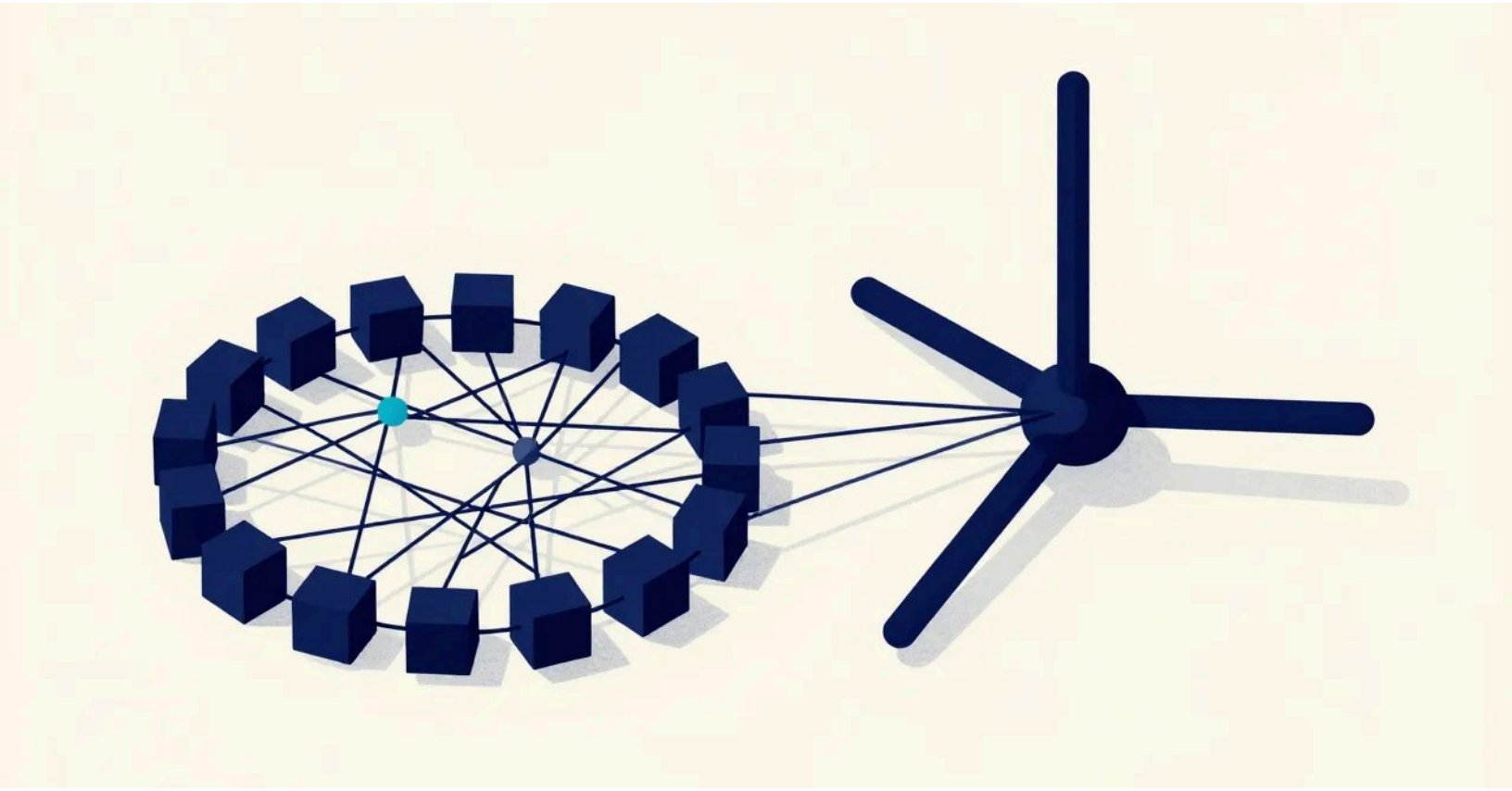


EXECUTIVE PAPER · INTEGRATIONS

Point-to-Point Integrations Are a Hidden Tax

Every rekeyed order, spreadsheet bridge and nightly file between your systems carries a cost nobody budgets and a failure nobody sees. Finance and operations leaders should inventory those connections, price them, and move the critical ones onto a governed integration layer.

AUTHOR

Chris Watkins

SERVICE

Integrations

FOR

CFO, COO, CTO, CIO · 12 min read

AT A GLANCE

The problem. Most companies connect their systems one pair at a time: a nightly file here, a custom script there, a person retyping orders from one screen into another. Each link was cheap when it was built. Together they form a web that nobody has drawn, where a feed can stop or send wrong data for months before anyone notices. Regulators have fined banks hundreds of millions of dollars for exactly that.

Why it persists. Integration work is spread across project budgets, so no single line item shows its total cost. The links work most days, and when one breaks the damage shows up somewhere else, usually in a reconciliation, a customer complaint or an audit finding.

The recommendation. Inventory every connection and price it. Move the feeds that touch money, customers or regulators onto a governed layer: documented APIs and events, one agreed data model, and monitoring on every feed. Adopt one rule for all of them: every feed has an owner, a monitor and a contract.

The Decision in Front of You

Your systems talk to each other through dozens or hundreds of connections. Some are modern APIs. Many are a CSV file dropped on a server at 2 a.m., a script someone wrote years ago, a spreadsheet finance moves between two systems, or a clerk who rekeys purchase orders. Each is an integration, whether or not anyone calls it one.

The decision is whether to keep paying for these connections one at a time, out of whatever budget happens to break them, or to treat them as a single asset with an inventory, a cost and a standard. The second path costs money up front. The first costs more, and the bill arrives as misstated numbers, regulatory findings and lost sales.

The scale is larger than most executives assume. MuleSoft's 2025 Connectivity Benchmark, a survey of more than 1,050 IT leaders run with Vanson Bourne and Deloitte Digital, found the average enterprise runs 897 applications and only 29% of them are integrated [1]. Only 2% of organizations had connected more than half their applications, and IT teams reported spending 39% of their time building custom integrations [1]. MuleSoft sells integration software, so treat these figures as a vendor's view of the problem.

What's Happening

The arithmetic of pairwise connections

When every system connects directly to every other system that needs its data, the number of possible links grows with the square of the system count. The formula is n(n-1)/2. Ten systems can need 45 links. Forty systems can need 780.

Exhibit 1. Direct connections grow far faster than the systems they connect

Systems	Possible point-to-point links, n(n-1)/2	Links through a shared layer, n
5	10	5
10	45	10
20	190	20
40	780	40
100	4,950	100

Source: author's calculation, checked in Python. The middle column is a ceiling; few companies build every possible link.

Each new system adds links to many existing ones, and each link carries its own format, schedule and error handling. When a field changes in a source system, every downstream link that reads it can break, and nobody holds the list.

Analysts name ownership as the root cause

Gartner calls the accumulated cost of these links integration technical debt. Its 2024 research note on preventing it says the debt reduces adaptability, raises costs and harms reliability, and that leaders put off paying it down because the business impact is hard to quantify [2]. A 2025 follow-up note covers managing and reducing it [3].

A Gartner senior director analyst for integration, writing in 2024, listed the causes plainly: no clear ownership of integrations, an outdated integration strategy, and underinvestment in tools, people and process [4]. He also reported that integration now falls under 60% of software engineering leaders, and recommended documenting integration timelines and outages and monitoring integrations continuously [4].

Recent cases: the feed that failed quietly

JPMorgan, 2024. In March 2024 the Federal Reserve and the Office of the Comptroller of the Currency fined JPMorgan about $348.2 million, of which the Fed's share was about $98.2 million, for an inadequate program to monitor trading for market misconduct between 2014 and 2023 [5]. The bank had

disclosed that it was reporting incomplete trading data to its surveillance platforms, and the OCC said billions of instances of trading on at least 30 global venues had not been properly monitored [6]. The surveillance platforms ran; the data feeding them was incomplete for years.

Sigma Broking, 2025. The UK Financial Conduct Authority fined the broker £1,087,300 in 2025 after finding that 924,584 of its transaction reports, close to 100% of the transactions it handled from December 2018 to December 2023, were incomplete or inaccurate [7][8]. The cause was incorrect system setup, and the FCA said the errors persisted uncorrected because of weaknesses in the firm's reporting processes [7]. The regulator's own monitoring spotted the problem in May 2023 [7]. Earlier the same year, the FCA's first fine under the UK MiFIR reporting regime went to Infinox Capital for 46,053 reports it never submitted [9].

Synapse Financial Technologies, 2024 to 2025. Synapse sold middleware that connected consumer fintech apps to partner banks. Its ledger of who owned which dollars had to agree with the banks' records. After Synapse filed for bankruptcy in April 2024, partner banks found a shortfall of $60 million to $90 million between the funds they held and the balances Synapse's records showed [10]. Consumers lost access to their money for weeks or months, and many have not received their full balances [10]. The Consumer Financial Protection Bureau's 2025 action centered on records that did not match the banks' records [10], and the Bureau later allocated about $46 million from its Civil Penalty Fund toward victims [11].

PayPal and German banks, August 2025. According to Süddeutsche Zeitung reporting carried by Reuters, the fraud filtering that normally screens PayPal's direct debits before they reach banks failed fully or largely, and unvetted debits flowed to German lenders [12]. The banks' own checks caught the anomaly and they blocked PayPal payments. The newspaper put the blocked volume above €10 billion; a banking source told Reuters it was hundreds of millions to billions of euros [12]. PayPal called it a temporary service interruption and said it was resolved [12]. When one control inside a partner's feed failed, the receiving banks had to shut the whole channel.

Asda, 2025. The UK grocer's stock problems after separating from Walmart's systems, which its chairman blamed partly on poor integration, are covered in Map the Systems Before You Fund the Project [13].

SIDEBAR: WHY INTEGRATION FAILURES ARE SILENT

A feed that delivers yesterday's file again, drops one trading venue, or maps a field to the wrong column usually raises no error at all. In the JPMorgan and Sigma cases the systems ran normally for years while the data was wrong [6][7]. Detecting this class of failure requires checking the content of the feed: row counts, totals, freshness and agreement with the source.

Why the Usual Approach Fails

Integrations are built inside projects. A team installing a new warehouse system writes the feeds it needs to go live, then the project closes. The feeds stay, and nobody owns them, because ownership was never a deliverable.

Costs are scattered. The clerk who rekeys orders sits in operations, the month-end reconciliation sits in finance, and the engineer who fixes the nightly job sits in IT. A lost sale from a stale inventory feed shows up as a sales miss. No budget line adds these together.

Each system also has its own idea of what a customer, product or order is. One system's customer number is another's account ID, and a third keys on email address. Every point-to-point link carries its own translation, and the translations drift apart as systems change. That is how two systems that both claim to be correct end up disagreeing about the same balance, as Synapse and its partner banks did [10].

Regulators in banking have treated this as a control issue for over a decade. The Basel Committee's BCBS 239 principles, issued in 2013, exist because many banks could not aggregate risk exposures fully, quickly and accurately during the financial crisis [14]. The European Central Bank's 2024 guide on risk data aggregation and reporting builds on those principles and raises supervisory expectations for data governance, architecture and lineage [15][18]. Citigroup's $135.6 million in 2024 penalties from the Fed and OCC followed insufficient progress fixing data quality management under its 2020 orders [16]. The same discipline applies to a manufacturer's order-to-cash chain, where the cost of a bad feed lands as write-offs and lost customers instead of fines.

The Framework: Owner, Monitor, Contract

Every feed that touches money, customers or a regulator should meet one rule: **it has an owner, a monitor and a contract.** A feed that cannot meet the rule is a candidate to retire or replace.

Owner. One named person accountable for the feed working, by role, with a deputy. The owner approves changes to the feed and is the person who gets the alert. This is the gap Gartner's analyst named first [4].

Monitor. Checks on the content of the feed, run on every delivery: did it arrive on time, are the row counts and totals within range of the source, does a sample reconcile end to end. An alert goes to the owner, by phone for critical feeds. The paper on monitoring as a financial control covers alert routing; this rule applies it to data moving between systems.

Contract. A written definition of what the feed carries: fields, formats, meanings, schedule, volume and what happens on failure. For APIs this is a machine-readable specification such as the OpenAPI Specification, version 3.2.1, a language-neutral description of an HTTP interface [17]. Files and events get a published schema and a check that rejects data that does not match it.

The governed integration layer is how a company applies the rule at scale. Systems publish and consume data through documented APIs and events instead of private links to each other. One agreed data model defines the core business entities, so translations happen once. Every feed passes through a place where it can be monitored. The layer can be a commercial integration platform or a message broker with an API gateway on infrastructure you already run. Older systems join through an adapter without being replaced, as the paper on extending legacy systems describes.

What the tax costs

The model below is an illustration for a hypothetical mid-size distributor with 40 systems and 120 active feeds. Substitute your own figures.

Exhibit 2. Illustrative annual cost of 120 ungoverned feeds versus a governed layer

Cost line	Point-to-point today	Governed layer
Feed maintenance and break-fix ($120 per engineer hour)	40 hours per feed: $576,000	12 hours per feed: $172,800
Integration platform and operations	none	$180,000
Manual rekeying ($75,000 loaded cost per person)	3 people: $225,000	0.5 person: $37,500
Feed failures reaching customers or the ledger ($30,000 each)	8 per year: $240,000	2 per year: $60,000
Month-end reconciliation (2 analysts, 8-hour days, $120 per hour)	5 days a month: $115,200	2 days a month: $46,080
Annual total	**$1,156,200**	**$496,380**
Annual difference		$659,820
Payback on a $900,000 one-time migration		about 16 months

Source: author's illustrative estimate. All inputs are assumptions, not survey data. Arithmetic checked in Python. The model excludes regulatory penalties and lost revenue from a long silent failure, which in the cases above dwarf every other line.

Costs, Risks, and Tradeoffs

Exhibit 3. What a governed integration layer costs and where it goes wrong

Area	Cost or risk	Mitigation
Up-front spend	Migration of existing feeds and a platform or broker to run	Migrate by risk: money, customer and regulatory feeds first; leave low-value links alone
Central bottleneck	A small integration team becomes a queue every project waits on	Central team owns standards and the platform; product teams build their own feeds to the contract
Platform concentration	One layer becomes a single point of failure for every feed	Run it with high availability; keep critical feeds able to queue and replay after an outage
Data model politics	Agreeing what a customer or order is takes executive time and causes friction	Start with the five entities that cross the most systems; settle disputes at COO or CFO level
False assurance	A monitored feed can still carry wrong data that passes every range check	Add periodic end-to-end reconciliation against the source of record for financial feeds
When this is wrong	A company with a handful of SaaS systems connected by vendor-supplied connectors gets little from its own layer	Keep the owner, monitor and contract rule on each connector; skip the platform

Source: author's analysis.

How to Act

Exhibit 4. A one-year roadmap

Window	Actions	Owner	Milestone
First 30 days	Build the feed register: every connection between systems, including files, scripts, spreadsheets and rekeying. Record source, destination, schedule, data carried and current owner if any.	CIO with finance and operations leads	Register covers every system in the order-to-cash and procure-to-pay chains
First 30 days	Tag each feed that touches money, customers or a regulator. Price the current cost of the top 20 using the Exhibit 2 lines.	CFO with CIO	Top 20 feeds tagged and priced; total reported to the executive team
First 90 days	Assign an owner to every tagged feed. Write a contract for each. Put freshness, count and total checks on each with alerts to the owner.	Engineering leads, feed owners	100% of tagged feeds have owner, monitor and contract; first alert-driven fix recorded
First 90 days	Agree the shared definitions of the five most-crossed business entities. Choose the integration layer.	COO and CTO	Data model for five entities signed off; platform decision made
First 365 days	Move tagged feeds onto the layer, highest risk first. Retire rekeying and spreadsheet bridges on those flows. Add monthly end-to-end reconciliation for financial feeds.	CTO with feed owners	80% of tagged feeds on the layer; manual rekeying hours down by half; zero feed failures found by customers or auditors first
First 365 days	Make the rule a gate: no new system goes live with a feed that lacks an owner, a monitor and a contract.	CIO with project governance	Rule written into project approval; first project held to it

Source: author's recommendation.

Questions to Ask Your Team

1. How many connections exist between our systems, counting files, scripts, spreadsheets and people who retype data?
2. Which of those carry money, customer orders or regulatory reports, and who owns each one by name?
3. If a nightly feed delivered yesterday's file again, what would alert us, and how soon?
4. How many hours a month do finance and operations spend reconciling numbers that two of our systems disagree on?

5. When we last changed a field in a core system, how did we find every downstream feed that read it?
6. Do we have one agreed definition of a customer, a product and an order, and which systems ignore it?
7. Would a regulator or auditor find a gap between our source systems and our reports before we did?

Closing

Point-to-point integrations look free because their cost is spread across every department and their failures look like someone else's problem. JPMorgan, Sigma and Synapse show what happens when a feed runs for years without anyone checking what it carries [5][7][10]. Inventory the connections, put a price on them, and move the ones that matter onto a governed layer. Hold every feed to one rule: it has an owner, a monitor and a contract.

Sources

[1] Salesforce. "MuleSoft Connectivity Benchmark 2025." Survey of 1,050 IT leaders with Vanson Bourne and Deloitte Digital. 2025. https://www.salesforce.com/blog/mulesoft-connectivity-benchmark-2025/.

[2] Gartner. "How to Prevent Integration Technical Debt." Research abstract. 2024. https://www.gartner.com/en/documents/5415363.

[3] Gartner. "How to Manage and Reduce Integration Technical Debt." Research abstract. 2025. https://www.gartner.com/en/documents/7050498.

[4] Humphreys, A. (Gartner). "Software engineering leaders must act to manage integration technical debt." SD Times. 2024. https://sdtimes.com/softwaredev/software-engineering-leaders-must-act-to-manage-integration-technical-debt.

[5] Board of Governors of the Federal Reserve System. "Federal Reserve Board issues enforcement action against JPMorgan Chase & Co. and fines the firm approximately $98.2 million for an inadequate program to monitor firm and client trading activities for market misconduct." Press release. 2024. https://www.federalreserve.gov/newsevents/pressreleases/enforcement20240314a.htm.

[6] CNBC. "JPMorgan to pay nearly $350 million in penalties for inadequate trade reporting." 2024. https://www.cnbc.com/2024/03/14/jpmorgan-to-pay-nearly-350-million-in-penalties-for-inadequate-trade-reporting-.html.

[7] Financial Conduct Authority. "FCA fines Sigma Broking Limited for transaction reporting failures." Press release. 2025. https://www.fca.org.uk/news/press-releases/fca-fines-sigma-broking-limited-transaction-reporting-failures.

[8] Financial Conduct Authority. "Final Notice: Sigma Broking Limited." 2025. https://www.fca.org.uk/publication/final-notices/sigma-broking-limited-2025.pdf.

[9] FinTech Global. "FCA issues first MiFIR transaction reporting fine to Infinox Capital." 2025. https://fintech.global/2025/02/03/fca-issues-first-mifir-transaction-reporting-fine-to-infinox-capital/.

[10] Consumer Financial Protection Bureau. "Synapse Financial Technologies, Inc." Enforcement action. 2025. https://www.consumerfinance.gov/enforcement/actions/synapse-financial-technologies-inc/.

[11] American Banker. "CFPB to refund $46 million to Synapse victims." 2025. https://www.americanbanker.com/news/cfpb-to-refund-46-million-to-synapse-victims.

[12] Reuters, via Business Recorder. "German banks halted 10 billion euros in PayPal payments on fraud concerns." 2025. https://www.brecorder.com/news/amp/40380012.

[13] The Register. "Asda's 'self-inflicted' SAP mess after Walmart divorce stalls financial revival." 2025. https://www.theregister.com/2025/12/01/asda_walmart_tech_divorce/.

[14] Basel Committee on Banking Supervision. "Principles for effective risk data aggregation and risk reporting." BCBS 239. 2013. https://www.bis.org/publ/bcbs239.htm.

[15] Regulation Tomorrow. "ECB final guide on effective risk data aggregation and risk reporting." 2024. https://www.regulationtomorrow.com/2024/05/ecb-final-guide-on-effective-risk-data-aggregation-and-risk-reporting/.

[16] Board of Governors of the Federal Reserve System. "Federal Reserve Board fines Citigroup $60.6 million for violating the Board's 2020 enforcement action." Press release. 2024. https://www.federalreserve.gov/newsevents/pressreleases/enforcement20240710a.htm.

[17] OpenAPI Initiative. "OpenAPI Specification." Version 3.2.1. https://spec.openapis.org/oas/latest.html.

[18] Crisil Coalition Greenwich. "RDARR signals." Summary of the ECB guide published May 3, 2024. 2024. https://www.crisil.com/en/home/our-analysis/reports/2024/07/rdarr-signals.html.

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.