Telecommunications in the Crosshairs

The Regulatory Push for Network & IT Operational Resilience

BUGZERO™

Introduction

"(Telcos) must take appropriate measures to prevent, or minimise the adverse effect of anything that compromises network availability, performance or functionality."

— Ofcom Security Act 2021 §105(4)

Executive Summary

A growing regulatory focus on third-party software risks is reshaping how organizations confront 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 in emphasis is exemplified by a recent publication, Managing the impact of third-party software defects on resilience, by the UK's Digital Regulation Cooperation Forum (DRCF), a collaboration between four UK regulators—Ofcom, the FCA, the CMA, and the ICO.

While the DRCF concentrates on UK-specific regulations, the risks and obligations addressed are global, and given the breadth of the four regulatory agencies represented, one can argue that they are universal. Few industries are impacted more than telecommunications operators, carriers, and service providers (telcos).

Connectivity's Growing Dependence on Third-Party Technology

When telecommunication services fail, financial markets, healthcare systems, manufacturing, retail operations, and most every other pillar of modern life fail with it.

When third-party systems fail, their resulting disruptions can no longer be confined to a single institution — interdependencies between mobile-core vendors, OSS/BSS suppliers, tower-sharing partners, and hyperscale clouds mean that a failure in one entity can cascade across the entire telco ecosystem.

Interdependencies Across Telecommunications Ecosystems: Roaming agreements, MVNO arrangements, peering exchanges, and shared towers/cloud cores bind carriers together, so a failure at one network or vendor can ripple instantly across many operators and geographies.

The Speed and Scale of Network Failures: DNS misconfigurations, corrupted BGP routes, or buggy EPC patches can spread in seconds, dropping millions of calls, texts, and data sessions before engineers have time to react.

Limits of Hardware-Centric Resilience Models: Traditional redundancy plans focus on links and switches yet often miss latent firmware flaws or orchestration-layer defects in vendor software, the very issues that now trigger most large-scale outages.

A Global Regulatory Movement Toward IT Operational Resilience

Telecommunications regulators across multiple 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
NIS 2 Directive & EECC Art 40. Availability & incident-reporting for electronic-communications networks.

United Kingdom
Telecommunications (Security) Act 2021 & Ofcom Security Code of Practice: Obliges telcos to identify and mitigate risks—including third-party software defects—and to report major incidents to Ofcom within predefined timelines.

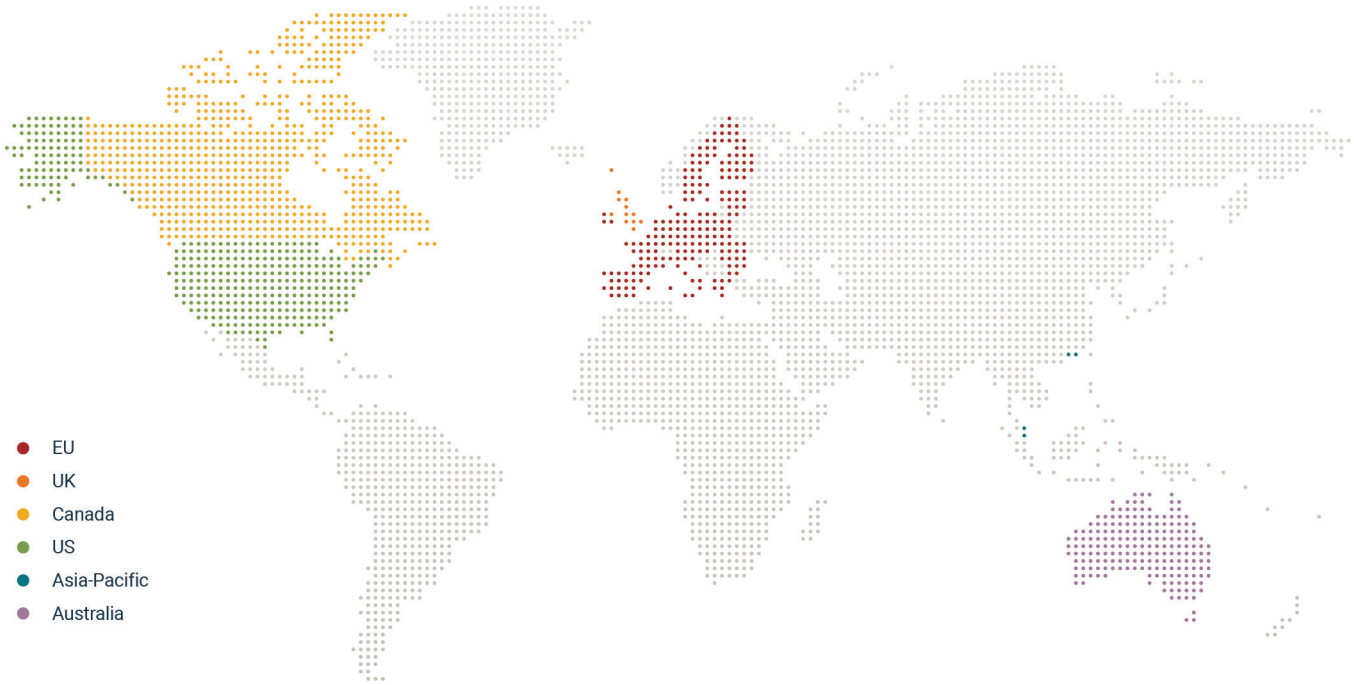
Canada
CRTC Telecom Decision 2023-80. Mandates resilience plans and software-update discipline.

United States
FCC Network Outage Reporting System (NORS) & Secure & Trusted Comms Act: Rapid outage disclosure, supply-chain vetting.

Asia-Pacific
Singapore IMDA Telecom Cyber Code 2022.

Australia
TSSR: Treat software defects as critical-infrastructure threats.

Like the DRCF's cross-sector findings, each regime recognises that non-security software defects in vendor equipment can cripple national communications services.



Regulatory Expectations lead to Strategic Advantage

IT operational resilience should not be seen as solely a compliance burden. Telcos that move first on resilience benefit from:

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

Subscriber Trust & Churn Reduction
A reputation for reliability can differentiate institutions in a competitive market.

Long-term Cost Efficiency
Avoids SLA penalties and spectrum-licence repercussions.

Telcos must continuously calibrate their IT risk investments to meet evolving expectations and to capitalize on opportunities.

Third-party Operational Bugs: Behind the Headlines

LATENT SOFTWARE FLAW MAGNIFIES SYSTEM FAILURE, RESULTING IN 250 MILLION FAILED CALLS

The Federal Communications Commission (FCC) said a June 2020 nationwide T-Mobile outage resulted in at least 250 million calls failing. The FCC reported that "the company did not follow several established network reliability best practices that could have potentially prevented or mitigated the outage." The FCC concluded that the outage was caused "by an equipment failure" that was "exacerbated by a network routing misconfiguration" and then **"magnified by a software flaw in T-Mobile's network that had been latent for months."**

Source: Reuters: June T-Mobile U.S. network outage disrupted more than 250 million calls: FCC

NON-CYBER-INCIDENT COSTS TELCO $450M, IMPACTS 10M USERS, AND TRIGGERS NEW REGULATIONS

Rogers Communications Inc. (Rogers) experienced a major service outage that affected its wireless and wireline services across Canada (July 2022 outage). While the specifics of the root cause were not fully disclosed, Public Safety Canada (PSC) stated that it was not a cyberattack and resulted, in part, from failure to follow best practices during upgrades and maintenance procedures. **The combination of rebates, fines, and mandated mitigation exceeded $450M and triggered new Telco regulations and oversight. Rogers' CTO and CIO leadership were ousted within three weeks of the incident.**

Source: 2022 Rogers Communications outage

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

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.

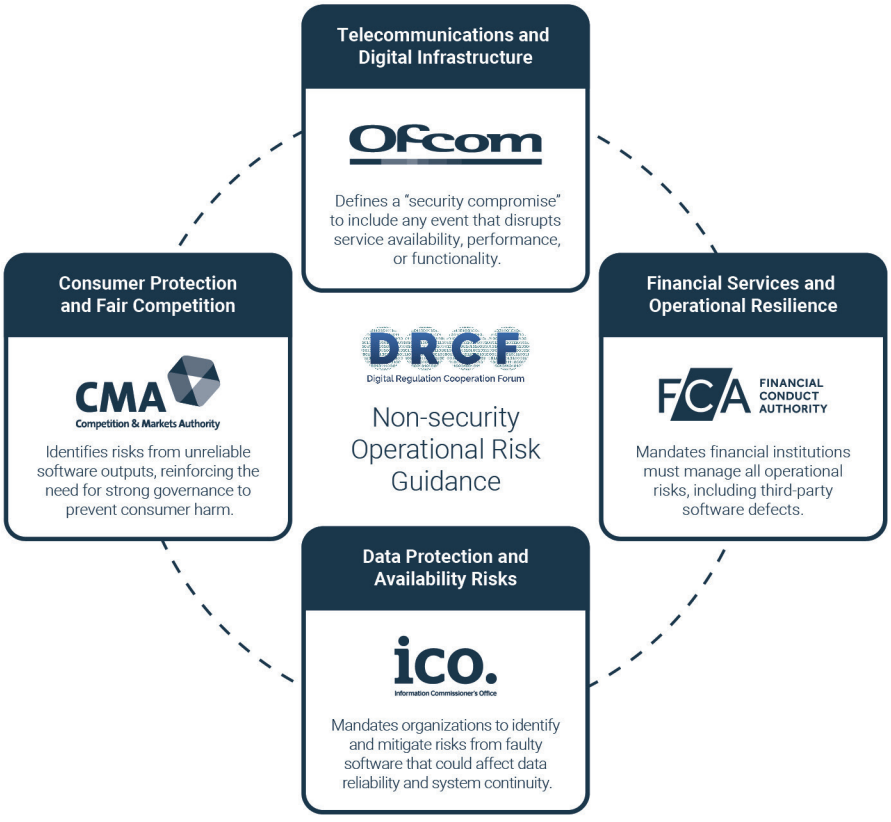
Managing Non-Security Third-Party Software Risks: A Cross-Regulatory Perspective from the DRCF

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 telecommunications, financial stability, consumer protection, and data integrity. See Appendix A: Four Regulators One Voice for a detailed breakdown of agency responses.



Telco Strategies 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, telcos must adopt a structured, proactive approach to third-party software risk management.

Comprehensive Visibility into Third-Party Software Defects

Regulatory mandates[1] require telcos to identify and continuously monitor third-party software dependencies.

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

Firms must 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

Regulations require telcos to go beyond periodic vendor reviews and maintain ongoing monitoring of third-party software providers.

Firms must assess the operational risks posed by third-party software failures in real time, ensuring that dependencies on external vendors do not introduce unchecked risks.

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

Automated Incident Response and Remediation Workflows

Regulations require telcos to rapidly detect, assess, and mitigate third-party software failures.

Firms must integrate 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.

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

1 *NIS 2 Art 21, UK Telecom Security Act Reg 12, FCC 47 § 4–9*

BugZero — for Automated, Intelligent, Proactive Compliance

As regulatory requirements for operational resilience and third-party software risk management continue to expand, telcos 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.
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 telecommunications services, ensuring that IT teams can take preventive action.

AI-Driven Risk Prioritization Based on Business Impact

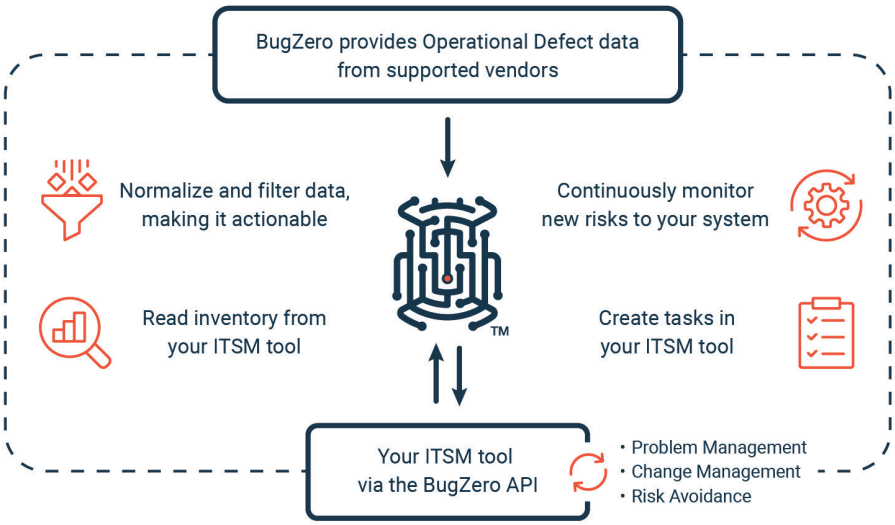
Regulatory Obligation	Prioritize risk mitigation efforts based on business-critical functions.
Automation Benefit	AI-driven solutions assess the potential business impact of third-party software defects, allowing telcos to allocate resources efficiently.
BugZero	• Correlates software defects with operational 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.

Real-Time Vendor Risk Visibility for Compliance Reporting	
Regulatory Obligation	Demonstrate proactive vendor risk management and support timely compliance reporting.
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 and compliance status. • Integrates with IT Service Management (ITSM) platforms, ensuring that remediation efforts are documented and auditable for regulatory review.

By leveraging BugZero, telecommunications 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.



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.

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.

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.

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

Global Telco Regulations

	What It Requires and Why It Matters for Software Defect Risk
European Union	**NIS 2 Directive (Art 21)** extends mandatory cybersecurity / incident reporting rules to electronic communications networks; Article 21 obliges operators to run "all hazards" risk management, business continuity and patch processes. **EECC Article 40** adds telecom-specific duties: providers must manage security risks, take "appropriate and proportionate" measures (including software update controls).
United Kingdom	**Telecommunications (Security) Act 2021 & Ofcom Security Code of Practice** amends the Communications Act 2003 to impose a legal duty to "identify and reduce risks" that could compromise network availability or functionality, with fines up to 10 % of global turnover for breaches. Ofcom's 2022 Code of Practice translates that duty into 14 granular measures: supplier security testing, software version control, staged rollbacks, and mandatory documentation of change management and defect tracking. From Oct 2025 the largest UK telcos will be audited annually, so unmanaged vendor software defects become a direct regulatory liability.
Canada	**CRTC Telecom Decision 202380 (Network Reliability & Resiliency)** sparked by the 2022 Rogers outage, the CRTC is working to make reliability and resiliency plans a condition of service for all carriers. Once final, carriers will need live inventories of third-party software defects and evidence of prompt remediation.
United States	**Secure and Trusted Communications Networks Act 2019** underpins the "rip and replace" program, blocking federal funds for equipment or software from untrusted vendors and requiring removal of existing gear; it institutionalizes supplychain/software vetting and patchtracking for telcos.

What It Requires and Why It Matters for Software Defect Risk	
Singapore	**IMDA Telecommunications Cybersecurity Code of Practice 2022** designated licensees (major ISPs & mobile operators) must follow 39 controls aligned to ISO 27011, covering software patch management, vulnerability remediation, secure config and supplier security reviews. IMDA audits compliance and can direct remediation work if software defects threaten availability.
Australia	**Telecommunications Sector Security Reforms (TSSR)** carriers and service providers must protect critical network assets from "all hazards", notify the Home Affairs Secretary of changes that could affect security, and maintain a written risk management program that includes supply chain software risks. Failure to comply can trigger ministerial directions or civil penalties.

Every regime now treats non-security third-party software defects — version bugs, misconfigurations, delayed patches — on par with cyberattacks. Operators that automate defect discovery, impact scoring and remediation (as outlined in this paper) will be better positioned to meet these converging global obligations.