Best Practices for Building — and Keeping — Customer Trust

Blind spots to avoid and essential components to supercharge security program ROI.

SAFEBASE

Executive Overview

We looked at SafeBase Trust Centers from over **800 leading companies** to identify foundational components every CISO should know.

Today, as organizations face increasing pressure to be open about their security practices, there is a shift towards greater collaboration, accountability, and proactivity across teams. More and more, companies are sharing information that might have traditionally been kept confidential to engender a culture that builds stronger relationships with customers.

The advent of AI and Trust Center technology has streamlined workflows, driven efficiency, and helped companies securely — and proactively — showcase up to date security, compliance, and governance programs. Customers can self-serve answers, and internal teams can leverage AI to streamline questionnaire reviews to name a few benefits. Using this technology to centralize other important company policies across departments like legal, HR, procurement, and ESG also accelerates questionnaire reviews, sales cycles, and accurately responds to customer concerns up front.

We looked at SafeBase Trust Centers from over 800 leading companies to identify foundational components every CISO should embed into their own infrastructure as well as blind spots to anticipate in this best practices guide.

Build trust through transparency.

In this guide, we'll share best practices from our customers embracing transparency, transforming their security review process, reducing friction, and building customer trust in the process.

We'll explore:

- Defining Customer Trust's expanding domain
- Foundational elements of an optimal Trust Center
- Blind spots and areas of opportunity when leveling up security and questionnaire reviews
- Trends and insights for teams to apply
- A look ahead - CISOs evolving role towards Chief Trust Officer (CTrO)

Be dedicated to answering customer questions and earning their trust.

Let's dive in.

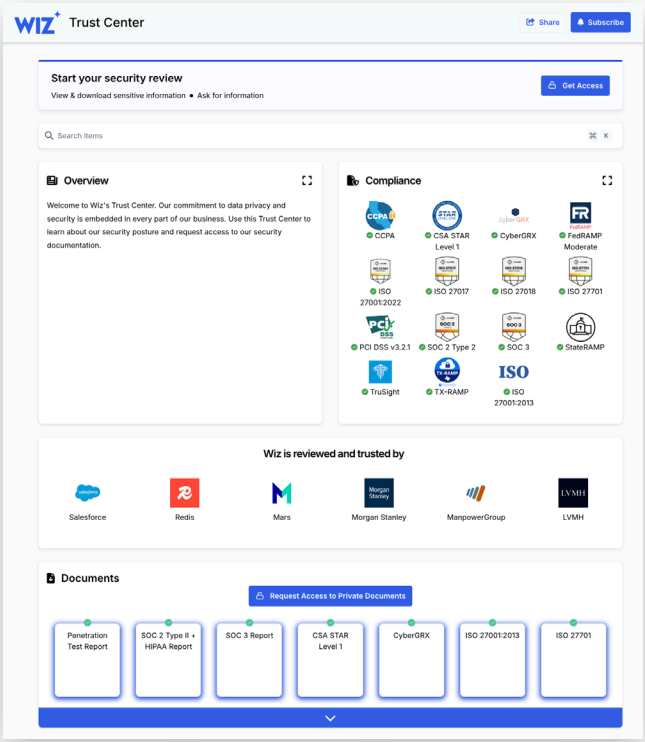
Defining Customer Trust

Level Set: What are the main tenets of Customer Trust?

Customer trust is evolving into a core strategic focus for organizations, particularly in the realm of security and data management. It encompasses security, privacy, availability (uptime), ethics, compliance, ESG, and customer experience and focuses on how trust impacts business objectives and revenue. It's a more holistic, business-oriented approach to building trust across the entire organization, reflecting a shift towards trust as a strategic business driver.

Many CISOs are taking on expanded scopes of trust-related responsibilities beyond their current technical security measures. As a result, they engage with a wider range of stakeholders, including customers, employees, partners, and the public and become a go-to-market enabler.

Foundational elements of an optimal Trust Center



Working with leading companies across the country, we've had firsthand experience with Trust Centers that employ best practices to drive customer trust. Here we share some insider tips from behind the curtain.

Level Set: What is a Trust Center anyway?

A centralized hub or platform that showcases an organization's security posture, compliance information, and related documentation.

Its core purpose is to improve and streamline the buyer security review process (also known as third-party risk assessment) by:

- Aggregating all information that builds customer trust in one place. Common segments of
- information include: security, compliance, privacy, and availability (uptime) but does not exclude ESG, HR, or legal information.
- Allowing buyers and customers to conduct and "subscribe" for future updates as the company's trust center makes updates.
- Providing sellers with customizable permission controls over their documentation

Insider Tips

1

Put your brand and personality into your Trust Center

Creating a trust center that reflects your company's brand and personality is crucial, yet often overlooked. It's important to let your team's unique voice shine through, reminding customers that there are real people behind the technology. This personal touch not only helps build initial trust during the sales process but also maintains it through regular updates and proactive notifications.

2

Make your Trust Center available on company's website + encourage subscription for updates

Transparently and securely share your security and trust posture by adding a link to your website. Encourage customers to subscribe to Trust Center updates for real-time notifications when new information is available versus relying on email back and forth. Proactively notify subscribers of changes to documentation. By embedding these practices into your customer interactions, you create a 'sticky' experience that keeps people coming back to a single source of transparent, accurate truth. Remember, customers want information on-demand so proactively guiding them to your trust center as the go-to, up to date, self-serve resource will enhance engagement and trust over time.

3

Be more transparent than opaque with company information and policies

Many companies fear sharing their policies in a more public forum. Some go so far as to leave areas blank on their Trust Centers. But, high level security and privacy information is what your customers need to understand — think HIPAA, 3rd party audits, SOC2s, how do you firewall, enforce product security, manage credentials, background check employees...the list goes on. With advanced integrations, you can track who has a signed NDA and release the right information to the right people at the right time. Once behind the NDA, enable public access to important information to increase efficiency for your internal teams and help customers get the self-serve answers they need.

Trust Center Insight

Remember...

Trust Centers serve as the outward-facing platform for sharing key security information with customers and prospects, BUT behind the scenes, it functions as the 'source of truth' for all trust related data.

AI Questionnaire Assistance plays a crucial role in this strategy, as it's designed to address any additional questions customers may have that aren't fully answered by the Trust Center, reinforcing a comprehensive 'customer trust' strategy.

Explore AI QA

Let's get back to insider tips...

4

Ensure cross team collaboration + context when uploading questionnaires to your Trust Center

Incomplete questionnaire responses often result from lack of up to date information in your Knowledge Base and inadequate cross-team input — so involve legal, product, and other relevant teams to provide thorough answers for your business and load them into your Trust Center. As AI-assisted questionnaire automation becomes more prevalent, it's crucial to go beyond simple Yes/No/N/A responses too. Add context, explanations, and supporting details to each answer. This is especially important for "No" or "Not Applicable" responses - always explain why. By providing this level of detail and context, you'll preemptively address potential follow-up questions, streamline the review process, and demonstrate your commitment to transparency and thorough security practices. Plus, a well-crafted, context-rich questionnaire can significantly enhance customer trust and help enable revenue.

Remember...

Any answers you leave blank or don't share are left to the imagination of your customers — a much more volatile prospect.

5

Use engagement analytics to see what external and internal stakeholders care about most

What information is being viewed most regularly on your Trust Center? You might think it's your SOC2, but it's actually your security org chart. Are you spending the right time building reports that are in demand for your target audience? Use these insights to customize your Trust Center experience and reflect what customers are engaging with most. Invest resources wisely and scale back on less critical areas to better align with customer needs and expectations.

Blind spots and areas of opportunity to build customer trust

We're often asked about things CISOs should keep on the radar as they grow their Trust program. Here we highlight a few, key examples of common blind spots to be aware of as you move forward.

1. Mitigate risk of outdated documents and unauthorized access with a Trust Center
A well-implemented Trust Center mitigates risk of outdated documents being circulated to customers or unauthorized access provided to sensitive data. Often teams have a limited idea

of how colleagues are using and sharing security info and documents. Without a single source of truth, a 2 year old security policy could be circulated to a customer by mistake or downloaded by an internal stakeholder. In contrast, Trust Centers centralize access and can integrate with Salesforce to ensure NDA compliance before critical information is shared.

2. Unlock visibility into engagement, document views, and customer feedback
Think everyone reviews every single answer in their questionnaires? Think again. In one customer case, a brownie recipe was loaded for every answer — and no one on the receiving team questioned it. But when security incidents occur or audits begin, the negative impacts of inaccurate or unanswered questions can be seismic. Ensure your Trust Center shares engagement metrics on document views as well as a portal for customer feedback. Your team can gain better visibility into what information is in high demand and also make adjustments to respond to customer needs. Improve the experience, collect data to drive shareable insights, and respond accordingly.

3. Think of building trust as a business enabler
Many security leaders are not thinking about how their job enables revenue - they're busy protecting it. Yet being able to measure how security programs have brought the length of the sales cycle down, or eliminated the need to answer redundant questionnaires helps communicate security's impact on business goals.

Being able to measure how security programs have brought the length of the sales cycle down, or eliminated the need to answer redundant questionnaires helps **communicate security's impact on business goals.**

4. Take a proactive — versus reactive — approach in communicating
Security can give Sales teams the tools and resources they need to be proactive in market, answering questions for customers around any areas of interest — product, legal, ESG, availability, HR and more. A Trust Center can house the accurate, up to date, company information customers need to assuage concern. What's more, when security incidents happen, it's a matter of how your teams handle it. Proactive notification sharing how your company was or wasn't affected can reassure customers that things are under control.

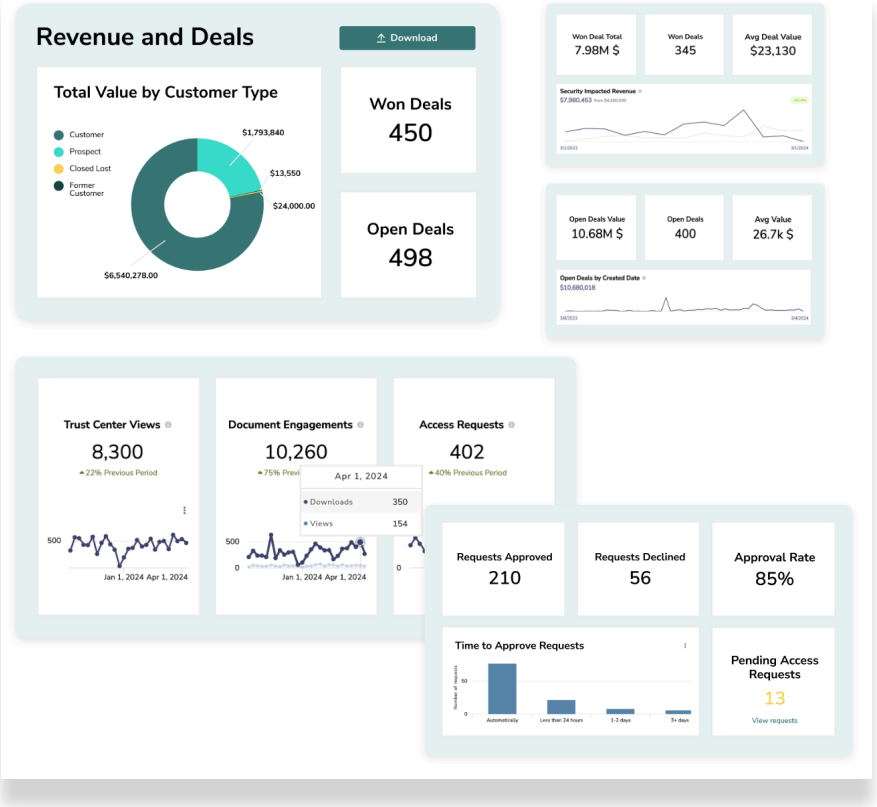
5. Make sure your Trust Center integrates with workflow tools like Slack, Salesforce, and Hubspot
Adopting new technology can be hard. Working within tools that you already engage in everyday — a much lighter lift. So...meet your cross functional collaborators where they work by integrating your Trust Center to Salesforce, Slack, Hubspot, Teams and other tools. Tag team members for reviews. Send lingering questionnaire answers needed via Slack. Notify in Teams. Approve NDA requests in Salesforce. Help Sales and other teams adopt a proactive approach to using your Trust Center as they help you build customer trust. Otherwise, you'll have new technology headwinds that are hard to win.

6. Train your Sales team to proactively share your Trust Center early in the deal cycle and with renewals
Familiarize your Sales team with the Trust Center and all that lives within the knowledge library to save time in the deal cycle and eliminate the back and forth bottleneck. With a single source of truth, Sales can confidently provide accurate, up to date information that customers can self-serve to audit your security posture. The same applies to customer renewals. Enable sales to proactively send customers to your Trust Center as the contract term is coming to a close. Eliminate any potential friction between your company and a renewal with a proactive stance.

One of the most common myths...
If we don't answer the questions on our trust center, the questions won't come.

The reality: Proactive answering of questions reduces inbound questionnaires and builds customer trust faster.

7. Break down cross-functional silos to optimize trust center content
Inbound questionnaires have changed over time. They're no longer just security focused. They also ask about legal policies, privacy, product, HR, and more. Cross-team collaboration ensures everyone is on the same page and keeps Trust Center documentation up to date. Too many teams turn off customer visibility of legal, ESG, and even AI cards on their Trust Centers, but if you're not populating thorough information from business partners in these units, customer trust and deal cycles could be compromised.



8. In 2023, Legal and Privacy were leading questionnaire topics — now AI is paramount.
Everyone is nervous about whether their data is training your internal AI. Customers need upfront communication about your company's AI posture. Begin populating as much information as possible around AI today and continue adding to it as more context grows.

Trends and Insights for Security Teams to Apply

Demonstrating influence on revenue is of growing importance
With SafeBase's Salesforce integration, security teams can now see their direct impact on faster sales cycles and deals won. This helps position security as a revenue generator versus a cost center.

New questions around AI are leading to new standards and questionnaires
As AI gains momentum, the questions your customers are asking about AI are evolving in real time. Answer as much as you can today, and continue to build on that foundation as clarity unfolds.

Benchmark against your peers
How does your security team's efficiency and effectiveness stack up against the competition? Analytics dashboards should give you a landscape view of where you stand today, and areas of improvement.

The evolving role of CISO to Chief Trust Officer

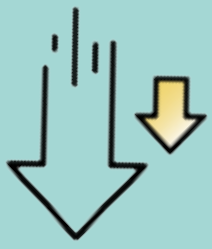
We've seen the evolution from CISO to CTrO percolating across the security landscape as leaders shift in perspective and responsibilities from a primarily technical role to a more strategic, business oriented position. In turn, focus is honing in on building and maintaining trust as a core business driver.

From CISO

Primarily focused on and oversees information security, cybersecurity, and protecting the organization's digital assets.

Often more technically oriented, focused on security operations and technologies.

A well established role in many organizations.



To CTrO

Broader focus on building and maintaining trust across the entire organization, including but not limited to security, privacy, ethics, compliance, and customer experience.

Business-oriented, acting as a go-to-market enabler and focusing on how trust impacts business objectives and revenue.

An emerging role that sometimes evolves from or incorporates the CISO role, reflecting a shift towards trust as a strategic imperative.

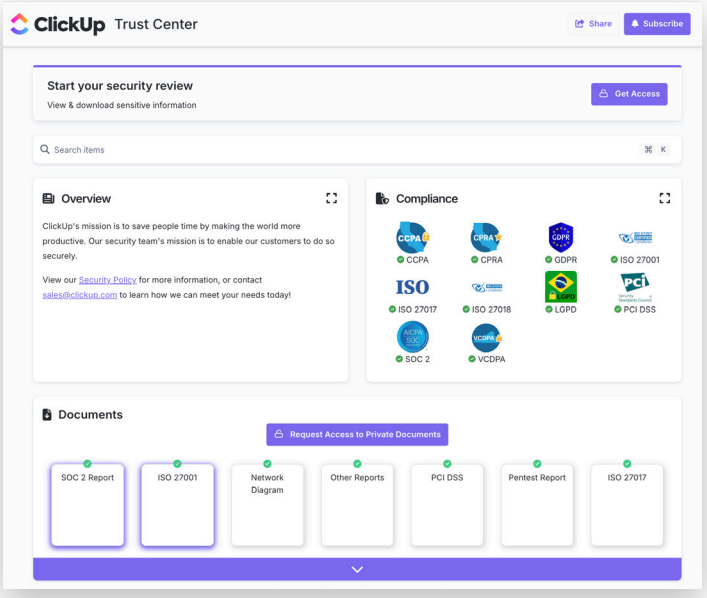
Remember...security is just one component of the larger trust umbrella.

As organizations explore this pivot, consider the following recommendations for the CISO leader

- **Broaden your focus** to encompass a wider range of trust-building initiatives including privacy, ethics, compliance, and customer experience.
- **Gain a deeper understanding of business operations** as well as product design and market dynamics. You'll be both a business leader and go-to-market enabler.
- **Become a translator** taking technical security measures and turning them into tangible trust building initiatives aligned to business objectives. Be ready to share those with a broad range of stakeholders — including the public.
- **Embrace trust as a competitive advantage** and driver of revenue vs a compliance requirement. Examine security, privacy, data, ethics, and ESG matters through a customer trust-centric lens.
- **Learn to measure and quantify trust** as well as its impact on business performance and customer relationships.

Trust is the foundation of every successful relationship.

By fostering collaboration across teams, leveraging AI for efficiency, and proactively addressing customer concerns, companies can create a culture of openness that not only enhances relationships with clients but also drives business success.



SAFEBASE

Built by trust-obsessed people for trust-minded organizations

The SafeBase Trust Center Platform streamlines the security review process by providing centralized, real-time access to up to date security and trust posture, compliance, and related documentation. Self-serve reviews are enabled with unified questionnaire management, and any remaining inbound questionnaires are answered by AI Questionnaire Assistance which cites Trust Center and Knowledge Base content — synced daily to ensure accuracy.

Robust permissioning helps teams confidently control access, and CRM integrations bring security reviews into go-to-market workflows driving quicker deals and higher win rates.

SafeBase collaboration features assigns questions to subject matter experts, specifies answer due dates, and notifies designated question owners to deliver a frictionless review process.

Analytics dashboards highlight security influenced revenue and share engagement data to inform your team on areas of focus for maximum impact.

Most importantly, your data never leaves your own private data store, and we never use it to train the AI. AI Questionnaire Assistance only pulls information to answer questionnaires with accuracy and speed.

Learn more at safebase.io

> Besides saving myself and our sales team time, it has increased customer confidence in our platform and shows one of our core values very transparently — Trust is Our Business. Our Security Portal puts that on display for all to see."

Chris Castaldo,
Chief Information Security Officer
CROSSBEAM

Ready to build customer trust, gain actionable insights, and prove security ROI with a SafeBase Trust Center Platform?

Book a Demo