor ICT risks, from service dependencies to subcontractor relationships. Entities are required to populate the register with details in relation to the categories of ICT third-party service providers, the type of contractual arrangements as well as the ICT services and functions which are being provided. Given the rigorous format and validation rules that will be used, it can be highlighted that data quality and accuracy will be closely monitored by regulators. Any discrepancies could result in delays, resubmissions, or regulatory penalties.

To effectively comply, financial institutions need to explore a possible move beyond manual spreadsheet-based tracking and integration of solutions that allow for efficient data management and automated reporting. This includes tools for CSV conversion, validation, and error checking to meet the DORA submission rules. Integrated, automated solutions can help entities in streamlining their RoI processes, ensuring timely, accurate, and transparent reporting to national and supranational regulators.

By meeting these regulatory requirements, financial institutions will not only achieve DORA compliance but also enhance their ability to manage ICT third-party risks proactively. The RoI facilitates better risk assessments, mitigates vulnerabilities, and provides the necessary data for critical decision-making. Ultimately, the RoI is a key element in ensuring long-term digital operational resilience. The coming months provide a crucial window for companies to optimize their processes, implement technological solutions when deemed appropriate, and ensure that the 15 April 2025 deadline is smoothly.

Introduction

The Digital Operational Resilience Act ("DORA") is a transformative regulation introduced by the European Union to fortify the digital and operational resilience of financial entities. DORA is applicable since 17 January 2025 and mandates in-scope financial entities to notably create and maintain a comprehensive Register of Information ("RoI") on their contractual arrangements with ICT third-party service providers, which shall be available "at entity level, and at sub-consolidated and consolidated levels" (Art.28(3) of DORA).

As mentioned by the 3 European Supervisory Authorities (the European Securities and Markets Authority "ESMA", the European Banking Authority "EBA" and the European Insurance and Occupational Pensions Authority "EIOPA", together referred to as the European Supervisory Authorities "ESAs") in their recent publication "Key Findings from the 2024 ESAs Dry Run exercise", this RoI will serve as a centralized internal repository enhancing the oversight and transparency of the monitoring of ICT third-party risk. For competent national authorities, it will be an important source of information in the supervision of the management of ICT third-party risk by in-scope entities. For the ESAs more specifically, the RoI will be a key element in the designation of the Critical Third-Party Service Providers (CTPP) who will be categorized as systemic entities and who will, as a result, be subject to the direct supervision of the ESAs through the appointment of a Lead Overseer at ESAs level.

The objective of this Paper is to provide in-scope entities within the PE industry with pragmatic insights from experts in the digital operational resilience field. This intends to help them in optimizing their implementation of an effective RoI in accordance with the requirements set out in the related ITS and ensure data quality meets the expectations of the company, in alignment with - and enhancing- their own risk management framework, but also of the regulators, at both national and supranational level.

In the following sections, LPEA members will share their expertise and explore best practices for effectively implementing the RoI under DORA, highlighting how this approach can help financial institutions manage third-party ICT dependencies, mitigate associated risks, and ensure compliance with regulatory requirements.

Understanding DORA RoI

By Christophe Buschmann, KPMG

Introduction

The RoI under DORA is a crucial tool for financial entities. It provides a clear and structured overview of outsourcing relationships and dependencies, ensuring that regulatory requirements are monitored and met.

Beyond compliance, the RoI helps entities understand their standing and trigger necessary actions to address potential vulnerabilities.

Dual Purpose of the RoI

1. **For Regulated Entities:** the RoI allows entities to comprehensively document their outsourcing relationships and ICT dependencies. It serves as a compliance requirement while also acting as an internal management tool, enabling entities to monitor and manage these dependencies effectively.
2. **For Supervisory Authorities:** the RoI provides regulators with critical data to consolidate sector-wide ICT dependencies. This enables them to identify systemic ICT providers and designate them for stricter oversight. The RoI's role in this process underscores its importance and explains the high level of scrutiny from supervisory authorities.

Prescriptive Nature and Its Implications

The RoI is one of DORA's most prescriptive components, with clearly defined requirements for its content and format. This brings several implications:

- **Objective and Transparent:** the RoI's standardized structure ensures a factual and consistent representation of an entity's outsourcing relationships, leaving little room for interpretation.
- **Increased Accountability:** entities must ensure the accuracy and completeness of their RoI to avoid unfavorable regulatory comparisons or scrutiny. Any discrepancies could raise concerns about the entity's risk management practices.
- **Limited Scope for Adjustments:** the rigid format of the RoI means there is minimal opportunity for contextual explanations, placing greater emphasis on the quality of the data submitted.

Insights from the ESAs' Dry Run Exercise

The RoI was tested during a dry run exercise organized by the supervisory authorities (ESAs) over the summer 2024. While feedback indicated that results were generally at the expected level, only 6.5% of participants submitted a register that passed all quality checks set by regulators. Additionally, 50% of the remaining

registers failed fewer than five out of 116 data quality checks. These results highlight that maintaining the RoI to the required standard remains a significant challenge for many entities.

Technical Challenges in Managing the RoI

Maintaining and reporting the RoI involves several technical challenges:

1. **Identifying Information Sources:** entities must first identify the correct sources of information to populate the RoI. This includes gathering data on contracts, service levels, and risk assessments from various internal and external systems.
2. **Data Encoding and Management:** the chosen tool for managing the RoI is critical. While smaller entities may find spreadsheets sufficient, larger organizations require more sophisticated solutions to ensure data consistency and accuracy.
3. **Transformation and Reporting:** entities must have processes in place to transform and export the RoI into the format required by regulators. This involves aligning the register's content with the Implementing Technical Standards (ITS).
4. **Ensuring Data Quality and Completeness:** supervisory authorities have emphasized that data quality is paramount. Entities must ensure their RoI is both complete and accurate, as regulators will rely on this information for systemic assessments. Any errors or omissions could lead to further scrutiny or requests for resubmission.

RoI as an Extension of the Outsourcing Register

The RoI can be viewed as an extension of the traditional outsourcing register, but with a scope aimed at managing digital operational resiliency risk. It reflects the complex relationships between entities and services, offering a granular view of dependencies. Effectively, the RoI represents the full ecosystem that the entity relies on, akin to a relational database capturing intricate service interdependencies.

Compliance Requirements under DORA RoI

By Aurélie Caillard, Pinsent Masons Luxembourg

DORA introduces stringent requirements for financial entities to enhance their digital resilience.

With the RoI, in-scope entities must document, maintain and update all contractual arrangements with third-party ICT service providers. It applies to contracts at entity, sub-consolidated and consolidated level, including intra-group ICT arrangements.

The RoI requirements are contained in DORA itself while a Commission implementing Regulation from 29 November 2024 lays down ITS with regard to standard templates for the RoI (Implementing Regulation 2024/2956)[1].

Navigating Compliance: Drafting the RoI

The Implementing Regulation 2024/2956 and its first Annex provide details that are essential for the drafting of the RoI. In the Register, in-scope entities must include detailed information about, among others, the (a) contractual arrangements with specific reference number, b) ICT services used and qualified as critical or important or not, c) the ICT providers and all the subcontractors on ICT service supply chain, considering the substitutability and the exit plan, d) figure information as annual expense or estimated cost of the contractual arrangement for the past year, and e) termination information.

On the regulators' side, it is worth mentioning that there was a debate between the European Commission and the ESAs regarding the method of identification of the ICT third-party provider. The European Commission would prefer to allow the use of either the Legal Entity Identifier (LEI) or the European Unique Identifier (EUID). On 15 October 2024[2], the ESAs expressed concerns that incorporating the EUID alongside the LEI would add unnecessary complexity and increase implementation costs. Standardized identifiers like the LEI indeed enable the consistent identification of the providers across borders. The LEI enhances corporate structure detection, facilitates data integration, and streamlines compliance and incident reporting, ultimately improving operational resilience for financial institutions and their interconnected systems. The CSSF, in its Communiqué published on 5 December 2024[3], reminded in-scope entities to proceed with the activation of the LEI if not already done.

Having consistent data, including a calendar of the contractual process with notice periods detailed (article 30.2, h of DORA), provides an opportunity to have clear,

[1] Commission Implementing Regulation (EU) 2024/2956 of 29 November 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to standard templates for the register of information.
[2] JC 2024 75, Opinion of the European Supervisory Authorities on the Draft Implementing Technical Standards regarding the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554.
[3] https://www.cssf.lu/fr/2024/12/reglement-dora-rappels-et-conseils-sur-la-preparation/

accessible and intelligible information in the event of needing to terminate or renegotiate contracts.

Furthermore, it is advised to ensure contractual provisions with third party suppliers are broad enough to ensure that the supplier is compelled to give all information necessary to complete the Register. It is not a mandatory contractual requirement set out in article 30 of DORA but necessary for the in-scope entities to meet its own compliance requirements. Engaging with the stakeholders throughout the value chain is a key aspect in managing the expectations under DORA.

Meeting the RoI requirements will also help entities focus on the important issues of the security measures and the question of where their data is located and stored[4].

Based on articles 28.5 and 30.3, c) of DORA, in-scope entities must engage ICT third-party service providers that meet high information security standards, especially for critical functions. This includes ensuring smaller providers also allocate sufficient budget for security to prevent ICT incidents and personal data breaches. Comprehensive security across all providers is essential.

Mitigating Data Loss Risks with ICT Service Providers

In any ICT outsourcing arrangement, there is a risk of loss of data. For example, in 2021, there was a fire within a high-profile European data center operator and one of the largest hosting companies. Due to the fire that ravaged its server centers, it was judged that there was a contractual breach in its automated backup offer. The backups were stored in the same building as the server, even though it had committed to ensuring they were physically isolated from the infrastructure where the client's virtual private server was set up. Thousands of clients have temporarily lost access to services and permanently lost data. The contractual failure allowed clients to claim compensation, but the damage was already done. In addition, expert reports revealed that the industrial site housing the servers had inadequate safety measures and defective equipment, exacerbating the impact of the fire.

This incident serves as a powerful reminder of the practical importance of maintaining a comprehensive register in contract management.

On another note, the RoI is not only a tool of contract management, but also necessary in the purpose of DORA specific obligations.

[4] In points B.02.02.015 and 0160 Instructions to complete template B_02.02 — Contractual arrangements – Specific information, Annex I - Instructions for completing the register of information, Part 2 – Template-specific instructions.

Meeting Reporting Obligations

1. Entities must report annually to national supervisory authority on new ICT service arrangements, categories of ICT service providers, and types of contractual arrangements[5].
2. The entire register must be made available upon request of the supervisory authority to ensure transparency and accountability[6].

Luxembourg supervisory Authorities will pay particular attention to the drafting of the register.

Supervisory Oversight and Sanctions: Complying with DORA's ROI Requirements

Based on the Luxembourg Law of the 1rst July 2024 (the Law), the CSSF is the competent authority responsible for overseeing the financial sector and the CAA is the competent authority responsible for supervising the insurance sector, for the purpose of DORA.

As the first RoI will need to be provided by the competent authorities to the ESAs by 30 April 2025, financial entities are required to submit their RoI to the CSSF from 1 April 2025 to 15 April 2025 via a specific tool[7].

Pursuant to article 20-23 of the Law, these Authorities would be able, among others, to monitor the register of information and the contracts mentioned therein via their powers of access to documents and data and make or receive copies. They can also, among others, summoning representatives in order to have explanations, either orally or in writing, regarding facts or documents related to the investigation (for instance linked with the RoI).

The Authorities may impose administrative penalties and other measures in accordance with Article 20-24 of the Act, which could apply to the entity itself, members of its management body and other responsible persons. Sanctions may take the form of, for instance, an injunction ordering the cessation of the wrongful conduct and preventing its recurrence, the temporary or permanent cessation of any practice deemed contrary to DORA by the competent Authority, administrative fine of up to EUR 5 million or 10% of the total annual turnover for legal persons, on the basis of the latest available consolidated financial accounts, or a public statement identifying the person responsible and detailing the nature of the offence.

Ultimately, meeting RoI requirements under DORA will help in-scope entities focus on critical security issues and ensure the resilience of their digital operations and in enhancing transparency and accountability.

[5] article 28.3, 3rd paragraph of DORA
[6] article 28.3, 4th paragraph of DORA
[7] Entry into application of DORA regulation on 17 January 2025 – CSSF

Implementing the RoI: enhancing organizational transparency and efficiency

By George Ralph, RFA

The implementation and ongoing maintenance of the RoI is a critical task for organizations in 2025 and after. The RoI serves as a centralized repository for tracking operational resilience, and ICT dependencies, ensuring compliance with DORA while enhancing organizational transparency and preparedness.

In the following, we are sharing 10 insights and takeaways for an effective integration of the RoI.

1. Understanding Regulatory Requirements

The foundation of an effective RoI implementation is a deep understanding of DORA's objectives and specific mandates:

- Familiarize yourself with the key components of the DORA framework, including its objectives, scope, and specific requirements.

2. Establishing a Cross-Functional Team

Successful implementation requires collaboration across departments:

- Form a dedicated, interdisciplinary team comprising IT, compliance, risk management, and business operations professionals to oversee the implementation process.
- Foster clear communication and cooperation among stakeholders to ensure unified efforts and efficient decision-making.

3. Building a Comprehensive Data Inventory and Classification

Accurate and complete data is the cornerstone of an effective RoI:

- Prepare the inventory of all data and digital assets along with ICT dependencies.
- Classify data based on sensitivity, criticality, and regulatory requirements.
- Clearly define the types of data to be collected for the RoI.
- Establish reliable sources for data gathering, such as IT systems, incident logs, and risk management tools.
- Document relationships between group entities, critical functions, and the services provided by third party ICT providers to facilitate risk assessments and exit strategies.

4. Developing a Robust Risk Management Framework

A proactive approach to managing ICT risks is essential for DORA compliance:

- Create a comprehensive framework to identify, assess, and mitigate operational digital risks.
- Continuously monitor and update risk assessments to address evolving threats.
- Create a clear oversight across providers and their relationships with your group entities critical functions and the types of services they are providing for each of them. This is extremely useful for risk calculation in regards to level of reliance and exit strategies.

5. Investing in Technology Infrastructure and Standardization

Leverage technology to streamline RoI management and compliance processes:

- Ensure your IT infrastructure is resilient and can withstand operational disruptions.
- Integrate the RoI with existing systems, such as risk management and incident reporting platforms, using APIs to ensure real-time updates and data accuracy.
- Develop templates for common data submissions to streamline the process and minimize errors by having a standardized end-to-end process for any upcoming critical ICT provider and reporting.
- Automate data collection, reporting, and risk monitoring using advanced technologies.
- Ensure alignment of the reporting tools with all reporting and data management requirements, including the latest Regulatory Technical Standards (RTS) and DPM 2.0 reporting framework[8].

6. Training and Awareness

Building a culture of compliance is key to the RoI's success:

- Conduct regular training sessions to educate staff on DORA requirements and best practices for maintaining the RoI.
- Promote a culture of compliance and awareness regarding the importance of operational resilience across the organization.

7. Documenting and Reporting

Transparent documentation supports regulatory compliance and operational clarity:

[8] "DPM 2.0" is a framework used to standardize the data reporting requirements outlined in the Digital Operational Resilience Act (DORA). It facilitates consistent data collection, processing, and reporting across financial institutions, ensuring that data is accurately represented and easily accessible for regulatory compliance.

- Ensure that reporting mechanisms are transparent and aligned with DORA expectations.
- Maintain detailed records of processes, decisions, and compliance efforts related to the RoI.
- Regularly validate reports against submission requirements to avoid errors, particularly when reporting to regulators.

- Implement systems that allow for continuous monitoring of operational resilience metrics and incidents to ensure real-time data availability.

8. Data Security and Access Control

Protecting the integrity and confidentiality of the RoI is critical:

- Implement role-based access controls to restrict unauthorized access. Use encryption and secure storage solutions to safeguard sensitive information.
- Regularly validate data to ensure quality and accuracy, and establish protocols for correcting discrepancies promptly.

9. Stakeholder Engagement and Feedback

Collaboration with internal and external stakeholders enhances the RoI's relevance and usability:

- Establish communication channels for updating stakeholders, including regulators, on changes to the register.
- Develop feedback mechanisms to gather input and improve register management practices.
- Collaborate with industry peers to share best practices and insights.

10. Fostering Continuous Improvement

To ensure the RoI remains effective and compliant over time:

- Regularly review and refine processes based on audit results, stakeholder feedback, and industry best practices.
- Benchmark practices against peers and stay informed about technological advancements and regulatory updates.

By implementing these best practices, organizations can effectively integrate and maintain the RoI, achieving compliance while bolstering their digital operational resilience. A well-maintained RoI not only fulfills regulatory requirements but also supports long-term organizational success in a rapidly evolving risk environment.

Use case: how appropriate Fintech tool can ease the RoI process

By Leonhard Kossmann, Fundvis

Since December 2024, the final form of the RoI has been established, along with the validation rules, reporting format, and the role of DPM 2.0.

It is worth mentioning that for many professionals, the Excel format used during the ESAs Dry Run Exercise was expected to serve as the basis for the first submission. However, this expectation was soon replaced by the confirmation that the official reporting framework will require ZIP and plain CSV formats, with XLS no longer being accepted.

In this context, it remains crucial to input the CSV codes correctly for the various dropdowns to maintain coherence in the RoI and ensure proper processing by regulators.

As highlighted by the ESAs during their workshop on "DORA Dry Run lessons learnt and data quality" held on 18 December 2024, exploring solutions to translate input into the correct format is advisable. In this section, we would like to showcase how the implementation of a software solution to support the creation, maintenance and export of the RoI can benefit a PE in-scope company, in order to achieve DORA readiness.

1. Transfer and aggregation of data points

Upon finalizing the contract, the solution provider enabled the client to onboard all existing providers' data from Excel spreadsheets to their designated environment using an Excel Converter. This streamlined process eliminated the need for duplicate data entry and manual efforts, allowing the company to commence operations efficiently from day one.

2. Gaining a centralised overview of data completeness

Once the data transfer was completed, the solution dashboard provided a clear visualization of critical information, including a comprehensive list of all ICT providers, group entities, and their associated functions. The dashboard highlighted any incomplete or missing information, facilitating quick identification of areas that required further action. By leveraging the platform's collaboration features, the DORA in-scope entity was able to invite third-party providers to participate directly in their workflows, fulfilling the need for data consolidation and integration.

3. Data quality check

With integrated validation rules[9], the client ensured that its RoI complied with required formats and successfully passed all initial checks. After completing and validating the necessary fields, the solution allowed for extracting a comprehensive audit trail encompassing all user interactions and approval flows. Finally, the entire RoI could be exported in the correct format and be integrated through CSSF S3 API.

Ensuring data quality by performing preliminary checks against the official submission rules before sending anything to the regulator was deemed a key aspect in saving time and reputation.

4. Export register

The national and supranational regulators made it indeed clear that technical validation checks would be performed after the submission of the RoI in April 2025. If, during these checks, the RoI fails the validations, in-scope entities will need to resubmit a corrected version. Following this initial national check, a second, supranational, check will be executed by the ESAs, again providing feedback or requesting changes if the validation rules are not met. Since the validation rules have been already published, there is a great opportunity to avoid unnecessary feedback or time-consuming revising of the RoI by performing all available tests before submitting the report.

Looking ahead, the software helps streamline tasks such as managing relationships, ensuring proper data formats and data quality checks, generating exports, meeting deadlines, and keeping up-to-date with regulatory changes.

DORA is a crucial exercise that will enable companies to better structure, understand and perform their IT risk assessment within their overall risk framework. In order to fully achieve this task, a deep understanding of DORA's roots is needed. Ensuring the right standardization of procedures, while maintaining proof of compliance through audit trails is key in minimizing human error and security risks. In order to make organizations benefit and spread understanding and knowledge, clear workflows need to be in place which can be triggered, and which should be followed and tracked in specific situations.

[9] "Validation rules" in the context of DORA refer to the criteria and guidelines used to ensure that data and processes meet regulatory standards for digital operational resilience.

Encompassing the RoI in the Risk Management Framework

By Onur Özdemir, KPMG

In today's financial environment, digital transformation has driven institutions to increasingly rely on third-party ICT providers for both critical and non-critical services. According to the European Central Bank, ICT services represent a significant portion of outsourced critical functions for systemic institutions, highlighting the importance of managing associated risks effectively. While this boosts efficiency and access to expertise, it also introduces significant risks that must be managed.

The RoI helps address these challenges by mandating a comprehensive, structured register of third-party dependencies. The RoI goes beyond cataloging third-party providers; it equips organizations with actionable insights to proactively monitor dependencies, assess vulnerabilities, and implement timely risk response measures. This register empowers organizations to anticipate risks, strengthen controls, and develop secure systems in an integrated manner. By leveraging the RoI, financial entities can prioritize risks, allocate resources effectively, and establish tailored mitigation strategies.

Integrating the RoI into existing risk management framework

Financial institutions commonly rely on ISO 31000, COBIT, or NIST for risk management guidance. By incorporating DORA's requirements for third-party risks, organizations can adopt a more comprehensive approach that strengthens both operational resilience and regulatory compliance.

The RoI provides a single repository for key information, including the type of outsourced service, the provider's geographic location, criticality levels, and any subcontracting relationships. For example, under ISO 31000, the RoI supports risk identification and evaluation by centralizing third-party information, while COBIT's governance and monitoring components can leverage RoI data for continuous oversight of ICT dependencies. This structured data facilitates alignment between third-party risks and broader enterprise risk management (ERM) systems, ensuring consistency in monitoring and reporting.

Identifying and assessing risks related to digital operational resilience

A central objective of DORA is to identify and assess risks that could undermine digital operational resilience. Institutions must consider threats ranging from cyberattacks and system failures to third-party disruptions, data breaches and concentration. Recent examples, such as the IT outage due to CrowdStrike update, leading to widespread system crashes on Microsoft Windows computers worldwide, highlight the cascading risks of extended enterprise vulnerabilities,

where disruptions in critical third-party services can jeopardize operations across dependent organizations. These incidents underscore the importance of having robust oversight and resilience measures in place. Emerging threats such as supply chain disruptions, ransomware attacks, and geopolitical instability underscore the need for a comprehensive view of third-party dependencies. The structured framework of the DORA register helps catalog and analyze these risks comprehensively. The process starts by mapping ICT assets and dependencies, including critical systems, data flows, and service providers. With this overview, institutions can evaluate risks based on factors such as likelihood, potential impact on core operations, and recovery time objectives. Activities integral to core services may warrant stricter oversight and contractual safeguards, while less critical functions might require simpler controls.

Methodologies like threat modeling, scenario analysis, and impact assessments allow organizations to systematically prioritize risks. In combination with accurate data captured in the RoI, these methods help optimize resource allocation and maintain operational continuity.

Developing mitigation strategies

Drawing on the granular insights provided by the RoI, financial institutions can integrate third-party risk management into their broader risk management framework, ensuring an integrated approach to mitigating potential vulnerabilities. By viewing outsourced services in the context of the organization's entire risk ecosystem, firms can identify interdependencies—for example, how a third-party service failure could cascade into operational disruptions, compliance violations, or reputational harm. The RoI not only supports the development of tailored mitigation strategies but could also fosters collaboration across departments, ensuring a coordinated response to third-party risks.

Building on this comprehensive view, institutions can devise tailored mitigation strategies to address the unique risks associated with each third-party relationship. The level of mitigation effort should reflect the criticality of the outsourced service. High-priority critical operations may necessitate robust redundancies, enhanced monitoring, and tighter contractual clauses, while less critical services can be managed with more basic safeguards. This prioritization ensures that resources are concentrated where they are needed most, maintaining organizational resilience and alignment with regulatory expectations such as those set by the DORA.

In addition to preventative measures, the RoI supports the creation of effective incident responses and recovery plans, ensuring that these plans are woven into the broader governance structure. Clear responsibilities, escalation paths, and communication procedures should be defined to ensure a coordinated response across all levels of the organization. Regular testing—through tabletop exercises or realistic simulations—can validate these plans and strengthen organizational preparedness. By integrating lessons learned from prior incidents, institutions can continuously refine their risk management practices, ensuring their relevance in a dynamic threat landscape.

Because the RoI should be continually updated, institutions can proactively adjust their mitigation strategies as new threats emerge or operational environments change. This iterative approach aligns with a holistic risk oversight philosophy, enabling organizations to enhance resilience while remaining agile in adapting to new challenges. By doing so, financial institutions can adapt quickly to evolving challenges, maintain regulatory compliance, and preserve operational resilience in a rapidly changing financial and technological landscape.

Conclusion

The implementation of the RoI is a pivotal requirement for financial entities, demanding meticulous attention to details and operational readiness to ensure compliance by 15 April 2025. As the RoI is now required in plain CSV format - with simple Excel no longer accepted - financial institutions must explore the adoption of more streamlined and automated approach to data collection, validation, and reporting.

In this context, it is key for in-scope entities to assess the interests of a transition from manual systems to technology-driven solution in order to meet the data quality requirements and avoid delays or resubmissions. The right tools can not only ensure accuracy and compliance but also enhance the organization’s ability to manage third-party ICT risks, thereby improving the overall digital resilience.

Integrating the RoI into an institution's broader risk management framework provides a structured way to track and assess the risks associated with outsourced services and critical dependencies. With the appropriate systems in place, financial entities can ensure that they not only meet the immediate RoI requirements but also lay the foundation for sustained operational resilience in the face of evolving digital risks. The RoI is more than a regulatory checkbox - it is an opportunity for financial institutions to strengthen their digital backbone, improve risk oversight, and demonstrate their commitment to robust operational resilience well into the future, leading at the end of the journey to increased operational excellence.

As the regulatory deadline approaches, institutions need to prioritize the implementation of reliable and robust technology solutions that support data quality and accuracy, efficient reporting, and integration with regulatory platforms like the CSSF S3 API.

LPEA