DORA fact sheet

June 2024

APS bank
values you can bank on

DORA applies to a wide range of financial entities including credit institutions, electronic money institutions, payment institutions, investment firms, fund managers, insurance and reinsurance undertakings and intermediaries as well as institutions for occupational retirement provision, credit rating agencies and administrators of critical benchmarks (in-scope entities). Most importantly, the scope of DORA requirements also cover **ICT Third-Party Service Providers (TPPs)**.

DORA applies to a broader range of contracts as it applies to the use of 'ICT Services' which are defined as digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis including hardware as a service and hardware services which include the provision of technical support via software or firmware updates by the hardware provider.

All entities in scope need to comply with DORA requirements as of **17 January 2025**.

What is DORA about?

In essence, DORA is divided across five core pillars that address various aspects or domains within ICT and cyber security, providing a comprehensive digital resiliency framework for in-scope entities. A summary of the key requirements is provided below:

ICT risk management

Principles and requirements on ICT risk management

ICT third-party providers risk management

Monitoring of TPPs and sub-contractors
Standard contractual provisions

Digital operational resilience testing

Basic and advanced security testing

ICT-related incidents

Managing and reporting of major ICT-related incidents

Information sharing

Exchange of information and intelligence on cyber threats

What are the DORA obligations on the Bank?

The Bank needs to ensure that it:

- maintains comprehensive ICT Risk Management Framework, which focuses amongst others, on (i) security of our networks; (ii) safeguarding against intrusions and data misuse; and (iii) preserving the availability, authenticity, integrity, and confidentiality of our own and our customers' data.
- establishes strong ICT governance, including roles and responsibilities allocated in line with our internal three lines of defence model.
- has strong controls in the area of incident management and security testing.

- maintains strong controls in terms of TPP Risk Management, which includes *inter alia*, (i) controls for audit, access, inspection and ICT security testing rights of the Bank; (ii) monitoring of the chain of sub-contracting; (iii) establishment of appropriate exit plans; (iv) conflict of interest controls; (v) business continuity and information security controls.

What are the DORA obligations on YOU, as a TPP/sub-contractor?

Contractual obligations You should satisfy:

- YOU inform us in a timely manner on any major threat and actual ICT-related incidents affecting Your systems, network or infrastructure, in particular when those affect the services provided to us.
- YOU participate in our audits, including pooled audits and ICT security testing covering the services provided to us. YOU may suggest to us participating in a pooled audit organised for a number of Your clients. In addition, YOU should grant access and participate in audits and inspections conducted by us, a third-party appointed by us and/or a relevant competent authority.
- YOU inform us on Your relationships with your sub-contractors, including intragroup providers and cloud providers and on any changes to the supply chain.
- YOU participate in our training and awareness activities focused on DORA and information security.

Digital resilience and cyber security best practices You are expected to have:

- YOU should cultivate a positive ICT and Cyber Security culture and implement sound ICT risk management controls.
- YOU should identify critical ICT-related assets within YOUR organisation, which may include hardware, software, virtual machines, cloud services and relevant key personnel.
- YOU should invest in tool which will help you understand the threat landscape of cyber security as well as in those, which used for digital resilience testing.
- YOU should implement comprehensive patch and vulnerability management practices ensuring timely application of updates and patches proportionate to the criticality of YOUR systems.
- YOU should establish strong relationships with YOUR sub-contractors by focussing on allocation of responsibilities and timely response to changes in the sub-contractors' situation.
- YOU should have in place well-defined ICT- related incident response plans which are vital for swiftly addressing any actual or potential security breaches.
- YOU should establish sound Business Continuity and Disaster Recovery Plans for maintaining the continuity and success of YOUR organization in the face of unexpected events.

For more information see below:

Digital resilience and cyber security best practices

Both ICT security and digital resilience are crucial in reducing ICT and cyber risks as well as risks relating to exposure to third-party service providers.

Adopting a methodical and proactive approach to ICT and cyber security and implementing basic safeguards can significantly reduce the risks, which may have negative impact on both Your Entity and the Bank.

1. Cultivating a Positive ICT and Cyber Security Culture and risk management

Integrating ICT and cyber security into Your entity's risk management and decision-making processes is essential, ensuring that all business units clearly understand their ICT and cyber security obligations and responsibilities. Effective risk management enables informed decision-taking. It is crucial to integrate ICT and cyber security risks into your overall risk management strategy. A sound cyber security culture is essential, as it emphasises that organizational security relies on people. Fostering a collective and collaborative effort ensures that employees perceive security as supportive to their daily activities and as an integral part of their responsibilities.

Continuous training helps organisations maintain cyber hygiene, detect threats and foster compliance with laws and regulations, reinforcing overall security measures.

2. Identifying critical ICT-related assets

Understanding the criticality of ICT-related assets within Your organisation's is essential for effective risk management. Amongst others, ICT-related assets include hardware, software, virtual machines and relevant key personnel.

3. Understanding the threat landscape of cyber security

Understanding the threats Your entity faces allows for strategic allocation of investments. Prioritizing specific targets ensures effective defence strategies and helps avoiding ineffective attempts to protect against potential risks. Moreover, integrating threat intelligence and detection capabilities remains crucial for enhancing cyber resilience.

4. Digital resilience testing

Regular testing identifies vulnerabilities and weaknesses in Your organization's digital infrastructure, allowing for proactive measures to enhance security and reduce the risk of cyber-attacks. It ensures that critical business lines can continue during and after a cyber incident, minimizing downtime and maintaining service availability for customers and stakeholders.

5. Effective patching and vulnerability management practices

Implementing comprehensive patch and vulnerability management practices is crucial for strengthening digital resilience. Timely application of updates and patches is essential to safeguard Your entity against known vulnerabilities that could be exploited by malicious actors. Thorough testing before deploying patches is necessary to ensure system stability and security while minimizing disruptions and optimizing performance of Your systems. Patching and vulnerability management should be proportionate to the criticality of ICT-related assets in Your entity.

6. Deploying effective ICT cyber security measures

Implementing effective ICT and cyber security measures is crucial for reducing the risk of significant incidents and can greatly reduce vulnerability to cyber-attacks while mitigating potential adverse reputational, financial, and legal impacts.

7. Engaging with your sub-contractors

Establishing strong relationships with Your sub-contractors is critical for ensuring supply chain security. Clear allocation of responsibilities and timely response to changes in the sub-contractors situation allows for sound management of risks resulting from exposure to third parties.

Implementing a robust process for continuous monitoring of sub-contractors, identifying interdependencies, evaluating their ICT and cyber security readiness, and taking necessary actions to address any issues that may arise limits risks of overreliance on Your third parties.

8. Developing your response strategy for ICT-incidents

Having well-defined incident response plans in place is vital for swiftly addressing any actual or potential security breaches. Preparedness to detect and promptly respond to incidents can prevent attackers from causing additional damage, thereby minimizing adverse financial and operational impacts.

9. Business Continuity Plans (BCP) and Disaster Recovery Plans (DR)

BCP and DR plans are instrumental for maintaining the continuity and success of Your organization in the face of unexpected events. They help minimize downtime, protect data and assets and enhance resilience. Moreover, sound BCP and DR planning helps to safeguard reputation, support employee safety, improve decision-making, facilitate communication, and ensure financial stability.