LAST-MINUTE CHECKLIST FOR DORA COMPLIANCE: CRITICAL CONSIDERATIONS FOR YOUR MAINFRAME



With the January 17 deadline for compliance with the Digital Operational Resilience Act (DORA) upon us, banking and financial firms across Europe are scrambling to finalize their preparations. While many organizations have spent the past months or even years aligning their systems and processes with DORA's requirements, some critical elements—such as mainframe systems—may still require attention. Given that mainframes power many of the financial sector's core operations, ensuring their compliance with DORA is not just a necessity, but a strategic imperative.

This article provides a comprehensive last-minute checklist for mainframe-related DORA compliance. Whether you're confident in your preparedness or seeking to confirm nothing has been overlooked, these steps will help you ensure that your mainframe systems are ready to meet the stringent requirements of DORA.

Focus areas of DORA for the mainframe

DORA's core principles emphasize the need for financial institutions to understand their entire IT landscape, including their third-party service suppliers, while identifying potential vulnerabilities and implementing robust, automated strategies to protect systems, data, and customers from cyberthreats and disruptions.

While DORA focuses broadly on information and communication technology (ICT) systems, third-party risk management, incident reporting, resilience testing, and information sharing, firms with

mainframe systems must address some unique considerations such as:

Service awareness and availability

- Conduct regular health checks, automate maintenance tasks, and implement predictive alarms based on workload patterns.
- Enhance visibility into mainframe activities through robust logging mechanisms that meet DORA's transparency requirements.
- Adopt proactive strategies for identifying and addressing potential issues to maintain system availability and meet accountability standards.

Risk management

- Perform regular vulnerability assessments and penetration testing to identify and remediate issues specific to mainframe architecture.
- Strengthen security controls, including encryption mechanisms, access controls, and real-time monitoring.
- Leverage threat intelligence feeds and implement robust incident detection and response protocols for mainframe-specific threats.

Business continuity management

- Develop and regularly test recovery plans tailored to mainframe failure scenarios, incorporating automated backups and immutable data copies.
- Ensure failover mechanisms are in place for continuous operations, and validate their effectiveness through simulation exercises.
- Leverage cloud storage for mainframe backup data to enhance scalability, availability, and disaster recovery options.

Incident management

- Integrate mainframe monitoring alerts into enterprise-wide service consoles for unified incident management.
- Collaborate with the Security Operations Center (SOC) to ensure real-time transmission of and response to critical security events.
- Develop automated response playbooks for common threat scenarios and continuously refine them to address emerging risks.

Governance and compliance

- Use automated vulnerability scanning tools and compliance checks to streamline governance processes.
- Maintain continuous adherence to regulatory standards with automated reporting and regular audits.
- Design governance frameworks that evolve alongside regulatory updates to ensure ongoing compliance.

By addressing these areas, financial institutions can position their mainframe systems as a

cornerstone of operational resilience, fully aligned with DORA's requirements.

The last-minute mainframe checklist for DORA compliance

Building on these focus areas, here's a specific checklist to ensure compliance readiness:

1. Assess operational resilience

- Conduct stress tests and simulations to identify vulnerabilities.
- Validate that disaster recovery (DR) and business continuity (BC) plans include mainframe-specific scenarios.
- Ensure backup and failover systems can restore operations within required timeframes.
- Ensure enough capacity to accurately process the data necessary for the performance of activities and the timely provision of services.

2. Verify data integrity and cyber resilience

- Audit data protection mechanisms, including encryption protocols.
- Review and update backup processes for secure, quick restoration.
- Confirm security patches and updates are current.

3. Monitor third-party dependencies

- Review third-party contracts for alignment with DORA.
- Confirm vendors have implemented appropriate risk management measures.
- Assess your ability to replace or compensate for third-party services during disruptions.

4. Strengthen incident reporting and response

- Enable real-time incident detection and logging.
- Update escalation procedures to integrate mainframe incidents into the broader response framework.
- Validate that reporting mechanisms meet DORA's timeliness and accuracy requirements.

5. Modernize risk and compliance tools

- Implement AI-driven tools for real-time monitoring and vulnerability analysis.
- Integrate operational risk management with cybersecurity risk management.
- Automate compliance reporting to ensure accuracy and minimize effort.

6. Align governance with DORA standards

- Assign specific responsibilities for mainframe resilience.
- Document governance processes to demonstrate alignment with DORA.
- Train executives on mainframe compliance needs.

7. Test business continuity in hybrid environments

- Conduct continuity tests that include mainframe and hybrid systems.
- Address integration issues to ensure seamless failover.
- Ensure systems can share data and resources with modern technologies.

8. Validate regulatory reporting mechanisms

- Automate and test DORA-compliant reporting systems.
- Ensure reporting mechanisms meet regulatory deadlines.

9. Review cross-border data transfers

- Audit data transfer processes for compliance with DORA and the EU's General Data Protection Regulation (GDPR).
- Implement safeguards to prevent unauthorized access or breaches.

10.Document evidence of compliance

- Maintain detailed records of audits, tests, and system upgrades.
- Ensure documentation is well-organized and accessible for audits.

The cost of non-compliance

Failure to comply with DORA can result in significant fines, reputational damage, and operational disruptions. For financial institutions, operational resilience is both a regulatory requirement and a cornerstone of customer trust and competitive advantage.

How BMC can help

BMC AMI offers comprehensive solutions for mainframe DevOps, AIOps, DataOps, SecOps, and hybrid cloud data protection to simplify mainframe management, enhance operational resilience, and streamline compliance. Our hybrid AI technologies help organizations predict and prevent disruptions, protect against cyberthreats, and maintain robust governance.

Conclusion

With DORA now in effect, now is the time to ensure your mainframe systems are ready. By addressing the focus areas above and following the checklist, you can not only achieve compliance, but also strengthen your organization's operational resilience.

Start implementing these steps today and explore BMC's solutions to simplify compliance and resilience for your mainframe systems.