DRATA

Building Real Trust in Compliance

Evaluating Automation and Audit Quality with Confidence

WHY COMPLIANCE QUALITY MATTERS MORE THAN SPEED ALONE

Automation can accelerate evidence collection and reporting when you're pursuing SOC 2, ISO 27001, or HIPAA, but the level of assurance depends on how that evidence is validated and reviewed. If not implemented correctly, they may not fully reflect how controls operate over time and may limit visibility into how independent testing was performed, which can lead to additional scrutiny if stakeholders cannot clearly understand how the report was produced.

The downstream impact can include increased scrutiny, additional audit work, and delayed trust with stakeholders. Strong assurance depends on independent auditor judgment, clear testing methodology, and transparent reporting from the independent auditor who issues the opinion.

HOW TO EVALUATE THE QUALITY OF YOUR AUDIT AND ATTESTATION

Use this checklist when you evaluate any automation vendor or audit engagement:

- [ ] Is the independent audit firm or certification body clearly identified, with relevant credentials?
- [ ] Does the report clearly define scope, testing procedures, and coverage period?
- [ ] Is there appropriate access to the audit firm to understand scope, methodology, and conclusions?
- [ ] Does evidence demonstrate clear traceability to systems and controls, whether automated or manual?
- [ ] Does the system description accurately reflect how controls operate in practice?

If you cannot quickly and easily tell who issued the opinion, how they tested, and what they tested, you are not looking at reliable assurance.

AREAS OF PARTICULAR CONCERN

Use this checklist when you evaluate any automation vendor or audit engagement:

- [ ] Limited visibility into the independent auditor or certifying body
- [ ] Reports that rely heavily on templated language without clear auditor context or commentary
- [ ] Limited use of system-based evidence, with heavier reliance on manual uploads
- [ ] Commitments that emphasize speed or certainty without clear explanation of scope and testing rigor

High-quality reports make it clear who performed the audit, what was tested, and how conclusions were reached.

FROM INITIAL REPORT TO CONTINUOUS TRUST

Use these principles to guide conversations with your platform and audit partners. Drata adheres to a rigorous Code of Ethics. See how we uphold these standards and help teams operationalize continuous trust with Drata.

See how leading teams operationalize continuous trust with Drata.

HOW TO EVALUATE AUTOMATION AND AUDIT QUALITY WITH CONFIDENCE

You can use these questions verbatim with any automation vendor or auditor.

01 Who actually issues my SOC 2 report / ISO certification?

The vendor should provide:

> The name of an independent CPA firm (SOC 2) or accredited certification body (ISO 27001).

> Clarity that the software vendor does not sign or issue your report.

How Drata approaches this question:

> Drata provides the Drata Agentic Trust Management Platform, which automates evidence collection, control monitoring, and readiness. Independent audit firms issue your SOC 2 report or ISO certificate, and remain responsible for the opinion.

> You can work with auditors familiar with Drata or bring your own qualified firm. The platform supports either choice without changing the auditor's independence.

02 Do you ever draft or pre-populate my audit report text?

Listen for a clear line between:

> Templates that help you describe your environment and controls.

> The formal opinion and testing language, which should come from the auditor.

> Transparency about any AI use.

> Explicit statements that the tool does not write or sign the auditor's opinion.

How Drata approaches this question:

> Drata provides structured workflows, templates, and AI capabilities to help you describe your system, document policies, and organize evidence—not to write the auditor's conclusion.

> Agentic and AI features are designed to remove repetitive trust work (for example, mapping evidence, preparing responses), while independent auditors retain control over testing and final report language.

03 Can I choose my own auditor? Can I speak with them directly?

You should hear that there is:

> Flexibility to work with different independent firms instead of a single bundled option.

> Direct access to your auditor for scoping, planning, and resolving findings.

> A clear separation between product support and the auditor's professional responsibilities.

How Drata approaches this question:

> Drata is built to support a broad ecosystem of independent audit and certification partners and customers who bring their own auditors.

> You and your auditor communicate directly. Drata centralizes evidence, tests controls continuously, and keeps a clean system-of-record so the audit can move faster without blurring roles.

04 What systems does your platform connect to and what constitutes "evidence"?

Answers should include:

> Direct integrations into your core systems (cloud infrastructure, identity, HR, code, ticketing).

> A concrete definition of evidence: configuration states, logs, user and access data, change history, and tickets—not just screenshots.

> How frequently data is refreshed, and how issues are flagged.

How Drata approaches this question:

> Drata connects to the systems that matter for trust—cloud providers, SSO, HRIS, ticketing, and others—to automate evidence collection and continuously test controls across frameworks.

> Evidence from those sources is mapped to your controls and frameworks (SOC 2, ISO 27001, HIPAA, and others) and kept current so you stay audit-ready, not just audit-prepared.

> The platform flags exceptions and potential gaps so your team can act before your auditor tests them, reducing last-minute fire drills.