Whitepaper

How AutomatePro helps you achieve DORA compliance

AutomatePro
Let's make progress

Official partner of
servicenow

Whitepaper

DORA, the Digital Operational Resilience Act, is a regulation issued by the European Union that aims to enhance the digital resilience of the financial sector. It outlines a comprehensive framework with five key pillars that financial institutions and ICT providers must adhere to:

1. ICT Risk Management

This pillar focuses on identifying, assessing, and mitigating risks associated with information and communication technology (ICT) infrastructure and processes. It emphasizes establishing a strong risk management framework and governance structure.

2. ICT-related Incident Management

This pillar emphasizes the importance of having robust procedures for detecting, reporting, and resolving ICT-related incidents. This includes establishing clear communication channels, incident response plans, and effective recovery mechanisms.

3. Digital Operational Resilience Testing

This pillar requires institutions to conduct regular testing of their digital operational resilience. This involves simulating various disruption scenarios and assessing the organization's ability to respond and recover effectively.

4. ICT Third-Party Risk Management

This pillar highlights the importance of managing risks associated with third-party ICT service providers. It requires institutions to have a comprehensive process for evaluating, selecting, and monitoring third-party vendors to ensure their alignment with DORA requirements.

5. Information and Intelligence Sharing

This pillar encourages collaboration and information sharing among financial institutions and authorities. It aims to facilitate the timely exchange of information on cyber threats and vulnerabilities to enhance the collective defense against cyberattacks.

By adhering to these five pillars, DORA aims to ensure that the financial sector is better prepared to withstand and recover from disruptions caused by cyberattacks, technological failures, or other unfo reseen events.

Whitepaper

Here's how AutomatePro can help you with your DORA compliance initiatives

While it's important to remember that there is no single solution that can address all your DORA compliance needs, AutomatePro plays a crucial role in helping you with four of the five pillars. That said, AutomatePro is not a DORA-compliance-built solution and should be used in conjunction with other DORA compliance measures like robust incident response plans, ongoing risk management practices, and more.

Risk Management	Incident Reporting	Digital Operational Resilience Testing	Thirdy-Party Risk Management	Information and Intelligence Sharing
AutoDoc	AutoMonitor	AutoTest	AutoTest	
		AutoDeploy	AutoDoc	
		AutoMonitor		

AutoTest

Pillar 2: Digital Operational Resilience Testing

This is an area where test automation plays a crucial role:

- **Running frequent tests:** Automated tests can be executed regularly without requiring manual intervention, ensuring continuous assessment of resilience.
- **Simulating diverse scenarios:** Different test types, such as functional testing and performance testing, can be automated to simulate a wide range of disruption scenarios.

Pillar 3: Third-Party Risk Management

While not entirely replacing due diligence, AutomatePro can support this process by:

- **Standardized testing:** Automated testing frameworks can be used to assess the security posture of third-party vendors consistently and efficiently.

AutoDeploy

Continuous deployment delivery is an important aspect to achieving DORA compliance, and featuers like AutoDeploy primarily contribute to one key pillar of DORA:

Pillar 3: Digital Operational Resilience Testing

This pillar emphasizes testing the organization's ability to respond and recover from various disruptions. Here's how AutoDeploy can support this:

- **Faster feedback loops:** By automating deployments and rollbacks, AutoDeploy enables frequent releases and faster feedback loops. This allows for quicker identification and correction of issues, enhancing overall system stability and resilience.
- **Reduced risk of regressions:** Having the power of AutoTest integrated within AutoDeploy helps ensure that new deployments don't introduce regressions or stability issues. This reduces the risk of disruptions caused by new releases and contributes to improved operational resilience.
- **Easier rollbacks:** In case of an issue after deployment, AutoDeploy can facilitate quick and efficient rollbacks to the previous stable version. This minimizes the impact of disruptions and helps the organization recover faster.

While not directly contributing to other DORA pillars like risk management or information sharing, continuous delivery tools, like AutoDeploy, indirectly contribute by enabling faster and more reliable deployments, which leads to **increased system stability** and **reduced risk of disruptions,** ultimately improving **operational resilience.**

AutoMonitor

Pillar 2: Incident Response

This pillar focuses on promptly detecting, reporting, and resolving incidents related to information and communication technology. Here's how continuous monitoring via AutoMonitor plays a crucial role:

- **Early detection:** By continuously monitoring system performance, security, and operational metrics, potential issues and anomalies can be identified promptly, allowing for faster intervention and mitigation of potential incidents.
- **Improved correlation and analysis:** Continuous monitoring helps you to analyze data from various sources. This facilitates the correlation of events and identification of root causes, leading to faster and more effective incident resolution.
- **Alerting and notification:** AutomatePro can be configured to trigger alerts and notifications when specific conditions are met, notifying your team of potential incidents or performance issues, enabling them to take timely action.

Pillar 3: Digital Operational Resilience Testing

This pillar emphasizes testing the organization's ability to respond and recover from various disruptions. AutoMonitor can support this in several ways:

- **Monitoring recovery processes:** By monitoring the performance of systems and applications during and after simulated disruptions, you can assess the effectiveness of recovery processes and identify potential bottlenecks.
- **Historical data analysis:** Analyzing historical data collected through continuous monitoring can provide valuable insights into past incidents and system behavior. This helps refine testing scenarios and identify areas where resilience needs to be strengthened.

Although not directly contributing to other pillars like risk management or information sharing, continuous monitoring indirectly supports them by providing **real-time insights** into system health and performance, which is crucial for proactive risk management and informed decision-making.

AutoDoc

Pillar 1: Risk Management

- **Improved transparency and traceability:** By centralizing and automating documentation, organizations can gain a clearer understanding of their systems, configurations, and processes. This transparency allows for better risk identification and facilitates impact assessments in case of incidents.
- **Reduced human error:** Manual documentation is prone to errors and inconsistencies, which can introduce additional risks. AutoDoc can help ensure consistency and accuracy in documentation, leading to improved risk management practices.

Pillar 4: Third-Party Risk Management

- **Standardized documentation:** AutoDoc can enforce consistent documentation practices across third-party vendors, ensuring that critical information about their systems and processes is readily available. This facilitates a standardized approach to third-party risk assessment and management.
- **Improved collaboration and communication:** AutoDoc can centralize information from various sources, including third-party vendors. This fosters better collaboration and communication between internal teams and external partners, allowing for a more comprehensive understanding of overall risk exposure.

Even though it is not directly addressing other DORA pillars like testing and incident response, improved documentation through automation can indirectly contribute to their effectiveness by providing a clear understanding of systems and processes, which is crucial for efficient testing and incident response activities.

Whitepaper

The AutomatePro Difference

The Digital Operational Resilience Act (DORA) presents a comprehensive framework for financial institutions to strengthen their digital resilience. By adhering to its five pillars, institutions can ensure they are prepared to withstand and recover from disruptions caused by cyberattacks, technological failures, or other unforeseen events.

AutomatePro's automated testing and DevOps platform can play a significant role in helping you achieve DORA compliance, including:

- **AutoTest** can streamline risk management processes and improve resilience testing.
- **AutoDeploy** can promote faster feedback loops and reduce the risk of regressions, ultimately improving resilience.
- **AutoMonitor** can aid in early detection and incident response, while also supporting operational resilience testing.
- **AutoDoc** can enhance transparency and facilitate risk management.

offers a **holistic approach** that can streamline compliance efforts and empower institutions to build a more resilient digital infrastructure. By leveraging automation, continuous monitoring, and a commitment to information sharing, financial institutions can achieve and maintain a robust digital operational resilience posture in accordance with DORA.

You can request a demo or learn more about the AutomatePro platform at AutomatePro.com

AutomatePro
Let's make progress

AutomatePro Ltd
4th Floor, Rex House 4-12
Regent Street London
SW1Y 4RG

+44 (0) 20 3473 2986
hello@automatepro.com

linkedin.com/company/automatepro-ltd

Official partner of

servicenow