

MANAGING OPERATIONAL RESILIENCE IS A BFSI IMPERATIVE FOR DORA AND FFIEC



Financial regulations exist to ensure stability and trust in global banking systems. They protect customers, preserve systemic integrity, and help mitigate the risk of financial crises. However, even in a heavily regulated industry, banks and financial institutions (BFSIs) worldwide routinely fail audits, often paying steep penalties amounting to billions of dollars.

While many penalties have historically addressed financial misconduct, regulatory bodies are increasingly targeting failures in operational resilience—penalizing lapses in the critical systems and services that underpin modern banking operations.

Two [regulatory frameworks](#), the Digital Operational Resilience Act (DORA) in the European Union (EU) and the Federal Financial Institutions Examination Council (FFIEC) guidelines in the United States, underscore the increasing emphasis on IT operational resilience. These regulations mandate strong risk management and incident response frameworks to safeguard financial operations against escalating technological threats. Meeting these requirements necessitates a shift in how CIOs, CTOs, and IT leaders manage their IT ecosystems, making comprehensive IT management platforms like BMC Helix essential.

Why operational resilience matters

Although DORA and FFIEC share a focus on operational resilience, their approaches differ. DORA mandates explicit compliance measures, including resilience testing, incident reporting, and third-party risk management, with non-compliance resulting in severe penalties. Meanwhile, FFIEC offers broader, non-binding guidelines, enforced selectively by regulatory bodies like the Federal Reserve

and the Federal Deposit Insurance Corporation (FDIC).

Despite their differences, both emphasize the interconnected nature of increasingly complex and evolving financial systems. Failures in one institution can cascade globally, underscoring the importance of strong information and communication technology (ICT) risk management. Compliance involves addressing issues such as cybersecurity threats, service disruptions, and third-party dependencies, which makes an advanced IT management platform like BMC Helix indispensable.

BMC Helix: A holistic solution for DORA and FFIEC compliance

BMC Helix is an artificial intelligence (AI)-powered platform that enables compliance with DORA, FFIEC, and similar frameworks. The platform automates IT operations (ITOps), integrates service and operations management, and provides real-time visibility into critical systems. By aligning IT processes with regulatory expectations, BMC Helix empowers financial IT leaders to meet the stringent demands of operational resilience.

Key features include:

- **Comprehensive service mapping:** IT leaders must first understand their service and application dependencies, including new dependencies from mergers and acquisitions, to prevent disruptions. BMC Helix automates the mapping of technology components to business services, creating real-time, dynamic service maps. These maps show interactions and dependencies across on-premises systems, cloud environments, mainframes, and third-party services, giving organizations a clear picture of their operational landscape.
- **Risk management through real-time monitoring and modeling:** Regulatory frameworks emphasize proactive risk management, requiring constant monitoring and vulnerability assessments. BMC Helix provides real-time alerts for emerging threats and uses predictive analytics to recommend corrective actions. Automated remediation processes restore services quickly while minimizing operational risks.
- **Incident and recovery management:** Both DORA and FFIEC highlight the importance of swift incident response and recovery. BMC Helix enables organizations to quickly detect, respond to, and report incidents efficiently. AI-driven insights help predict and mitigate risks, while automated recovery workflows minimize service disruptions and deliver faster recoveries. Additionally, the platform generates comprehensive reports to meet audit requirements.
- **Governance and compliance reporting:** Meeting governance standards is vital for avoiding fines and reputational damage. BMC Helix automates key governance processes, including reporting and change management, to ensure institutions are ready in the event of an audit. And dashboards tailored to DORA and FFIEC compliance provide actionable insights into vulnerabilities so organizations can proactively address gaps.
- **Mainframe integration for enterprise visibility:** Many financial institutions rely on mainframes for critical operations. BMC Helix integrates with BMC's mainframe resiliency suite, providing unified monitoring and security across all systems. This cross-platform integration is critical for compliance, ensuring operational visibility and continuity.

The future of operational resilience

DORA and FFIEC represent a broader trend in regulatory frameworks, where operational resilience is

intertwined with financial stability and is no longer optional. It's mandatory to ensure trust is maintained and to avoid significant penalties.

With its AI-driven insights, automated workflows, and comprehensive service and operations management, BMC Helix is at the forefront of this transformation. The integrated solution empowers financial organizations to meet regulatory requirements, reduce risks, and enhance operational efficiency, positioning them for success in a time when resilience is paramount.

[Contact](#) BMC Helix to learn more about how we can help you meet the IT resiliency requirements of DORA, FFIEC, and other financial regulations.