Bottomline

Bottomline Insider Threat Management

Navigating DORA and UK Operational Resilience

The regulatory landscape for operational resilience is evolving rapidly, with the Digital Operational Resilience Act (DORA) in the EU imposing stringent regulatory requirements on financial institutions and ICT service providers, while the UK's Operational Resilience Framework (ORF) takes a broader, principles-based approach. While both frameworks aim to strengthen resilience against operational disruptions, they differ significantly in their regulatory oversight and implementation.

Summary of Major Differences

- DORA is an EU-wide regulation focused on ICT and cyber resilience, directly regulating ICT service providers, and requiring financial entities to strengthen their digital operational resilience.
- The UK Operational Resilience Framework (ORF) is broader, encompassing all critical business services. It follows a principles-based approach, giving firms flexibility in defining impact tolerances. Compliance is based on self-assessment rather than direct regulation, but firms are required to manage risk effectively.
- DORA directly regulates ICT service providers, imposing strict oversight and compliance requirements. In contrast, UK ORF places the responsibility on financial firms to ensure their third-party providers meet resilience expectations, but without direct regulatory oversight of ICT vendors.
- DORA imposes strict, standardised incident reporting timelines and resilience testing requirements. The UK framework, while requiring operational resilience testing, follows a principles-based approach, focusing on continuous resilience improvements rather than fixed regulatory standards.
- DORA mandates compliance by January 2025, whereas UK firms have been implementing ORF requirements since 2022.

While both frameworks aim to strengthen resilience against operational disruptions, they differ significantly in their regulatory oversight and implementation.

How Bottomline's Insider Threat Management (ITM) Supports Compliance for EU and UK Firms

As financial institutions and ICT service providers work to meet these regulatory expectations, Bottomline's Insider Threat Management (ITM) provides a crucial layer of protection, enabling compliance with both DORA and UK ORF requirements.

1. Advanced Investigations for Real-Time Threat Visibility

- Easy-to-understand dashboards, reports, and charts provide clear insights into risks, threats, and user activity.

- Screen-by-screen data capture with Record-and-Replay functionality eliminates time-consuming searches through log files.

- Google-like index search enables investigators to quickly locate key data (e.g., phone numbers, social security numbers, last names) across applications, enabling rapid forensic analysis.

2. Continuous Monitoring and Real-Time Detection

- For DORA compliance, Bottomline's ITM provides activity monitoring to help detect and respond to internal risks such as data leaks, policy violations, unusual employee behaviour, and unauthorized access attempts. This supports DORA's ICT risk management requirements (Articles 6-10), which mandate the implementation of a framework to 'duly and adequately protect all information assets and ICT assets' (DORA, Article 6(2)). ITM enhances threat detection, incident reporting (Article 17), and continuous monitoring of information systems (Article 9). Its ability to identify vulnerabilities and anomalous activities aligns with DORA's emphasis on proactive risk management and operational resilience testing (Article 12).

- For UK ORF compliance, ITM continuously monitors critical business applications, providing real-time visibility into operational disruptions and insider risks. While internal applications are not classified as important business services under the framework, they are often critical dependencies that support externally delivered services. This aligns with the Bank of England, PRA (PS6/21), and FCA's Operational Resilience framework (PS21/3), which requires firms to identify, map, and monitor important business services and their key dependencies. By enabling early detection and rapid response to disruptions, ITM helps organisations strengthen resilience, meet impact tolerance requirements, and ensure they can withstand, respond to, and recover from operational shocks within defined thresholds.

3. Risk-Based Alerts and Automated Investigations

- For DORA compliance, ITM continuously monitors and detects anomalous behaviours and internal risks, with a specific focus on insider threats. This supports DORA's risk management framework (Articles 6-10), which requires firms to establish mechanisms to 'promptly detect anomalous activities, including ICT network performance issues and security incidents' (Article 10). ITM's system automatically triggers alerts and records screen-level interactions, providing forensic replay capabilities that enhance internal investigations. In line with DORA's incident detection and classification requirements (Article 17), ITM enables financial entities to implement 'a well-documented incident management process to detect, manage, and notify security incidents.' By facilitating automated investigations, evidence collection, and structured reporting, ITM helps firms proactively identify, mitigate, and respond to insider threats, ensuring compliance with DORA's operational resilience and incident response mandates.

- For UK ORF compliance: ITM supports threat analysis and continuous monitoring of critical business applications, aligning with the UK regulators' principles-based approach to operational resilience (PS6/21 & PS21/3). By enabling firms to detect and assess operational disruptions, ITM enhances preparedness for severe but plausible scenarios, a key requirement under UK impact tolerance frameworks.

4. Compliance with Incident Reporting Requirements

- For DORA compliance: Bottomline ITM enables structured incident investigations by capturing and replaying user interactions, providing forensic evidence to support regulatory breach reporting under DORA (Articles 17-20). While firms remain responsible for submitting reports, ITM ensures they have the necessary evidence for compliance and audit readiness.

- For UK ORF compliance: ITM enables firms to capture and replay user interactions linked to operational disruptions, providing detailed forensic evidence for regulatory audits and impact assessments. This aligns with UK ORF (PS6/21 & PS21/3) and FCA/PRA expectations for operational disruption reporting, which require firms to log, investigate, and document incidents affecting critical business services. By offering visibility into anomalous activities and resilience gaps, ITM helps organisations enhance their incident response and reporting frameworks, enabling compliance with the UK's impact tolerance and disruption mitigation obligations.

5. Enhancing Operational Resilience and Threat Intelligence

- For DORA compliance: While ITM does not perform penetration testing, it enhances firms' operational resilience by monitoring insider threats, detecting anomalous behaviour, and supporting forensic investigations—all essential for pre- and post-resilience testing analysis. This aligns with DORA's ICT risk management and resilience testing requirements (Articles 6-12), which mandate that financial entities identify vulnerabilities, assess risk exposure, and implement continuous monitoring strategies. ITM also supports incident detection, forensic analysis with replay capabilities (Article 17), enabling firms to effectively respond to security breaches and derive key learnings.

- For UK ORF compliance: ITM strengthens resilience scenario testing and impact tolerance assessments, in line with UK regulatory expectations (PS6/21 & PS21/3). By providing visibility into employee activities, detecting suspicious access patterns, and generating forensic recordings, ITM supports firms in evaluating their ability to prevent, respond to, and recover from operational disruptions. This enhances post-test evaluations, helping organisations refine their business continuity and cyber resilience strategies.

- For Both Jurisdictions: ITM provides firms with a continuous feedback loop from resilience assessments, helping them refine access controls, strengthen insider threat detection, and improve overall operational resilience. This supports both DORA's resilience testing obligations (Article 12) and the UK's regulatory focus on scenario-based risk assessments. By delivering actionable intelligence from monitoring and forensic investigations, ITM helps firms maintain compliance, reduce operational risk, and enhance long-term resilience.

6. Mitigating Third-Party Insider Risks

- For DORA compliance: Bottomline's ITM enhances incident investigation and reporting by providing structured forensic evidence through record and replay capabilities. This supports DORA's ICT-related incident reporting requirements (Articles 17-20) by enabling firms to capture, analyse, and document security breaches with detailed user interaction data. While ITM does not directly handle mandated reporting submissions, it helps firms generate evidence-based reports that support regulatory notifications, post-incident reviews, and compliance audits. By capturing and replaying system activity to provide forensic evidence, ITM assists organisations in meeting DORA's expectations for incident analysis, root cause investigation, and lessons learned reporting (Article 18).

- For UK ORF compliance: ITM enables firms to continuously monitor third-party behaviour and detect unusual activities within internal systems, aligning with the PRA's outsourcing and third-party risk management expectations (SS2/21) and operational resilience requirements (PS6/21). By providing granular visibility into vendor interactions with critical business services, ITM helps organisations identify resilience vulnerabilities, assess potential disruptions from outsourced services, and ensure third-party compliance with operational resilience frameworks. This aligns with the UK regulators' focus on impact tolerance and third-party accountability, enabling firms to mitigate risks arising from supply chain dependencies

Conclusion: A Unified Approach to Compliance

DORA and UK ORF present distinct yet complementary regulatory challenges. Bottomline's Insider Threat Management (ITM) offers a scalable, adaptive solution that helps financial institutions and ICT service providers in both the EU and UK stay compliant while strengthening their resilience. With ITM, organisations can:

- ⊕ Detect and respond to insider threats and cyber incidents in real time.
- ⊕ Support structured incident reporting with forensic evidence to help firms meet regulatory requirements.
- ⊕ Provide forensic analysis and record-and-replay visibility to support resilience testing and operational risk assessments.
- ⊕ Monitor third-party activities and detect insider risks associated with external access.

With DORA now in full effect and UK regulators actively enforcing operational resilience requirements, firms must implement robust solutions to ensure compliance and mitigate risk. Bottomline Insider Threat Management (ITM) provides a strong foundation for compliance, security, and resilience. More than just a monitoring tool, ITM serves as a compliance enabler, empowering organisations to proactively manage insider threats and strengthen their operational resilience strategies—whether under DORA's ICT risk management framework or the UK's Operational Resilience requirements PS6/21 (PRA) and PS21/3 (FCA).

REV US062425KG

Corporate Headquarters
100 International Drive, Suite 200
Portsmouth, NH 03801
United States of America

Phone: +1 603-436-0700
Toll-free: +1 800-243-2528
info@bottomline.com