How can you trust a vendor?

Independent external assessments of vendors can reveal some of their operational and security practices, and often telegraph the state of their internal environment. However, external assessments only see the perimeter. For a true risk assessment, vendors are often asked to answer a series of questions about their methods, software, and vendors, so that the company contracting them can get visibility into the environment which will be handling their data.

The importance of such questionnaires are probably self-evident, but the difficulties they entail may not be— unless you’ve ever done it. Writing, sending, and reviewing vendor questionnaires is a time consuming process for a company— and when that company has several dozen, hundred, or even thousand vendors, it becomes a logistical impossibility to thoroughly manage them all and keep track of technical self-assessments, making the entire exercise performative, and without real value.

UpGuard CyberRisk platform

UpGuard’s CyberRisk product not only performs a thorough external assessment and scoring of vendors, but automates the questionnaire process and integrates it into the product itself, creating a single intuitive repository for vendor assessment data. UpGuard offers a selection of prepared questionnaires that cover every area of vendor cyber risk.

Sending them out is as easy as creating a contact email for a vendor and clicking a button. Questionnaires are then stored in UpGuard and tracked over time, automatically renewed at your specified interval to keep answers up to date and create a defensible record of vendor due diligence.
Total coverage

Why it matters

The questionnaires provided by UpGuard cover every area of risk, from web applications to physical security. Total coverage is important, because a vendor risk assessment that fails to account for some vector of risk is incomplete, and blindspots can create massive vulnerabilities that fly under the radar, despite best efforts to secure that which is being covered.

Because of this breadth of coverage, UpGuard’s questionnaires are flexible enough to adapt to each business and get the information they care about from the vendors handling their data.

We’ll look at the core questionnaires provided in UpGuard CyberRisk and how organizations can customize them for optimal assessment.

Web application security

For vendors providing a service through a web application, we provide a questionnaire that covers every surface of web application and data storage risk. With this questionnaire we can answer the following kinds of questions:

• Does the web application use proper encryption to protect client traffic?
• Is the authentication mechanism used to access sensitive data secure?
• What vendors are used by the application? (Cloud providers, for example)
• Does the application contain known vulnerabilities with available exploits?
• Do the operational methods of the vendor minimize the risk of data exposure? (For example, do they test their configurations as part of the deployment process?)

Infrastructure security

For vendors that will be hosting data or services in their data center, UpGuard provides a questionnaire that validates network and server technology and processes. The Infrastructure Security questionnaire can help answer:

• Does the web application use proper encryption to protect client traffic?
• Does the vendor have a network policy that protects customer data?
• Are best practice network defenses in place and properly configured?
• How are servers hosting customer data and services hardened against attack?
• Is access to customer data within the vendor limited to the appropriate people?
• What are the vendor’s backup and recovery methods?
Physical & data center security

Cybersecurity has to encompass old-fashioned physical security to protect assets against theft and fraud from both insiders and attackers.

This UpGuard questionnaire details the vendor’s physical security practices and measures the risk of their access control, answering questions like:

- Are vendor facilities exclusive, or shared with other tenants?
- How are technological assets secured against theft and tampering?
- Is the vendor data center local, in the cloud, or hybrid?
- Does the vendor have a written security policy for office facilities?
- What parts of the data center are outsourced, if any?

Security and privacy programs

While the other core questionnaires focus on operational practices and technology, this questionnaire helps understand what active measures a vendor takes to protect customer assets from cyber attacks and misuse.

This UpGuard questionnaire can answer important questions about vendor risk mitigation and security controls, including:

- Does the vendor perform internal and/or third party audits of systems and data?
- How does the vendor manage risk in their vendors?
- What does the vendor do in the event of a data breach?
- Does the vendor have a resilient change management process?
- Are best practices followed regarding internal access controls and least privilege?
Custom tailored

These core questionnaires cover the digital environment in general terms, but every vendor is different, and every company cares about different things from their vendors. This is why UpGuard provides customization options for vendor questionnaires, so that information can be tailored to specific concerns, without overwhelming either party with irrelevant technical details.

What the vendor sees

To reduce the amount of time necessary to complete and review questionnaires, our forms change dynamically based on how questions are answered so that non-applicable information isn’t asked for or gathered. It’s not just about asking and answering questions either.

As a vendor answers the questionnaire, risks are pointed out to them with severity ratings, along with notes about why their answer is risky and what can be done to mitigate it. When the questionnaire is opened by the vendor, the status within UpGuard changes to “in progress,” so you can better understand the questionnaire workflow. Vendors can access a read only version of completed questionnaires at any time by using a link provided to them in email.
Vendor contacts

Create email contacts for each vendor within UpGuard to track contact points for questionnaires and other communication.

Questionnaires are sent per contact, so different questionnaires can be given to different people at the same vendor if, for example, different teams handle web applications and physical security. This granularity ensures that everybody does only the necessary work relevant to the relationship at hand.

External assessment

UpGuard CyberRisk performs continuous external assessment of all internet facing domains for all vendors to ensure up to date risk profiles. Every vendor is ranked using CSTAR, UpGuard’s risk scoring engine, and given a score between 0-950, like a credit score. The score provides the high level overview of vendor risk, while the CyberRisk interface can drill down into details, and offer suggestions on how to remediate problems.

Questionnaire results

Completed questionnaires are stored in UpGuard for each vendor, and available for review at any time. When viewing a completed questionnaire, the same feedback given to the vendor is available for review, so the risks of that vendor can be better understood, along with what it takes to fix them. Answers that don’t meet security best practices or otherwise introduce cyber risk are clearly flagged and categorized into three severity levels.

Recorded and tracked over time

UpGuard acts as an automated system of record for vendor security assessments and third party due diligence. In the event of a third party breach or data exposure, these assessments can be used in forensics to understand vendor claims and practices. UpGuard tracks vendors over time, showing the trends and trajectory of their risk profile. By retaining questionnaires for the entirety of the vendor relationship, UpGuard is able to detect variance in vendor status, so that changes in a vendor’s reported practices and policies don’t go undetected.
Auto-renewal

Manual renewal is unsustainable

While an initial questionnaire is crucial to determine whether a vendor relationship is feasible, refreshing questionnaires at regular intervals helps ensure that the most up-to-date information is available, and that changes to the initial acceptable questionnaire are noted and understood. But renewing questionnaires at scale requires a massive amount of work and documentation, most of which goes undone, as tedious due diligence tends to fall to the bottom of the priority list when things are hectic—even when compliance regulations require regular reassessment.

How UpGuard helps

UpGuard handles questionnaire renewal automatically, keeping track of which vendors need to be renewed, and automatically sending the selected questionnaires to the appropriate contact.

Renewals are stored alongside originals so the full documentation trail is available for each vendor, and changes in policy can be mapped out easily. UpGuard will also automatically remind vendors to complete their assessments on a regular schedule, to help move the process along to completion without manual intervention.

Conclusion

Managing third and fourth party cyber risk shouldn’t be difficult. In fact, it can’t be difficult to function effectively, especially at scale. UpGuard consolidates and automates the vendor assessment process to document, understand, and explain the possible ways in which an organization’s data and technology can be damaged by third parties.

By performing a comprehensive technical assessment and providing integrated questionnaire services, UpGuard allows vendors to be managed at scale without special technical knowledge, while providing technical users with the details they need to make better decisions.
About UpGuard

UpGuard's products provide a better, smarter way to automate cybersecurity risk assessments and prevent breaches

UpGuard is a cybersecurity company that helps businesses manage IT security risks, both internally and in the supply chain. UpGuard’s integrated risk platform combines third party security ratings, security assessment questionnaires, and proactive threat intelligence capabilities to give businesses a full and comprehensive view of their risk surface.

UpGuard VendorRisk

Monitor your third-party vendors

UpGuard VendorRisk monitors, rates and sends targeted security questionnaires to your vendors. We also automate security questionnaires so you don’t have to.

- Automated vendor reports and scoring
- Intelligent questionnaire engine
- 3rd and 4th party supply chain analysis
- Industry benchmarking and classification

UpGuard BreachSight

Monitor your external security posture

UpGuard BreachSight continuously monitors your business for data exposures, enabling you to prevent breaches, protect your reputation and avoid regulatory fines.

- Continuous monitoring of your digital posture
- Modular plugins for new security vectors
- Billions of signals being discovered daily
- Remediation workflow automation

UpGuard Core

Monitor your internal IT infrastructure

UpGuard Core automates internal security and compliance for enterprises with hybrid on-premise/cloud IT, giving you instant visibility into your entire infrastructure.

- Automated security configuration monitoring
- Agent and agentless data collection
- Smart infrastructure policy and scoring
- Change detection and compliance
About UpGuard cybersecurity ratings

UpGuard Cyber Security Ratings (CSR)

Historically, cyber risk has been measured through a combination of manual processes such as employee surveys and rudimentary automated scanning. However, without reliable, comparable risk assessments, organizations cannot benchmark their cybersecurity performance and improve it over time.

UpGuard Cyber Security Ratings (CSR) are a single, easy-to-understand score from 0-950 that represent an organization’s cybersecurity performance. Similar to a consumer credit score for cybersecurity, a higher rating represents better performance. UpGuard CSR also takes into account historical security performance and performance over time.

Based on millions of data points, we calculate an instant snapshot of each company that covers the following basic elements of security:

- Security misconfigurations
- Indicators of malware, phishing, and similar attacks
- Susceptibility to web vulnerabilities
- Weaknesses in security practices and hygiene
- What parts of the data center are outsourced, if any?
Know your vendors. Secure yourself.

Looking for a better, smarter way to protect your data and prevent breaches?

UpGuard offers a full suite of products for security, risk and vendor management teams.

Book a demo  Learn more