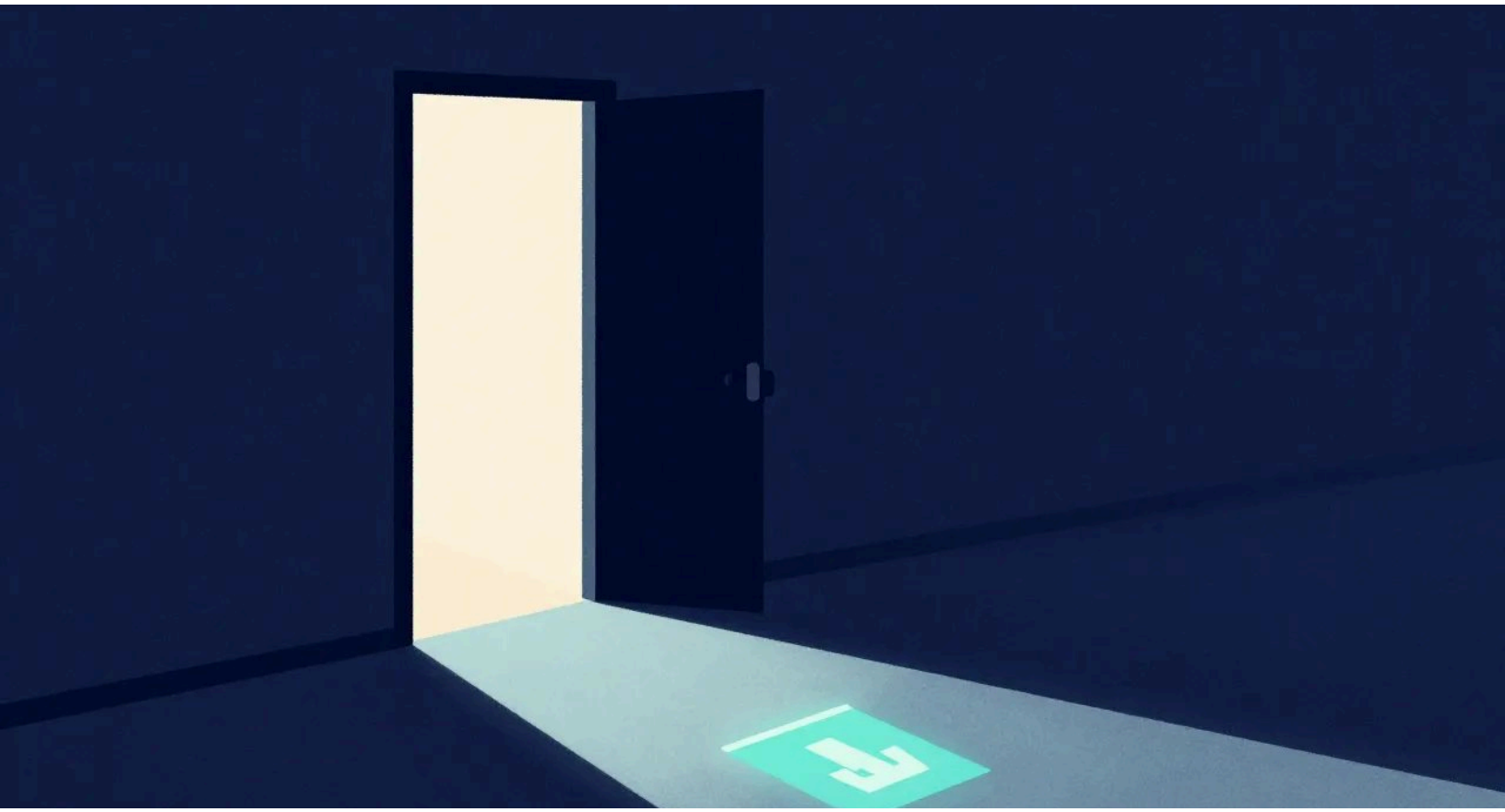


EXECUTIVE PAPER · MIGRATIONS

Every Critical Vendor Needs an Exit Plan

Vendors fail, get sold, change their prices and get banned. Executives who have not written down how they would leave a critical vendor will make that move on someone else's schedule.

AUTHOR

Chris Watkins

SERVICE

Migrations

FOR

CEO, CFO, COO, CTO · 12 min read

AT A GLANCE

The problem. Companies depend on a small number of vendors for payments, customer records, core operations and security. When one of those vendors goes bankrupt, is acquired, reprices or is prohibited by a government, the customer has to move within a deadline set by a court, a regulator or the vendor itself. Most have never worked out what that move involves.

Why it persists. Exit is negotiated once, as a contract clause, and then forgotten. Nobody exports the data to see whether it is usable, prices the alternative or times a rehearsal. Termination assistance clauses assume a solvent, cooperative vendor, which is exactly what is missing in the worst cases.

The recommendation. For every critical vendor, keep a one-page exit plan with four facts: the data you would take and proof that the export works, the named alternative, the measured time to move and the estimated cost. Define the warning signs that would start the move. Test the plan for the top vendors each year. European and UK financial regulators already require this of the firms they supervise.

The Decision in Front of You

Every company has vendors it could not run without for a week. The decision is whether to spend a modest, recurring amount of staff time keeping a working plan to leave each of them, or to accept that any forced move will be improvised.

The forced move is the case that matters. A planned migration, started when the business chooses, is a project. A forced one arrives with a deadline attached: a bankruptcy court freezing accounts, a regulator setting a cutoff date, a vendor switching off a product or deleting data after a notice period. The work is the same in both cases. The difference is whether it begins with a plan or with a search for one.

This paper covers the planned response to losing a vendor permanently. A companion paper in this series covers the shorter problem of a vendor's outage.

What's Happening

Forced exits from 2024 to 2026

Synapse, 2024: the vendor fails and takes the records with it. Synapse was a banking-as-a-service middleman that connected consumer fintech apps to partner banks. It filed for Chapter 11 in April 2024; its filings listed as many as 100 fintech clients, and one industry observer estimated up to 10 million end customers could be affected [1]. Customers of several apps lost access to their money for months. A court-appointed trustee found up to $96 million in customer funds missing [2]. The central problem was

the ledger: the partner banks could identify the funds they held, but not which end customer owned them, because the record of ownership had lived with Synapse [2]. One app, Yotta, said 13,725 of its customers had deposited $64.9 million and were offered $11.8 million back [2]. The FDIC proposed a rule requiring banks to keep detailed records for fintech customers [2]. The lesson for any company: when a vendor holds the only authoritative copy of who owns what, its failure leaves you unable to reconstruct your own position.

Builder.ai, 2025: warning signs came months early. Builder.ai, a Microsoft-backed software development company that had raised more than $450 million, entered insolvency proceedings in May 2025 and said it would appoint an administrator [3]. The company had told staff that funds had run out [4]. The signals were public well before then. Bloomberg reported that it had cut its revenue estimate for the second half of 2024 by 25%, and former employees alleged sales had been inflated by more than 20% on several occasions; the company hired auditors and replaced its chief executive in February 2025 [3]. A customer that treated those reports as an exit trigger would have had months to retrieve its source code and documentation. One that waited had to do it during an insolvency.

Kaspersky, 2024: a government sets the deadline. In June 2024 the US government added Kaspersky to the Entity List and banned sales of its software to new US customers from July 20 and updates to existing customers after September 29 [5][6]. That left US customers about three months to replace their endpoint security. Many consumers who did not choose found that Kaspersky had removed its own product from their computers in mid-September and installed a replacement from another company, often without clear notice [6]. The lesson: when you do not pick the alternative, the departing vendor may pick it for you.

Shorter reminders. When CDK Global, the dealership software provider, shut down its systems after cyber incidents in June 2024, dealers lost an estimated $600 million or more in the first two weeks [7]. Microsoft's retirement of a nonprofit licensing grant in 2025 required affected customers to move plans and export their data, and The Register reported in 2026 that Microsoft deleted some of that data early by mistake [8]. A third paper in this series covers how VMware's licensing changes turned renewals into migration decisions.

Exhibit 1. Forced exits set their own clock

Case	Trigger	Warning available	Time the customer had	What the exit needed first
Synapse, 2024	Vendor insolvency	A major partner left and disputes went public before the filing [1]	Little; app accounts froze in the weeks after the filing [1]	An independent record of who owns which funds [2]
Builder.ai, 2025	Vendor insolvency	Revenue cut, audit and CEO change months earlier [3]	Days once insolvency began [3][4]	Source code and documentation in the customer's hands
Kaspersky, 2024	Government prohibition	Ban announced with dates [5][6]	About three months [5][6]	A chosen replacement, installed before the cutoff
CDK Global, 2024	Prolonged vendor outage	None [7]	About two weeks of disruption [7]	Manual procedures and an export of current data

Source: cases as cited; author's analysis of the warning and the first need.

Regulators now require exit plans

Financial regulators have turned this into an obligation. The EU's Digital Operational Resilience Act, Regulation (EU) 2022/2554, requires financial entities to have exit strategies for ICT services that support critical or important functions [9]. They must be able to exit without disrupting the business, weakening compliance or harming service to clients [9]. Exit plans must be comprehensive, documented, sufficiently tested and periodically reviewed, and firms must identify alternative solutions and transition plans that move the service and its data to another provider or back in-house [9]. In November 2025 the European Supervisory Authorities designated the first critical ICT third-party providers for direct oversight under the same regulation [10].

The UK Prudential Regulation Authority's supervisory statement SS2/21 asks firms to distinguish a stressed exit, such as the insolvency of a provider, from a non-stressed exit made for commercial, performance or strategic reasons [11]. The PRA expects firms to start exit planning before they sign: identify alternative providers during due diligence, estimate the cost, resources and time of an exit in both scenarios, identify the data they would need first, and define the indicators that would trigger an exit [11]. It asks firms to define success in measurable terms such as cost, functionality and time, and to test the plans, particularly for stressed exits [11]. Firms that keep a copy of cloud data outside the cloud can focus their testing on reconciling the two sets [11].

The EU Data Act, which has applied since September 12, 2025, makes cloud exits easier for every business in the EU, financial or not [12]. Software-as-a-service and platform providers must allow export of customer data in a commonly used, machine-readable format, providers must remove

obstacles to switching, and switching and data egress charges are being withdrawn, ending entirely from January 12, 2027 [12]. The law lowers the cost of leaving. Choosing where to go and proving that the exported data will load remain the customer's work.

Why the Usual Approach Fails

The exit clause is mistaken for an exit plan. Legal teams negotiate termination rights, data return and transition assistance. Those clauses assume the vendor is solvent and willing. In a stressed exit, which the PRA describes as the insolvency or liquidation of a provider, the vendor may have no staff left to help [11].

The data export is assumed and never tried. Many contracts promise data in a standard format. Nobody checks whether the export includes attachments, history, configuration and the relationships between records, or how many days it takes to produce a full copy. Synapse showed that the critical data may be a record the customer never thought to hold [2].

The alternative is a name on a slide. A plan that says "move to a competitor" without confirming that the competitor can onboard the volume, meets the same compliance requirements and has a realistic implementation lead time will fail its first contact with a deadline.

Nobody watches for the trigger. Vendor reviews happen at renewal. Insolvency, acquisition, repricing and regulatory action happen on their own timetable, and the warning signs, such as layoffs, auditor changes, an acquirer's history with acquired products, or a regulator's notice, sit in the news while the vendor file sits unread.

Cost grows silently. Each year a company builds more integrations, customizations and reports on a platform, and the cost of leaving rises. Without a periodic estimate, nobody notices the point at which leaving became impractical.

The Framework: Four Facts and a Trigger

An exit plan can be short. It holds four facts that someone has verified, and a list of signals that would start the move. One page per critical vendor is enough.

Exhibit 2. The exit plan card: four facts and a trigger for each critical vendor

Element	What it records	Evidence that it is real
Data	Every dataset and configuration you would need, the export method and format	A full export completed within the last year, loaded into a test system and reconciled with the live system
Alternative	A named provider, an in-house option, or a manual procedure for the interim	A recent conversation or proposal from the alternative; confirmation that it meets your compliance needs
Timeline	Weeks to move in a planned exit and in a forced one	A rehearsal or a dated estimate from people who would do the work
Cost	One-time migration cost, change in running cost, contract penalties	An estimate reviewed by finance in the last year
Trigger	The signals that start the plan: insolvency indicators, acquisition, price change above a threshold, regulatory action, repeated outages	A named owner who reviews those signals each quarter
Interim measures	How the business keeps working during the move: escrow, extended licenses, manual processes	Contract terms in place; manual process written down

Source: author's framework, informed by DORA Article 28(8) [9] and PRA SS2/21 Chapter 10 [11].

Rank vendors before writing cards. A vendor is critical if its loss would stop a revenue-earning or regulated activity for more than a few days, or if it holds the only authoritative copy of records you need. That usually yields between five and fifteen vendors for a mid-size company. Everything else gets a line in the inventory and a note on how its data could be retrieved.

The data element deserves the most effort. Export on a schedule, store the copy where the vendor cannot reach it, and reconcile it against the live system. The PRA suggests exactly this check for firms that keep a copy of cloud data outside the cloud [11]. A recent, usable copy turns a stressed exit into a planned one: you still have to move, but you are no longer negotiating for your own records with an administrator or a bankruptcy trustee.

What it costs

The following is the author's illustrative estimate for a hypothetical company with ten critical vendors. Assumptions: three person-days a year per vendor to export, check and update the card; one full rehearsal a year for each of the two most critical vendors at 15 person-days each; $1,200 per fully loaded person-day. The total is (10 × 3 + 2 × 15) × $1,200 = $72,000 a year, before any tooling. Compare that with two weeks of disruption at a single critical vendor, which cost CDK's dealer customers an estimated $600 million or more combined [7].

Costs, Risks, and Tradeoffs

Exhibit 3. Tradeoffs of keeping tested exit plans

Area	Cost or risk	Mitigation
Staff time	Exports, card updates and rehearsals take engineering and procurement hours	Limit full plans to critical vendors; one rehearsal a year for the top two
Vendor relationship	Asking for full exports and alternatives can read as a threat	Make it a standard clause for every critical contract; regulators expect it of financial firms [9][11]
Data exposure	Every export creates another copy of sensitive data	Encrypt, restrict access, and apply the same retention rules as production
Testing risk	A rehearsal can disrupt operations or leak data	The PRA notes this risk; use test environments and sampled data [11]
Dual running	Keeping an alternative warm costs money	Most alternatives can stay cold; reserve warm standby for vendors where days of loss are unacceptable
When this is wrong	A vendor that is easily replaced, holds no unique records and supports nothing that stops revenue	An inventory line and a contact for data return are enough

Source: author's analysis.

How to Act

Exhibit 4. A one-year roadmap

Window	Actions	Owner	Milestone
First 30 days	List vendors, rank by impact and substitutability, and select the critical set. Name an owner for each.	COO with CIO and procurement	Critical vendor list signed off; each has a named owner
First 30 days	For each critical vendor, identify any records it holds that you hold nowhere else.	CIO with business owners	List of single-copy records complete
First 90 days	Write the exit plan card for every critical vendor. Complete a full data export for the top five and load each into a test system.	Vendor owners with engineering leads	Cards complete; five exports reconciled against live data
First 90 days	Set trigger signals and start a quarterly review of them.	Risk or procurement lead	First quarterly trigger review delivered to leadership
First 365 days	Rehearse a full exit for the two most critical vendors, including a timed restore of exported data into the alternative. Add exit, export and transition terms to renewals.	CIO with CFO	Two rehearsals completed with measured time and cost; every critical renewal carries exit terms

Source: author's recommendation, aligned with DORA Article 28(8) [9] and PRA SS2/21 [11].

Questions to Ask Your Team

1. Which five vendors would stop the business within a week if they disappeared tomorrow?
2. Which of them hold records we do not hold anywhere else?
3. When did we last export all our data from each one, and did it load into anything?
4. For each, who is the alternative, and have we spoken to them this year?
5. How many weeks would a move take, and who estimated that?
6. What signals would tell us a critical vendor was in trouble, and who is watching for them?
7. If a regulator gave us 90 days to replace one of these vendors, what would we do first?
8. Has the cost of leaving any critical vendor grown to the point where we could not realistically do it?

Closing

Every critical vendor will eventually be replaced, by choice or under pressure. The companies that come through a vendor failure, acquisition or ban with the least damage are the ones that had already checked the data export, picked the alternative and timed the move. Keep a one-page, tested exit plan for each

critical vendor, review the warning signs every quarter, and rehearse the move for the vendors you depend on most.

Sources

[1] TechCrunch. "With a16z-backed Synapse's collapse, BaaS fintech is a mess and 10 million consumers could be hurt." May 25, 2024. https://techcrunch.com/2024/05/25/with-a16z-backed-synapses-collapse-baas-fintech-is-a-mess-and-10-million-consumers-could-be-hurt/.

[2] CNBC. "Synapse bankruptcy: thousands of Americans see their savings vanish." November 22, 2024. https://www.cnbc.com/2024/11/22/synapse-bankruptcy-thousands-of-americans-see-their-savings-vanish.html.

[3] TechCrunch. "Once worth over $1B, Microsoft-backed Builder.ai is running out of money." Includes coverage of Bloomberg reporting on revenue estimates. May 20, 2025. https://techcrunch.com/2025/05/20/once-worth-over-1b-microsoft-backed-builder-ai-is-running-out-of-money/.

[4] The Register. "Builder.ai insolvency." May 21, 2025. https://www.theregister.com/2025/05/21/builderai_insolvency/.

[5] The Register. "Kaspersky offers US customers a goodbye gift." Coverage of the US Commerce Department rule. July 17, 2024. https://www.theregister.com/2024/07/17/kaspersky_goodbye_gift/.

[6] BleepingComputer. "Kaspersky deletes itself, installs UltraAV antivirus without warning." September 23, 2024. https://www.bleepingcomputer.com/news/security/kaspersky-deletes-itself-installs-ultraav-antivirus-without-warning/.

[7] Fox Business. "Car dealership losses from CDK software outage could soon reach $1 billion, study finds." Coverage of Anderson Economic Group estimate. July 2, 2024. https://www.foxbusiness.com/markets/car-dealership-losses-from-cdk-software-outage-could-reach-1-billion-study-finds.

[8] Page, C. "Microsoft tells nonprofits their deleted M365 data isn't coming back." The Register. September 28, 2026. https://www.theregister.com/saas/2026/09/28/microsoft-tells-nonprofits-their-deleted-m365-data-isnt-coming-back/5299433.

[9] European Union. "Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)." Article 28, paragraphs 7 and 8. OJ L 333, 27.12.2022. Via SpringLex. https://www.springlex.eu/packages/dora/dora-regulation/article-28/.

[10] European Banking Authority. "European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act." Press release. November 18, 2025. https://www.eba.europa.eu/publications-and-media/press-releases/european-supervisory-authorities-designate-critical-ict-third-party-providers-under-digital.

[11] Prudential Regulation Authority, Bank of England. "Outsourcing and third party risk management." Supervisory Statement SS2/21, Chapter 10, paragraphs 10.1 to 10.25. November 2024 update, effective December 31, 2024. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2024/ss221-november-2024-update.pdf.

[12] European Commission. "Data Act explained." Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/data-act-explained.

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.