THE DIGITAL OPERATIONAL RESILIENCE ACT (DORA) AND CONTROL-M

The Digital Operational Resilience Act (DORA) is a European Union (EU) regulation designed to enhance the operational resilience of the digital systems, information and communication technology (ICT), and third-party providers that support the financial institutions operating in European markets. Its focus is to manage risk and ensure prompt incident response and responsible governance. Prior to the adoption of DORA, there was no all-encompassing framework to manage and mitigate ICT risk. Now, financial institutions are held to the same high risk management standards across the EU.

DORA regulations center around five pillars:

Digital operational resilience testing: Entities must regularly test their ICT systems to assess protections and identify vulnerabilities. Results are reported to competent authorities, with basic tests conducted annually and threat-led penetration testing (TLPT) done every three years.

ICT risk management and governance: This requirement involves strategizing, assessing, and implementing controls. Accountability spans all levels, with entities expected to prepare for disruptions. Plans include data recovery, communication strategies, and measures for various cyber risk scenarios.

ICT incident reporting: Entities must establish systems for monitoring, managing, and reporting ICT incidents. Depending on severity, reports to regulators and affected parties may be necessary, including initial, progress, and root cause analyses.

Information sharing: Financial entities are urged by DORA regulations to develop incident learning

processes, including participation in voluntary threat intelligence sharing. Shared information must comply with relevant guidelines, safeguarding personally identifiable information (PII) under the EU's General Data Protection Regulation (GDPR).

Third-party ICT risk management: Financial firms must actively manage ICT third-party risk, negotiating exit strategies, audits, and performance targets. Compliance is enforced by competent authorities, with proposals for standardized contractual clauses still under exploration.

Introducing Control-M

Financial institutions often rely on a complex network of interconnected application and data workflows that support critical business services. The recent introduction of DORA-regulated requirements has created an urgent need for these institutions to deploy additional tools, including vulnerability scanners, data recovery tools, incident learning systems, and vendor management platforms.

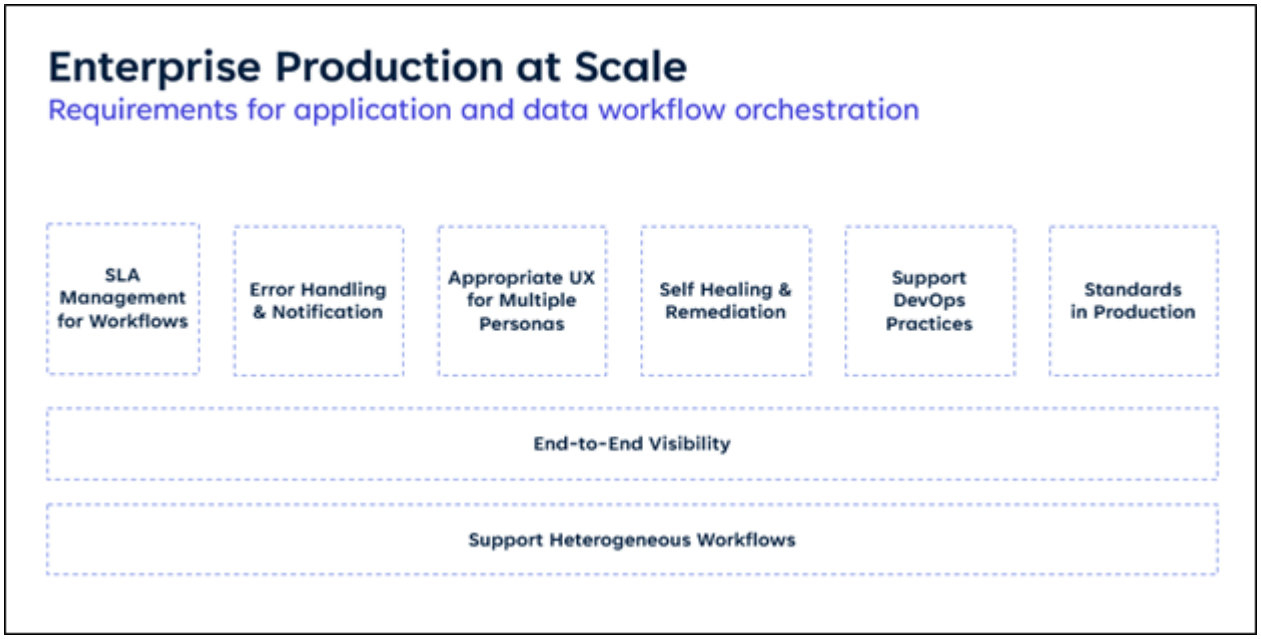
As regulatory requirements continue to evolve, the complexity of managing ICT workflows grows, making the need for a robust workflow orchestration platform even more critical.

Control-M empowers organizations to integrate, automate, and orchestrate complex application and data workflows across hybrid and cloud environments. It provides an end-to-end view of workflow progress, ensuring the timely delivery of business services. This accelerates production deployment and enables the operationalization of results, at scale.

Why Control-M

Through numerous discussions with customers and analysts, we've gained valuable insights that reinforce that Control-M embodies the essential principles of orchestrating and managing enterprise business-critical workflows in production at scale.

They are represented in the following picture. Let's go through, in a bottom-up manner.



Support heterogeneous workflows

Control-M supports a diverse range of applications, data, and infrastructures, enabling workflows to run across and between various combinations of these technologies. These are inherently hybrid workflows, spanning from mainframes to distributed systems to multiple clouds, both private and public, and containers. The wider the diversity of supported technologies, the more cohesive and efficient the automation strategy, lowering the risk of a fragmented landscape with silos and custom integrations.

End-to-end visibility

This hybrid tech stack can only become more complex in modern business enterprise. Workflows execute interconnected business processes across this hybrid tech stack. Without the ability to visualize, monitor, and manage your workflows end to- end, scaling to production is nearly impossible. Control-M provides clear visibility into application and data workflow lineage, helping you understand the relationships between technologies and the business processes they support. While the six capabilities at the top of the picture above aren't everything, they're essential for managing complex enterprises at scale.

SLA management for workflows

Business services, from financial close to machine learning (ML)-driven fraud detection, all have service level agreements (SLAs), often influenced by regulatory requirements. Control-M not only predicts possible SLA breaches and alerts teams to take actions, but also links them to business impact. If a delay affects your financial close, you need to know it right away.

Error handling and notification

Even the best workflows may encounter delays or failures. The key is promptly notifying the right team and equipping them with immediate troubleshooting information. Control-M delivers on this.

Appropriate UX for multiple personas

Integrating and orchestrating business workflows involves operations, developers, data and cloud teams, and business owners, each needing a personalized and unique way to interact with the platform. Control-M delivers tailored interfaces and superior user experiences for every role.

Self-healing and remediation

Control-M allows workflows to self-heal automatically, preventing errors by enabling teams to automate the corrective actions they initially took manually to resolve the issue.

Support DevOps practices

With the rise of DevOps and continuous integration and continuous delivery (CI/CD) pipelines, workflow creation, modification, and deployment must integrate smoothly into release practices. Control-M allows developers to code workflows using programmatic interfaces like JSON or Python and embed jobs-as-code in their CI/CD pipelines.

Standards in production

Finally, Control-M enforces production standards, which is a key element since running in production requires adherence to precise standards. Control-M fulfills this need by providing a simple way to guide users to the appropriate standards, such as correct naming conventions and error-handling patterns, when building workflows.

Conclusion

DORA takes effect January 17, 2025. As financial institutions prepare to comply with DORA regulations, Control-M can play an integral role in assisting them in orchestrating and automating their complex workflows. By doing so, they can continue to manage risk, ensure prompt incident response, and maintain responsible governance.

To learn more about who Control-M can help your business, visit www.bmc.com/control-m.