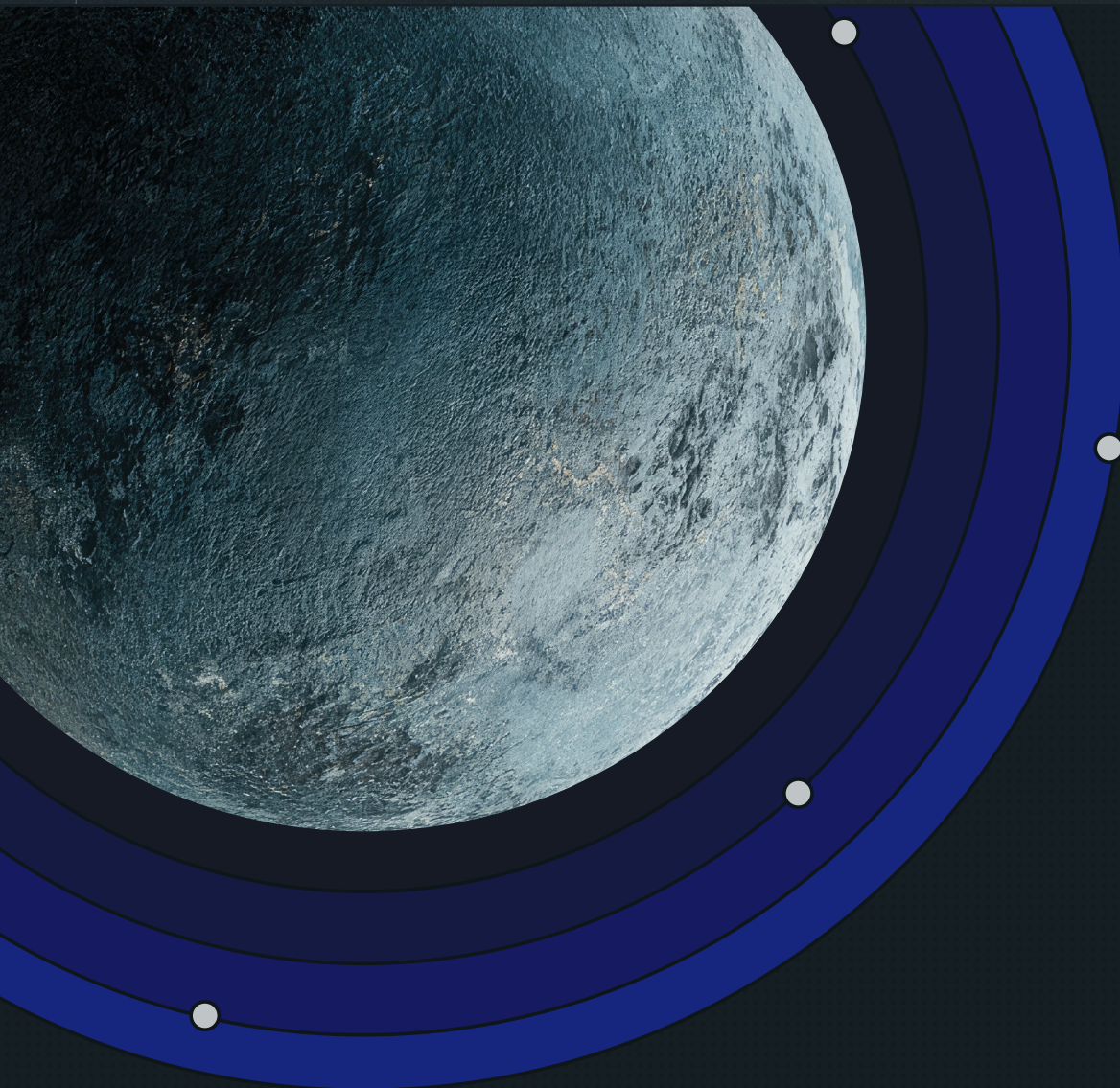


**DRATA**

# How to Build Your Trust Center

A Data-Driven Guide to Designing a Trust Center Your Buyers Love



A scalable Trust Center turns security reviews from a bottleneck into a revenue enabler. When your sales team can point prospects to a single, current source of truth, you see fewer bespoke security questionnaires and a smoother experience for buyers. But where do you start?

We analyzed how buyers engage with hundreds of live Trust Centers to identify the elements they care about most.\* These should be your first focus areas as you build or expand your Trust Center.

## Top 5 Trust Center Focus Areas

### 01 Company Overview

For many prospects, this is their first impression of your organization's security posture. Use the Company Overview to clearly articulate your security philosophy, outline your product and customer base, and set expectations for what buyers will find in your Trust Center. Keep it focused on why your approach to security is trustworthy and mature.

### 02 Product Security

Product Security is typically one of the most-clicked sections in a Trust Center. Use it to explain how customers can use your product securely, including:

- Audit logging and monitoring
- Data security features (encryption, data segregation, regional hosting, etc.)
- Integrations and how they're secured
- Access control, authentication, and authorization
- Secure development and testing practices

Ground this section in concrete controls and tooling rather than marketing language.

### 03 Compliance Badges

Buyers scan Compliance at a glance to understand how your program maps to their requirements. Highlight your key attestations and certifications, including industry-specific frameworks such as HIPAA where relevant. Common examples include:

- SOC 2 attestation
- ISO 27001 certification
- GDPR
- CCPA

Link badges directly to underlying reports or summaries housed in your Trust Center.

### 04 Data Security

Use the Data Security section to go deeper on how you protect data throughout its lifecycle. Typical topics include:

- Data classification and handling
- Encryption at rest and in transit
- Access monitoring and least-privilege controls
- Backup and restore procedures
- Data retention and deletion

These details give security reviewers confidence that your controls extend beyond policy into day-to-day operations.

### 05 Reports

Buyers often come to your Trust Center looking for specific documents. Make a dedicated Reports section that includes commonly requested artifacts, such as:

- Penetration test summaries
- SOC 2 reports
- ISO 27001 certificates
- Network or architecture diagrams
- Security or privacy whitepapers

From here, buyers can request access to sensitive documentation or self-serve content that does not require an NDA or approval workflow. You can also use Trust Center controls to gate specific assets, track who accessed them, and streamline NDA requests.

# Optimizing Your Trust Center

Once you have the core sections in place, focus on keeping your Trust Center current and proactive—not just a static document library.

## Share Trust Center Updates

Many customers regularly communicate changes in their security posture—from new certifications to policy updates—via Trust Center updates. This creates a clear, auditable record of what changed, when, and for whom, and reduces ad hoc “what’s new?” emails from buyers.

## Centralize Questionnaire Response

Use your Trust Center as a source of truth for reusable answers to common security questions. Housing completed standardized questionnaires (such as CAIQ or SIG Lite) and curated Q&A content makes it easier to handle any remaining one-off questionnaires without starting from scratch each time.

## Support Self-Service Security Review

A well-structured Trust Center lets prospects answer most of their own questions by browsing documents, policies, and FAQs, and—where available—searching across approved content. This reduces the volume and complexity of inbound questionnaires and shortens overall security review timelines.

Adding these elements is the first step toward a streamlined, buyer-friendly security review process. The next step is building a cross-functional Trust Center strategy that aligns security, sales, legal, and customer success on how and when to use your Trust Center in the deal cycle.

If you’d like to see how Trust Center supports this end to end—from securely sharing reports to tracking buyer engagement and reducing manual questionnaire work—our team can walk you through a live environment.

[Book time with our team](#) to see Drata Trust Center in action and explore how it can accelerate your next security review.

**Methodology:** This analysis is based on engagement data from paying customers across the legacy SafeBase Trust Center network, now part of Drata. Metrics include average subscriber counts, Knowledge Base depth, Trust Center updates, the percentage of customers that surface specific types of information, and engagement with the most-viewed sections and documents.

# About Drata

Drata provides the trust network that enables businesses to operate, scale, and partner with confidence. Powered by AI and designed to operationalize trust, the Drata Agentic Trust Management platform continuously interprets controls, risk, and assurance signals—reducing repetitive manual work while improving visibility into internal and third-party risk, enabling always-on audit readiness across frameworks, and accelerating security reviews.

Purpose-built for enterprise complexity, Drata unifies governance, risk, compliance, and assurance to deliver faster time-to-value, reduce operational overhead, and enable continuous trust for 8,000+ organizations worldwide.

For more information, visit [drata.com](https://drata.com).

© Drata Inc. – All Rights Reserved

## Navigate Trust Management with Confidence

Discover the entire Drata Agentic Trust Management Platform and explore the solutions that fit your needs.

Get a Demo

