Bottomline

Operational Resilience Readiness Checklist:

NAVIGATING DORA AND UK ORF COMPLIANCE

As the regulatory environment evolves, financial institutions and Information and Communication Technology (ICT) service providers must prepare for stricter oversight and higher expectations under the EU's **Digital Operational Resilience Act (DORA)** and the UK's **Operational Resilience Framework (ORF).**

In brief, DORA focuses on ICT and cyber resilience: it directly regulates ICT service providers and requires financial entities to strengthen their digital operational resilience. 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.

While both DORA and ORF aim to strengthen resilience against operational disruption, they differ significantly in scope, oversight, and implementation. The following checklist provides a structured approach to help you ensure readiness across key areas of compliance. It also shows how Bottomline's Insider Threat Management (ITM) offers a scalable, adaptive solution that can give you an advantage in aligning with DORA and ORF.

Resilience Readiness Checklist

1. Advanced Investigations for Real-Time Threat Visibility

□ Do you have easy-to-understand dashboards and reports that provide clear insights into risks, threats, and user activity?

□ Can you perform screen-by-screen forensic analysis using record-and-replay capabilities?

□ Do you have the ability to conduct fast, indexed searches across applications to assist investigations?

ITM Advantage: Bottomline's ITM provides a powerful combination of intuitive dashboards, real-time user behavioural analytics, and searchable screen-level session records. This gives compliance and security teams deep visibility into what is happening across systems—essential for identifying ICT risks and potential disruptions as required by both DORA and ORF.

2. Continuous Monitoring and Real-Time Detection

□ Are you continuously monitoring internal and critical business systems for policy violations, unusual behaviour, and unauthorised access?

□ Can you detect operational disruptions in real time and tie them to potential insider threats?

□ Do you have systems in place to meet DORA's ICT risk management and ORF's mapping and monitoring expectations?

ITM Advantage: ITM's continuous monitoring of user and system activity enables organisations to detect threats and suspicious behaviour as they occur. By linking anomalies to operational or service disruptions, ITM helps meet real-time detection obligations under DORA and ORF's resilience mapping guidelines.

3. Risk-Based Alerts and Automated Investigations

□ Have you implemented automated alerts for anomalous behaviours, policy violations, and insider threats?

□ Can your system capture and replay screen-level interactions to support incident analysis and response?

□ Are your investigations aligned with structured incident detection and classification requirements?

ITM Advantage: ITM facilitates automated detection and investigation workflows through real-time alerting and advanced behavioural analytics. Its Record-and-Replay capability offers irrefutable evidence for incident review, while structured workflows support DORA's requirements for detection, classification, and response, dramatically reducing investigation time.

3. Risk-Based Alerts and Automated Investigations

□ Have you implemented automated alerts for anomalous behaviours, policy violations, and insider threats?

□ Can your system capture and replay screen-level interactions to support incident analysis and response?

□ Are your investigations aligned with structured incident detection and classification requirements?

ITM Advantage: ITM facilitates automated detection and investigation workflows through real-time alerting and advanced behavioural analytics. Its Record-and-Replay capability offers irrefutable evidence for incident review, while structured workflows support DORA's requirements for detection, classification, and response, dramatically reducing investigation time.

4. Compliance with Incident Reporting Requirements

□ Can you capture, investigate, and replay incidents with sufficient forensic detail to support regulatory reporting?

□ Do you have the capability to log and document incidents that affect critical business services or ICT systems?

□ Is your incident evidence audit-ready and aligned with the requirements of both DORA and ORF?

ITM Advantage: Bottomline's ITM ensures every incident is captured with high-fidelity forensic detail, including user actions, system access, and data movement. This audit-ready evidence aligns with DORA's strict reporting timelines and ORF's expectations for assessing and documenting disruptive incidents across critical business services.

5. Enhancing Operational Resilience and Threat Intelligence

□ Do you have the continuous monitoring and rich data necessary to identify vulnerabilities and support resilience testing or scenario assessments?

□ Can your systems help evaluate whether your organisation can withstand, respond to, and recover from severe but plausible disruptions?

□ Are you leveraging insights from threat detection and investigations to refine resilience strategies over time?

ITM Advantage: ITM turns behavioural data into actionable intelligence—pinpointing process gaps, security risks, and systemic weaknesses. These insights are invaluable for resilience planning and scenario testing, helping you meet DORA's ICT continuity requirements and ORF's principle of "impact tolerance" for critical operations.

6. Mitigating Third-Party Insider Risks

□ Are you monitoring third-party access to internal systems to detect suspicious activity?

□ Do you maintain forensic records of vendor interactions with systems supporting important business services?

□ Can you assess and document potential resilience gaps linked to outsourced services?

ITM Advantage: Third-party access does not have to be a blind spot. ITM monitors and records all vendor interactions within your systems, enabling you to detect inappropriate behaviour, verify contract compliance, and assess third-party risk—supporting both DORA's third-party ICT risk rules and ORF's dependency management framework.

Strengthening Resilience with Confidence

Achieving compliance with DORA and ORF demands a dynamic and continuous approach to identifying threats, managing risks, and reinforcing critical business services. This readiness checklist is designed to help you assess and elevate your operational resilience across key domains, from real-time threat detection to audit-ready incident reporting.

Bottomline's Insider Threat Management (ITM) solution is uniquely positioned to support this journey. By combining deep forensic visibility, continuous monitoring, and intelligent automation, ITM empowers financial institutions and ICT providers to meet current regulatory expectations with confidence. Whether it is uncovering hidden risks, responding to incidents, or preparing for future disruptions, ITM delivers the clarity and control needed to thrive in today's demanding regulatory landscape.

Bottomline™

About Bottomline

Bottomline helps businesses transform the way they pay and get paid. A global leader in business payments and cash management, Bottomline's secure, comprehensive solutions modernize payments for businesses and financial institutions globally. With over 30 years of experience, moving more than $10 trillion in payments annually, Bottomline is committed to driving impactful results for customers by reimagining business payments and delivering solutions that add to the bottom line. Bottomline is a portfolio company of Thoma Bravo, one of the largest software private equity firms in the world, with more than $130 billion in assets under management.

For more information, visit **www.bottomline.com**

REV US061125KV

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

Europe, Middle East, Africa Headquarters
1600 Arlington Business Park
Theale, Reading, Berkshire RG7 4SA
United Kingdom

Tel (Local): 0870-081-8250
Tel (Int): +44-118-925-8250
emea-info@bottomline.com