Deloitte.

Positive Impact of Serviceorganisations on Their Own Operational Resilience

This article explains how service organisations, also known as third-party service providers, play a crucial role in the operational resilience of financial institutions. 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 these supply chains, and provide practical tips for effective management. Finally, we highlight how Deloitte can support financial institutions in meeting the complex requirements surrounding third-party risk management.

Background

Financial institutions have become increasingly dependent on external ICT services, such as cloud storage, payment processing, and data analytics. This shift has markedly 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. An understanding of the role and oversight of service organisations is therefore 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 through the due diligence process. 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.

Responsibilities of service organizations

Service organisations must proactively report incidents, vulnerabilities, and operational deviations so that timely and effective measures can be taken (art. 22). 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. 25). Monitoring these plans ensures that in the event of unexpected incidents, services can continue without customers experiencing (serious) inconvenience.

Governance of service organisations plays a decisive role in this. 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 and not under 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.

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

Monitoring service organizations

Financial institutions must ensure robust contractual arrangements that define not only responsibilities and service levels but also essential elements such as audit and access rights (Arts. 28 and 30), incident reporting (art. 22), continuity plans, and exit strategies (art. 25). These contracts form the foundation on which financial institutions build effective supervision. Access to service provider systems, data, and personnel is crucial. This allows financial institutions to carry out their own audits and verify that the service meets legal and contractual requirements (art. 28). Regular due diligence prior to engagement and continuous risk assessments ensure that potential vulnerabilities are identified and addressed in a timely manner (art. 26). Oversight takes place through performance indicators, reports, and active incident management (arts. 22 and 27), 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 (art. 25). Collaboration with regulators is essential. Financial institutions facilitate inspections and share information, keeping supervision transparent and effective (art. 29).

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.

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. 28). In practice, obtaining this information—especially from foreign service providers—often proves challenging.
- **Incident management and reporting obligations**
  DORA requires rapid and proactive reporting of ICT incidents by service organisations (art. 22). Financial institutions must manage these incidents adequately, but coordinating and interpreting reports from various providers can be complex.
- **Managing operational and cyber risks**
  DORA emphasises holistic risk management (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.
- **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..

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 member 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 crucial 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 of DORA, which requires full and timely access to data, systems, and reports from service organisations, it is crucial that financial institutions establish clear contractual agreements with their service providers, including foreign parties. These agreements must include explicit rights of access and audit to 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.
- **Implementation of integrated and standardized incident management process (see challenge II)**
  To comply with the rapid and proactive ICT incident reporting obligation prescribed in art. 22 of DORA, it is essential to implement an integrated and standardised incident management process. This involves centrally collecting and monitoring incident reports from all service organisations, using uniform reporting formats. Clear communication protocols and regular coordination with service providers must be established to ensure timely and unambiguous interpretation and follow-up of reports.
- **Implement a robust risk management framework (seechallenge III)**
  DORA emphasises the importance of holistic risk management (art. 9), which requires 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].
- **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. Continuous skills development and knowledge sharing within the organisation enable financial institutions to meet the complex requirements of DORA and strengthen resilience to ICT risks.

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) (see tip I/II)**
  To support audits, Deloitte conducts readiness assessments according to ISAE 3000 standards. Key topics assessed include incident management and reporting, encryption, network segmentation, awareness sessions, and board responsibilities. Deloitte assists clients in preparing for audits by compiling comprehensive documentation, testing controls, and training process owners on their audit roles. Once an organisation is 'audit-ready', Deloitte can provide assurance through an ISAE 3000 report, confirming the effectiveness of controls and processes, thus providing insight into compliance and operational robustness.
- **Risk assessment and gap analysis (plus second opinion) (see tip I/II)**
  Deloitte conducts in-depth assessments to evaluate current governance, risk management processes, and contractual frameworks surrounding service organisations. This identifies gaps relative to DORA requirements. Deloitte also offers second opinion-services providing independent critical reassessment of previous internal or external analyses. These reviews verify quality and completeness while uncovering blind spots or risks. Based on these insights, Deloitte advises on priorities and improvement measures to strengthen third-party risk management and regulatory compliance.
- **Development and implementation of governance and management frameworks (see tip III)**
  Deloitte supports organisations in designing and implementing robust internal governance structures, policies, and procedures covering the full lifecycle of third-party relationships. From thorough due diligence and continuous monitoring to effective incident management and strategic exit planning, Deloitte ensures each stage is carefully managed.
- **Training and awareness (see tip IV)**
  Deloitte offers tailor-made workshops and training courses for management, risk management, compliance, and IT teams focusing on the content and impact of DORA. Emphasis is placed on best practices for managing third-party risks and effectively applying the proportionality principle. These sessions align with DORA's requirements, helping organisations comply with regulations while strengthening knowledge and skills to manage risks proactively and efficiently..
- **Capacity building and knowledge development (see tip IV)**
  By temporarily deploying experienced experts, Deloitte strengthens the internal capacity of financial institutions in IT risk management, contract management, and compliance. This support ensures governance and oversight are firmly and sustainably embedded within organisations, enabling them to manage complex risks effectively and meet increasingly stringent regulations..

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

De auteurs

Shahil Kanjee
Partner—IT Audit & Assurance
shkanjee@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