UpGuard

What to Expect During Your Security Review

Security reviews are an important part of how organizations assess vendor security and manage third-party risk. Your customer uses UpGuard to manage their cyber risk program and vendor assessments, giving you a faster, more efficient way to complete your security review in one purpose-built platform rather than juggling spreadsheets and emails.

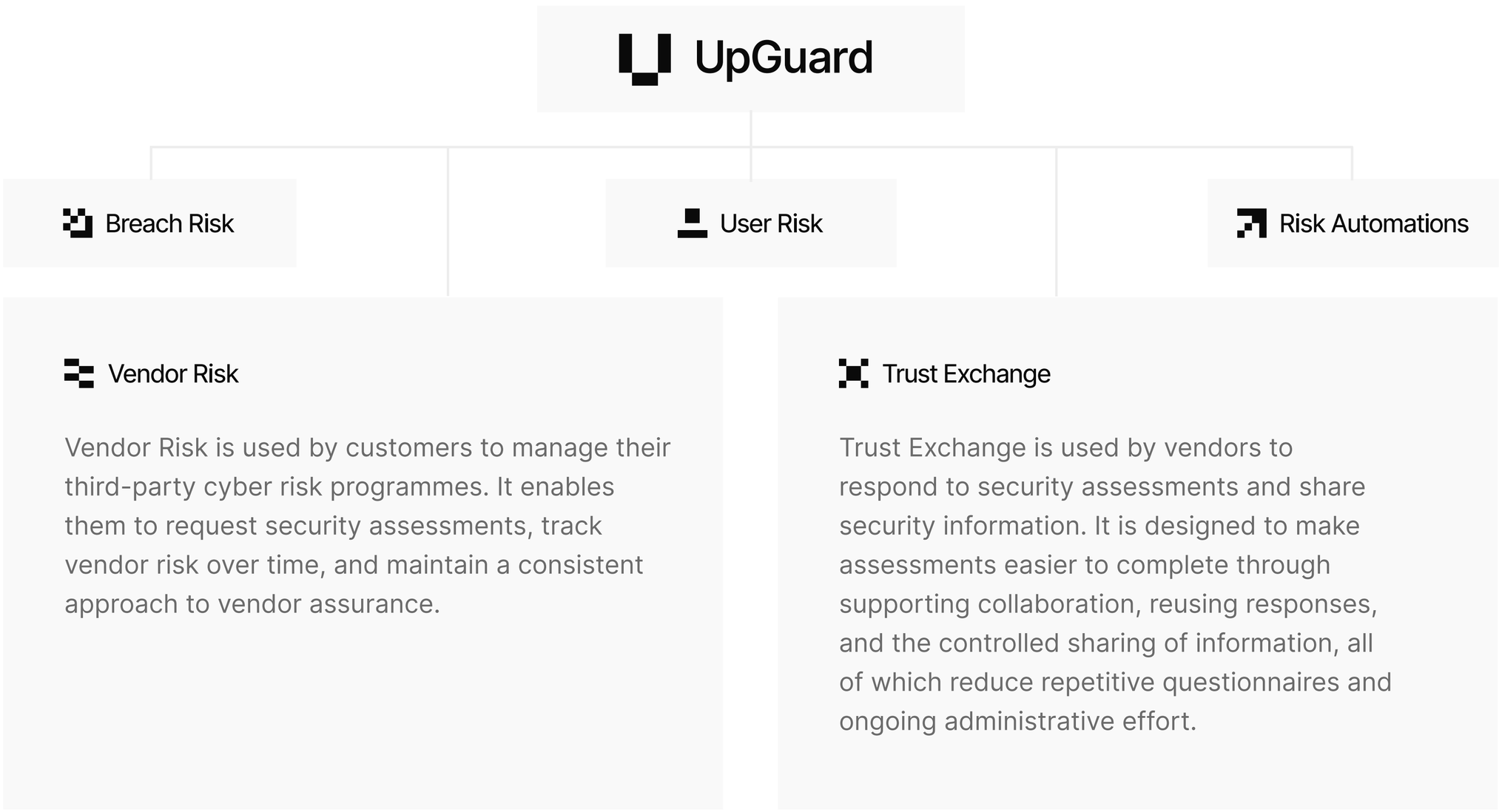
A security review may include one or more of the following: completing a security questionnaire, sharing supporting documentation, or responding to follow-up questions. The exact requirements will be defined by your customer as part of their security review.

This guide walks you through the steps involved, explains how UpGuard is used during the assessment process, and highlights how you can fast-track this and subsequent security reviews.

About UpGuard

UpGuard is a cyber risk management platform used by organizations to assess and manage security risk across their vendors, external attack surface, and internal environment. More than 45,000 companies worldwide have used UpGuard.

UpGuard offers a suite of products, each designed to support a specific aspect of cyber risk management. For this security review, two products are relevant: Vendor Risk and Trust Exchange, which together support how organizations request, manage, and complete vendor security assessments.



How to complete your security review

Your customer will initiate a security assessment through UpGuard. You'll respond to that request in Trust Exchange, where you can manage and share security information with your customer in a single place.

Trust Exchange supports collaboration with colleagues, reuse of responses across requests, and control over which customers can access your information, helping to reduce the manual effort typically involved in security reviews. In fact, 39% of questionnaires completed using Trust Exchange AI Autofill are submitted within two days, compared to a typical turnaround of around three weeks.

Security review steps:

1. Receive email invitation from your customer via UpGuard
2. Create your free Trust Exchange account
3. Collaborate on the request securely in-platform with your team and your customer
4. Use Trust Exchange to streamline future security assessments—even those not initiated via UpGuard

Trust Exchange can be used at no cost for this assessment. Optional paid capabilities are available if you choose to upgrade. More information about Trust Exchange is available on our website.

UpGuard’s security ethos

Sharing security information or uploading confidential documentation as part of a review can raise reasonable questions about how that information will be handled. This section explains how information shared during the security review through UpGuard is protected.

Governance, compliance, and oversight

Security underpins how UpGuard designs, builds, and operates its platform. Privacy, data protection, and regulatory compliance are embedded into day-to-day operations through defined policies, processes, and technical controls, with clear ownership and accountability.

UpGuard maintains a formal security program aligned with ISO/IEC 27001, controls are independently assessed through an annual SOC 2 Type II audit, and UpGuard also undergoes annual third-party application penetration testing.

For more information, visit our Security Page or Trust Page.

Secure development practices

UpGuard follows a Secure Software Development Lifecycle (SSDLC), embedding security throughout design, development, testing, and deployment. Development practices align with OWASP Secure Coding Practices.

New functionality is subject to peer review and automated testing prior to release. Code and third-party dependencies are regularly reviewed and scanned to identify and remediate potential vulnerabilities.

How we safeguard your data

UpGuard protects customer data through secure infrastructure, strong access controls, and secure software development practices.

The platform is hosted on the Google Cloud Platform (GCP) and deployed using Kubernetes-managed containers. Google Cloud provides a secure and resilient infrastructure designed to protect data from unauthorized access, intrusion, and service disruption, and maintains independent compliance certifications including SOC 2 and ISO 27001. Further detail is available in Google Cloud’s public compliance and security documentation.

Customer data is encrypted in transit and at rest. Access to systems and data is restricted on a least-privilege basis, with employees required to use multi-factor authentication and granted only the access required to perform their authorised duties.

UpGuard maintains audit logging to provide visibility into system and user activity. Application logs are retained for 180 days and security logs for 400 days, with continuous monitoring and alerting in place.

Controlling access to your information

Access controls and sharing permissions

Trust Exchange provides granular access controls so you remain in control of who can view your responses and shared documentation. Information is logically segregated between customers, ensuring only authorised parties can access what you choose to share.

You decide what information is shared, with whom, and when, and can update or revoke access as needed.

AI-assisted features in Trust Exchange

Trust Exchange includes AI-assisted features designed to reduce manual effort while keeping you in control. These features are delivered using OpenAI's Enterprise API. Features such as AI Autofill and AI Enhance assist with drafting and refining questionnaire responses based only on the information you choose to provide. All AI-generated output requires human review and approval before it can be shared. You can learn more about Trust Exchange's AI features in our Help Centre article.

UpGuard does not build, train, or fine-tune its own AI models, and customer data is never used to train any AI model. When AI features are used, relevant data is sent securely to OpenAI via encrypted APIs for that specific request only. Contractual and technical controls prohibit any use of customer data for model training or secondary purposes. For more information about OpenAI's security practices visit their privacy page.

Use of AI features is optional. AI-powered capabilities are clearly labelled, and account administrators may request that AI features be disabled across their account.

Helping 12,000+ security professionals work smarter

Using UpGuard allows you to complete security reviews in a structured, central platform rather than across emails or spreadsheets, helping reduce manual effort and repeated requests over time. Throughout the process, you remain in control of what information is shared, who can access it, and when.

Once submitted, your responses are available for reuse and can be updated as your security posture changes, making future security reviews faster and easier to manage.

If you have any questions, need help completing the review, or want to better understand how information is handled in UpGuard, additional resources and support are available below.

- UpGuard Security Page
- UpGuard's Trust Page
- Trust Exchange product overview
- UpGuard AI FAQs
- Google Cloud's Security page
- Open AI's enterprise-grade privacy commitments

If you need help during the review, contact us at support@upguard.com