varmour

DORA Readiness

9 Step ICT Risk Management Compliance Checklist

DORA goes into effect in January 2025. While the date may seem far off, organizations must act now in order to hit DORA's detailed operational resilience requirements on time. The best way to get started is through a strategic planning approach that follows DORA's workflow.

Here's a straightforward checklist to help get you started.

✓ 1

Identify your internal stakeholders

Identify key players in your organisation that will be responsible for driving your DORA program — such as accountable senior leadership, risk management experts and other crucial stakeholders such as Technology Resilience and Procurement professionals.

✓ 2

Define your required efforts and deliverables

Outline the efforts and deliverables of your ICT Risk Management strategy plan in line with the key requirements of DORA. Article 8 is a really good place to start.

✓ 3

Identify your critical business functions and entities

Categorize each of your business functions and entities that are critical to your operations. Define your Impact Tolerances for each function, in terms of the maximum tolerable level of disruption which can be tolerated.

✓ 4

Begin to define a process for scenario testing and risk assessing your critical business functions

Engage stakeholders and subject matter experts to define a set of serious but plausible scenarios against which to test your ability to recover, and to define a set of Risk Tolerances which are likely to be indicative of future risk and resilience scenarios (e.g, unmanaged systems or systems with material vulnerabilities accessing Critical Business functions). Start simple, iterate, and think carefully about how to make this process sustainable and automated.

vArmour

5 Choose an operational resilience mapping solution

Pick a best-in-class operational resilience mapping solution that will help you map, identify, and monitor your critical business functions and entities. Look for a solution that automates your mapping and monitoring efforts, in a continuous fashion, and eliminates the risk of manual errors.

6 Map and document your critical business functions and entities and their interdependencies

Use the solution you chose in Step 5 to map the configuration of your critical ICT assets, including the interdependencies between those assets.

7 Assess your controls against Articles 9 and 10 and the associated regulatory technical standards

DORA defines a set of controls around standard cyber practices (encryption, identity and access management, segmentation, vulnerability management) which are already achieved by many organizations. Conduct a gap analysis, remediate where necessary and put in place a continuous controls monitoring and reporting framework.

8 Continuously monitor and assess your ICT environment

Define continuous monitoring policies and processes (based upon your risk and impact tolerances) to help you identify new risks and threats to your organization. The solution you chose in Step 5, if automated, should help you here.

9 Test, review, and improve

Testing enables you to identify gaps and prepare for incidents. Test scenarios should extend to severe but plausible scenarios and can be conducted physically, theoretically (via table top exercises), and virtually (against a digital twin, which you might have adopted at Step 5). Regularly review your findings and documents for assessment by auditors and ESAs.