CherryHill ADVISORY

Is Your Compliance Real?

Lessons from the Delve Incident. A Diagnostic Guide for GRC Customers.

Delve faked 494 compliance reports for 1,700+ customers. The fallout raises hard questions for every company that relies on a GRC platform.

This guide gives you the red-flag checklist, 25-question self-assessment, and decision framework to determine whether your compliance is built on real controls or checkbox theater.

March 2026 | Cherry Hill Advisory
info@cherryhilladvisory.com
cherryhilladvisory.com

Inside This Guide

01 The Problem with Checkbox Compliance
02 Case Study: What the Delve Incident Revealed
03 Five Warning Signs of Compliance Theater
04 The 25-Question Compliance Integrity Checklist
05 What to Do Next: A Decision Framework
06 What Intentional Compliance Looks Like

Who This Guide Is For

This guide is for compliance leaders, CISOs, CTOs, and founders who rely on GRC automation platforms for SOC 2, ISO 27001, HIPAA, or GDPR compliance. It is written from an internal audit and risk management perspective. The diagnostic framework applies to any vendor, not just the one featured in the case study.

"The question is not whether your vendor gave you a certificate. The question is whether your controls would survive independent examination."

01 The Problem with Checkbox Compliance

In March 2026, a detailed investigation revealed that **Delve**, a $32M-funded GRC automation platform, had generated nearly 500 compliance reports from a single template, complete with pre-written auditor conclusions, fabricated evidence, and unverifiable audit firms. The incident was covered by TechCrunch and discussed widely across the security community. But the Delve case is a symptom, not an anomaly. It exposed structural problems that exist across the GRC automation market.

The market for compliance automation is projected to exceed $1.3 billion in 2026, growing at over 50% year-over-year. That growth is driven by a real need: companies face expanding regulatory obligations and enterprise customers who require proof of security before signing contracts. The tools that emerged to meet that need have, in many cases, optimized for speed and cost rather than substance.

The result is what practitioners call **checkbox compliance**: a process that produces the artifacts of security (reports, certificates, trust pages) without necessarily producing security itself. Policies get adopted without being read. Risk assessments get generated without being tailored. Evidence gets accepted without being verified. The certificate ships on time. The underlying controls may or may not exist.

This is not a new problem. Internal auditors have long understood that a control that exists on paper but not in practice provides no assurance. What is new is the scale at which automation platforms can produce compliance artifacts without the underlying substance, and the speed at which companies adopt them without scrutiny.

Why Checkbox Compliance Fails

Checkbox compliance fails because it confuses documentation with assurance. A SOC 2 report is not a security guarantee. It is an auditor's professional opinion that your controls, as described and evidenced, were operating effectively during a specific period. If the description is generic, the evidence is fabricated, or the auditor's opinion was pre-written, the report communicates nothing about your actual security. It is a document that looks like assurance but functions as a sales tool.

The problem compounds downstream. Enterprise buyers make vendor risk decisions based on SOC 2 reports and trust pages. Partners accept ISO certificates at face value. Regulated entities rely on HIPAA compliance documentation to manage third-party risk. When those artifacts are hollow, every party in the chain is exposed.

The Cost of Getting It Wrong

Framework	What Is at Stake	Maximum Exposure
SOC 2	Lost enterprise deals, vendor disqualification, breach-of-contract claims from customers who relied on your report to make risk decisions.	Contractual damages + pipeline loss
ISO 27001	If the certifying body lacks recognized accreditation (ANAB, UKAS, DAkkS), the certificate has no regulatory or procurement standing.	Certificate invalidation
HIPAA	The Office for Civil Rights does not distinguish between unknowing reliance on invalid compliance and deliberate neglect when patient data is at risk.	Criminal charges + $1.5M/yr per category
GDPR	Fabricated compliance documentation is not a valid defense. If controls were never implemented, individuals whose data you process are unprotected.	4% of global revenue or EUR 20M

02 Case Study: What the Delve Incident Revealed

In March 2026, a detailed investigation by former clients of **Delve**, a Y Combinator-backed GRC automation startup, provided a detailed look at what checkbox compliance looks like when taken to its logical extreme. The investigation, subsequently covered by TechCrunch and widely discussed in the security community, was based on a leaked Google spreadsheet containing links to 494 draft SOC 2 and ISO 27001 reports.

Delve had raised $32 million at a $300 million valuation. Its pitch was speed: SOC 2 compliance in days rather than months, powered by what it called "agentic AI" through an "AI-native" platform. The company served approximately 1,700 customers.

What the Investigation Found

Reports generated from a single template. 493 of 494 SOC 2 reports contained identical text in sections that should be unique to each company, including the same grammatical errors. Companies using AWS, GCP, Azure, Render, Railway, and Vercel all received identical network segmentation descriptions.

Auditor conclusions written before the audit. Draft reports arrived with test procedures, test results, and auditor conclusions already populated, before clients had submitted company descriptions, architecture diagrams, or management signatures. All 259 Type II reports contained identical "could not be tested" conclusions for four controls, including the same typo in every document.

Unverifiable auditor firms. The primary auditors (Accorp and Gradient) were traced to operations based in India, using virtual office addresses to claim a U.S. presence. Over 99% of clients were routed through these firms. Delve marketed them as "US-based CPA firms."

Pre-fabricated evidence as a platform feature. The platform offered one-click adoption of board meeting minutes, risk assessments, security simulations, and employee records for events that never occurred. Trust pages were fully populated with security claims before any compliance work began.

Denial when confronted. Delve's CEO initially called the allegations "falsified claims" from an "AI-generated email." The company later published a blog post characterizing the investigation as "misleading," stating it provides "templates" and that auditors independently issue final reports. Industry observers noted this response did not address the core structural concern: that Delve, not the auditors, produced the report content.

> **Why This Case Matters Beyond Delve**
>
> The Delve incident is not an isolated event. It is a visible example of structural incentives that exist across the GRC automation market: platforms that compete on speed, auditors with no commercial incentive to look closely, and customers who need certificates more than they need security. The patterns identified here can exist in varying degrees at any vendor. The diagnostic framework in this guide helps you evaluate your own situation regardless of which platform you use.

03 Five Warning Signs of Compliance Theater

These patterns were identified through the Delve investigation and generalized as diagnostic criteria. They apply to any GRC vendor relationship. The presence of one or more warrants further examination.

01 Auditor conclusions that predate the audit

In a legitimate SOC 2 engagement, the auditor independently designs test procedures, examines evidence, and forms conclusions based on their own professional judgment. Under AICPA AT-C Section 205, the practitioner must maintain independence and cannot assume management responsibilities. If your draft report arrived with the auditor's verdict already written, the separation between implementer and examiner has collapsed. That is not a technicality. It is a structural failure that invalidates the attestation.

INDICATORS:

- Draft report contains test procedures and conclusions before auditor engagement begins
- Conclusion language is identical across multiple clients of the same platform
- Auditor section contains template artifacts, repeated typos, or generic phrasing
- Report delivery and auditor engagement happen simultaneously rather than sequentially

02 System descriptions that are not specific to your system

SOC 2 Section 3 is your company's signed representation of its security environment. It should describe your actual architecture, tools, processes, and organizational structure. In the Delve case, 99.8% of reports used identical system description language. Cloud providers as different as AWS and Vercel received the same network segmentation narrative. A system description that could belong to any company describes no company.

INDICATORS:

- Section 3 contains generic language that does not reflect your specific technology stack
- Network segmentation description is identical regardless of cloud provider
- Company-specific content is limited to a name, logo, and a few paragraphs of description
- Subservice provider sections are interchangeable across fundamentally different platforms

03 An auditor you cannot independently verify

SOC 2 auditors must be licensed CPA firms. ISO 27001 certification bodies must hold accreditation from a government-recognized body. These are verifiable facts. If you have never spoken directly with your auditor, if the firm uses a virtual office address, or if the accreditation cannot be confirmed through an independent registry, the attestation may carry no legal or regulatory weight.

INDICATORS:

- Auditor firm has only a virtual office or registered agent address
- CPA license cannot be verified through the relevant state board of accountancy
- ISO certification body is not listed in any recognized accreditation body's directory
- All communication with the auditor was mediated through the platform
- The platform selected the auditor without offering you a meaningful choice

04 Evidence that was adopted, not produced

Compliance evidence must reflect activities that actually occurred in your organization. Board meetings that were never held, risk assessments that were never conducted, and security simulations that were never run are not evidence. They are fabrications. Adopting pre-populated evidence means making formal representations to your auditor, your customers, and potentially to regulators about activities that did not take place.

INDICATORS:

- Board meeting minutes were available before any meeting occurred
- Risk assessments contain identical default risks with no company-specific tailoring
- Security simulations and incident response exercises were pre-populated
- Employee evidence (training completion, background checks) was auto-generated
- You achieved compliance primarily through form acceptance, not control implementation

05 Trust pages that outpace your controls

A trust page is a public representation of your security posture. Enterprise buyers and partners use it to make vendor risk decisions. If it lists controls that have not been implemented, penetration tests that were not performed, or certifications that were not independently verified, it is a misrepresentation. In past enforcement actions, regulators have treated inaccurate security disclosures as consumer protection violations regardless of intent.

INDICATORS:

- Trust page was populated before compliance work began
- Listed measures include items your organization has not implemented
- Penetration testing is claimed but only a vulnerability scan was performed
- Trust page content did not change after compliance work was completed
- You cannot map every claim to a specific, documented control

04 The 25-Question Compliance Integrity Checklist

Answer each question based on your direct experience. A "No" or "Unsure" indicates a gap. The scoring matrix at the end maps your result to a risk tier and a recommended response.

A. Auditor Independence

#	Question	Y	N	?
1	Can you name the CPA firm or certification body that issued your report?			
2	Have you verified their license or accreditation through a government registry?			
3	Have you communicated directly with the auditor outside the platform?			
4	Did the auditor request evidence or clarification beyond what the platform provided?			
5	Were auditor conclusions delivered after evidence review, not simultaneously?			

B. Evidence Integrity

#	Question	Y	N	?
6	Did your team personally create or verify every piece of evidence in your compliance file?			
7	Were board meeting minutes based on meetings that actually occurred?			
8	Was your risk assessment tailored to your specific business and threat environment?			
9	Did every employee individually complete their security training and device hardening?			
10	Were security simulations conducted with real participation and documented outcomes?			

C. Platform Substance

#	Question	Y	N	?
11	Do your platform integrations pull live data from your systems (not just screenshot uploads)?			
12	Can you distinguish automated evidence from manually uploaded evidence?			
13	Does your SOC 2 Section 3 accurately describe your specific architecture?			
14	Is your network segmentation description specific to your actual cloud topology?			
15	Did compliance require meaningful technical work beyond filling forms?			

D. Regulatory Accuracy

#	Question	Y	N	?
16	Does your HIPAA compliance include verified encryption for all PHI-handling endpoints?			
17	Does your GDPR compliance include a legitimate Data Protection Impact Assessment?			
18	Are your adopted policies accurate to your actual practices, not aspirational templates?			
19	Can you defend every claim on your trust page with documented evidence?			
20	Has your penetration test met the scope and methodology your report claims?			

E. Vendor Conduct

#	Question	Y	N	?
21	Has your vendor responded to concerns transparently and in writing?			
22	Did the vendor answer hard questions directly, not deflect to calls or charm?			
23	Is pricing consistent with the level of work required for legitimate compliance?			
24	Has the vendor ever marked controls as passing for work that was not completed?			
25	Can you independently verify the claims your vendor makes about their results?			

Scoring

Yes	Tier	Interpretation	Recommended Action
22-25	LOW	Compliance posture appears sound.	Document verification. Annual independent review.
16-21	MODERATE	Gaps that could create exposure under scrutiny.	Gap assessment within 60 days. Prioritize weak categories.
10-15	ELEVATED	Significant deficiencies. Artifacts may not withstand due diligence.	Independent readiness assessment within 30 days.
0-9	CRITICAL	Compliance posture likely compromised.	Immediate independent review. Pause reliance on existing certs.

05 What to Do Next: A Decision Framework

Three Actions for Every Organization

1. Verify your auditor independently. For SOC 2, confirm the CPA firm's license through the relevant state board of accountancy. For ISO 27001, confirm accreditation through IAF MLA signatories (ANAB, UKAS, DAkkS, JAS-ANZ). If you cannot verify, your certification may not carry legal standing.

2. Audit your trust page against reality. Map every public claim to a specific control and evidence artifact. Remove anything you cannot substantiate with documentation that reflects actual practice.

3. Read your own SOC 2 Section 3. Compare the system description to your actual architecture, tools, and processes. If the language is generic or describes technologies you do not use, it is a signed misrepresentation that needs to be corrected.

Tiered Response by Risk Level

Tier	Priority Actions	Timeline
LOW	Document your verification. Schedule annual independent artifact review. Evaluate auditor rotation every 2-3 years.	90 days
MODERATE	Conduct a gap assessment against applicable frameworks. Replace template-adopted evidence with documented, verifiable controls. Engage directly with your auditor to confirm their testing methodology.	60 days
ELEVATED	Commission an independent compliance readiness assessment. Identify which controls are real versus documentation-only. Rebuild evidence for fabricated artifacts. Select a different, independently verified auditor for your next cycle.	30 days
CRITICAL	Treat as an incident. Pause reliance on existing certifications in active sales cycles until validated. Engage compliance counsel. Conduct emergency readiness assessment. Evaluate notification obligations to enterprise customers.	Immediate

06 What Intentional Compliance Looks Like

Checkbox compliance asks: *How fast can we get the certificate?* Intentional compliance asks: *Would our controls survive independent examination?* That distinction determines whether your compliance program is a defensible asset or a latent liability.

At Cherry Hill Advisory, we approach compliance through an internal audit and risk management lens. We evaluate programs the way an independent examiner would: by testing whether controls exist, whether evidence reflects real activity, and whether the people accountable for those controls understand their obligations.

How We Work

We test controls, not templates.	We verify whether the underlying security activity occurred, not whether a form was filled out. A pre-populated risk assessment is not a risk assessment. One built around your specific threats, scored against your environment, and used to drive control decisions is.
We verify auditor independence.	We evaluate your auditor relationship for structural independence, licensing, and testing methodology. If the auditor's conclusions were written by someone other than the auditor, we identify that.
We evaluate evidence integrity.	We trace every material control back to verifiable evidence. Board minutes should tie to actual meetings. Pen test reports should document actual testing against your production environment, not a templated scan.
We build programs designed for examination.	We structure compliance programs to withstand the questions regulators, enterprise customers, and independent auditors will ask. Real policies. Real evidence. Real auditor independence.

What We Offer

Service	What You Get	Best For
Compliance Readiness Assessment	Independent review of your compliance artifacts, auditor relationships, and evidence integrity. Delivered as a prioritized remediation roadmap with specific findings.	Elevated and Critical tier
Compliance Program Design	Ground-up compliance program built on real controls, verifiable evidence, and qualified independent auditors. Covers framework selection through audit readiness.	Starting over or building new
GRC Vendor Due Diligence	Independent evaluation of GRC platforms against auditor independence standards, evidence integrity requirements, and qualification criteria.	Selecting or re-evaluating vendors
Ongoing Compliance Advisory	Managed compliance support that keeps your program current, your evidence defensible, and your auditor relationships sound. Continuous, not annual.	Sustained compliance maturity

07

Update: Delve Responds

On March 24, 2026, Delve distributed a public communication to its customer base announcing new support measures. The message, sent by Delve's CEO, stated that the company does not fake evidence or sign audit reports, and characterized the platform as a tool that helps customers collect and organize evidence using structured workflows and templates aligned to industry standards. Delve also noted that independent, licensed audit firms are responsible for issuing SOC 2 reports, ISO 27001 certifications, and similar attestations.

The communication announced several changes: direct auditor communication channels via Slack and email, clearer labeling of platform-generated templates, an expanded SOC 2 controls dashboard, and complimentary re-audits and penetration tests by independent auditors.

How This Maps to the Five Warning Signs

Warning Sign (Section 03)	Status	Notes
01. Auditor conclusions predate the audit	**Open**	Response affirms auditors issue final reports. Does not speak to whether draft reports contained pre-written conclusions or test results.
02. Generic system descriptions	**Acknowledged**	Template disclosure improvements are planned. Whether system descriptions will be rewritten to reflect each customer's architecture is not specified.
03. Auditor verifiability	**Open**	References independent, licensed firms without naming them or addressing the specific findings in the original investigation.
04. Evidence integrity	**Open**	Platform described as an evidence collection tool. Does not address the availability of pre-populated board minutes, risk assessments, or simulations.
05. Trust page accuracy	**Open**	Not referenced in the communication.

> **What to take from this:** The announced measures are a step toward greater transparency, particularly the direct auditor communication channels and the offer of complimentary re-audits. These are positive developments. What remains unaddressed is the integrity of certifications already issued and the evidence already in customer compliance files. If you take Delve up on a re-audit, three things are worth confirming: that a different, independently verifiable auditor firm is conducting it; that your team produces new evidence from actual activities; and that the auditor writes their own conclusions after examining that evidence. The 25-question checklist in Section 04 of this guide remains the recommended diagnostic tool for evaluating your compliance posture regardless of which platform you use.

Analysis based on Delve's publicly distributed customer communication dated March 24, 2026. This guide is provided for informational purposes and does not constitute legal, regulatory, or audit advice.

Free 30-Minute Compliance Diagnostic

Bring your checklist results. We will review your findings, identify your highest-priority gaps, and map concrete next steps.

info@cherryhilladvisory.com

cherryhilladvisory.com

This guide is provided for informational purposes and does not constitute legal, regulatory, or audit advice. Cherry Hill Advisory recommends consulting with qualified legal counsel regarding specific compliance obligations. References to Delve are based on publicly available reporting as of March 2026, including the DeepDelver Substack investigation, TechCrunch coverage, and Delve's published response.