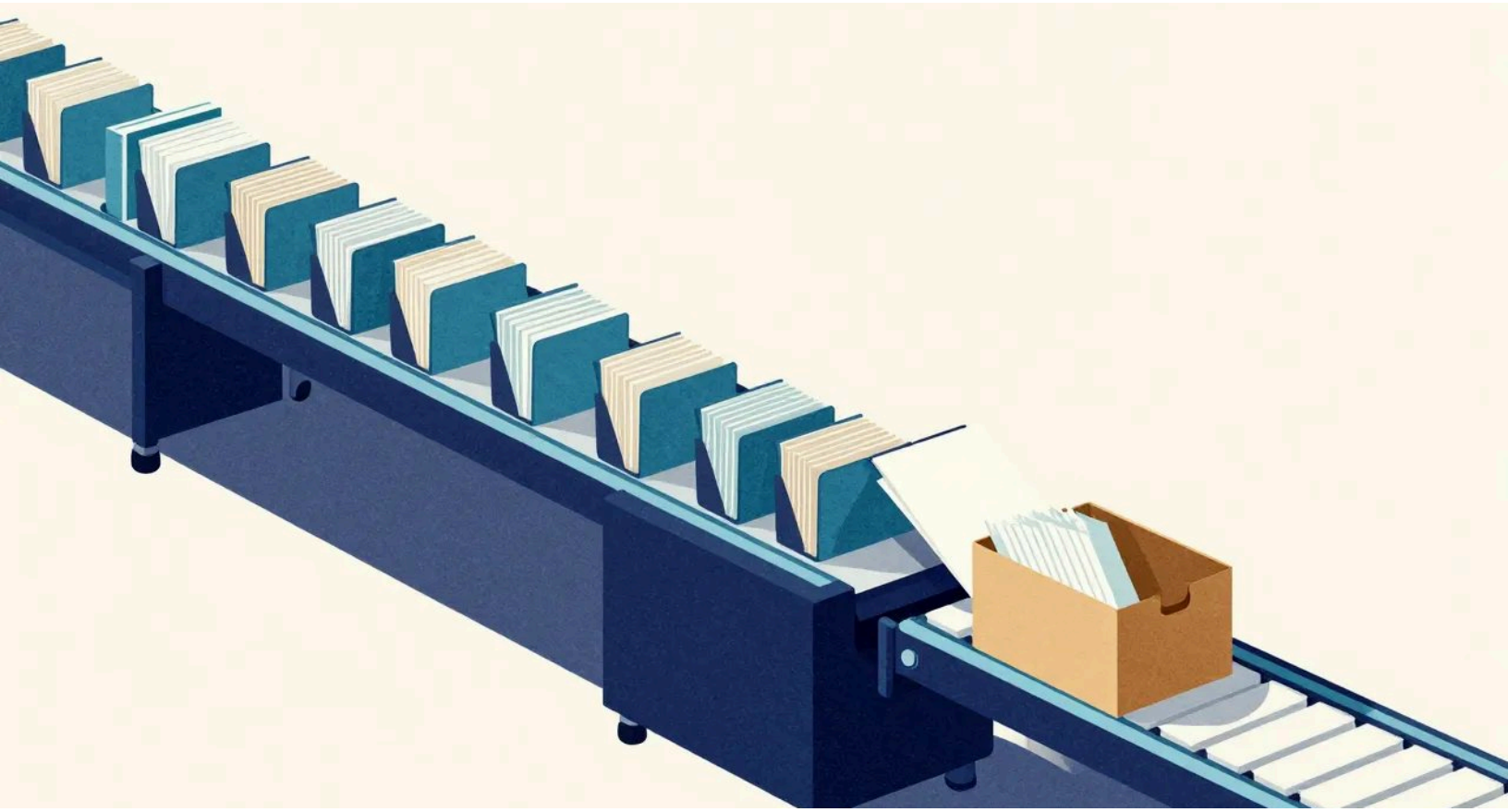


EXECUTIVE PAPER · INFRASTRUCTURE

Compliance Should Fall Out of Engineering

Companies that run SOC 2, ISO 27001, PCI and customer questionnaires as separate manual projects pay for the same evidence several times, and the paperwork drifts from what the systems actually do. Build the evidence into the engineering system once.

AUTHOR

Chris Watkins

SERVICE

Infrastructure

FOR

CEO, CFO, CTO · 11 min read

AT A GLANCE

The problem. A growing company soon answers to several frameworks at once: SOC 2 for customers, ISO/IEC 27001 for international buyers, PCI DSS for card data, and a stream of security questionnaires. Each is usually run as its own project, with screenshots and spreadsheets gathered by hand before the auditor arrives. The work repeats, and the documents describe the company as it was on the day they were written.

Why it persists. Compliance sits outside engineering, so evidence is collected by people asking engineers for proof. Nobody owns a single list of controls. Regulators are now penalizing statements that do not match the systems, and the U.S. government is moving its own cloud authorizations to machine-readable, continuously checked evidence.

The recommendation. Keep one internal control set mapped to every framework you answer to. Express the controls as checks in code where you can, collect evidence automatically from the systems of record, and generate each audit and questionnaire from that data. Measure success by how little audit preparation takes and by how often a failing control is caught before an auditor sees it.

The Decision in Front of You

Every company that sells to other businesses eventually has to prove its security. The question is how. The common answer is a project for each audit: a consultant, a readiness phase, weeks of engineers taking screenshots, and a binder or shared folder handed to the auditor. Then the next audit starts, with a different framework and often a different team.

The alternative is to treat compliance as an output of the engineering system. Controls are defined once, checked automatically where possible, and their evidence is collected as a by-product of normal work. An audit becomes a report run against data the company already keeps.

The money involved is mostly people's time, and it grows with every framework and every enterprise customer. The risk is larger than the cost. When compliance documents are written separately from the systems they describe, they drift apart, and regulators now treat that gap as misrepresentation.

What's Happening

The frameworks multiply and change

SOC 2 reports are built on the AICPA's Trust Services Criteria, issued in 2017 with revised points of focus in 2022, covering security, availability, processing integrity, confidentiality and privacy [1]. ISO/IEC 27001:2022, the third edition of the international standard for information security

management systems, was published on October 25, 2022 [2]. PCI DSS version 4.x added 64 new requirements; 51 of them were future-dated and became mandatory on March 31, 2025 [3].

Customer questionnaires add another layer. The Cloud Security Alliance's Cloud Controls Matrix, now at version 4.1, contains 197 control objectives in 17 domains and includes a yes-or-no questionnaire, the CAIQ, that many buyers send to cloud providers [4]. CSA maps the matrix to ISO, NIST and PCI requirements and publishes the mappings in machine-readable formats [4].

These frameworks overlap heavily. Access reviews, change approval, logging, backups and vendor oversight appear in nearly all of them under different numbers. NIST runs a program, the National Online Informative References program, to publish standard mappings between its documents and other frameworks for this reason [7].

Government is moving to machine-readable evidence

NIST's Open Security Controls Assessment Language, OSCAL, provides formats in XML, JSON and YAML for control catalogs, baselines and security plans, so that they can move out of Word and Excel documents [6]. NIST describes the goal as shorter audits, fewer human errors and less time spent on documentation [6].

The U.S. government's cloud authorization program, FedRAMP, announced FedRAMP 20x in March 2025 [5]. It replaces document-heavy reviews with Key Security Indicators validated automatically, and FedRAMP says the approach is meant to replace static yearly manual assessments as it matures [5]. In the first pilot, which ran from April to September 2025, FedRAMP received 26 complete packages and issued the first pilot authorizations in late July 2025 [5]. The second pilot, at the Moderate level, granted its first authorization on March 6, 2026 [5]. FedRAMP plans to stop accepting new certifications under its older Rev5 process on June 11, 2027 [5].

Continuous evidence has a long history. NIST SP 800-137, published in 2011, set out continuous monitoring as ongoing visibility into assets, threats and the effectiveness of controls [8]. What has changed is that FedRAMP is now building its authorizations on it [5].

Three cases where the paperwork and the systems disagreed

Georgia Tech, 2025. In September 2025 Georgia Tech Research Corporation agreed to pay $875,000 to settle False Claims Act allegations over U.S. Air Force and DARPA contracts [10]. The government alleged that a lab doing sensitive cyber-defense research ran without anti-malware tools until December 2021 and had no system security plan until at least February 2020 [10]. It also alleged that in December 2020 the institution submitted a cybersecurity assessment score of 98 for a campus-wide environment that did not exist [10]. The case began with a suit by two former members of the cybersecurity team, who received $201,250 [10]. No liability was determined [10]. A score that described a fictional environment met the reporting requirement on paper and failed it in fact.

GoDaddy, 2025. In January 2025 the Federal Trade Commission announced an action alleging that GoDaddy had failed since 2018 to inventory its assets, manage software updates, log and monitor security events, and segment its shared hosting [11]. The FTC said the company advertised reasonable security and compliance with the Privacy Shield frameworks while attackers reached customer websites and data between 2019 and 2022 [11]. The proposed order bars GoDaddy from misrepresenting its compliance with any security program and requires independent assessments every two years [11]. Each failure the FTC listed is a control that can be checked automatically.

Delve, 2026. In March 2026 an anonymous whistleblower who said they worked at a former customer accused Delve, a venture-backed compliance automation startup, of producing fabricated evidence of board meetings, tests and processes that never happened, and of routing most clients through two audit firms that rubber-stamped its reports [12]. Delve disputed the claims, said final reports are issued only by independent licensed auditors, and said it provides templates [12]. Its lead investor, Insight Partners, temporarily removed its published article about the investment [13]. These are allegations, and no regulator had acted on them in the coverage reviewed [12][13]. The lesson holds either way: automating the paperwork is different from automating the controls, and a buyer cannot tell the two apart from a report alone.

Why the Usual Approach Fails

Audit-as-project collects evidence at the wrong time. Screenshots taken the week before fieldwork show that a control worked that week. They say nothing about the other fifty-one.

It also collects evidence from the wrong place. A compliance analyst asks an engineer for proof, and the engineer produces something that looks right. The evidence is a description of the system, made by hand, and it can be wrong without anyone intending it. The Georgia Tech allegations turned on exactly this gap between a reported score and real systems [10].

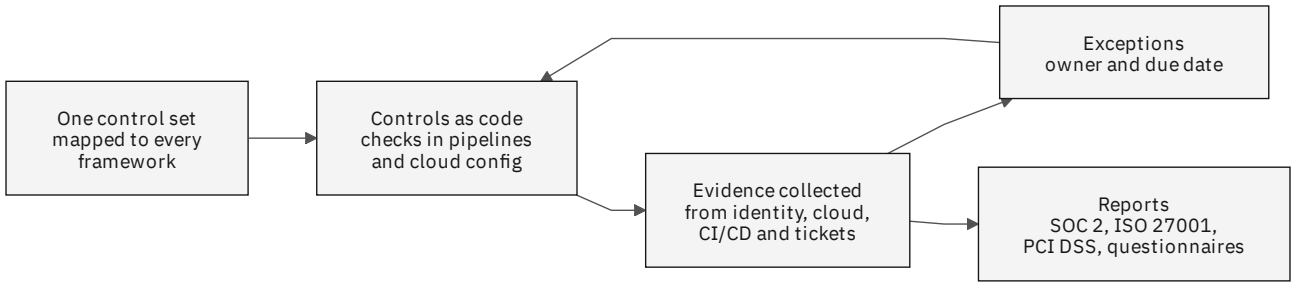
Separate projects for each framework multiply the work. The same access review is evidenced three times in three formats for three auditors, and then summarized again in answers to customer questionnaires. When the frameworks change, as PCI DSS did in March 2025 [3], each project is reworked on its own.

Finally, nobody is accountable for whether controls work between audits. The compliance team owns the report, and engineering owns the systems. A control can fail for months and surface only at the next audit, or in an incident.

The Framework: One Control Set, Evidence by Default

The model has four parts. The company keeps one control set. Each control is checked by the system where possible. Evidence flows automatically from the systems of record. Each audit and questionnaire is a view of that data.

Exhibit 1. Evidence flows from the systems that run the business into every report



Source: author's framework, drawing on NIST OSCAL [6], NIST SP 800-137 [8] and FedRAMP 20x [5].

One control set. Write the company's own controls once, in plain language, each with an owner. Map each to the framework requirements it satisfies. The Cloud Controls Matrix and NIST's published mappings give a starting crosswalk [4][7]. A control that satisfies no framework and no internal risk is a candidate for removal.

Controls as code. Where a control is technical, express it as an automated check. Infrastructure is defined in code and checked against policy before it is deployed. Production changes go through a pipeline that records the approval and the test result. Encryption, logging and network segmentation are verified by scheduled checks against the live cloud configuration. These are the failures the FTC described at GoDaddy [11].

Evidence by default. The identity provider already records who has access and when it was reviewed. The deployment pipeline records every change and its approver. The ticketing system records incidents and their resolution. Collect evidence from these systems on a schedule and store it with a timestamp. Use OSCAL or a similar structured format so that the evidence can be shared with auditors and customers without rework [6].

Exceptions with owners. A failing check opens an exception with an owner and a due date. The exception count by age is the measure leadership watches.

Exhibit 2. One control, one evidence source, several frameworks

Internal control	Evidence collected automatically from	Frameworks it serves
Access to production is reviewed every quarter	Identity provider review records and removal logs	SOC 2 security criteria [1]; ISO/IEC 27001 [2]; PCI DSS [3]; CAIQ answers [4]
Every production change is approved and tested	Deployment pipeline records of approver, test result and rollback	SOC 2 [1]; ISO/IEC 27001 [2]; PCI DSS [3]
Security events are logged and monitored	Log platform retention settings and alert history	SOC 2 [1]; PCI DSS [3]; CCM [4]
Assets and software are inventoried and patched	Cloud asset inventory and patch status by system	ISO/IEC 27001 [2]; PCI DSS [3]; NIST SP 800-137 [8]
Backups are taken and restore-tested	Backup job records and restore test results	SOC 2 availability criteria [1]; ISO/IEC 27001 [2]; NIST CSF 2.0 [9]

Source: author's mapping at the level of control families; check exact requirement numbers against each framework's current version.

What it saves: an illustration

The following is the author's illustrative estimate for a hypothetical software company with SOC 2, ISO/IEC 27001 and PCI DSS obligations and 150 customer security questionnaires a year. Assumptions: manual preparation takes 600 hours for SOC 2, 400 for ISO 27001 and 500 for PCI DSS, and each questionnaire takes 8 hours, for 2,700 hours a year. With one control set and automated evidence, each audit takes 150 hours of support, each questionnaire 1.5 hours drawn from a maintained answer library, and the system needs 300 hours a year of upkeep, for 975 hours. The build costs an assumed 1,200 hours in the first year.

On those assumptions the first year costs 2,175 hours, 525 fewer than the manual approach. Every following year saves 1,725 hours. The larger return is outside the arithmetic: a control that fails in March is found in March.

Costs, Risks, and Tradeoffs

Exhibit 3. Tradeoffs of engineering-led compliance

Area	Cost or risk	Mitigation
Up-front build	Engineering time to write checks, connect evidence sources and build the control map	Start with the controls every framework shares: access, change, logging, backup
Automating paperwork instead of controls	A platform can generate polished documents for controls that do not run, as alleged in the Delve case [12]	Require that every piece of evidence comes from a system of record with a timestamp; sample it internally
Auditor acceptance	Some auditors still expect screenshots and sampled tickets	Agree the evidence format with the auditor before the period starts; offer read access to the evidence store
False assurance from green checks	Automated checks cover technical controls and miss process failures such as a help desk skipping identity checks	Keep human testing for process controls; record those results in the same store
Ownership shift	Engineering teams take on work compliance teams used to do	Make compliance a requirement of the platform team, funded as such; compliance owns the control set and mapping
When this is wrong	A small company with one SOC 2 report and a handful of questionnaires a year will not recover the build cost	Buy a reputable compliance platform, check that its evidence comes from your live systems, and revisit at the second framework

Source: author's analysis.

How to Act

Exhibit 4. A one-year roadmap

Window	Actions	Owner	Milestone
First 30 days	List every framework, audit and recurring questionnaire the company answers. Count hours spent on each last year. Draft one control set from the overlap.	Head of compliance with CTO	Inventory of obligations and hours; draft control set with an owner per control
First 90 days	Map the control set to each framework. Automate evidence for access reviews, change approvals, logging and backups. Agree evidence formats with auditors.	Platform engineering lead	Four control families collecting evidence automatically; auditor sign-off on formats
First 90 days	Build a maintained answer library for customer questionnaires, drawn from the control set.	Head of compliance with sales engineering	Median questionnaire turnaround and hours per questionnaire recorded
First 365 days	Express remaining technical controls as checks in code. Run every audit from the evidence store. Report open exceptions by age to leadership monthly.	CTO with CFO	At least 80% of technical controls checked automatically; audit preparation hours down by half against the baseline; no audit finding that the exception report had not already shown

Source: author's recommendation.

Questions to Ask Your Team

1. How many frameworks, audits and questionnaires did we answer last year, and how many hours did each take?
2. Do we have one list of controls, or one per framework?
3. For our ten most important controls, where does the evidence come from, a system or a person?
4. If a control failed today, how long before we would know?
5. Does every public statement we make about security match what our systems would show an investigator?
6. Could an auditor read our evidence directly, or does someone assemble it first?
7. If we use a compliance platform, can we trace each piece of its evidence to a live system?

Closing

Running each audit as a separate manual project pays for the same evidence several times and produces documents that drift from the systems they describe. Regulators now penalize that drift, and the federal government is moving its own authorizations to continuous, machine-readable evidence. Keep one control set, check it in code, collect evidence from the systems that run the business, and let each audit and questionnaire be a report on that data.

Sources

[1] AICPA and CIMA. "2017 Trust Services Criteria (With Revised Points of Focus, 2022)." 2022. https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022.

[2] International Electrotechnical Commission Webstore. "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: Information security management systems: Requirements." Edition 3.0. 2022. https://webstore.iec.ch/publication/79694.

[3] PCI Security Standards Council. "Now is the Time for Organizations to Adopt the Future-Dated Requirements of PCI DSS v4.x." PCI Perspectives blog. 2025. https://blog.pcisecuritystandards.org/now-is-the-time-for-organizations-to-adopt-the-future-dated-requirements-of-pci-dss-v4-x.

[4] Cloud Security Alliance. "Cloud Controls Matrix and CAIQ." Version 4.1. https://cloudsecurityalliance.org/research/cloud-controls-matrix.

[5] FedRAMP, U.S. General Services Administration. "FedRAMP 20x." 2026. https://www.fedramp.gov/20x/.

[6] National Institute of Standards and Technology. "OSCAL: the Open Security Controls Assessment Language." https://pages.nist.gov/OSCAL/.

[7] National Institute of Standards and Technology. "National Online Informative References Program (OLIR)." https://csrc.nist.gov/projects/olir.

[8] National Institute of Standards and Technology. "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations." NIST SP 800-137. 2011. https://csrc.nist.gov/pubs/sp/800/137/final.

[9] National Institute of Standards and Technology. "The NIST Cybersecurity Framework (CSF) 2.0." NIST CSWP 29. 2024. https://doi.org/10.6028/NIST.CSWP.29.

[10] U.S. Department of Justice. "Georgia Tech Research Corporation Agrees to Pay $875,000 to Resolve Civil Cyber-Fraud Litigation." 2025. https://www.justice.gov/opa/pr/georgia-tech-research-corporation-agrees-pay-875000-resolve-civil-cyber-fraud-litigation.

[11] Federal Trade Commission. "FTC Takes Action Against GoDaddy for Alleged Lax Data Security for Its Website Hosting Services." 2025. https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-godaddy-alleged-lax-data-security-its-website-hosting-services.

[12] TechCrunch. "Delve accused of misleading customers with 'fake compliance'." 2026. https://techcrunch.com/2026/03/21/delve-accused-of-misleading-customers-with-fake-compliance/.

[13] TechCrunch. "Insight Partners scrubs investment post about Delve amid 'fake compliance' allegations." 2026. https://techcrunch.com/2026/03/23/insight-partners-scrubs-investment-post-amid-fake-compliance-allegations/.

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.