

Resilient by Regulation: Batch Migration Under DORA

What DORA, the UK resilience regime and US guidance ask of a firm that moves its mainframe batch, or decides to keep it where it is

Bill Ahlbrandt

President and CEO, Ahlbrandt Software

Abstract

Operational resilience rules now apply in full in the European Union and the United Kingdom, and as guidance in the United States. None of them mentions batch. They all apply to it anyway, because the overnight cycle is where payments get posted, statements get produced and regulatory returns get put together. I went through the primary texts (DORA and its technical standards, the PRA and FCA operational resilience and outsourcing rules, the UK critical third parties regime and the US interagency guidance) and worked out what a batch migration, or a decision not to migrate, has to be able to show. I also look at the two UK enforcement cases with the clearest batch and migration angle. The short version: the rules are neutral on whether you move or stay, and they want evidence either way. You have to be able to show that each important service stays within its tolerance through the change, and that every supplier in the batch chain, right down to the sort utility and the scheduler, can be exited or replaced.

What I found

- The rules regulate the **service**. A batch chain that posts payments or produces statements is part of an important business service, so migrating it is a change to that service, and it has to be mapped and tested like one.
- **Staying put has obligations too**. DORA requires a specific risk assessment of legacy ICT systems at least yearly, and the UK rules have required firms to be able to stay within tolerance since March 31, 2025.
- Two of the best-known UK fines for IT disruption, £56 million for RBS, NatWest and Ulster Bank in 2014 and £48.65 million for TSB in 2022, both came down to **change that wasn't tested well enough**. In the RBS case it was a batch scheduler.
- Exit planning goes all the way down to the **smallest suppliers in the chain**. A sort utility or scheduler that's hard to replace is a concentration and substitutability question in its own right.
- **Watch the headroom**. After a failed night, the spare time in each batch window decides how fast you catch up, and so whether you stay within tolerance.

I'm summarizing public regulatory texts here for planning purposes. This isn't legal advice, and you should get your own.

1. Why batch is a resilience question

Of all places, one of the clearest descriptions of what batch does in a bank is in an enforcement notice. In 2014 the Financial Conduct Authority explained that banks “generally update that day’s transactions in the evening”, using a batch scheduler to coordinate the processing of data that includes customer withdrawals and deposits, interbank clearing, money market transactions, payroll, and changes to standing orders and addresses.¹ When that processing failed at RBS, NatWest and Ulster Bank in June 2012, at least 6.5 million UK customers were affected. The disruption lasted until June 26 for RBS and NatWest customers and until July 10 for Ulster Bank.²

The resilience rules that came after are built around exactly this kind of dependency. The UK regime defines an **important business service** as one that, if disrupted, could threaten the firm’s safety and soundness or, for the largest firms, financial stability. An **impact tolerance** is “the maximum tolerable level of disruption” to it, “measured by a length of time” among other metrics.³ Firms have to map the people, processes, technology, facilities and information behind each of those services, and test whether they can stay within tolerance in “a severe but plausible disruption”.^{3, 4, 5} DORA talks about **critical or important functions**. It requires firms to identify and document the ICT assets that support them, their dependencies, and every process that depends on an ICT third-party provider.⁶ US supervisors ask the largest firms to map “operational interconnections and interdependencies” for their critical operations.⁷

None of these texts says anything specific about batch. They’re written around the service. Whether a statement run executes on z/OS, on Linux in a data center or in a public cloud, the rules can’t see it. What they see is whether statements come out on time, and whether the firm can prove they’ll keep coming out through a severe disruption, including one it causes itself by changing platform.

2. The rules in brief

European Union: DORA

Regulation (EU) 2022/2554, the Digital Operational Resilience Act, entered into force in January 2023 and has applied since January 17, 2025.⁶ For a batch shop, the parts that matter fall into five groups. **ICT risk management** requires the mapping described above and, in Article 8(7), a specific risk assessment of all legacy ICT systems “at least yearly” and before and after connecting new technologies to them. **Continuity** provisions require business continuity and response and recovery plans to be tested at least yearly and after any substantive change to systems supporting critical or important functions (Article 11(6)), and backups to be restorable on segregated systems (Article 12). **Testing** requires appropriate tests of all systems supporting those functions at least yearly (Article 24(6)) and, for firms their supervisors select, threat-led penetration testing on live production systems at least every three years (Article 26).⁶ **Third-party risk** requires a register of information on every ICT contract, exit strategies for services supporting critical or important functions (and those have to be tested too), and specific contract terms, including a mandatory adequate transition period (Articles 28 and 30). **Concentration** requires firms to consider whether a provider is “not easily substitutable” before signing with it (Article 29).⁶

The first registers reached the European Supervisory Authorities by April 30, 2025.⁸ On November 18, 2025 the ESAs designated 19 critical ICT third-party providers for direct oversight. The list includes the three biggest hyperscale cloud providers and, if you run a mainframe, both IBM and Kyndryl.⁹

United Kingdom

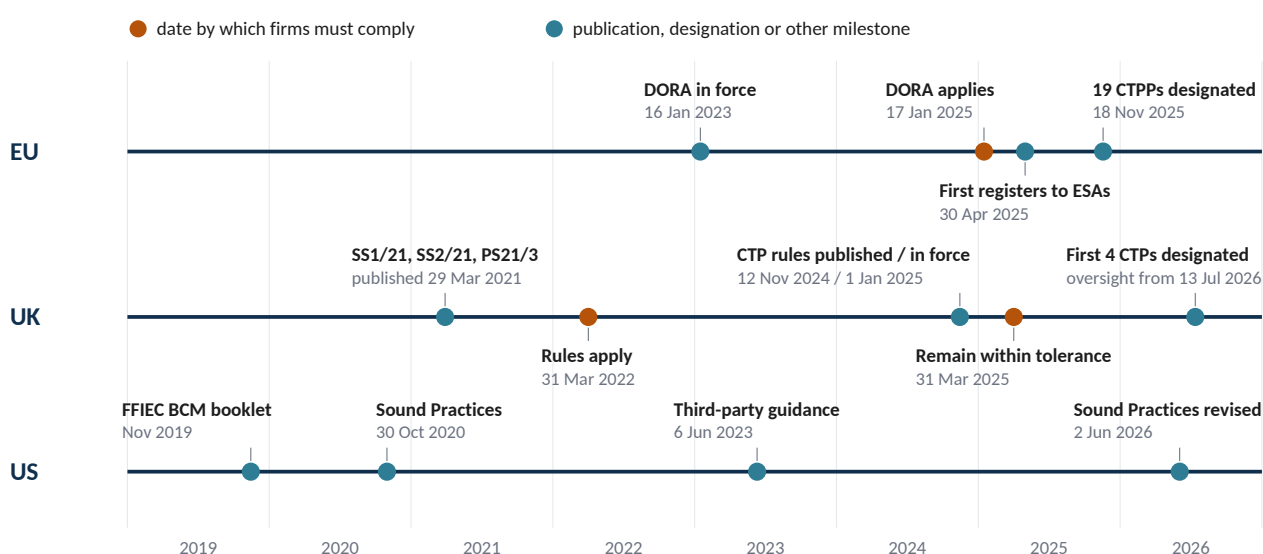
The PRA’s SS1/21 and the FCA’s PS21/3, published on March 29, 2021, required firms to identify important business services and set impact tolerances by March 31, 2022, and to be able to stay within those tolerances “as soon as possible” and no later than March 31, 2025.^{4, 5} SS2/21 covers outsourcing and third-party risk. It expects documented exit plans for material outsourcing arrangements that cover both stressed and non-stressed exit, and it lists software purchases among the non-outsourcing arrangements firms have to assess.¹⁰ Under powers in the Financial Services and Markets Act 2023, rules for critical third parties took effect on January 1, 2025.¹¹ In July 2026 HM Treasury

designated the first four: the UK or EMEA entities of Amazon Web Services, Google Cloud, Microsoft and Oracle. The Bank of England made a point of saying the regime “complements, but does not replace” firms’ own responsibility for their third-party arrangements.¹²

United States

In the US it's guidance, and there's no single rule. The FFIEC's Business Continuity Management booklet of November 2019 sets out what examiners expect on continuity and resilience.¹³ The interagency *Sound Practices to Strengthen Operational Resilience* of October 2020 applies to the largest banking organizations and expects business continuity tests to “incorporate dependencies of critical operations and core business lines on third parties”.⁷ The interagency guidance on third-party relationships from June 2023 expects contingency plans for when a bank “needs to transition the activity to another third party or bring it in-house”.¹⁴ Exhibit 1 puts the dates side by side.

Exhibit 1. Operational resilience milestones, 2019–2026



Sources: the primary texts and announcements cited in section 2. Dates are placed on the axis to the nearest month.

3. Two cases with a batch angle

RBS, NatWest and Ulster Bank, 2012. On June 17, 2012 the group’s central IT function upgraded the batch scheduler that processed updates to customer accounts, “because this software could no longer be sufficiently supported”. Two days later it backed the upgrade out, without knowing that the new version “was not compatible” with the old one. By June 21, Ulster Bank’s batch was more than a day behind, so the next day’s processing started before the previous day’s had finished.¹ The FCA fined the banks £42 million and the PRA £14 million, £56 million in total, citing among other things “inadequate testing procedures for managing changes to software”.^{1,2}

TSB, 2018. On April 22, 2018 TSB moved its customer services and data to a new platform. The data transfer worked, but the platform failed, and services were disrupted for a significant proportion of TSB’s 5.2 million customers. The FCA and PRA fined TSB £48.65 million in December 2022, after TSB had paid £32.7 million in redress.¹⁵ The Final Notice says the scope of one kind of non-functional testing was cut back, and that if it had been done, a configuration problem in the data centers would probably have been found. System integration testing was held up by an unstable test environment. Rehearsals assumed incidents would be fixed in days, and many took weeks. And the main supplier relied on 85 third parties of its own.¹⁵

In neither case was the platform the problem. Both came down to the evidence behind a change. RBS had to change because a utility could no longer be supported, and nobody tested the back-out. TSB ran a migration with reduced testing and a supply chain nobody fully understood. Since 2021 the rules want that evidence up front.

4. What the rules ask of a batch migration

DORA's technical standards get more specific than the Regulation. Every ICT system has to be tested and approved before use, with testing as deep as the criticality of the business processes calls for. Third-party software, and its source code where feasible, has to be analyzed and tested before it goes into production. Non-production environments may hold only anonymized, pseudonymized or randomized production data, except under an approved derogation for specific tests and limited periods.¹⁶ Change management has to identify “fall-back procedures”, including procedures for aborting changes or recovering from changes that didn't go in successfully.¹⁶ If you run batch, two things here are easy to miss. A parallel run that compares old and new output on production data needs that derogation, or an equivalent approval, planned in advance. And the fallback is itself a change that has to be tested. RBS didn't test theirs.

If something does go wrong, the reporting clock is short. Under the incident reporting standards, the first notification of a major ICT-related incident is due within four hours of classifying it as major and no later than 24 hours after the firm becomes aware of it, with an intermediate report within 72 hours.¹⁷ A missed month-end batch at a large firm could well meet the thresholds. Exhibit 2 maps each obligation to the work a migration team has to do.

Exhibit 2. What the rules require, mapped to batch-migration work

Obligation	Where it comes from	What it means for a batch migration
Map the service	DORA Art. 8(1), (4), (5); PRA Op. Res. 4.1; US Sound Practices	Trace every job, utility, file and supplier behind each important service, including the month-end and year-end variants that rarely run.
Set a tolerance	PRA Op. Res. 1.2, 2.6; FCA PS21/3; DORA Art. 11(2)	Put the deadline in terms of time, and check that recovery from a failed night fits inside it on both platforms.
Test the change	DORA Art. 11(6), 24(6); RTS 2024/1774 Art. 16; PRA Op. Res. 5.1	Test at production volume and the month-end peak. Plan the approval to use production data in a parallel run.
Plan the fallback	RTS 2024/1774 Art. 17; RBS and TSB Final Notices	Write down and rehearse the rollback, including the point after which you can't roll back anymore.
Know the suppliers	DORA Art. 28(3), 30; SS2/21; US third-party guidance	Put the scheduler, sort utility, runtime and platform in the register; check contract terms and subcontractors.
Plan the exit	DORA Art. 28(8), 30(3); SS2/21 §§4.14, 6.4, 10.7; US third-party guidance	Keep a tested exit plan, stressed and non-stressed, for each supplier to a critical function.
Weigh concentration	DORA Art. 29; UK CTP regime; HM Treasury 2022	Show whether the migration makes you more dependent on one provider, and what the alternative would be.
Assess the legacy	DORA Art. 8(7)	If the batch stays, assess the legacy system at least yearly. Deciding to stay needs evidence too.

Primary texts as cited.^{6, 3, 5, 16, 10, 14, 7} Article references are to the Regulation unless an RTS is named. Planning summary only; it isn't legal advice.

5. Impact tolerances and the batch night

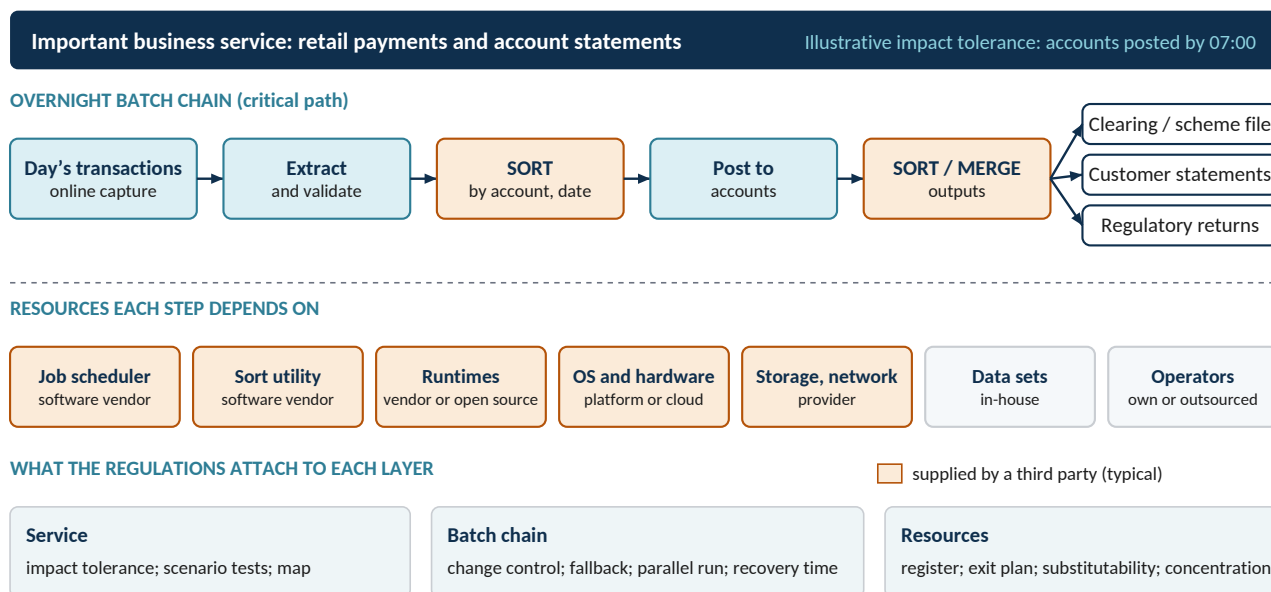
Impact tolerances are set in time, and batch has an odd relationship with time. It piles up. An online service that's down for three hours loses three hours of transactions. A batch cycle that misses a night leaves a whole day of work still to do, on top of the next day's. That's what the FCA described at Ulster Bank. So how fast you recover depends much more on how much spare time the window leaves you than on how fast the batch runs.

Here's an example. Let's say a chain needs six hours of an eight-hour window. After one lost night you have a six-hour backlog to work off from two spare hours a night, which takes three nights if you do nothing else. Now say a migration stretches the run to seven hours. That still fits comfortably inside the window on a normal night, but the same catch-up now takes six nights. Neither number describes any real firm, and extra capacity or putting off

non-urgent jobs can shorten both. The arithmetic holds in general, though. Catch-up time is the backlog divided by the headroom, and headroom shrinks faster than run time grows. Elastic capacity only helps where the critical path can be parallelized. You can't hurry a chain of dependent steps by adding machines.

For a migration, test the tolerance on the target platform using a failed night as the scenario, since a good night doesn't exercise recovery at all. Let the month-end, quarter-end and year-end cycles, which are longer and rarer, set the test volumes. And when you compare the old and new platforms, include restart and rerun times, because those are what a severe but plausible scenario exercises. Exhibit 3 shows how a single service depends on a batch chain, and the chain on a stack of resources, most of them supplied by third parties.

Exhibit 3. An important business service and its batch dependency chain (illustrative)



Made-up service and tolerance. Which resources come from third parties varies by firm; amber marks the ones that typically do.

6. Third parties, large and small

The small suppliers

Registers and exit plans tend to be built around the big contracts. But the RBS incident started with a scheduler, and every batch chain depends on a handful of utilities (the scheduler, the sort product, compilers and runtimes, file transfer) that come from software vendors, often under licenses that are decades old. At least one leading law firm reads DORA's definition of ICT services as able to include on-premises software licenses even without support services.¹⁸ Whether a given license is in scope is a question for your lawyers. Either way, a utility on the critical path of a critical function is a dependency in fact, whatever its legal classification. The subcontracting standards push the same scrutiny down the chain, to the providers your own providers rely on.¹⁹

An exit plan for a utility has to answer a few questions. **What exactly do we use?** An inventory of the control statements, options and exits in production is the spec any alternative has to meet. (That's the census described in *Changing Your Sort Engine Without Changing Your Batch*, the sixth paper in this series.) **What would replace it, and how long would that take?** A utility driven by a documented, declarative control language is easier to substitute than one buried in application code, and on z/OS more than one commercial sort product has long accepted a common core of control statements. **What if the vendor fails?** Source code escrow is the usual contract answer. The source is deposited with an agent and released on defined events such as insolvency or withdrawal of support. It's a useful backstop, with known limits. Released source only helps if you have the build environment, the skills and the time to use it, and a deposit nobody has ever test-built may not compile. For critical utilities a tested alternative is usually a stronger exit than escrow alone, and there's no reason you can't have both.

The large suppliers

At the other end of the scale, concentration is a system-wide worry. HM Treasury noted in 2022 that, as of 2020, over 65 percent of UK firms used the same four cloud providers for infrastructure services.²⁰ Moving batch from a mainframe to a hyperscaler swaps one concentrated dependency for another. The EU list of critical providers has IBM on it, and the three biggest cloud platforms too.⁹ Direct oversight of those providers doesn't shift the responsibility. The firm still owns its exit plan.¹² For batch, the realistic questions are whether the migrated chain uses provider-specific services that would have to be rebuilt somewhere else, how long it would take to move the data sets themselves (a throughput question, which the seventh paper in this series, *The Batch Window After the Mainframe*, works through), and whether multiple regions of one provider are being counted as diversity when they share a control plane. None of these is an argument for or against moving. You just have to answer each one in the file.

7. The evidence file

Supervisors don't approve migrations in advance, and the texts don't prescribe a set of documents. They do require that firms be able to demonstrate their resilience. Exhibit 4 lists evidence that a well-run batch migration would normally produce anyway, and that a supervisor looking at it might reasonably ask to see.

Exhibit 4. Evidence a supervisor may expect for a batch migration

Stage	Evidence	Anchored in
Before	Service map from each important service down to jobs, utilities, data sets and suppliers	Mapping (DORA Art. 8; PRA 4.1)
Before	Tolerances in terms of time, with measured run, restart and rerun times on the current platform	Impact tolerance
Before	Register entries and contract review for every supplier in the chain, utilities included	DORA Art. 28, 30; SS2/21
Before	Exit plan for each supplier to a critical function, stressed and non-stressed	DORA Art. 28(8); SS2/21
Before	Concentration assessment of the target platform and its alternatives	DORA Art. 29
During	Test results at production and month-end volume, with output compared record for record	DORA Art. 24; RTS Art. 16
During	Approval for any use of production data in non-production testing	RTS Art. 16
During	Scenario test of a failed night on the target: detection, rerun, catch-up within tolerance	Scenario testing
Cutover	Go/no-go criteria, rollback procedure, rehearsal record and the point of no return	RTS Art. 17
After	Incident classification and reporting runbook for the new platform	RTS 2025/301
After	Updated map, register and business continuity plan; first annual test	DORA Art. 11(6)

My checklist, drawn from the texts cited in Exhibit 2. It isn't complete, and it isn't legal advice.

If you decide to stay, the same file works with the migration rows taken out. Mapping, tolerances, registers, exit plans and the yearly legacy assessment apply either way.

8. Bottom line

- **The rules are about outcomes.** They don't favor or penalize leaving the mainframe. What they penalize is change without evidence, as RBS and TSB show.
- **Batch belongs in the service map.** Payments, statements and regulatory returns depend on overnight chains, and the map should reach every job, utility and supplier on the critical path.
- **Test the failure.** A good night is the easy test. The headroom after a lost night decides whether a service stays within tolerance, and rollback is a change you have to rehearse like any other.
- **Small suppliers need exit plans too.** An inventory, a tested alternative and, where it makes sense, escrow are what make a utility actually substitutable.
- **Concentration moves around.** Whichever platform runs the batch, the firm owns the exit plan.

About the author

Bill Ahlbrandt is President and CEO of Ahlbrandt Software, which he founded in 1993. Before that he was a systems programmer, Director of Information Security and Director of R&D at Acxiom. He has been working on mainframe sort and batch for more than thirty years, and his company's sort engine runs mainframe sort jobs on Linux and other platforms for banks, insurers and government agencies.

Full disclosure: my company sells sort software for platforms other than the mainframe, so we're one of the small suppliers I talk about in section 6. I'm not taking a position here on whether any firm should migrate.

References

1. Financial Conduct Authority, Final Notice to The Royal Bank of Scotland plc, National Westminster Bank Plc and Ulster Bank Ltd, November 2014, paras 4.5–4.11; FCA press release, "FCA fines RBS, NatWest and Ulster Bank Ltd £42 million for IT failures", 20 November 2014.
2. Prudential Regulation Authority, press release, "PRA fines Royal Bank of Scotland, NatWest Bank and Ulster Bank £14 million for IT failures", 20 November 2014.
3. PRA, *PRA Rulebook: Operational Resilience Instrument 2021*, Annex A, Operational Resilience Part, rules 1.2, 2.6, 4.1 and 5.1; published with PS6/21, 29 March 2021.
4. PRA, Supervisory Statement SS1/21, *Operational resilience: Impact tolerances for important business services*, 29 March 2021, effective 31 March 2022.
5. FCA, PS21/3, *Building operational resilience*, 29 March 2021.
6. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA), OJ L 333, 27.12.2022; Articles 8, 11, 12, 24, 26, 28, 29, 30, 31 and 64.
7. Board of Governors of the Federal Reserve System, FDIC and OCC, *Sound Practices to Strengthen Operational Resilience*, 30 October 2020 (Federal Reserve SR 20-24, 2 November 2020; attachment revised 2 June 2026).
8. Commission Implementing Regulation (EU) 2024/2956 (templates for the register of information); CSSF, "DORA – Submission timeframe for register of information", April 2025 (competent authorities to submit to the ESAs by 30 April 2025).
9. EBA, EIOPA and ESMA, "European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act", joint press release, 18 November 2025, with the list of designated CTPPs (names as reported by PwC Legal, November 2025).
10. PRA, Supervisory Statement SS2/21, *Outsourcing and third party risk management*, March 2021, paras 1.4, 2.4, 4.14, 6.4 and 10.7.
11. Bank of England, PRA and FCA, PS16/24 (FCA PS24/16), *Operational resilience: Critical third parties to the UK financial sector*, 12 November 2024, rules in force 1 January 2025.
12. Bank of England, "UK financial regulators to begin overseeing Critical Third Parties announced by HM Treasury", news release, 10 July 2026.
13. FFIEC, *IT Examination Handbook: Business Continuity Management* booklet, November 2019 (OCC Bulletin 2019-57, 14 November 2019).
14. Federal Reserve, FDIC and OCC, "Interagency Guidance on Third-Party Relationships: Risk Management", 88 FR 37920, 9 June 2023.
15. FCA, Final Notice to TSB Bank plc, December 2022, paras 2.14, 2.19, 2.22, 2.29, 4.4 and 4.100; FCA press release, "TSB fined £48.65m for operational resilience failings", 20 December 2022.
16. Commission Delegated Regulation (EU) 2024/1774 (RTS on ICT risk management framework), Articles 16 and 17.
17. Commission Delegated Regulation (EU) 2025/301 (RTS on major ICT-related incident reporting), Article 5.
18. Herbert Smith Freehills Kramer, "DORA is now live – are your ICT contracts compliant?", 2025. Law-firm commentary.
19. Commission Delegated Regulation (EU) 2025/532 (RTS on subcontracting of ICT services supporting critical or important functions).
20. HM Treasury, *Critical third parties to the finance sector: policy statement*, June 2022, para 1.7.