ivalua

Digital Operational Resilience in Financial Services

Navigating DORA's Requirements for Procurement and Finance Leaders

The Digital Operational Resilience Act (DORA) is a regulation implemented by the European Union (EU) to enhance the IT security of financial entities such as banks, insurance companies, and investment firms. It aims to ensure that the financial sector in Europe remains resilient in the face of digital challenges.

DORA addresses the risks posed by the significant digital transformation of financial services and the increasing interconnections between different systems. It establishes a comprehensive framework for managing information and communication technology (ICT) risks within the EU financial sector.

While this might seem to primarily concern IT Departments of financial institutions, it is actually very much in the hands of Procurement and Finance. In fact, while the technology architecture and the day to day operations belong with IT, maintaining compliant relationships with third parties is the responsibility of Procurement and Finance leaders.

The Key Objectives of DORA:

1. **Strengthen IT security:** DORA sets out requirements for enhanced IT security measures. This includes measures to prevent and respond to cyber threats, ensure the confidentiality and integrity of data, and protect critical systems and infrastructure.

2. **Promote operational resilience:** The regulation aims to improve the overall operational resilience of financial entities by ensuring they have robust systems and processes in place to withstand disruptions, such as cyberattacks or system failures. This includes measures to identify, assess, and mitigate operational risks.

3. **Enhance risk management:** DORA emphasizes the importance of effective risk management practices within the financial sector. It requires financial entities to establish clear governance structures, implement risk management frameworks, and conduct regular assessments of their ICT systems and processes.

4. **Facilitate supervision and coordination:** The regulation enhances the supervisory powers of governmental authorities, allowing them to monitor and enforce compliance with DORA requirements. It also promotes coordination and information sharing among authorities to address cross-border risks and ensure consistent implementation across the EU.

Overall, DORA aims to create a harmonized and comprehensive framework for digital operational resilience within the EU financial sector, strengthening its ability to withstand and respond to digital risks and disruptions. DORA also serves to reinforce the role of the European Supervisory Authorities (ESAs), which include the European Bank Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA), and European Securities and Market Authority (ESMA).

Compliance Requirements of DORA

To be compliant with the Digital Operational Resilience Act (DORA), financial entities must fulfill several key requirements. Here are the five main compliance requirements that organizations need to adhere to:

1. **Risk Management Requirements:** Financial entities are required to establish and maintain effective risk management measures to identify, classify, and mitigate digital operational risks. This includes identifying and assessing potential risks related to information and communication technology systems, processes, and services. All with regular measurement and review.

2. **Incident Reporting:** DORA mandates the reporting of significant cyber and IT-related incidents to competent authorities, improving sector-wide awareness and facilitating coordinated responses. This includes reporting of any cybersecurity breaches, disruptions, or other incidents that could impact their operational resilience.

3. **Digital Operational Resilience Testing:** Financial entities must regularly test their digital systems and processes to assess resilience against disruptions and cyberattacks. Advanced testing methods, such as threat-led penetration testing, are encouraged.

4. **Third-party Risk Management:** DORA introduces a regulatory framework for the oversight of third-party IT service providers. Financial entities must ensure that their contracts with these providers do not compromise operational resilience. This involves conducting due diligence on third-party providers, implementing contractual measures to ensure compliance with DORA requirements, and establishing processes to monitor and assess the ongoing performance and security of these providers.

5. **Information Sharing:** The regulation promotes the sharing of information related to cyber threats and vulnerabilities within the financial sector to enhance collective defense mechanisms and resilience.

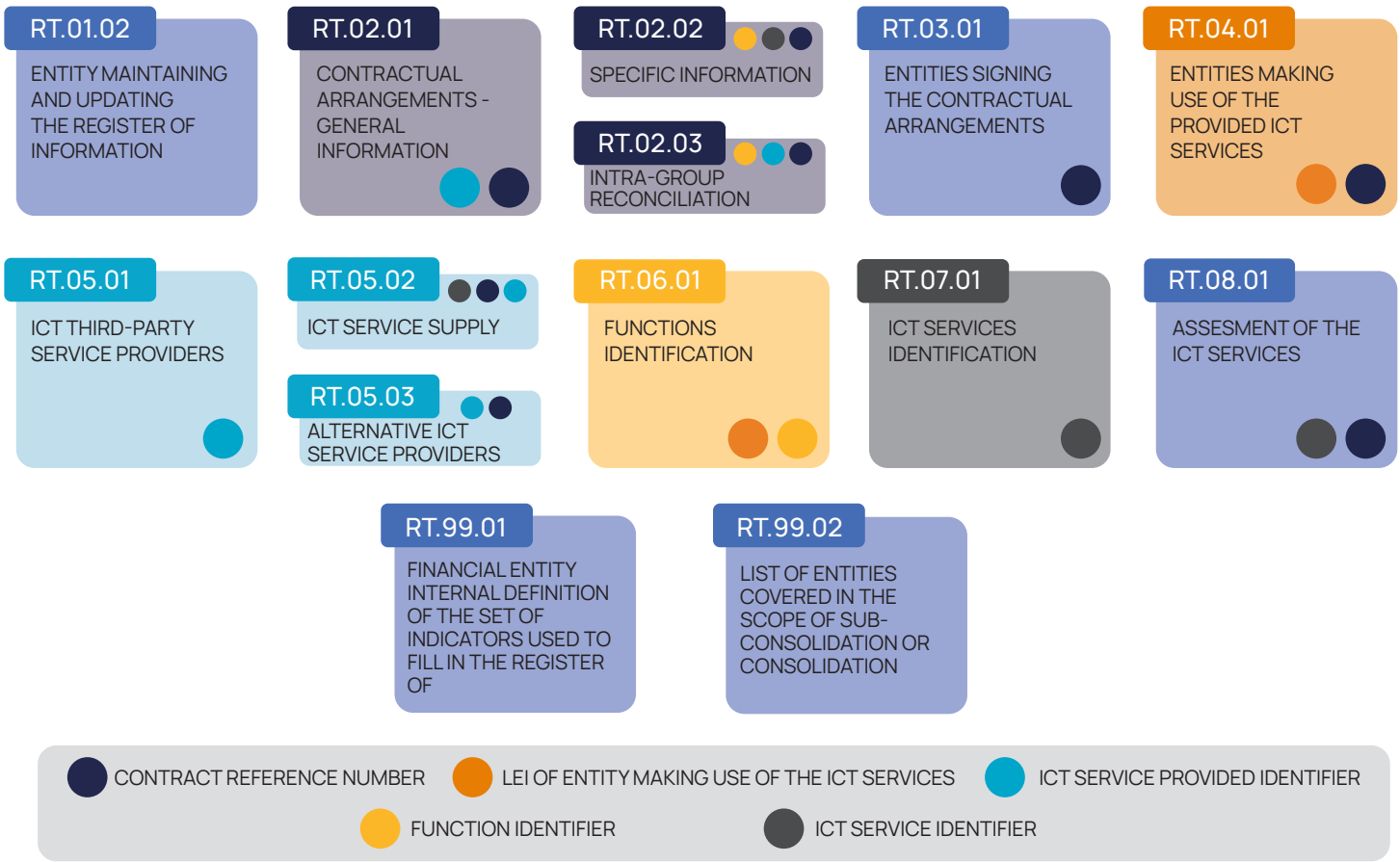
It's important to note that DORA provides a comprehensive framework, and organizations should carefully review the regulation and consult legal and compliance experts to ensure full compliance with all applicable requirements and obligations.

How Ivalua Supports DORA Compliance

While Ivalua is not directly supervised by the ESAs, it is committed to supporting its customers in meeting their regulatory requirements. However, it is important to note that as an ICT vendor to many financial institutions in Europe we understand what is required from a vendor. For instance, Ivalua supports and encourages penetration testing, unlike most cloud vendors since data is both physically and logically separated so even in case of a successful breach, no other customer's data is exposed

Ivalua's Source-to-Pay platform offers the following capabilities to help organisations meet DORA compliance requirements:

Ivalua can serve as the digital repository required by the regulations for financial institutions subject to DORA (Digital Operations and Regulatory Analysis). This repository goes beyond being a mere contract database. In the technical specifications of DORA, it is explicitly defined as a collection of 14 databases that must be interconnected through 5 distinct identifiers to facilitate seamless communication between them.



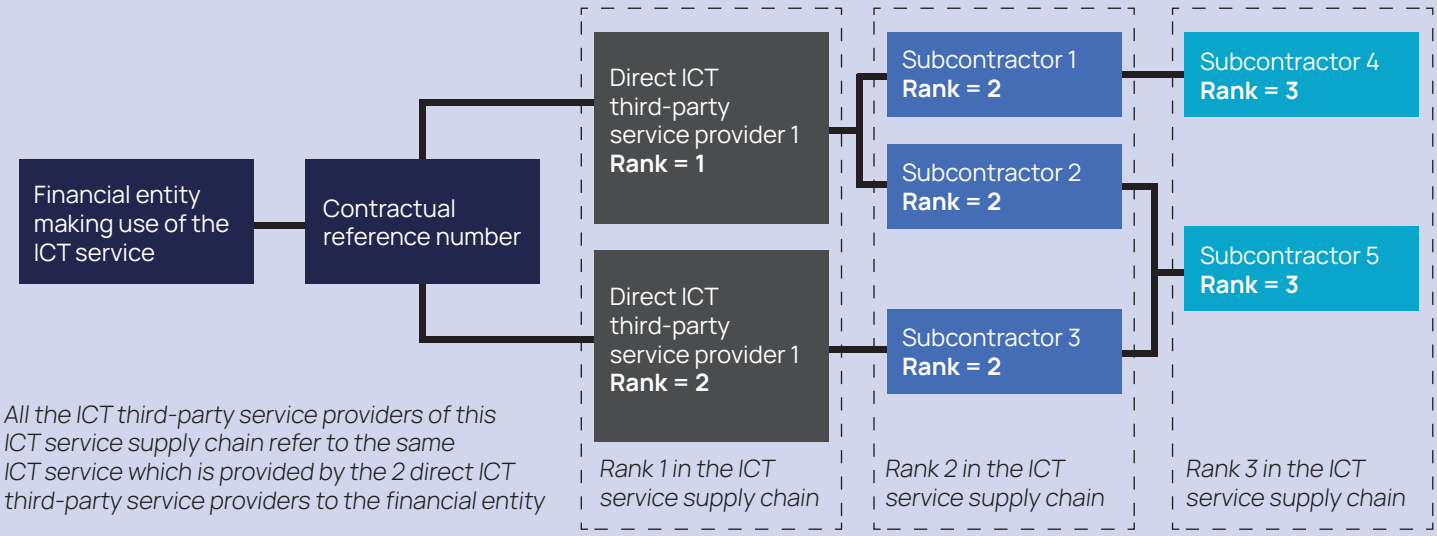
Source: DORA technical details

Thanks to both its **extensive, unified data model** and **integrated platform,** Ivalua supports compliance with this architecture:

- All **data tables** exist or can be created via configuration (e.g, the new concept of "Function").
- All data points are connected through a **unique identifier:**
  - The contract reference number.
  - The LEI of the entity making use of the ICT services.
  - The ICT third-party service provider identifier; required to rank them (tier 1 or tier 2 supplier - i.e, subcontractor).
  - The function identifier.
  - The ICT service identifier.
- Information can be **aggregated** at many levels like group (by the financial entities part of a group), national (by the country of activity) and European (by the ESAs) levels, as per requirements.
- Monitoring of the **service supply chain** with visibility into Tier N subcontractors, as per requirements:

ICT service supply chain

The ICT service supply chain is identified by the combination of both:
-the contractuak reference number between the financial entity and the direct ICT third-party service providers;
-the ICT service identifer



All the ICT third-party service providers of this ICT service supply chain refer to the same ICT service which is provided by the 2 direct ICT third-party service providers to the financial entity

Source: DORA technical details

Ivalua is in a **unique position** to support compliance with DORA regulation:

- Not every procurement vendor will be able to support **all those data points** that are specific and new (e.g., "Function").
- Many vendors are **not able to extend their data model** to the degree required.
- Having this complex requirement with multiple data tables and identifiers is difficult to do with a multi-tenant architecture.

In terms of modules that a customer would need to be compliant with DORA regulation, the following are required at minimum:

- **Supplier Risk and Performance Management:** supplier due diligence, supplier information, supplier risk, supplier performance, issue tracking and improvement plans.
- **Sourcing:** for risk management prior to entering any new agreement.
- **CLM:** contract templates, mandatory clauses, contract risk assessment, supplier performance against a contract.

To conclude, the Ivalua platform provides the following **benefits to our customers** with regards to DORA regulation:

- A **central repository** where all DORA-related agreements are identified (critical contracts as well as others).
- Supplier **due diligence** steps before entering any agreement (embedding concentration risk questions).
- Contract **templates** where all DORA-specific clauses can be embedded (cooperation with the competent authorities, data integrity & accessibility, exit strategies, migration provisions, etc.).
- A full **Third Party Risk Management** solution (including subcontractors).
- Complete audit **tracking** & automated **reporting.**

Complying with DORA is crucial for financial entities operating in the EU. Ivalua offers a robust platform that supports DORA compliance through data security, contractual terms, supplier due diligence, contract management, and third-party risk management capabilities. By leveraging Ivalua's solution, organizations can effectively navigate the requirements of DORA and ensure their digital operational resilience.

Disclaimer: This whitepaper is for informational purposes only and does not constitute a commitment. The information provided is intended to assist organizations in understanding and evaluating capabilities that may help them to comply to DORA requirements. Ivalua as a technology provider cannot ensure compliance to DORA, this responsibility lies with each organization.

About Ivalua

Ivalua is a leading provider of cloud-based, AI-powered Spend Management software. Our unified Source-to-Pay platform empowers businesses to effectively manage all categories of spend and all suppliers, increasing profitability, improving sustainability, lowering risk and boosting employee productivity. We are trusted by hundreds of the world's most admired brands and recognized as a leader by Gartner and other analysts. Learn more at www.ivalua.com Follow us on LinkedIn and X.