Panorays

Guide

A Guide to DORA Compliance and Third-Party Risk Management

How to achieve full DORA compliance by 2025

Financial services organizations are increasingly nervous about the latest EU regulation, and it's not hard to understand why.

DORA, or the Digital Operational Resilience Act, is an EU regulation focused on financial sector data protection and privacy. Its goal is to strengthen the operational resilience of organizations in this industry, with a particular focus on the third parties that supply critical information communication technology (ICT) services.

> *Here's the catch: Although some of the technical standards of the regulation have been adopted, DORA's security control requirements aren't detailed yet. Even so, DORA will be enforced January 17, 2025. If you want to be ready in time, start preparing now.*

It's reasonable to assume that DORA will align with the European NIS2 directive. While NIS2 is currently stated on a conceptual, and not practical and detailed level, many believe that NIS2's security controls will reflect an evolution of the nearly universally adopted ISO 27001/2 control framework. That means many companies may already be aligned with at least some of the controls that this regulation will require – but some adjustments will be needed.

It's important to note that the UK is in the process of adopting a very similar regulation, CP26/23. In each case (DORA and CP26/23) the financial services-specific regulation overrides NIS2. An organization that must comply with DORA does not also need to comply with NIS2.

Fast Facts About DORA Compliance

What is DORA?

The Digital Operational Resilience Act (DORA) is a regulatory measure established by the European Union to establish a mandatory and thorough framework for managing information and communication technology (ICT) risks within the EU financial industry.

What is the goal?

Ensure that companies follow rules for protection, detection, containment, recovery and repair capabilities against information communication technology (ICT)- related incidents.

How will it be enforced?

On and off-site inspections will help enforce compliance as well as the request of specific information, such as ICT details, incident reporting logs and details of implemented cyber risk defenses.

What are its areas of focus?

DORA has five main areas of focus with regards to financial services organizations:

1. **ICT Risk Management.** This includes the mapping of ICT systems and identifying of assets to conduct risk assessments on their ICT systems.
2. **Incident Reporting.** Require mandatory rapid incident reporting to manage and mitigate disruptions and threats related to ICTs, security payments and operations.
3. **Digital Operational Resilience Testing.** Demand the regular testing of ICT systems and that they have recovery plans in place.
4. **Third-Party Risk Management.** Require the rigorous oversight of ICT third-party providers, including cloud services, to ensure that they do not become a source of vulnerability.
5. **Information and Intelligence Sharing.** Although not a unique area to DORA specifically, the sharing of information and intelligence is encouraged as it supports the goal of strengthening resilience and security along the entire supply chain.

Why now?

It unifies the current multiple ICT risk management frameworks, combining them in a unified approach to enhance the European Union financial industry security and business continuity.

Why DORA Compliance is Urgent Now

Financial services organizations already know that stronger third-party security risk management is crucial. The news is full of headlines about well-known firms that suffered operational disruption due to third-party data breaches and supply chain attacks. As organizations rely increasingly on third parties, it's a virtual certainty there will be many more attacks. Regulations such as DORA focus board and executive attention on the need to improve security to minimize these types of attacks, as well as to mitigate the effects when the inevitable incident happens.

Recent attacks include:

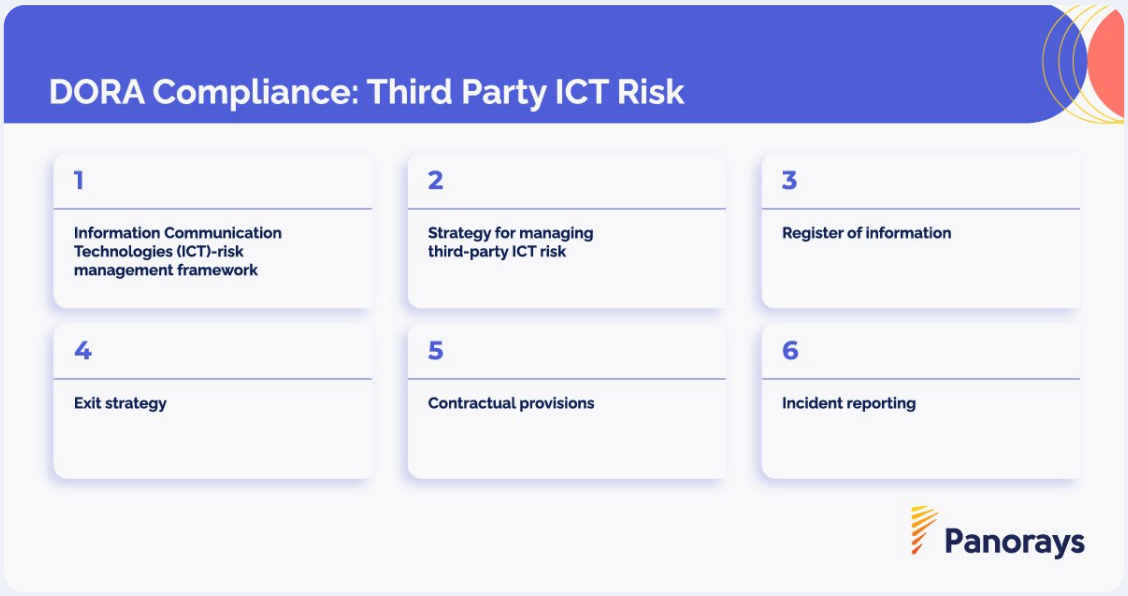
- **Deutsche Bank.** Deutsche Bank suffered a data breach when attackers gained access due to a vulnerability in a third-party software service. It was unknown how many customers were affected by the breach, but the origin of the leak was traced to Majorel, a bank account switching service provider impacted by the MOVEit supply chain attack.
- **Bank of America.** This data breach targeted and exposed the social security numbers, names and dates of birth of deferred compensation plans managed by third-party provider Infosys McCamish. It exposed the personally identifiable information (PII) of 57,028 customers.
- **MOVEit.** The supply chain attack on the third-party file transfer program affected more than 17.5 million individuals and contributed to 600 breaches worldwide. In the EU, ING Bank, Postbank, and Comdirect also reported data leaks as a result of a third-party provider impacted by the MOVEit attack.

DORA and Third-Party Cyber Security

Virtually all regulations with a third-party spin require businesses to both classify and report on third-party partners according to specific characteristics. DORA goes deeper with its highly detailed "Register of information" (more about that later). DORA also requires finserve firms to assess what the regulations calls "Information Communication Technology Third Parties" according to an as-yet-unspecified set of security controls, as we mentioned above. Incident reporting is crucial in many regulations, but DORA specifically mandates "monitoring" third, fourth and fifth parties, in part to facilitate incident notification to relevant authorities.

The 6 Pillars of DORA Third-Party ICT Risk

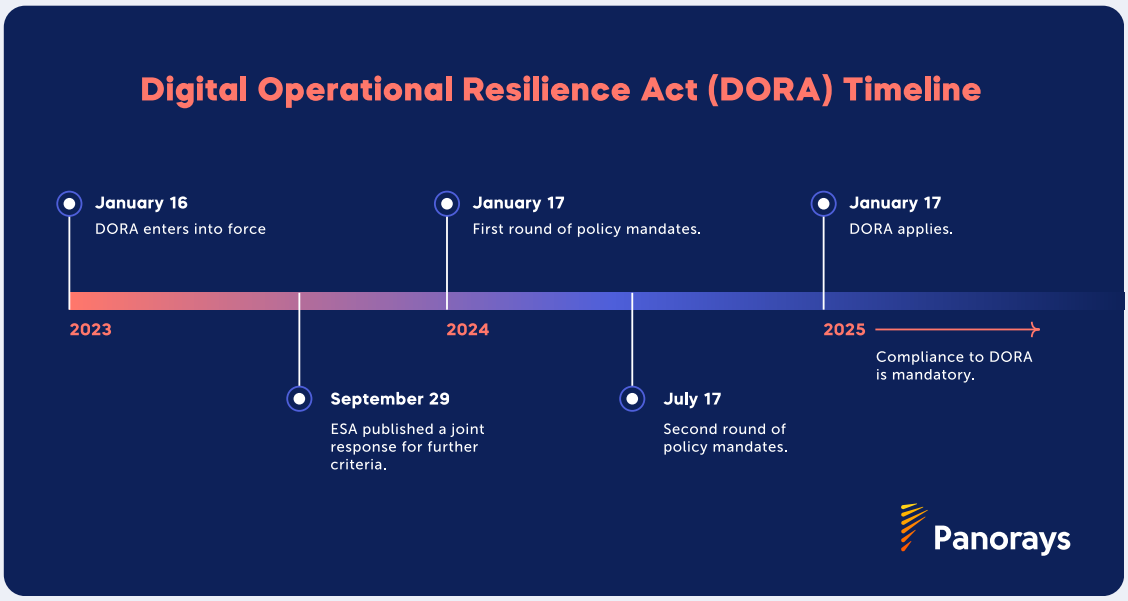
The DORA regulation has six pillars related to third-party security.



1. **Adopt a framework.** Adopt an ISMS (Information Security Management System), which is a security control framework, like ISO 27001/2. DORA may reference the NIS2 Directive, which is likely to be an evolution of IS0 27001/2.
2. **Implement a strategy.** Create a framework and process to designate third-party ICT services that support critical functions, determine the criticality of the ICT services and "sensitiveness" of the data shared with the third-party, and identify the ICT service in the terms DORA requires for the "Register of information." In addition, it should assess the ICT's security controls (most likely leveraging questionnaires and document requests as is typically done) and identify third, fourth and fifth parties that may represent potential concentration risk.
3. **Register of information.** Provide reports to the "Supervisory Authority" for categorizing third-party Information and Communication Technology (3P ICT) services supporting "critical and important functions" (CIFA).
4. **Exit strategy.** Plan how to end a 3P ICT relationship, ensuring the "resiliency" of your business, regardless of the success or failure of any supplier relationship.
5. **Contractual provisions.** Enforce the implementation and operation of the security controls required by DORA with contractual terms in your agreement with a 3P ICT.
6. **Incident reporting.** Report on a breach or other cyber incident to the supervisory authority ("SA") or regulator your firm is responsible to.

DORA and TPRM: Get Prepared in Time

DORA will be enforced on January 17, 2025. Since its inception in 2022 it has gone through many reviews and iterations. With DORA compliance going into effect soon, companies need to be prepared for closer collaboration with European Supervisory Authorities (ESAs), including defining policies, reporting of ICT-related incidents, and designing robust Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs).



To start preparing, analyze the current process in place for third-party security risk management, identify gaps and explore solutions. See the draft technical standards listing the criteria for critical ICT third-party service providers here.

You can also prepare with:

- **DORA Profiling.** Categorize your third parties, identifying those that support critical or important functions, and create a complete profile for each of the third parties identified. Use the "Register of Information" format (Pillar 3 above), so you can report on them as needed. Identify any fourth or fifth parties that support these third parties, and rank all of them according to the specific relationships (third, fourth or fifth party).
- **Prepare compatible questionnaires and documents.** Shared Assessments, for example, expects to deliver a version of their SIG questionnaire content library, supporting and mapped to the DORA standards.
- **Monitor third, fourth and fifth party ICTs carefully.** DORA requires companies to report incidents to the Supervisory Authority (SA). When a fourth or fifth party has a breach, malware attack or other incident, you must contact the related third party to learn details and plans to mitigate the damage. Needless to say, prepare to report to your SA.

How Panorays Can Help You Meet the DORA Criteria

Panorays helps companies execute against several of the pillars so that companies can prepare for DORA now, before the regulation goes into effect. Here are the steps your organization can take to develop a strategy for managing third-party ICT risk.

Categorize Your Third Parties

The first step of the strategy, like with all third-party risk management, is to categorize all of your third parties and tier them according to their inherent risk. Panorays delivers DORA-specific inherent risk questionnaires matching the "Register of information" format, including:

Identifying the provider: LEI (Legal Entity Identifier) and contractual agreement reference number	**What is the annual expense of the contract?**
Identify the ICT-related services (out of 19 DORA categories)	**Location of data stored and location of data processed?**
Rank the provider: direct ICT service provider, subcontractor, or supplier to a subcontractor?	**Do the services purchased support critical or important functions ("CIFA")?**
Where are services provided?	**What is the sensitiveness of the data?**
What is the governing law of agreement?	**What is the level of reliance on the ICT provider?**

Assess Your Third Parties

Panorays partners with third-party best practices and content leader Shared Assessments for regulatory questionnaire content. Shared Assessments actively maps their "SIG" questionnaire content library to support DORA. They expect to release SIG 2025 with robust support for DORA later this year.

Identify Fourth and Fifth Parties and Potential Concentration Risk

Panorays' Supply Chain Discovery functionality identifies your third, fourth and fifth-party digital technology relationships, which may be suppliers and subcontractors (and even suppliers to the subcontractors). A periodic review of the Supply Chain Discovery function may reveal new subcontractors, who your suppliers may have yet to inform you of. These can be added to Panorays for monitoring.

After adding newly revealed suppliers, you can then use the Panorays inherent risk questionnaire to specify the DORA "rank" of the supplier, enabling optimal monitoring and reporting. In addition, Panorays reports identify concentration risk in the supply chain as well.

Register of Information

After gathering information from the questionnaires, Panorays will enable reporting on third-party ICT relationships:

- Level of sensitivity of the data shared
- Degree of reliance on the ICT service supporting a critical or important function
- Identification of subcontractors and subcontractors' suppliers (e.g. concentration risk) through Panorays' Supply Chain Discovery.

Prepare for Incident Reporting

Panorays Risk Insights portal maps threats and cybersecurity events to your digital supply chain, alerting you to potentially significant risks to your business as early as possible. You'll know which third parties to communicate with, even if the event occurred at the fourth or fifth party level.

Strengthening the Resilience of Finance Services in the EU

According to Akamai Technologies, the number of attacks on European financial services doubled in 2023, with the industry being the third most attacked within the EMEA (Europe, Middle East and Africa) region. At the same time Gartner has reported that 45% of organizations experienced third-party related business interruptions over the past two years. More than half of CISOs (65%) view third-party security threats as a top priority today.

This rising trend in third-party attacks coupled with increasing regulation in the industry make it essential for CISOs to ensure they do everything in their power to minimize third-party risks. Even though the DORA security control requirements aren't detailed yet, you can still prepare for full compliance. As you prepare to do so, you'll also strengthen the security posture of your organization, proactively prepare to mitigate attacks and build your brand. It's a winning combination, but you should start getting ready as soon as possible.

Panorays

About Panorays

Panorays is a leading provider of third-party cyber risk management solutions, helping businesses optimize their defenses for each unique third-party relationship. Trusted by the most complex supply chains in the world, Panorays goes far beyond the generic third-party risk management solution with its AI powered platform making assessments adaptable and more personalized. Panorays provides businesses the tools to stay ahead of emerging third-party threats and delivers actionable remediations with strategic advantages.

Learn more about how Panorays' TPCRM platform can help you comply with DORA.

Get a Demo Today