The IT leader's playbook for turning compliance into a competitive advantage

RIPPLING IT | CIO DIVE

Custom content for Rippling from Studio by Informa TechTarget

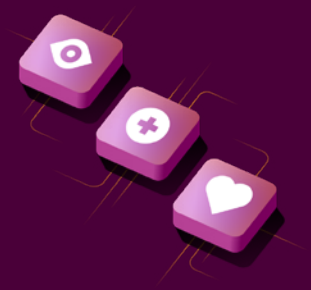
Introduction

The SaaS era promised scaling organizations' agility. Instead, it delivered fragmentation disguised as flexibility.

Over the last decade, companies were encouraged to buy the "best tool for every job." At 20 employees, that strategy helps accelerate growth. At 200, it multiplies complexity. Disconnected systems, overlapping vendors, and unclear ownership distort how organizations operate.

Compliance is where that distortion becomes visible. Kick off a compliance audit, and you quickly realize it will start to stall. Suddenly, evidence collection turns into a fire drill, and access drift appears everywhere.

Audits don't create these problems, but they can reveal them.



As a result, many organizations are solving for this in the wrong way. It's not compliance that's adding a burden to their operating speed, but infrastructure. Things that do relieve "compliance burden":

- ✓ Consolidating identity
- ✓ Clarifying ownership
- ✓ Integrating core systems
- ✓ Automating control enforcement

This playbook goes even deeper into why compliance challenges are ultimately infrastructure challenges. We'll cover how a more unified approach can transform compliance from a burden into your competitive edge. Whether you are an IT director who is responsible for compliance or a security officer at a larger organization, there are plenty of real-world use cases within this guide to help you make the case for a more integrated compliance solution.

The clarity crisis: When flexibility becomes fragmentation

Today's environment is different. Budgets are tighter. AI is accelerating tool proliferation, and regulatory expectations are expanding. According to Deloitte, 62% of CIO's noted that their legacy operating model, built on best-in-breed software, cannot support current and future strategic objectives and plans.

Some recent industry data from Cisco shows that 59% of organizations cite tool maintenance as a primary source of inefficiency. At the same time, 78% report that their security tools are dispersed and disconnected, and 69% say this lack of cohesion creates moderate to significant operational challenges.

The result is what can be understood as **operational drag**.

The hidden tax of fragmented infrastructure

Operational drag is the hidden loss of time, efficiency, and clarity caused by fragmented systems, manual processes, and disconnected data across an organization. It consists of:

- **Decision drag** – Conflicting dashboards and incomplete data slow executive decisions
- **Audit drag** – Manual evidence gathering and reactive compliance work
- **Security drag** – Access drift and inconsistent policy enforcement
- **Financial drag** – Redundant vendors and unclear spend ownership
- **Human drag** – Context switching, ticketing overhead, burnout, and the headcount needed to manage specialized tools.

How to Solve: Implementing more agile software that can be used as your single source of truth to integrate your IT data into one system of record.

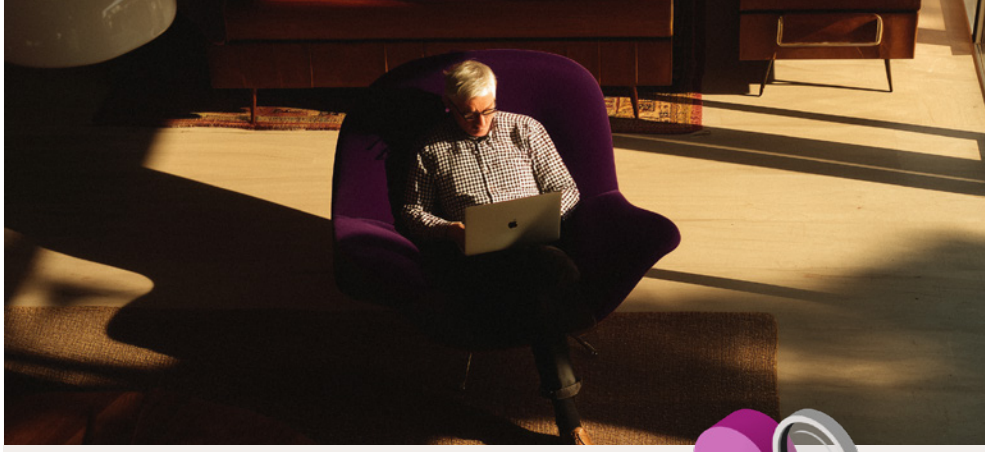
These challenges are not edge cases. They are becoming the default state of modern infrastructure. The moment this becomes undeniable is during an audit.

Audits as forced visibility events

Audits are not checklists. They are stress tests of how your systems and processes actually operate. For many organizations, audits are the first time leadership sees their full system end-to-end. What they uncover is rarely just compliance gaps. It is operational misalignment. In fact, according to PwC, 47% of organizations failed a formal audit 2-5 times in the past three years. Compounding the issue are the reasons businesses are failing. 18% cite tedious, manual evidence collection as their top audit challenge.

Teams still rely on tickets, spreadsheets, and memory to manage access and controls. That works until it doesn't, and audits surface this reality. Fragmented employee, device, and access data make information collection more difficult than it needs to be.

Even with Governance, Risk, and Compliance (GRC) tools in place, fragmentation continues to compound risk.



What audits examine:
Critical policies and processes

- Identity and access governance
- System ownership and accountability
- Integration integrity across tools
- Offboarding discipline
- Evidence traceability
- Security trainings taken
- Performance reviews completed
- Device security requirements
- Policy acknowledgements

What audits reveal:
Operational and security gaps

- Access persists long after employees leave
- Onboarding and offboarding processes are inconsistent
- Tools exist without clear ownership
- Documentation doesn't match reality
- Broken people processes

Where traditional GRC tools fall short

Many organizations adopt governance, risk, and compliance (GRC) tools to address these challenges. These tools play an important role by centralizing evidence, running checks to flag gaps, and generating audit-ready reports.

GRC platforms can only report on compliance, but they do not enforce it. They can surface gaps and generate audit-ready evidence, but they don't enforce identity or device policies, fix underlying security issues, or automate the operational workflows required to maintain compliance. For example, a GRC platform may identify unencrypted laptops before an audit, but IT still has to remediate them manually. Making matters worse, 59% of compliance professionals say they **"always"** compromise on compliance due to business pressure.

GRC tools were never designed to enforce compliance, and expecting them to is why so many programs stall. To be effective, compliance must identify problems and enable rapid resolution.

59%

of compliance professionals say they "always" compromise on compliance due to business pressure.

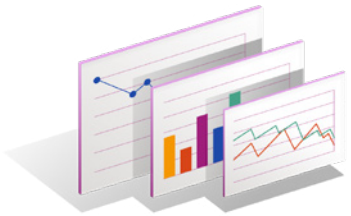
Why fragmentation compounds risk

To achieve a single compliance standard like SOC 2, organizations often assemble and appropriately configure a “stack of stacks”: identity providers, device management tools, HR systems, training platforms, cloud infrastructure, and more. And it’s all stitched together through integrations. Think about how many times you need to connect with each department to understand who owns what tools and who has access to them.

This creates what many teams experience as a laundry list problem and a collection nightmare: multiple tools required to prove a single control.

Most of the work does not happen generating reports. It focuses on procuring and configuring tools, connecting with teams, and finding the right information. Time is spent connecting systems often through complex integrations or resolving issues across teams and platforms.

This work is often referred to as **compliance orchestration**. It’s the effort required to make fragmented systems function as a cohesive compliance environment. And the negative impact is significant.



The consequences of compliance orchestration

When compliance depends on stitching systems together, the impact extends far beyond IT:

- Slower enterprise sales cycles due to audit delays
- Increased friction during M&A or due diligence
- Higher dependency on key individuals who understand the system
- Less reliable reporting at the executive level

AI adoption introduces another layer of risk. Tools adopted outside centralized governance create new access pathways and data exposure risks that are difficult to track. As organizations begin to embed AI into workflows, these tools start acting across systems by accessing data, triggering actions, and interacting with other applications. Without identity-based controls and centralized visibility, organizations lose track of who has access to AI tools, what data they can reach, and how those tools are being used across the environment. 93% of organizations know that generative AI creates business risk, but only 9% are prepared to handle those threats. Of those businesses, only 70% have a well-defined AI governance model or ongoing monitoring controls.

The eventual result is predictable. Compliance failures are rarely audit failures. They are process failures.

The infrastructure coherence maturity model

In response to these inefficiencies and risks, organizations are seeking to evolve past the limits of GRC. They are transforming compliance into an asset, not a liability. In doing so, organizations tend to evolve through predictable stages in how they manage infrastructure and compliance.

Stage 1: Tool Accumulation	Stage 2: Reactive Governance	Stage 3: Visibility & Ownership	Stage 4: Continuous Compliance
Department-driven purchasing	Introduction of GRC tools	Improved visibility into systems	Automated evidence collection
Manual onboarding and offboarding	Compliance as periodic effort	Centralized identity and device management	Real-time control monitoring
Reactive, ad hoc compliance	Spreadsheet-based evidence tracking	Defined ownership and accountability	Integrated HR, IT, and security workflows

Continuous compliance is not something organizations add on. It emerges when infrastructure is designed coherently. Good compliance is a well thought out strategy and this starts with your IT stack and a plan to reduce tool sprawl. As time has proven, the exercise of centralizing all your data into one stack is an almost insurmountable objective. According to recent Bizdata360 data, 87% of organizations struggle with disconnected data sources.

These data silos only started to pop up when businesses started investing in best-of-breed softwares. So, in order to simplify compliance, businesses need to simplify their tech stack in order to improve ease of data collection and improve compliance enforcement. Good compliance is a well thought out strategy and this starts with your IT stack and a plan to reduce tool sprawl. As time has proven, the exercise of centralizing all your data into one stack is an almost insurmountable objective.

From reporting compliance to enforcing it

The core shift in modern compliance is simple:

Reporting is not enough. Enforcement is required.

Traditional approaches focus on proving compliance after the fact. Modern approaches embed compliance into how systems operate.

In practice, continuous compliance means:

- Automated evidence collection from live systems
- Persistent monitoring of controls
- Identity-first governance across tools
- Centralized visibility across the environment
- Real-time policy enforcement
- Governed AI access and usage tracking

This shift matters because the real work of compliance isn't reporting. It's operational control.

The Continuous Compliance Loop

Teams often underestimate the effort required to write and maintain policies. The coordination needed across departments drains resources. In many environments, resolving a single issue can take days. A GRC tool may flag a problem, but remediation requires identifying the responsible system and contacting the relevant team. Then there's the time gap until action is taken in addition to verifying the fix.

This chain of events introduces delays, dependencies, and risk.

In a **unified environment**, remediation becomes immediate. Issues can be addressed at the source, often in a single step, because the systems responsible for enforcement are integrated.

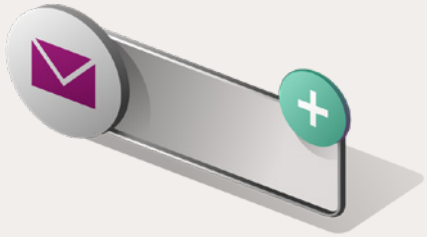
Upstream enablers of this model include:

- Identity and access management as a control backbone
- Device management integration
- HR system alignment
- Cloud and code repository integration
- Vendor lifecycle oversight
- AI tool governance tied to identity

The overall impact is significant. Audit preparation shifts from weeks to minutes. Operational burden is reduced, and fewer vendors mean fewer failure points. And **AI adoption becomes governed** rather than risky.

Platform integration is not about reducing tools for its own sake. It is about simplifying the system so it can function reliably.

What compliance looks like: Reporting vs. Enforcement



Before:
Reporting Compliance (Fragmented Stack)

During a routine check, the GRC tool flags that several employee laptops are missing required encryption. The issue is logged, but IT now has to investigate which devices are affected, contact each employee, and manually ensure encryption is enabled. Some devices are missed, others are delayed, and follow-ups are needed. It can take days to fully resolve, and evidence is only collected once the work is complete.

After:
Continuous Compliance (Coherent Infrastructure)

A compliance check detects that a laptop is not properly encrypted. Because device management is integrated into the system, a policy is automatically enforced to enable encryption. If needed, access to sensitive systems is restricted until the requirement is met. The issue is resolved immediately without manual coordination, and evidence is generated automatically as the policy is enforced.

Evaluating a modern IT & compliance platform

As organizations rethink their approach, the evaluation criteria must evolve. When moving toward continuous compliance, key areas to consider include:

1. **Visibility**
   Can you clearly see who has access to what, and why?

2. **Ownership & Accountability**
   Is responsibility for systems and controls defined and enforced?

3. **Architecture**
   Are systems unified and native, or stitched together through integrations?

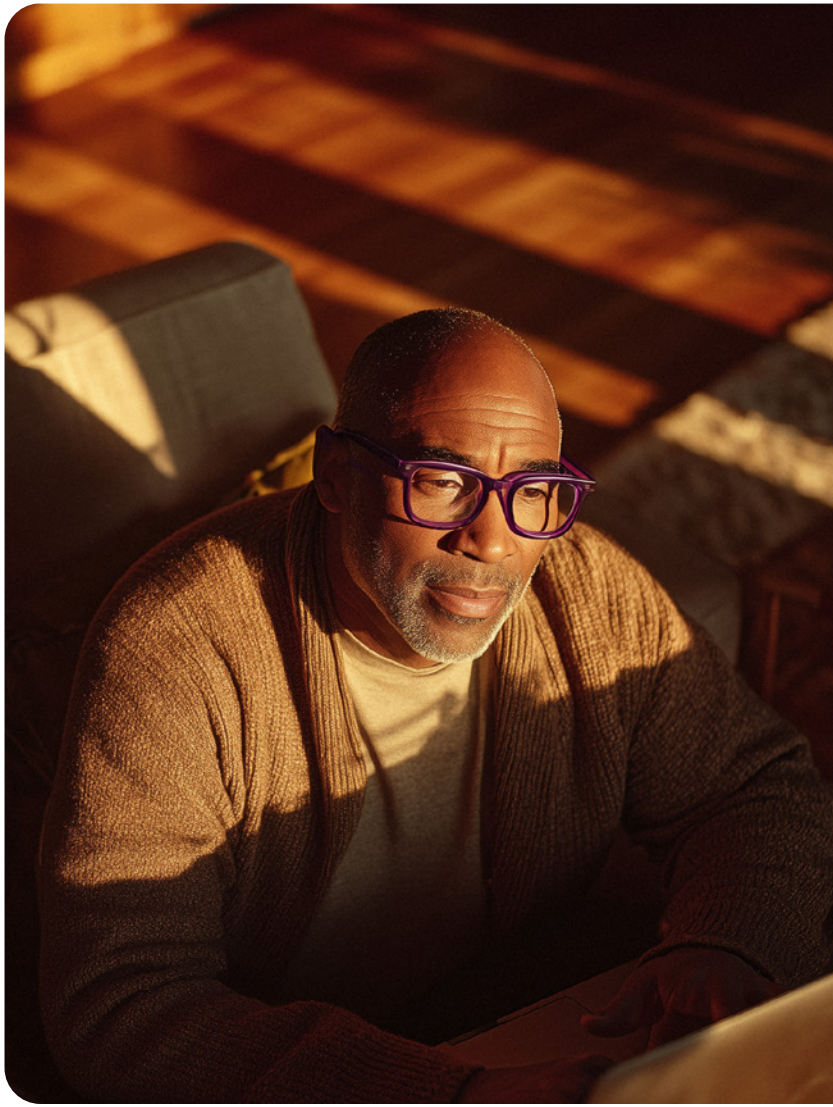
4. **Evidence Automation**
   Is evidence continuously collected from real workflows or manually assembled?

5. **Enforcement Capability**
   Can issues be resolved directly within the platform, or only identified?

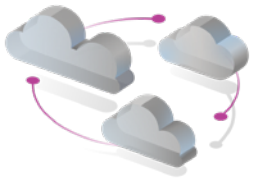
6. **Scalability**
   Does complexity grow with the organization, or does the system absorb it?

7. **AI Governance**
   Is AI usage tied to identity, access, and auditability?

The goal is not simply to reduce tool count. It is to increase clarity and control.



Infrastructure as a strategic asset



The era of unchecked SaaS expansion is ending.

Organizations are shifting toward consolidation, not as a cost-cutting measure, but as a necessity for control, security, and scalability.

When infrastructure is coherent, the impact becomes immediately visible across the organization:

- Financial visibility improves, enabling more accurate forecasting and better control over spending.
- Enterprise deal cycles move faster because compliance becomes an enabler of growth.
- Confidence at the board level strengthens as governance becomes more transparent and reliable.
- Organizations are better prepared for audits, partnerships, and acquisitions, with systems that can support scrutiny without disruption.

The next decade will reward organizations that treat infrastructure as architecture, not accumulation.

Clarity is the goal. And clarity is what allows organizations to scale without multiplying complexity.

Most compliance failures aren't audit failures. They're the accumulated cost of fragmented infrastructure: disconnected tools, manual evidence collection, access drift that nobody caught, and remediation that takes days when it should take minutes. Stitching together an identity provider, a device management tool, an HR system, and a GRC platform doesn't solve the problem. It just distributes it across more vendors and more failure points.

Rippling is built differently. Instead of bolting compliance onto a fragmented stack, Rippling runs it from a single system where HR, IT, identity, device management, payroll, and compliance share the same first-party data. There are no integrations to maintain, no evidence gaps for auditors to flag, and no context-switching between tools to track down a remediation. When a control fails, the platform doesn't just log it, it fixes it at the source, automatically, and captures the evidence in real time. For teams just starting their compliance journey, Rippling guides every step. For organizations scaling a mature program, it adapts without requiring a rebuild.

The result is compliance that doesn't require a fire drill to prove. It's enforced continuously, through the same operations that run your business every day.

How a 4-Person Startup Got Enterprise-Grade Compliance Without Adding Headcount

Rippling Automated Compliance is the only platform that enforces SOC 2, not just reports on it. For Nikolas Huebecker, co-founder of a in-stealth four-person customer operations startup in San Francisco, getting compliant without growing the team was non-negotiable. As a beta customer of Rippling Automated Compliance, he found that it let his small team stand up compliance functions that would have otherwise required significantly more headcount. "It makes it really easy for us as a team of four people to get way more done and stand up way more functions inside of the business, where normally we would have to throw lots of heads," he said. For lean, fast-moving startups, Rippling makes enterprise-grade compliance achievable without the enterprise-sized team.

"It makes it really easy for us as a team of four people to get way more done and stand up way more functions inside of the business, where normally we would have to throw lots of heads."

Nikolas Huebecker
Co-founder

30

hours saved on systems integration setup alone

2

20 questions to 2 questions for Enterprise Security Reviews

How Surepass Went From a Months-Long Process for SOC 2 to Two Weeks

When Surepass set out to achieve SOC 2 compliance, they weren't starting from zero, they'd been through the process before with another leading compliance tool and knew how painful it could be. Manual evidence collection, formatting issues that failed to satisfy auditor requirements, and a platform that surfaced information without actually reducing work. This time, they used Rippling Automated Compliance for SOC 2. Before the audit even began, 80% of their evidence had already been automatically collected, compared to barely 30% with their previous tool, moreover, that 30% wasn't even structured correctly.

Achieving SOC 2 readiness took 2 weeks, required minimal team involvement, and the process felt nothing like their prior experience because Rippling is the system of record for devices, identity, access, and HR, evidence collection becomes a byproduct of normal operations rather than a separate project. SOC 2 went from a months-long undertaking to something Surepass described as "surprisingly straightforward."

80%

of all evidence collected automatically

2 weeks

to SOC 2 readiness with limited time investment

RIPPLING IT

Rippling IT unifies identity, access and devices into one system built on shared data across your environment. Instead of stitching together tools or maintaining complex workflows, IT defines how systems should work — access, device policies, and compliance — and Rippling keeps everything in sync as your business changes. AI is embedded in the system itself, helping execute provisioning, resolve requests, surface risk, and reclaim wasted spend. It doesn't replace control but instead extends it across your entire environment. The result is an IT system that continuously operates as designed, giving teams full visibility and reducing the manual work required to keep everything running. Visit www.rippling.com and follow us on LinkedIn to learn more.

Learn more