Are you ready for DORA?

Petter Glenstrup, Director of Sales Engineering at Arctic Wolf, and AJ Thompson, COO of Northdoor plc, outline five steps the channel should take before the introduction of The Digital Operational Resilience Act early next year

The Digital Operational Resilience Act (DORA) will soon establish a universal framework for managing, reporting and outsourcing IT risk for the European Union's financial sector.

Looking to mitigate a recent rise in cyber attacks on the industry, the legislation will require organisations to withstand, respond to and recover from related disruption to ensure they remain operational in the event of an attack.

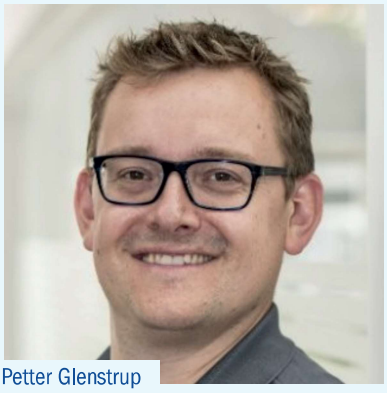
Organisations and their third-party suppliers, including providers of digital and IT solutions, are expected to comply with the regulation by January 2025, making it crucial for IT service providers and the wider channel to prepare for its introduction now.

Here are five simple steps your organisation can take to ensure it complies with the requirements for cyber resiliency outlined in the legislation.

❶ Determine whether your organisation will need to comply

DORA applies to all financial institutions in the EU, including banks, insurance companies and investment firms – regardless of their size or revenue.

It also extends to third party suppliers in an organisation's supply chain. This includes businesses that supply financial services organisations with IT systems and services – cloud providers, data centre companies, even AI vendors must all comply with the Act's requirements.



Petter Glenstrup

When preparing for the legislation, it is crucial to take into account every business across the supply chain, from resellers to partners. Channel organisations, in particular, must ensure they're partnering with and selling to DORA-compliant organisations, because failure to comply could lead to heavy financial penalties.

❷ Identify gaps in your identification, reporting and testing procedures

DORA will require organisations to prove that they can withstand IT-related disruption, including cyber attacks, so it is vital for leaders to take the time to understand where there are gaps in their organisation's defences – as well as how they identify, report and recover from an incident.

Conducting a risk assessment of your organisation and its wider supply chain can allow you to identify areas of vulnerability in your network and develop a plan of action to address these. This should include evaluating the key areas DORA will assess, such as incident reporting, scenario testing and risk governance, and should extend to third party providers.

❸ Develop a plan of action to address vulnerabilities

Once you have conducted a risk assessment, you can start developing a plan of action for compliance. This should meet the requirements outlined in Article 6(8) of the DORA legislation, and should explain how an IT risk management programme supports your organisation's business objectives and wider strategy.

It should also establish a risk tolerance level; explain your organisation's existing IT infrastructure; outline the different mechanisms in place to detect an incident; and include a comprehensive strategy for communicating within your organisation and to the wider public in the event of an attack.

❹ Conduct regular employee training

Alongside the establishment of a risk management programme, DORA mandates security awareness and digital operational resilience training for board members, senior management and employees.

AJ Thompson

This should be an important focus given that an estimated 60% of data breaches are caused by insider threats – whether deliberate or accidental. It is crucial that every member of your organisation is educated on IT risk and how to spot the signs of an attack via regular workplace cybersecurity training. This should also cover what to do in the event of an attack, including reporting an incident to your IT teams.

❺ Regularly review and update your plan

Once the legislation has been implemented in 2025, each affected organisation will have their risk management plan reviewed at least once a year (periodically for smaller businesses), as well as upon the occurrence of an IT-related incident.

It's important to conduct regular reviews of these plans internally to ensure they still comply with DORA and are continuously improved and updated in line with the legislation's requirements. This will not only ensure your organisation remains compliant with the new regulations, but that your wider operational resilience strategy stays effective over time.

By understanding and implementing these five steps, financial service organisations and their suppliers can ensure they're prepared for the implementation of DORA in early 2025. A year might feel like a long time to ensure compliance, but organisations that don't start preparing now will find it difficult to get everything in order in time. The time to act is now – before it's too late.