Deloitte.

Enhancing Operational Resilience: The Strategic Role of Service Organisations in the Financial Sector

How Financial Institutions Can Strengthen Third-Party Risk Management and Comply with DORA

Executive Summary

Financial institutions increasingly depend on third-party service organisations, especially ICT providers, creating new operational and cyber risks that demand rigorous management.

DORA Compliance: The EU's Digital Operational Resilience Act (DORA) sets out detailed requirements for identifying, monitoring, and mitigating risks arising from outsourced ICT services critical to financial stability.

Key Challenges: Institutions face difficulties such as obtaining timely access to service provider data, managing complex incident reporting, adapting to evolving cyber threats, and ensuring sufficient governance capacity.

Essential Practices: Clear contracts with explicit access rights, integrated incident management processes, holistic risk frameworks, and well-trained, multidisciplinary teams are crucial for effective third-party risk oversight.

Deloitte's Role: We support financial institutions through audit readiness, risk gap assessments, governance framework development, training, and capacity building—helping you meet regulatory demands while strengthening operational resilience.

How resilient is your organisation in the face of growing ICT risks and new regulation? We discuss the impact of relevant standards on the management and supervision of these service providers. Furthermore, we explore the differences between ICT and non-ICT service providers, the challenges financial institutions face in managing your service providers, and provide practical tips for effective management. Finally, we highlight how Deloitte can assist you in meeting the complex requirements surrounding third-party risk management.

Background

Financial institutions have become increasingly dependent on external ICT services, such as cloud computing services (e.g., for data storage), payment processors (e.g., for transaction processing, mobile payments, and digital wallets), and core banking platforms (e.g., to handle day-to-day banking operations like account management). This shift has significantly amplified the strategic importance of external service organisations. Service organisations often provide essential services for day-to-day operations and innovation within the financial sector. This growing dependency introduces new risks, such as concentration risk, loss of control over critical processes, and increased vulnerability to cyber threats.

To manage these risks and increase the sector's digital resilience, the European Union introduced the Digital Operational Resilience Act (DORA)[1]. DORA emphasises identifying, controlling, and monitoring risks that arise from the involvement of service organisations. In addition, DORA aims to strengthen the transparency and supervision of critical ICT service providers. Therefore, understanding the role and oversight of service organisations is essential to comply with DORA and safeguard uninterrupted financial services.

RTS Subcontracting (update July 2025)
The Regulatory Technical Standard (RTS) on subcontracting[2] has recently been published. This standard sets out specific requirements and conditions for the use of outsourced ICT services that support critical or important functions or material components. Financial institutions should assess outsourcing risks as early as the pre-contractual phase, including conducting thorough due diligence. The standard sets requirements for the implementation, monitoring, and management of contractual ICT outsourcing agreements. This ensures that financial institutions can monitor and control the entire ICT outsourcing chain.

1 Regulation—2022/2554—EN—DORA—EUR-Lex
2 Final report on Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554

Responsibilities of service organisations

Service organisations must proactively report (major) incidents, vulnerabilities, and operational deviations (arts. 17–20; contractual provider duties in art. 30(2)(f) and 30(3)(b); supervisory feedback in art. 22) so that timely and effective measures can be taken. Trust in the digital foundation of financial services depends on this openness and rapid communication. Financial institutions not only draw up business continuity and disaster recovery plans but also regularly test and monitor these plans (art. 11(6); backup and recovery in art. 12; general ICT testing in art. 25). Monitoring these plans ensures that in the event of unexpected incidents, services can continue without customers experiencing (serious) inconvenience.

Effective governance of service organisations plays a decisive role in this process. Supervisors require a clear structure with defined responsibilities and sufficient resources to manage risks effectively. This prevents operational blind spots or inadequate resources from leading to unforeseen vulnerabilities. In short, DORA transforms service organisations from mere suppliers into active partners in safeguarding the digital future of the financial sector.

Consultation draft Guidelines on the sound management of third-party risk (update July 2025)
The ongoing consultation on the new EBA guidelines for third-party risk[3] shows a clear distinction between ICT service providers and non-ICT service providers. This distinction is essential due to the different regulatory frameworks and specific risks associated with each type of service. Risk management for ICT service providers falls under DORA, rather than the new EBA guidelines. Non-ICT service providers fall within the scope of the EBA guidelines. The EBA sets requirements for risk management, governance, due diligence, contractual audit rights, continuity plans, and exit strategies.

Monitoring service organisations

Financial institutions must ensure robust contractual arrangements that defining responsibilities and service levels. These contracts should also cover essential elements such as audit and access rights (art. 11(6); backup and recovery in art. 12; general ICT testing in art. 25), incident reporting (art. 19; supported by art. 17–18; harmonised templates/content in art. 20; supervisory feedback in art. 22), continuity plans of providers (art. 30(3)(c)); exit strategies (arts. 28(8) and 30(3)(f)). These contracts form the foundation on which financial institutions build effective supervision (art. 26). Access to service provider systems, data, and personnel is vital. This allows financial institutions to carry out their own audits and verify that the service meets legal and contractual requirements (art. 30(3)(e)(i–iv); audit planning in art. 28(6)). Regular due diligence prior to engagement and continuous risk assessments ensure that potential vulnerabilities are identified and addressed in a timely manner. Oversight takes place through performance indicators, reports, and active incident management (arts. 28 and 30 for contractual oversight and monitoring; incident processes in arts. 17–21), allowing financial institutions to respond quickly to operational disruptions.

It is essential to review the continuity and disaster recovery plans of service providers and to ensure clear exit plans, so that services can be taken over or restructured internally without disruption (provider continuity in art. 30(3)(c); exit strategies in arts. 28(8) and 30(3)(f)). Collaboration with regulators is essential. Financial institutions facilitate inspections and share information, keeping supervision transparent and effective. (arts. 31–42 for oversight framework and inspections; cooperation and exercises in arts. 47–49)

In summary, by shaping supervision through strict contracts, full access, thorough risk assessment, constant monitoring, and close cooperation, financial institutions maintain their operational resilience and reliability.

3 Consultation on draft Guidelines on the sound management of third-party risk | European Banking Authority

Challenges

Based on DORA, financial institutions face several challenges in managing service organisations. The four main challenges are:

- **Access to relevant information and transparency**
  Financial institutions must have full and timely access to data, systems, and reports of service organisations to effectively conduct audits and controls (art. 30(3)(e)(i–iv) for rights of access/inspection/audit; audit planning in art. 28(6)). In practice, obtaining this information—especially from foreign service providers—often proves challenging.
  Business Risk: Limited or delayed access to critical information can hinder timely audits and effective oversight, increasing the risk of undetected non-compliance or operational failures. This may result in regulatory sanctions, reputational damage, or financial loss due to inadequate monitoring.
- **Incident management and reporting obligations**
  DORA requires rapid and proactive reporting of ICT incidents by service organisations (arts. 17–20; supervisory feedback in art. 22). Financial institutions must manage these incidents adequately, but coordinating and interpreting reports from various providers can be complex.
  Business risk: Inconsistent or delayed incident reporting may lead to slow or ineffective responses to ICT incidents, exacerbating the impact of disruptions. Failure to comply with regulatory reporting timelines can expose the organisation to fines, legal action, and reputational harm.
- **Managing operational and cyber risks**
  DORA emphasises holistic risk management (art. 6 for the ICT risk management framework; supporting controls in arts. 8–14; protection/prevention specifically in art. 9), but the ever-evolving nature of cyber threats and operational risks requires continuous adjustment of management and monitoring processes. This demands significant resources and expertise.
  Business Risk: Insufficient or outdated risk management practices can make the institution vulnerable to emerging threats, data breaches, and service interruptions. This compromises operational resilience, undermines stakeholder confidence, and may result in regulatory penalties.
- **Capacity and knowledge issues**
  To effectively meet DORA requirements, financial institutions must have a sufficient number of qualified employees with expertise in ICT risk management, contractual obligations, and compliance.
  Business Risk: A shortage of skilled personnel can lead to gaps in compliance, inadequate risk assessments, and ineffective control implementation. This increases the likelihood of regulatory breaches, adverse audit findings, and an overall reduction in the institution's ability to manage ICT risks proactively.

RTS Register of Information (November 2024)/ mandatory request for information register (April 2025)

In April 2025, the Dutch Central Bank (DNB) and the Netherlands Authority for the Financial Markets (AFM) started the mandatory request for the information register (art. 28 paragraph 3). This register provides a detailed and standardised overview of all contractual arrangements related to ICT services with third parties—including intra-group suppliers and key subcontractors—that are vital for the operational resilience of financial institutions

Financial institutions must report the register of information through uniform templates that include:

- Provide insight into all contractual ICT arrangements and their mutual relationships in the ICT service chain;
- Use unique identifiers such as LEI and EUID for clear and unambiguous recognition of service providers;
- Prescribe the ranking of ICT service providers in the chain (direct parties and subcontractors);
- Contain extensive information on the nature of ICT services, risk assessments, relevance of functions, and possible impact of outages;
- Ensure that data is recorded consistently, accurately, and comprehensively at entity, sub-consolidated, and consolidated levels within groups.

DORA increases transparency and ensures that regulators, such as DNB and AFM, can steer digital resilience to manage the risks associated with external ICT services.

Tips

To effectively address the four challenges financial institutions face in managing service organisations under DORA, the following tips can serve as a guide:

- **Conclude clear and comprehensive contracts (see challenge I)**
  To comply with art. 28 and 30 of DORA, which requires full and timely access to data, systems, and reports from service organisations, it is vital that financial institutions establish clear contractual agreements with their service providers, including foreign parties. These agreements must include explicit rights of access and enable effective audits and controls. Additionally, standardised reporting and communication processes should be implemented to ensure information availability and reliability. Close collaboration with service providers can remove practical barriers, ensuring compliance with DORA requirements and strengthening the integrity of audit and control processes.
  Business value: A standardised and integrated incident management process enables faster and more accurate incident response, reducing the potential impact of disruptions on business operations. This supports continuous service delivery, minimises financial and reputational losses, and demonstrates strong operational resilience to regulators and stakeholders.

- **Implementation of integrated and standardised incident management process (see challenge II)**
  To comply with the rapid and proactive ICT incident reporting obligation prescribed in art. 19, 20 and 22 of DORA, it is essential to implement an integrated and standardised incident management process. This involves centralised collection and monitoring of incident reports from all service organisations. Clear communication protocols and regular coordination with service providers must be established to ensure timely and unambiguous interpretation and follow-up of reports.
  Business value: Establishing clear and comprehensive contracts ensures uninterrupted access to essential information, enabling swift detection and resolution of compliance issues. This lowers the risk of regulatory breaches, enhances the effectiveness of audits, and bolsters operational transparency. As a result, the organisation can maintain regulatory trust and safeguard its reputation.

- **Implement a robust risk management framework (see challenge III)**
  DORA emphasises holistic risk management (art. 6; supporting requirements in arts. 8–14), requiring continuous adaptation of management and monitoring processes due to rapidly evolving cyber threats and operational risks. This demands a proactive approach whereby financial institutions invest in specialised knowledge, advanced technologies, and flexible processes. Integration of real-time threat intelligence, regular risk assessments, and automated monitoring tools optimises risk control and detection. Collaboration with external experts and service providers is essential to stay current and deploy resources efficiently, ensuring risk management remains effective and future-proof. This includes NOREA's DORA in control framework[4].
  Business value:
  A robust risk management framework increases the organisation's ability to identify, assess, and mitigate risks in real-time. This maximises business continuity and minimises vulnerabilities to cyber threats and operational disruptions. The result is improved stakeholder confidence, reduced regulatory exposure, and long-term organisational resilience.

- **Invest in strong governance and internal capacity (see challenge IV)**
  Effective compliance with DORA requires financial institutions to have suitably qualified employees with deep expertise in ICT risk management, contractual obligations, and compliance. Organisations should invest in targeted training, knowledge development, and recruitment of specialists. It is also important to form multidisciplinary teams integrating knowledge of technology, legal aspects, and risk management. Ongoing skills development and knowledge sharing within the organisation enable financial institutions to meet DORA's complex requirements and strengthen resilience to ICT risks.
  Business value: Strengthening governance and internal capacity ensures the organisation can effectively implement and maintain DORA controls. This leads to sustained compliance, a higher degree of preparedness for regulatory changes, and greater agility in responding to emerging ICT risks. Ultimately, it supports the development of a resilient, future-ready organisation that can navigate a complex risk landscape.

4 NOREA | Digital Operational Resilience Act—DORA

What can Deloitte do for you?

Deloitte can support financial institutions in various ways to effectively manage service organisations and comply with DORA requirements:

- **Audit Readiness and Assurance (ISAE 3000)**
  Deloitte's audit readiness assessments and ISAE 3000 assurance help clients identify financial, operational, compliance, and cyber risks early—before they escalate into major issues. By thoroughly testing controls, compiling robust documentation, and training process owners, this service strengthens internal controls, governance, accountability, and response capability. Independent ISAE 3000 assurance reports build stakeholder trust by increasing confidence among investors, regulators, and partners. The process ensures organisations are regulatory-ready, supporting ongoing compliance with DORA and the ability to adapt to new requirements (such as ESG and digital). Audit findings serve as a catalyst for operational insight, improved efficiency, cost reduction, and informed strategic decisions.
- **Risk Assessment and Gap Analysis (including second opinion)**
  Through in-depth risk assessments and independent gap analyses, Deloitte identifies and addresses financial, operational, compliance, and cyber risks before they escalate. The service highlights weaknesses and blind spots in internal controls, enabling targeted improvements that enhance governance and risk management. Independent second opinions and critical reviews build stakeholder trust by providing assurance of thorough risk oversight. This approach supports regulatory readiness by benchmarking against DORA and other emerging standards, ensuring the organisation remains compliant and agile. Insights from the assessment drive operational improvements, boost efficiency, reduce expenditure, and support strategic planning.
- **Development and Implementation of Governance and Management Frameworks**
  Deloitte assists organisations in designing and implementing governance structures, policies, and procedures that proactively identify financial, operational, compliance, and cyber risks throughout the entire lifecycle of third-party relationships. These robust frameworks strengthen internal controls, clarify lines of governance and accountability, and enhance organisational response capabilities. Effective governance fosters stakeholder trust by demonstrating a culture of proactive risk management and transparency. The frameworks support ongoing regulatory readiness, enabling the organisation to remain compliant and responsive to changes in regulations (including DORA, ESG, and digital). Management data and feedback are used to generate insights, inform continuous improvement, increase efficiency, and reduce costs.
- **Training and Awareness**
  Deloitte's bespoke training and awareness programmes equip management, risk, compliance, and IT teams to identify and address financial, operational, compliance, and cyber risks before they escalate. Training fosters a culture of strong internal controls and governance, ensuring best practices are consistently applied. By investing in ongoing staff development, organisations build stakeholder trust and signal a commitment to regulatory compliance and operational excellence. The programmes ensure teams remain regulatory-ready and able to adapt to evolving rules and requirements. Feedback and lessons learned from training are used to continuously improve processes, drive operational efficiency, and inform strategic initiatives.

To discuss how these insights translate to your organisation, we invite you to contact Shahil Kanjee, Jesper de Boer, Bas Freriks or Rick Vissers.

The authors

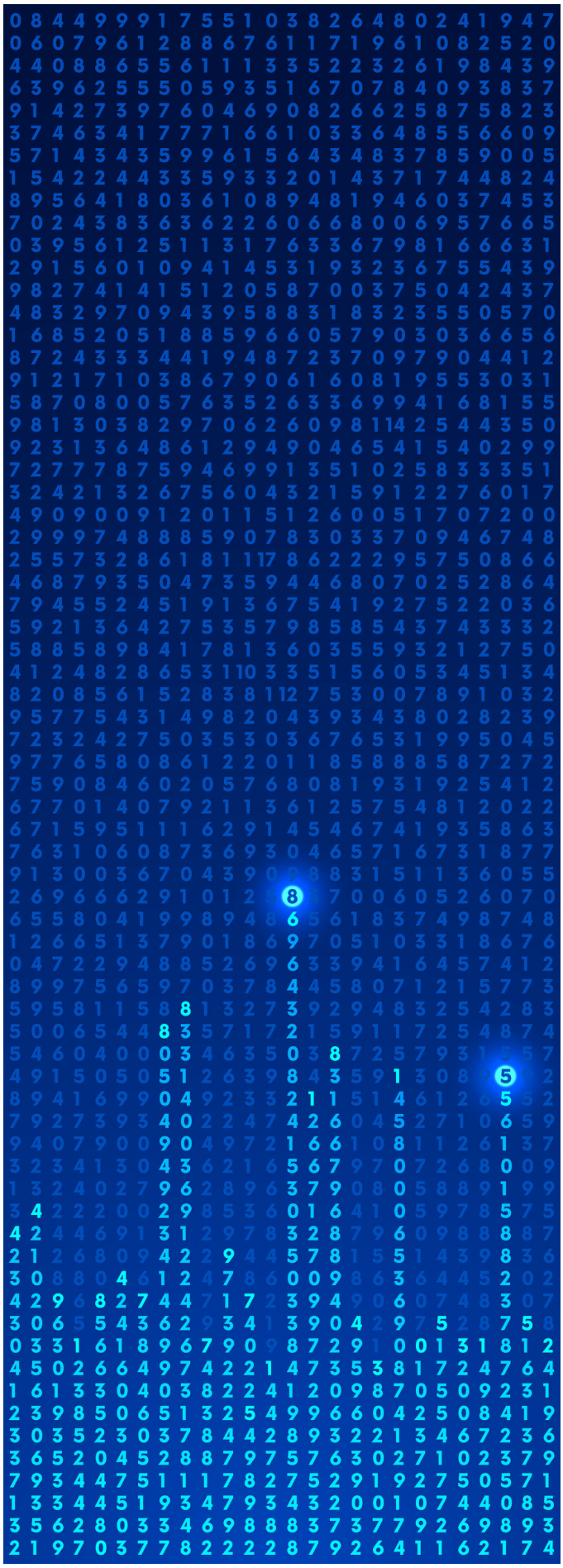
Shahil Kanjee
Partner—IT Audit & Assurance
shkanjee@deloitte.nl

Delisa Stone
Partner—T&T—Cyber
dstone@deloitte.nl

Jesper de Boer
Director—IT Audit & Assurance
jedeboer@deloitte.nl

Bas Freriks
Senior Manager—IT Audit & Assurance
bafreriks@deloitte.nl

Rick Vissers
Manager—IT Audit & Assurance
rvissers@deloitte.nl



Deloitte.

Designed by CoRe Creative Services. RITM2191468