Financial Services in the Crosshairs

The Regulatory Push for IT Operational Resilience

BUGZERO™

Introduction

"Authorised financial services firms must manage risks in software and applications through an established risk framework, process and procedures, **regardless of whether they are caused by security or non-security known or unknown bugs...**"

— UK Financial Conduct Authority

Executive Summary

For financial institutions, IT risk management has traditionally centered on cybersecurity and fraud prevention. However, a growing regulatory focus on third-party software risks is reshaping how organizations think about operational resilience and risk management. **Ensuring the stability and reliability of critical third-party software has become an increasingly prominent component of regulatory guidance and obligations.**

This shift is exemplified by a recent publication by the UK's Digital Regulation Cooperation Forum (DRCF), a collaboration between four UK regulators—Ofcom, the FCA, the CMA, and the ICO. The DRCF published a case study of operational resilience risks stemming from non-security third-party software failures.

While the DRCF concentrates on UK-specific regulations, the risks and obligations they address are global — and given the breadth of the four regulatory agencies represented — one can argue that they are universal.

Financial Systems' Growing Dependence on Third-Party Technology

When third party systems fail, their resulting disruptions can no longer be confined to a single institution — interdependencies between banks, payment processors, and infrastructure providers mean that a failure in one entity can cascade across the entire financial ecosystem.

Interdependencies Across Financial Services: The reliance on third-party vendors means that operational disruptions at one service provider can have market-wide consequences.

The Speed and Scale of IT Failures: System crashes, failed software deployments, and outages can propagate rapidly, affecting millions of customers within minutes.

The Inadequacy of Traditional Risk Models: Many institutions have not fully integrated third-party IT risk into their operational resilience strategies, leaving gaps in their ability to prevent and respond to failures.

A Global Regulatory Movement Toward IT Operational Resilience

Financial regulators across jurisdictions are aligning their policies to ensure institutions can withstand IT disruptions, regardless of their origin. Key global regulatory initiatives emphasizing third-party IT resilience include:

European Union
Digital Operational Resilience Act (DORA): Requires financial institutions to assess, test, and mitigate risks associated with IT service providers.

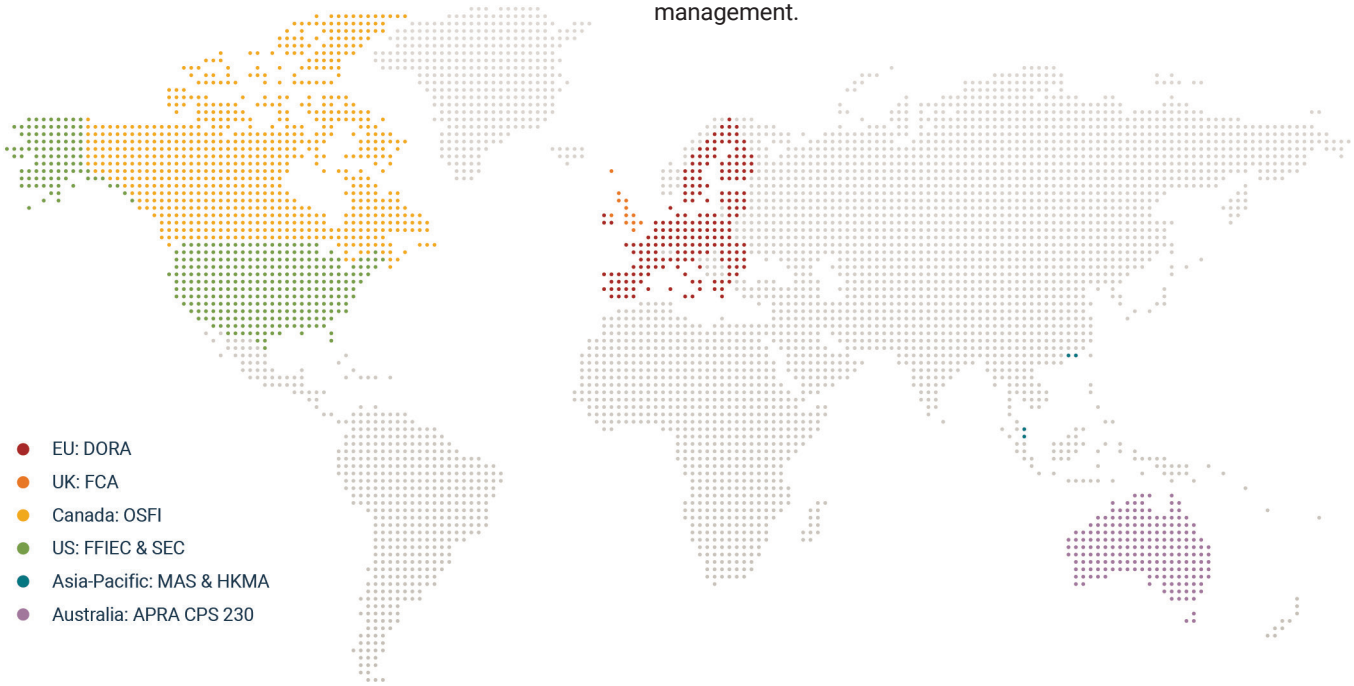
United Kingdom
Financial Conduct Authority (FCA): Implementing operational resilience rules requiring financial firms to identify important business services, set impact tolerances, and manage risks from third-party IT providers.

Canada
Office of the Superintendent of Financial Institutions (OSFI): Strengthening operational resilience expectations for financial firms with an emphasis on IT disruptions.

United States
Federal Financial Institutions Examination Council (FFIEC) & SEC: Expanding operational resilience guidelines to include third-party vendor failures.

Asia-Pacific
Monetary Authority of Singapore (MAS) & Hong Kong Monetary Authority (HKMA): Integrating IT resilience into broader financial stability regulations.

Australia
Australian Prudential Regulation Authority (APRA) CPS 230: Introduces new obligations for third-party IT resilience, reinforcing proactive risk management.



Regulatory Expectations lead to Strategic Advantage

IT operational resilience is not solely a compliance burden. Financial institutions that take a proactive approach to resilience stand to benefit significantly through:

Increased Availability with Fewer Business Disruptions
Eliminating system outages translates into increased availability and measurably more productive and profitable operations.

Improved Customer Trust
A reputation for reliability can differentiate institutions in a competitive market.

Long-term Cost Efficiency
Investing in proactive resilience strategies is more cost-effective than reacting to operational failures after they occur.

In order to accrue these benefits, financial institutions must continuously calibrate their IT risk investments to meet evolving expectations and to capitalize on opportunities.

Third-party Operational Bugs: Behind the Headlines

Third-party bugs don't fit into a headline, but the damage they can cause certainly can.

HOSPITAL FACES ELECTRONIC HEALTH RECORD BLACKOUT PUTTING PATIENTS AT RISK.

AUTOMATED DISPATCH SYSTEMS FAILED DURING PEAK FREIGHT VOLUMES, STRANDING CONTAINER TRAINS.

Behind the headlines: Microsoft's 24H2 update introduced a memory addressing error in the Windows Kernel Transaction Manager (KTM). **Despite Microsoft releasing KB5034209 in January 2025, 18% of enterprise workstations remained unpatched as of March 2025.**

THOUSANDS OF WORKERS IDLED ACROSS AUTO PLANTS AS JUST-IN-TIME PARTS ORDERING SYSTEMS FAILED.

NOT SO SMART ENERGY GRID: 48-HOUR SMART METER FAILURE DURING HEATWAVE.

Behind the headlines: A memory leak in SAP HANA 2.0 SPS06's columnstore engine caused OOM (Out of Memory) errors on large join operations. **Though patched within 14 days, 61% of DBAs couldn't apply kernel updates without vendor support contracts due to skill gaps.**

Seemingly obscure software flaws can cascade into serious system outages and disruptions. Software vendors lack the operational context to assess the potential for harm — that responsibility rests with each enterprise — and that is only scalable with automated, integrated, and intelligent vendor operational defect monitoring and management.

Four Regulators, One Voice

Meet the Digital Regulation Cooperation Forum

The Digital Regulation Cooperation Forum (DRCF) is a collaboration between four UK regulators — Ofcom, the FCA, the CMA, and the ICO — working together to address the complex, cross-sector challenges of digital and AI regulation. This unique partnership reflects the increasing interdependence of regulatory domains.

Their AI and Digital Hub is a groundbreaking initiative providing a structured environment for firms to engage with regulators on emerging technology and compliance issues. A key component is their Case Study, which explores how cross-regulator cooperation can streamline compliance while fostering innovation.

The DRCF's work reflects a modern regulatory paradigm where technology governance extends beyond cybersecurity to ensure uninterrupted critical services.

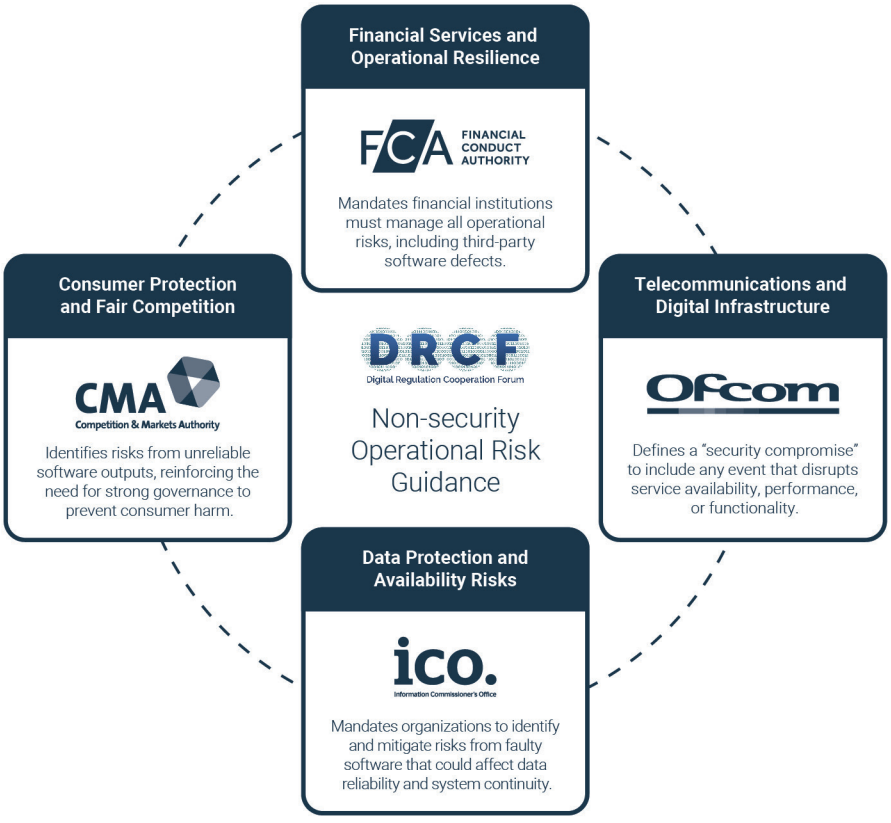
Managing Non-Security Third-Party Software Risks: A Cross-Regulatory Perspective from the DRCF

The DRCF initiative is unique in its recognition of the interconnected nature of regulatory domains spanning finance, telecommunications, consumer protection, and data governance.

In their recent case study, *Managing the impact of third-party software defects on resilience*, the DRCF calls out the importance of recognizing that operational risk can be compromised by software defects, misconfigurations, and vendor failures.

Beyond the DRCF summary statement, each regulator within the DRCF addressed this issue as well, reinforcing the need for firms to proactively manage non-security software risks alongside security vulnerabilities.

The DRCF's collective approach acknowledges that non-security third-party software defects pose a substantial risk to financial stability, telecommunications, consumer protection, and data integrity. See Appendix A: Four Regulators One Voice for a detailed breakdown of agency responses.



Strategies for Financial Institutions to Mitigate Third-Party Software Risks

Non-security software defects, such as unpatched bugs, flawed software versions, and vendor service failures, pose significant risks to operational resilience. To meet evolving regulatory expectations and ensure continued service availability, financial institutions must adopt a structured, proactive approach to third-party software risk management.

Comprehensive Visibility into Third-Party Software Defects

Identify and continuously monitor third-party software dependencies.

Track known defects and software vulnerabilities in third-party products to assess their potential impact on operations and prioritize remediation efforts.

Establish a structured, centralized repository of third-party software issues, ensuring that risk management, IT operations, and compliance teams have a consolidated view of software-related operational risks.

Continuous Vendor Risk Assessment and Oversight

Go beyond periodic vendor reviews and maintain ongoing monitoring of third-party software providers.

Continuously assess the operational risks posed by third-party software failures, ensuring that dependencies on external vendors do not introduce unchecked risks.

Implement automated tracking, risk scoring, and assessment mechanisms to evaluate software defects, vendor responsiveness, and version stability.

Automated Incident Response and Remediation Workflows

Rapidly detect, assess, and mitigate third-party software failures.

Third-party software failure detection and tracking into their IT Service Management (ITSM) platforms to facilitate real-time remediation and ensure compliance with reporting obligations.

Establish structured workflows for defect tracking, impact analysis, and coordinated remediation to minimize disruptions to critical operations.

BugZero — for Automated, Intelligent, Proactive Compliance

As regulatory requirements for operational resilience and third-party software risk management continue to expand, financial institutions must move beyond manual risk tracking and adopt automation-driven solutions to streamline compliance.

Automated Monitoring for Third-Party Software Defects

Regulatory Obligation	Continuously monitor third-party software dependencies for known defects and vulnerabilities[1].
Automation Benefit	Automated tools scan vendor software updates, defect reports, and system logs to detect potential non-security software risks before they disrupt operations.
BugZero	• Maintains an up-to-date repository of known third-party software defects. • Automatically integrates with vendor feeds and databases to track emerging issues. • Flags software bugs linked to critical financial services, ensuring that IT teams can take preventive action.

AI-Driven Risk Prioritization Based on Business Impact

Regulatory Obligation	Prioritize risk mitigation efforts based on business-critical functions[2].
Automation Benefit	AI-driven solutions assess the potential business impact of third-party software defects, allowing financial institutions to allocate resources efficiently.
BugZero	• Correlates software defects with operational dependencies, using organizational configuration to identify which systems and services may be at risk. • Applies AI-based risk scoring to categorize software defects based on user configurable priorities. • Through ITSM integration, allows prioritized remediation actions, ensuring that high-impact issues are addressed first.

1 *as required by DORA (EU), FCA SYSC 15A (UK), and FFIEC IT Examination Guidelines (US)*

2 *per DORA (EU), SEC Cybersecurity Rules (US), and APRA CPS 230 (Australia)*

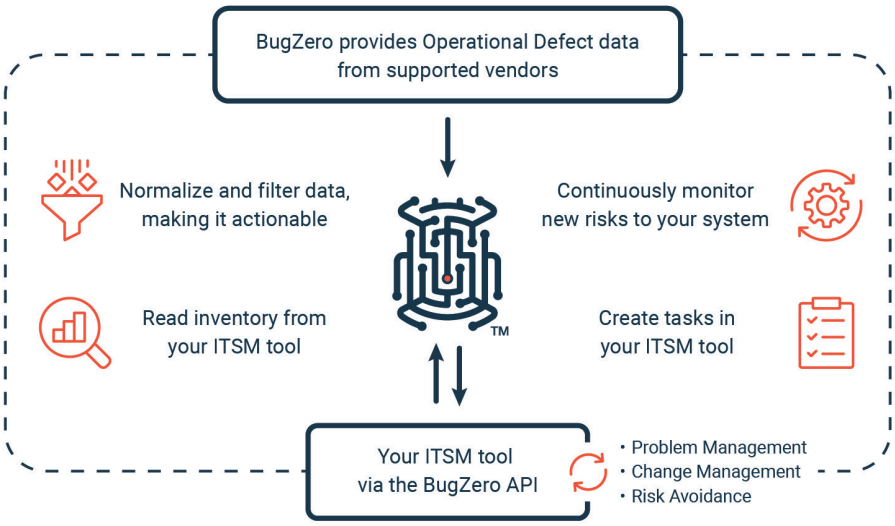
Real-Time Vendor Risk Visibility for Compliance Reporting

Regulatory Obligation	Demonstrate proactive vendor risk management and provide timely compliance reporting[1].
Automation Benefit	Automated reporting tools streamline vendor risk assessments and regulatory disclosures, reducing manual compliance efforts.
BugZero	• Provides a real-time dashboard showing software defects, vendor response times, and compliance status. • Integrates with IT Service Management (ITSM) platforms, ensuring that remediation efforts are documented and auditable for regulatory review.

By leveraging BugZero, financial institutions can reduce manual compliance burdens, improve risk visibility, and ensure proactive response to third-party software risks. BugZero's capabilities align with key regulatory expectations, helping firms maintain operational resilience while streamlining compliance with evolving global standards.

BugZero Prevents Outages

BugZero is a first-of-its-kind IT Operational Resilience platform that aggregates multi-vendor operational defect data, presenting IT organizations with a unified view of risks that could cause outages or otherwise adversely affect business.



1 *as required by OSFI B-10 (Canada), HKMA Guidelines (Hong Kong), and FCA Operational Resilience Mandates (UK).*

Appendix

BUGZERO™

APPENDIX A

Four Regulators, One Voice

Four Regulators

Here are a sampling of regulatory citations highlighted by the regulatory agencies themselves in their effort to document these requirements.

Financial Conduct Authority (FCA): Financial Services and Operational Resilience

The FCA's Policy Statement on Building Operational Resilience **(SYSC 15A)** mandates that financial institutions must manage **all operational risks**, including third-party software defects, that could impact critical business services.

- **SYSC 15A.4.2G:** Requires firms to understand vulnerabilities in third-party services, whether security-related or not. Firms must work closely with vendors to mitigate risks.
- **SYSC 15A.5.5G:** Stresses scenario testing, which includes assessing dependencies on third-party software to prevent disruptions from software flaws.
- **Guidance on Outsourcing to the Cloud and Third-Party IT Services (FG16/5):** Emphasizes ongoing risk assessment, change management, and continuous oversight of third-party software providers to prevent service interruptions.

Ofcom: Telecommunications and Digital Infrastructure

Ofcom regulates communications networks and digital infrastructure and emphasizes the need for resilience beyond cybersecurity.

- **The Communications Act 2003** (as amended by the Telecommunications Security Act 2021) broadens the definition of a "security compromise" to include any event that disrupts service availability, performance, or functionality, regardless of whether it stems from a cybersecurity breach or a non-security software defect.
- **The Telecommunications Security Code of Practice** highlights risks from low product quality and systemic failures in network equipment and software, which could cause widespread disruption even in the absence of security threats.
- **Regulation 12 on "Patches and Updates"** requires firms to proactively deploy software updates, reinforcing the need for vendor oversight beyond security patches.

Information Commissioner's Office (ICO): Data Protection and Availability Risks

While the ICO primarily oversees data security and privacy, its regulatory scope includes the availability and integrity of IT systems that store or process personal data.

- **UK GDPR Article 32 (Security of Processing):** Requires organizations to ensure resilience against software failures that impact data availability, including third-party software defects.
- **Data Protection by Design (Article 25):** Mandates organizations to identify and mitigate risks from faulty software that could affect data reliability and system continuity.

Competition and Markets Authority (CMA): Consumer Protection and Fair Competition

The CMA enforces consumer protection laws to ensure fair business practices, including transparency in third-party software dependencies.

- **The Consumer Protection from Unfair Trading Regulations (CPRs) 2008** prohibits businesses from misleading consumers about the stability or reliability of digital services that rely on third-party software.
- **The AI Foundation Models Initial Review** identifies risks from unreliable software outputs, reinforcing the need for strong software governance to prevent consumer harm.

APPENDIX B

Beyond the UK: DORA and Global Financial Sector Regulations

Cross-Border Compliance Challenges

Financial institutions operating in multiple jurisdictions face overlapping and evolving regulatory requirements. In response, U.S., EU, and APAC regulators increasingly align on third-party software risk governance, requiring harmonized compliance strategies to manage global operational resilience.

Europe – Digital Operational Resilience Act (DORA):

- Establishes stringent operational resilience requirements for financial institutions.
- Mandates continuous risk assessment and oversight of third-party IT service providers to ensure financial stability.

United States – FFIEC & SEC:

- FFIEC IT Examination Handbook: Expands operational resilience guidelines to include third-party software and vendor failures.
- SEC Cybersecurity Rules: Require financial firms to disclose material third-party IT risks and implement resilience measures against non-security software defects.

Other Key Jurisdictions:

- **Canada (OSFI B-10):** Strengthens governance and oversight of third-party IT providers.
- **Hong Kong (HKMA Guidelines) & Singapore (MAS Outsourcing):** Require firms to actively monitor vendor risks and ensure business continuity.
- **Australia (APRA CPS 230):** Introduces new obligations for third-party IT resilience, reinforcing proactive risk management.