



The Story of Six Touches: How Trust Portals Streamline Compliance

Compliance and Ethics

Technology, Privacy, and eCommerce



Banner artwork by U-STUDIOGRAPHY DD59 / *Shutterstock.com*

It was 5:30 pm on a Friday when sales emails and Slack messages lit up. A high-stakes deal, months in the making, was on the verge of falling apart. The customer's privacy and security diligence team would not sign off until a crucial compliance questionnaire was completed. The deal was stuck. Procurement deadlines loomed. The sales team scrambled. Legal and compliance teams braced for late-night negotiations.

But there was no shortcut. The customer's team was backlogged and unwilling to rush. The deal stalled, frustration mounted, and blame shifted to the negotiation team.

How did we get here? A broken diligence process.

The six touches

At many organizations, the customer diligence process is slow and frustrating because it isn't designed for efficiency. It often takes six distinct "touches" to simply exchange compliance materials — far more effort than most assume.

Here's how it typically unfolds:

1. **Customer security and privacy team** initiates diligence, requiring security, privacy, compliance, and technical documentation.
2. **Customer procurement team** relays requirements and technical security questionnaires to the business unit and seller.



SHARED

ASSESSMENTS

2023 SHARED ASSESSMENTS STANDARDIZED INFORMATION GATHERING (SIG) QUESTIONNAIRE

Version: 2023.09 Licensed to: NYSP

ASSEESEE INSTRUCTIONS FOR SIG QUESTIONNAIRE COMPLETION:	ISSUER/OUTSOURCER ADDITIONAL INFORMATION:
<p>Before You Start: Review the instructions provided by your Issuer/Outsourcer on how to answer the SIG. Issuer/Outsourcer should provide you with the scope of services for which to provide responses. The SIG is complex. If you did not receive instructions from your Issuer/Outsourcer it is recommended that you contact them before you start and seek guidance on how to proceed with the SIG to meet their needs.</p> <p>Don't be overwhelmed by the volume of questions. Some are filtering questions to remove out of scope services or have a question hierarchy to reduce the need to complete items that are not Primary or "parent" questions, indicated in bold, are followed by numbered sub or "child" questions. If a parent question is answered yes, child questions will display. There can be up to four generations of questions below a parent question.</p> <p>NOTE: To display all of the questions (parent, child, grandchild, etc.) disable macros when opening the file or select Disable from the File Automation dropdown on each risk domain worksheet.</p> <p>Steps for each SIG Worksheet:</p> <ol style="list-style-type: none"> 1) Complete the Business Information worksheet. Open the worksheet and complete all of the gray fields. It is recommended that you provide as much detail as possible in your responses. 2) Review and Complete the Documentation worksheets. Open the Documentation worksheet. Review the list of documents and complete all of the appropriate corporate policies and processes as listed on this worksheet. List the document's name in the gray field to correspond to the appropriate document list. This will allow the Outsourcer to identify the documents provided along with the completed SIG. Complete the documentation requested on the Documentation worksheet and update it with the documents provided. 3) Answer the Questions in each question worksheet, Risk Domain or SIG 2023. <ul style="list-style-type: none"> * The background color will change depending on the response provided. * If facial macros are enabled, then Child questions will either be displayed if the response is Yes or 	

Figure 1. Standardized security questionnaire

3. **Seller's account manager** receives the request and passes it along internally.
4. **Seller's compliance team** begins compiling documentation, often via a ticketing process.
5. **Legal team** negotiates an NDA to protect the materials.
6. **Cross-functional teams** (security, audit, compliance) scramble to address non-standard questions, pulling them away from their core responsibilities.

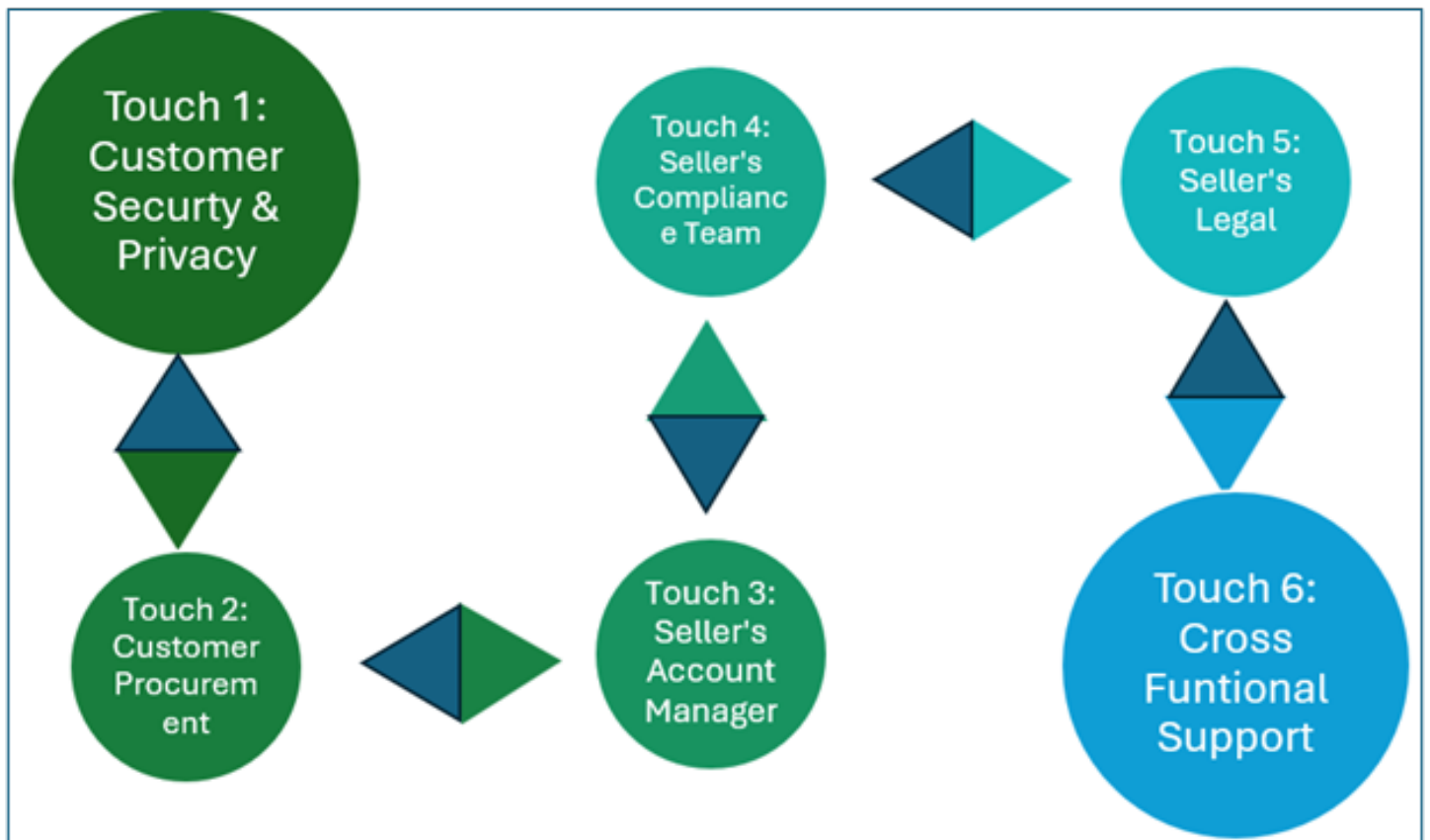


Figure 2. Six Points of Contact (Bidirectional Flow)

Each touchpoint risks delay, especially when teams juggle full workloads. At scale, the burden is amplified by:

-
- High volumes of security questionnaires;
 - Decentralized or inconsistent compliance documentation;
 - Integration issues following mergers and acquisitions; and
 - Evolving regulations like GDPR, AI governance, and new resilience frameworks.

Highly skilled professionals spend hours exchanging PDFs and spreadsheets, instead of driving strategic value.

[The 2025 ACC Chief Legal Officer Global Summit will be hosted in Barcelona, Spain, 21-23 May 2025. Register today!](#)

The trust portal solution

Trust portals streamline this entire process. A trust portal is a centralized, self-service hub where customers, vendors, and auditors access security, privacy, and compliance documentation.

Trust Center

Share

Subscribe

Start your security review

View & download sensitive information

Get access

Featured Documents

ARCHITECTURE, DATA FLOW & PEN TEST
Architecture Overview

ARCHITECTURE, DATA FLOW & PEN TEST
Penetration Test Reports

COMPLIANCE
SOC 2

SUSTAINABILITY
Everbridge Sustainability Library

Overview

At Everbridge, we strongly believe in transparency and open communication around our Security, Privacy, Compliance and Sustainability initiatives and processes. Instead of responding to individual customer questionnaires or answering detailed questions over email, we've published our policies and white papers that contain detailed answers to commonly asked questions provided by our experts. These materials are readily available for easy access, review, and download, and they provide more comprehensive answers than a questionnaire format permits.

Questionnaires: We have provided responses to industry

Compliance

C5

CCPA

EU-US DPF

FedRAMP
Moderate

G-Cloud

GDPR

HIPAA

ISO 22301

ISO 27001
SoA

ISO 27701

ISO 9001

Figure 3. Everbridge Trust Center (<https://trust.everbridge.com>)

With a trust portal, the process shrinks from six steps to two — without sacrificing thoroughness:

1. The customer accesses the trust portal.
2. They download exactly what they need.

```

graph LR
    A((Touch 1:  
Buyer  
Security &  
Privacy)) <--> B((Touch 2:  
Trust Portal))
  
```

This shift reduces friction, accelerates contracting, and gives customers immediate confidence in your organization's readiness. A modern trust portal provides:

- **Pre-populated standardized questionnaires** (SIG Lite, CAIQ, etc.);
- **Downloadable documentation** for common customer diligence needs;
- **A single source of truth** for compliance materials;
- **Version control and standardized updates**, reducing risk and rework; and
- **Engagement metrics** that offer insight into customer behavior.

Beyond compliance: Trust as a strategic asset

While trust portals were designed to streamline compliance, they deliver other unexpected and lasting benefits.

1. Customer trust becomes a competitive advantage

Transparency earns trust. Trust accelerates sales, improves customer satisfaction, and builds long-term loyalty. A trust portal signals commitment to accountability by giving customers easy, direct access to up-to-date information.

A trust portal signals commitment to accountability by giving customers easy, direct access to up-to-date information.

2. Support for broader commitments

A trust portal can also centralize:

- AI governance disclosures;
- ESG reports;and
- Other ethical and regulatory commitments.

3. Streamlined onboarding and renewals

Customers and internal teams alike benefit from clear, consistent, self-serve access to current

materials during onboarding and renewals — reducing errors, delays, and repetitive questions.

4. Security ratings integration

Portals can integrate security ratings (e.g., SecurityScorecard, BitSight, UpGuard) to objectively demonstrate the organization's security posture.

Operationalizing a trust portal

When are you ready?

Trust portals aren't just for the largest tech companies anymore. To be effective, you'll need:

- Mature documentation across security, privacy, compliance, and resilience programs; and
- Clear ownership from a leader capable of navigating internal teams and maintaining the portal.

If your programs are still maturing, the promise of efficiency can actually drive better internal alignment.

Build vs. buy

We explored both options when implementing our own trust portal. Initially, we built a basic portal on our customer service platform. It worked — but had limitations:

- Manual onboarding;
- No NDA workflows;
- No usage metrics; and
- No integrated version control.

Ultimately, we realized the trust portal isn't just a compliance tool — it's one of the first impressions we make on customers. Given its direct impact on trust and deal velocity, we needed something purpose-built for their needs.

We evaluated several vendors, including SafeBase, Whistic, Vanta, and SecurityPal, and selected a commercial solution that delivered:

- NDA gating, watermarking, and download logging;

-
- Metrics on customer engagement; and
 - Seamless customer access with minimal manual work.

For organizations considering the same choice, the key question is not just about cost or control, but about elevating the customer experience during the most sensitive part of the relationship — procurement and diligence.

Implementing the portal

We recommend a phased approach:

1. Prioritize content most critical to the sales cycle.
2. Develop governance for content maintenance.
3. Train internal teams through enablement programs.
4. Use external communications (customer updates, social media) to promote the portal.

Cultural change is just as important as technical implementation. We built a sales enablement course to equip our teams with:

- The value proposition of the portal;
- Customer-facing email templates; and
- Talking points.

The future of trust portals

What's next? AI-powered portals. Instead of static repositories, future portals will:

- Auto-complete customer questionnaires;
 - Integrate with audit workflows;
 - Surface live metrics on security, compliance, and resilience; and
 - Enable real-time Q&A via AI chatbots.
-

Organizations investing in trust portals today are preparing for this smarter, faster future.

Trust portals turn bureaucratic friction into strategic advantage. Deals close faster, customers self-serve with confidence, and highly skilled teams focus on creating value — not routing PDFs.

Perhaps most importantly, with a trust portal, there will be fewer Friday night surprises.

[Join ACC](#)

Disclaimer: The information in any resource in this website should not be construed as legal advice or as a legal opinion on specific facts, and should not be considered representing the views of its authors, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical guidance and references for the busy in-house practitioner and other readers.

[Noah Webster](#)



Chief Legal and Compliance Officer

Everbridge

Noah Webster is chief legal & compliance officer for Everbridge, a global software company that empowers enterprises and government organizations to anticipate, mitigate, respond to, and recover stronger from critical events. In today's unpredictable world, resilient organizations minimize impact to people and operations, absorb stress, and return to productivity faster when deploying critical event management (CEM) technology. Everbridge digitizes organizational resilience by combining intelligent automation with the industry's most comprehensive risk data to Keep People Safe and Organizations Running.

[Andrew Evangelos](#)



Director of Sales Engineering

Everbridge

Andrew Evangelos is the senior director of sales engineering at Everbridge. He is responsible for the pre-sales program that supports Everbridge's customer facing teams with technical knowledge, RFP support, and presales security and compliance. With over a dozen years at Everbridge, he has helped the organization grow from a startup Mass Notification vendor to the world's leading provider of Critical Event Management solutions that enable customers to get better outcomes when they face the most challenging and potentially dangerous situations.

LinkedIn: <https://www.linkedin.com/in/andrew-evangelos/>

[Jeremy Capell](#)



Chief Trust Officer

Everbridge

Jeremy Capell is the chief trust officer at Everbridge. Previously, he served as the company's chief information security officer. Prior to his roles at Everbridge, Capell served as the vice president of Wireless Information Security at DISH Network Corporation, holding two patents in 5G security, and VP of Cyber Resilience at Dimension Data.

Capell is an acclaimed leader in the cyber and resilience industry. Capell received the 40 under 40 Award by the Denver Business Journal for his contributions to the security industry.

Over his 20+ year career, his leadership and practical experience includes running internal security teams, leading managed security services, and building large resilience consulting teams.

He has been a technology speaker at a number of events including ISSA and MSSF, and has been featured on prestigious global events, including Mobile World Congress and Ignite, for his insights into securing 5G technology.

Capell has evolved from traditional security team and expanded his focus, bring security, privacy, compliance and resilience into a single focus on fostering "Trust".

An immigrant from South Africa, recognized internationally as an acclaimed resilience leader, Capell

was key in developing the African cyber resilience industry, resulting in his receiving the 2017 London-based award for the African Industry Personality.

Capell earned a degree in informatics, IT management, and business management from the University of Johannesburg.