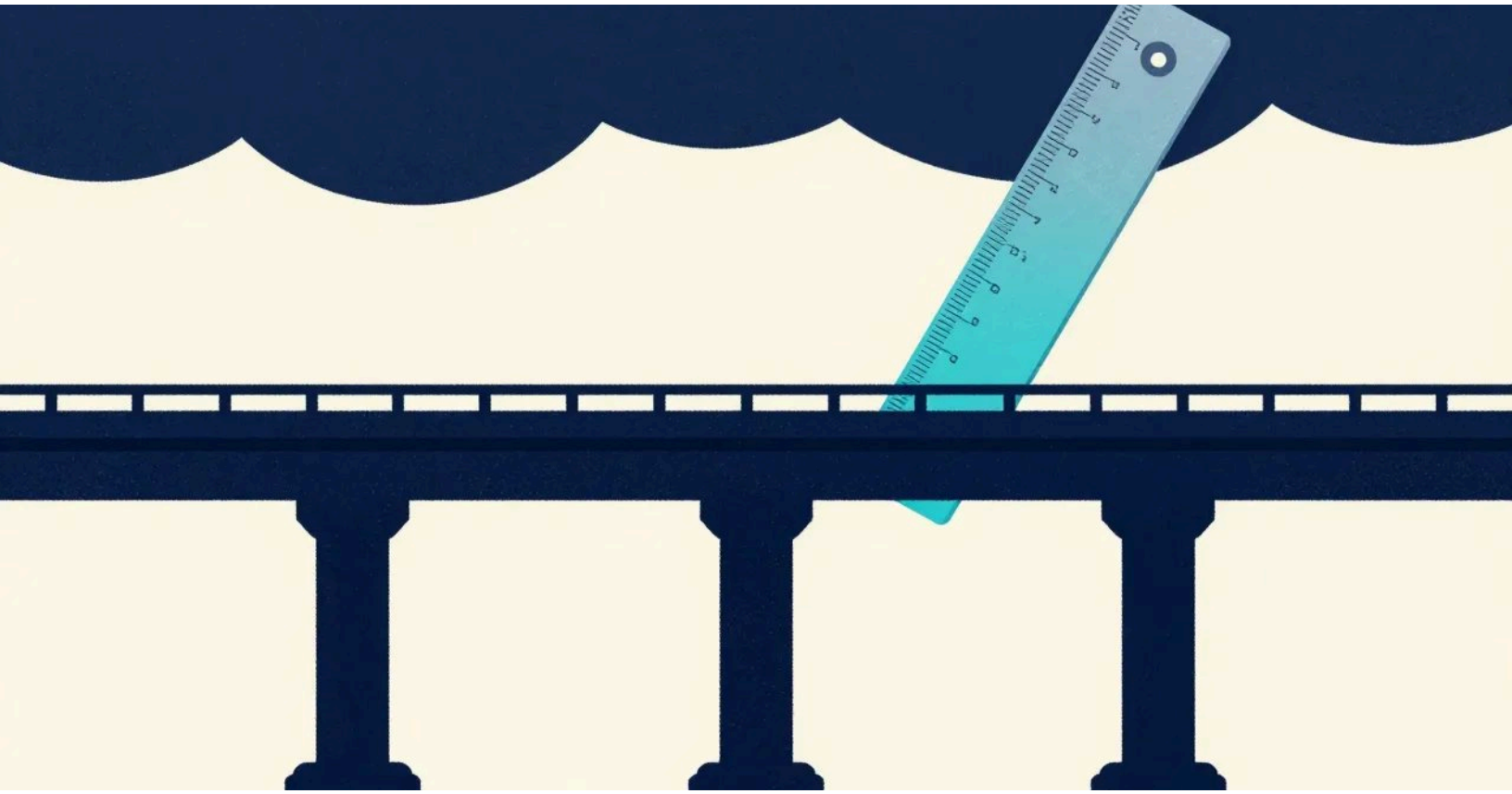


EXECUTIVE PAPER · DISASTER RECOVERY

Operational Resilience Is Now a Regulation

Financial regulators in the EU, UK, Australia and the United States now expect firms to name their critical services, set how much disruption each can bear, and prove it with severe tests. The same terms are moving down to every supplier those firms rely on.

AUTHOR

Chris Watkins

SERVICE

Disaster Recovery

FOR

CEO, CFO, COO, CTO, Board · 12 min read

AT A GLANCE

The problem. Since January 2025 the EU's Digital Operational Resilience Act has applied to about 20 types of financial firm. UK firms had until March 31, 2025 to show they can stay within their own limits for disruption, and Australia's CPS 230 commenced in July 2025. In November 2025 EU supervisors designated 19 technology providers, including the largest cloud platforms, for direct oversight.

Why it persists. Most firms built continuity plans around systems and data centers. Regulators now ask about services that customers use, measured in hours of harm, and tested against scenarios severe enough to break the plan. That needs business owners, not only IT, and a supplier map few firms have.

The recommendation. Name your critical business services. Set a tolerance for each in time, data loss and minimum service. Map the people, technology, facilities and suppliers behind them. Test against severe but plausible scenarios at least yearly and report the gaps to the board. Suppliers to financial firms should prepare the same evidence, because their customers' contracts will ask for it.

The Decision in Front of You

For two decades, business continuity in most firms meant a disaster recovery plan for the data center and a call tree. Regulators in four major jurisdictions now ask, for each service customers depend on, how long it can be down before the harm becomes intolerable, and whether the firm can prove it would recover inside that limit.

The decision is whether to build that capability now, on your own schedule, or to build it under a supervisor's finding or a customer's contract deadline. For a regulated financial firm the obligation already applies. For a technology, payments, data or outsourcing company that sells to financial firms, the same terms arrive through procurement, because those firms must show their regulators that each critical supplier meets them.

This paper takes no position on the rules themselves. It describes what they require and how to meet them.

What's Happening

Four regimes, one model

EU: DORA. Regulation (EU) 2022/2554, the Digital Operational Resilience Act, has applied since January 17, 2025, to 20 types of financial entity and to their technology providers [1][2]. It covers ICT risk management, incident reporting, resilience testing, third-party risk, and oversight of critical providers [1]. Firms identified by their supervisors must run threat-led penetration tests on live production systems at least every three years [2]. Every firm must keep a register of information listing all its contracts for technology services [2]. Contracts for services that support critical or important functions must include precise service levels, audit and access rights, exit strategies with transition periods, and the provider's participation in the firm's threat-led testing [2].

UK: FCA PS21/3 and PRA SS1/21. The UK rules took effect on March 31, 2022. Firms had to identify their important business services, set an impact tolerance for each, and map and test them [5]. An impact tolerance is the first point at which disruption to a service would cause intolerable harm to consumers or risk to market integrity [5]. By March 31, 2025, firms had to be able to remain within those tolerances in severe but plausible scenarios and to have made the investments needed to do so [5]. The rules cover banks, building societies, insurers, investment exchanges, payment and e-money firms, and larger investment firms [5][6].

Australia: APRA CPS 230. The standard commenced on July 1, 2025 [7]. Banks must treat payments, deposit-taking, custody, settlement and clearing as critical operations, and insurers must include claims processing [7]. For each critical operation the firm sets a maximum period of disruption, a maximum data loss, and the minimum service it will run during disruption [7]. It must notify APRA within 24 hours of a disruption outside tolerance, run an annual business continuity exercise against severe but plausible scenarios that include supplier failures, and keep a register of material service providers [7]. Firms submitted their first registers by October 1, 2025, and an amended standard applies from July 1, 2026 [8].

United States: interagency sound practices. On October 30, 2020 the Federal Reserve, FDIC and OCC issued "Sound Practices to Strengthen Operational Resilience" for the largest banks, those with $250 billion or more in assets or $100 billion with other risk characteristics [9][10]. The paper draws on existing rules for operational risk, business continuity, third-party risk, cybersecurity and recovery planning, and does not add new requirements [10]. It asks each firm to set a tolerance for disruption to its critical operations and core business lines, informed by severe but plausible scenarios [10]. The Federal Reserve revised the attachment in June 2026 to remove references to reputational risk [10].

Exhibit 1. The four regimes ask for the same evidence under different names

	EU DORA	UK FCA and PRA	Australia CPS 230	US sound practices
In force	January 17, 2025 [1]	March 31, 2022; tolerances met by March 31, 2025 [5]	July 1, 2025 [7]	October 30, 2020 [9]
Unit of analysis	Critical or important functions [2]	Important business services [5]	Critical operations [7]	Critical operations and core business lines [10]
Disruption limit	Business impact analysis of severe disruptions [2]	Impact tolerance [5]	Tolerance levels for time, data and service [7]	Tolerance for disruption [10]
Testing	Continuity plans tested at least yearly; threat-led tests every three years for designated firms [2]	Severe but plausible scenarios [5]	Annual exercise, severe but plausible, including suppliers [7]	Severe but plausible scenarios inform tolerance [10]
Suppliers	Register of all ICT contracts; mandatory contract terms; direct oversight of critical providers [2][3]	Mapping covers third parties; critical third parties regime from 2025 [5][17]	Register of material service providers; formal agreements [7][8]	Third-party risk management [10]
Applies to	About 20 types of financial entity [1]	Banks, insurers, payments, exchanges, larger investment firms [5] [6]	All APRA-regulated entities [7]	Banks with $250 billion or more in assets, or $100 billion with other risk factors [10]

Source: author's summary of the cited regulations.

The rules now reach the suppliers

On November 18, 2025, the three European Supervisory Authorities designated the first critical ICT third-party providers under DORA [3]. They built the list from the registers of information that financial firms had filed, assessing each provider's systemic importance, its role in critical functions, and how easily it could be substituted [3]. The 19 providers named include Amazon Web Services, Microsoft, Google Cloud, Oracle, SAP, Bloomberg, LSEG Data and Risk, Equinix, Deutsche Telekom and several large outsourcing firms [4]. Their lead overseer can inspect them and impose daily penalties of up to 1% of average daily worldwide turnover for up to six months [2].

The UK built a parallel regime. Rules for critical third parties took effect on January 1, 2025, with HM Treasury deciding which providers to designate [17]. From March 18, 2027 most UK firms must also keep a register of their material third-party arrangements, submit it to the FCA every year, and report new or

changed arrangements [16].

A supplier that never appears on a designation list still feels this. Each financial customer must list the contract in its register, write DORA's mandatory terms into it, map it in its service maps, and include its failure in scenario tests [2][7]. EU supervisors counted about 15,000 technology providers serving the EU financial sector directly in 2023 [18].

Cases from 2024 to 2026

CrowdStrike, July 2024. A faulty security update crashed about 8.5 million Windows machines [12]. The FCA's review found that firms which had mapped their important business services and tested scenarios hitting several services at once could restore their most important services first [11].

Barclays, January and February 2025. From January 31 to February 2, 2025, a failure in Barclays' mainframe processing caused about 56% of online payments to fail, on a payday and the UK self-assessment tax deadline [14]. Barclays estimated £5 million to £7.5 million in compensation for that outage and up to £12.5 million for IT failures over two years [14]. The House of Commons Treasury Committee gathered figures from nine banks and building societies showing at least 158 incidents and 803 hours of outages from January 2023 to February 2025 [14]. The outage came two months before the deadline for UK firms to show they could stay within their impact tolerances [5].

Citigroup, July 2024. The Federal Reserve and OCC imposed penalties of about $135.6 million on Citigroup for slow remediation of data quality problems named in a 2020 enforcement action [15]. The case concerned risk and data management, and shows how supervisors price remediation that runs years behind plan.

FCA findings, March 2026. A year after the UK deadline, the FCA reported that firms' mapping still focused mainly on technology and neglected people, facilities, processes and supplier testing [13]. Some firms claimed no scenario was unrecoverable without showing they had tested scenarios severe enough to prove it [13]. Remediation actions often lacked owners or deadlines, and it was unclear whether boards understood the investment needed [13].

SIDEBAR: IMPACT TOLERANCE IS A BUSINESS NUMBER

An impact tolerance measures harm to a customer or a market, such as card payments down for more than four hours on a payday. A service can depend on twenty systems that each meet their recovery time and still breach its tolerance, for example because the staff who run the fallback process work in the same building as the data center. CPS 230 asks for tolerances in time, data loss and minimum service [7].

Why the Usual Approach Fails

Most continuity programs are organized by system. They hold a recovery time and recovery point for each application, a disaster recovery site, and a yearly failover test of a few systems. The regulations are organized by service, and a service crosses many systems, teams, buildings and suppliers. The FCA's finding that mapping still centers on technology describes this gap [13].

Tests are chosen to pass. A planned failover of one database on a quiet weekend proves the runbook and little else. The rules ask what happens when a supplier, a region and a key team fail together [5][7]. The FCA saw firms claim every scenario was recoverable without testing severe ones [13].

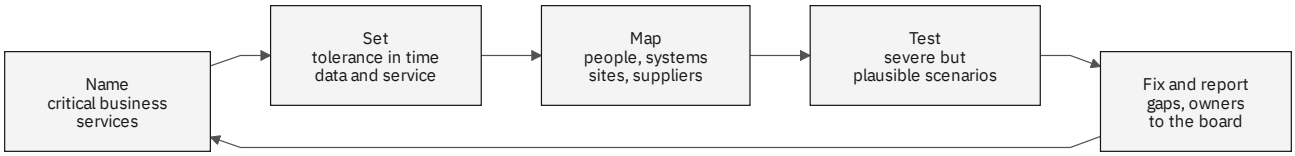
Ownership sits with IT. Regulators expect the board to approve tolerances and self-assessments, and the FCA found unclear approval trails and actions with no owner [13]. A program run by IT alone leaves the business without a decision on how much disruption it will accept.

Supplier evidence is missing. Contracts signed before 2025 rarely include exit plans, audit rights or a duty to join the customer's tests, and DORA requires them for critical functions [2].

The Framework: The Tolerance Loop

The Tolerance Loop turns the regulations into one program that a non-regulated supplier can also run. It has five steps, repeated each year and after any major change.

Exhibit 2. The Tolerance Loop: from named services to board-reported gaps



Source: author's framework, drawing on FCA PS21/3 [5], APRA CPS 230 [7], and DORA [2].

Name. List the services customers or markets depend on, in a customer's words: make a payment, settle a trade, pay a claim. CPS 230 gives a floor for banks and insurers [7]. A supplier names the services its financial customers have marked critical.

Set. For each service, the business owner sets the maximum tolerable disruption, the maximum data loss and the minimum service level under fallback [7]. Use non-time measures such as transaction volumes where they describe harm better [13]. The board approves them.

Map. Record everything the service needs: applications, infrastructure, data, people, buildings and every supplier, including the supplier's own key suppliers. Use the DORA register of information or the APRA service provider register as the supplier half of the map [2][7].

Test. Choose scenarios that combine failures, such as a cloud region and a key supplier lost together on a peak day. Include at least one test of a supplier failure each year, as CPS 230 requires [7]. Record whether the service stayed within tolerance, and with what confidence.

Fix and report. Each breach of tolerance becomes a funded action with an owner and a date. The self-assessment the board signs lists the gaps, the investments and the residual risk [5][13].

Costs, Risks, and Tradeoffs

Exhibit 3. Tradeoffs of building to the regulatory model

Area	Cost or risk	Mitigation
Mapping effort	Service maps take months and go stale quickly	Start with the five most important services; generate the technology layer from configuration data
Severe testing	Live tests can cause the outage they rehearse	Use tabletop and partial tests first; isolate production tests; get board approval for risk
Investment to close gaps	Staying within a tight tolerance may need a second region, a second supplier or more staff	Let the business owner set tolerance with the price of meeting it in view
Supplier renegotiation	Contract changes take a renewal cycle, and large providers resist bespoke terms	Prioritize contracts behind critical services; use providers' standard regulatory addenda where they exist
Overlapping regimes	Groups in several jurisdictions face different terms and deadlines	Run one program with a mapping to each regime, as in Exhibit 1
When this is wrong	A small supplier with no financial-sector customers and no regulator gains little from formal tolerances and registers	Keep tested backups, an incident plan and a simple service list; adopt the full loop when a regulated customer asks

Source: author's analysis.

How to Act

Exhibit 4. A one-year roadmap

Window	Actions	Owner	Milestone
First 30 days	Confirm which regimes apply directly or through customers. Name the critical services. Assign a business owner to each.	COO with chief risk officer	Service list approved by the executive committee; owner named for each service
First 90 days	Set tolerances for each service. Map the top five services end to end, including suppliers. Compare supplier contracts against DORA and CPS 230 terms.	Service owners with CTO and procurement	Board-approved tolerances; five complete maps; list of contracts missing required terms
First 90 days	Run a tabletop of a combined supplier and cloud-region failure.	Head of resilience	Test report showing whether each service stayed within tolerance
First 365 days	Map all critical services. Run at least one live test and one supplier test. Amend critical contracts at renewal. File the self-assessment.	Chief risk officer with CTO	100% of critical services mapped and tested; every breach has a funded action and date; self-assessment signed by the board

Source: author's recommendation.

Questions to Ask Your Team

1. Which of our customers or regulators already expect us to meet DORA, the UK rules, CPS 230 or the US sound practices?
2. What are our critical business services, and who owns each one?
3. For each, how long can it be down, how much data can we lose, and who approved those numbers?
4. Which suppliers sit behind each service, and which of their contracts lack exit plans, audit rights or test participation?
5. What was the most severe scenario we tested last year, and did every service stay within tolerance?
6. If a key supplier failed tomorrow, which services would breach first, and how would we know?
7. What open gaps does the board know about, and when will each be fixed?

Closing

Financial regulators in the EU, UK, Australia and the United States now judge resilience by service, by tolerance and by test, and their reach extends through contracts to the suppliers behind each critical service. Name your critical services, set tolerances the business owns, map everything behind them,

test against severe scenarios, and report the gaps to the board with owners and dates. The same body of evidence then serves regulators, customers and the incident team.

Sources

[1] European Insurance and Occupational Pensions Authority. "Digital Operational Resilience Act (DORA)." https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.

[2] European Parliament and Council. "Regulation (EU) 2022/2554 on digital operational resilience for the financial sector." OJ L 333, 27.12.2022. 2022. Articles 11, 26, 28, 30, 35 and 64 as reproduced by Springlex: https://www.springlex.eu/en/packages/dora/dora-regulation/article-11/; https://www.springlex.eu/en/packages/dora/dora-regulation/article-26/; https://www.springlex.eu/en/packages/dora/dora-regulation/article-28/; https://www.springlex.eu/en/packages/dora/dora-regulation/article-30/; https://www.springlex.eu/en/packages/dora/dora-regulation/article-35/; https://www.springlex.eu/en/packages/dora/dora-regulation/article-64/.

[3] European Securities and Markets Authority. "European Supervisory Authorities designate critical ICT third-party providers." 2025. https://www.esma.europa.eu/press-news/esma-news/european-supervisory-authorities-designate-critical-ict-third-party-providers.

[4] European Supervisory Authorities. "List of designated critical ICT third-party service providers." 2025. https://www.eiopa.europa.eu/document/download/56b1ca78-5dd2-4d36-8377-47a538eb7558_en?filename=List%20of%20designated%20CTPPs.pdf.

[5] Financial Conduct Authority. "PS21/3: Building operational resilience." 2021. https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience. Policy statement text: https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf.

[6] Bank of England Prudential Regulation Authority. "Operational resilience: Impact tolerances for important business services." Supervisory Statement SS1/21. 2021, updated 2022. https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-impact-tolerances-for-important-business-services-ss.

[7] Australian Prudential Regulation Authority. "Prudential Standard CPS 230 Operational Risk Management." 2023, version of July 2025. https://www.apra.gov.au/sites/default/files/2023-07/Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management%20-%20clean.pdf.

[8] Australian Prudential Regulation Authority. "Operational risk management." https://www.apra.gov.au/operational-risk-management.

[9] Board of Governors of the Federal Reserve System, FDIC, and OCC. "Agencies release paper on sound practices to strengthen operational resilience." Press release. 2020. https://www.federalreserve.gov/newsevents/pressreleases/bcreg20201030a.htm.

[10] Board of Governors of the Federal Reserve System. "SR 20-24: Interagency Paper on Sound Practices to Strengthen Operational Resilience." 2020, revised 2026. https://www.federalreserve.gov/supervisionreg/srletters/SR2024.htm. Attachment: https://www.federalreserve.gov/supervisionreg/srletters/SR2024a1.pdf.

[11] Financial Conduct Authority. "CrowdStrike outage: lessons for operational resilience." 2024. https://www.fca.org.uk/firms/operational-resilience/crowdstrike-outage-lessons-operational-resilience.

[12] Microsoft. "Helping our customers through the CrowdStrike outage." 2024. https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/.

[13] Financial Conduct Authority. "Operational resilience: insights and observations one year on." 2026. https://www.fca.org.uk/publications/good-and-poor-practice/operational-resilience-insights-observations-one-year.

[14] The Global Treasurer. "Banks face growing scrutiny over IT failures as compensation costs mount." Coverage of Treasury Committee evidence. 2025. https://www.theglobaltreasurer.com/2025/03/06/banks-face-growing-scrutiny-over-it-failures-as-compensation-costs-mount/?amp=1.

[15] Board of Governors of the Federal Reserve System. "Federal Reserve Board fines Citigroup $60.6 million." Press release. 2024. https://www.federalreserve.gov/newsevents/pressreleases/enforcement20240710a.htm.

[16] Financial Conduct Authority. "PS26/2: Operational incident and third party reporting." 2026. https://www.fca.org.uk/publications/policy-statements/ps26-2-operational-incident-third-party-reporting.

[17] Financial Conduct Authority. "PS24/16: Operational resilience: Critical third parties to the UK financial sector." 2024. https://www.fca.org.uk/publications/policy-statements/ps24-16-operational-resilience-critical-third-parties-uk-financial-sector.

[18] European Banking Authority. "ESAs publish report on the landscape of ICT third-party providers in the EU." 2023. https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-report-landscape-ict-third-party-providers-eu.

The views in this paper are the author's own and do not represent any employer. Scenarios are hypothetical. This paper is not legal, financial, or compliance advice.