Whitepaper

Ultimate Guide to Security Questionnaires

How to accurately evaluate vendor security in an age of accelerating digital transformation.
# Table of Contents

The importance of security questionnaires  
What are security questionnaires?  
Why perform cyber risk assessments?  
How to perform a third-party risk assessment  
   Step 1: Identify all critical assets  
   Step 2: Identify each asset's information value  
   Step 3: Identify all potential cyber threats  
   Step 4: Identify all vulnerabilities  
   Step 5: Analyze controls and implement new controls  
   Step 6: Calculate the likelihood and impact of various scenarios  
   Step 7: Prioritize risks based on the cost vs value  
   Step 8: Send security questionnaires  
Limitations of security questionnaires  
The future of security questionnaires  
UpGuard: The future of security questionnaires  
   Customizable security questionnaires  
   Digital risk assessment management  
   How to perform risk assessments with a custom questionnaire  
   Question styles
The importance of security questionnaires

Vendor relationships have become a standard feature of the new business model. By outsourcing processes to third parties, organizations can expand their expertise across any industry while keeping overheads lean.

The transition to cloud technology has further sharpened this process, making scaling a faster and more streamlined process.

But the enhanced fluidity of vendor onboarding has forged a menacing category of digital risk known as third-party risks. Third-party risks are now the primary exploits threatening an organization's security posture.

Organizations have a 27.7% chance of suffering a data breach (an increase of 2.7% compared to 2019), and 58% of these breaches involve third parties.

Non-intrusive security solutions (such as security ratings) provide an outside-in view of a vendor's cybersecurity posture. Security ratings offer a leading indicator that trouble may lay ahead but alone, ratings do not provide in-depth visibility of a vendor's security policies or risk mitigation strategies. To mitigate the prevalent risk of a breach, onboarding and ongoing management of vendors should involve a thorough evaluation of security policies and procedures.
Security questionnaires help meet this critical requirement. Questionnaires exist to identify any compliance gaps within third-party networks.

Vendor security assessment questionnaires empower organizations to scrutinize the security postures of potential vendors before entrusting them with sensitive data.

To maximize data collection efficiency and encourage vendors to respond, questionnaires are often standardized according to third-party security standards or regulatory requirements.

While using standardized questionnaires is the recommended strategy for the majority of organizations, many enterprises need the additional flexibility of customized questionnaires. Customization is often driven by complex regulatory requirements, business needs, or specific risk appetite.

In this whitepaper, both security questionnaire alternatives (standardized, custom) will be discussed.
What are security questionnaires?

Security questionnaires, also known as risk assessments, evaluate a vendor’s approach to cybersecurity. Their objective is to discover any vulnerabilities that could result in a third-party breach.

If distributed promptly, security questionnaires empower organizations to uncover and remediate third-party risks before they’re discovered and exploited by cybercriminals.

Besides discovering third-party attack surface exposures, security questionnaires also help organizations achieve regulatory compliance.

There are at least 19 globally recognized cybersecurity regulatory and compliance frameworks. Every country has multiple regulatory authorities, typically spanning citizen privacy, financial services, healthcare and energy industries. Each authority may have multiple regulatory regimes that require compliance. So the problem of demonstrating regulatory compliance is exponential for organizations that operate across multiple jurisdictions.

NIST CSF

1. Security and Privacy Programs Assessment

1.1. Security and Privacy

Why this section matters: An information security and privacy program is a comprehensive set of policies, guidelines, and processes for identifying and addressing the threats and risks to company information and systems. An established security and privacy program can help assure customers that their information will be safe while it’s in your custody.

1.1.1. Does your company have a strong, established security program, and does the scope of the program include all information processed within the organization?

☑ Yes, our security program covers all aspects of information security within the organization.
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>CIS Controls</td>
<td>Center for Internet Security Controls</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>HITECH</td>
<td>Omnibus Rule</td>
</tr>
<tr>
<td>PCI-DSS</td>
<td>The Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>CCPA</td>
<td>California Consumer Privacy Act</td>
</tr>
<tr>
<td>AICPA</td>
<td>American Institute of Certified Public Accountants</td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes-Oxley Act</td>
</tr>
<tr>
<td>COBIT</td>
<td>Control Objectives for Information and Related Technologies</td>
</tr>
<tr>
<td>GLBA</td>
<td>Gramm-Leach-Bliley Act</td>
</tr>
<tr>
<td>FedRAMP</td>
<td>The Federal Risk and Authorization Management Program</td>
</tr>
<tr>
<td>FERPA</td>
<td>The Family Educational Rights and Privacy Act of 1974</td>
</tr>
<tr>
<td>ITAR</td>
<td>International Traffic in Arms Regulation</td>
</tr>
<tr>
<td>COPPA</td>
<td>Childern's Online Privacy Protection Rule</td>
</tr>
<tr>
<td>NERC CIP Standards</td>
<td>NERC Critical Infrastructure Protection Standards</td>
</tr>
<tr>
<td>APRA</td>
<td>The Australian Prudential Regulation Authority</td>
</tr>
</tbody>
</table>
Why perform cyber risk assessments?

Risk assessments shouldn’t only be performed when they’re enforced, they should be a standard protocol of vendor due diligence efforts.

The following list outlines some of the benefits of security questionnaires:

1. **Reduction of long-term costs**

   The global average cost of a data breach is expected to reach $6 trillion by the end of 2021. Security questionnaires empower organizations to remediate third-party exposures before they develop into costly breaches.

2. **Better organizational knowledge**

   By continuously identifying new vendor vulnerabilities, security questionnaire keep organizations aware of all risk in their vendor network.

3. **Avoid regulatory fines**

   When poor compliance leads to customer data theft, the resulting regulatory fines are astronomical. For example, the maximum GDPR fine is €20 million, or 4% of annual global revenue.

4. **Avoid application downtime**

   Internal or customer-facing systems need to be available and functioning for staff and customers to do their jobs.

5. **Data loss**

   By mitigating third-party breaches, the theft of trade secrets and intellectual data is also minimized.
Step-by-step guide

How to perform a third-party risk assessment

The primary purpose of a cyber risk assessment is to help inform decision-makers and support proper risk responses. They also provide an executive summary to help executives and directors make informed decisions about security.

To identify the specific risk assessment frameworks that apply to your organization, you must first establish a rough evaluation of your security posture.

The following workflow will identify the critical exposures in your ecosystem and highlight the risk assessment frameworks most relevant to your organization.
Step 1
Identify all critical assets

The first step is to identify assets to evaluate and determine the scope of the assessment. This will allow you to prioritize which assets to assess. You may not want to perform an assessment on every building, employee, electronic data, trade secret, vehicle, and piece of office equipment. Remember, not all assets have the same value.

You need to work with business users and management to create a list of all valuable assets. For each asset, gather the following information where applicable:

- Software
- Hardware
- Data
- Interface
- End-users
- Support personal
- Purpose
- Criticality
- Functional requirements
- IT security policies
- IT security architecture
- Network topology
- Information storage protection
- Information flow
- Technical security controls
- Physical security controls
- Environmental security
Step 2

Identify each asset’s information value

Most organizations don't have an unlimited budget for information risk management so it's best to limit your scope to the most business-critical assets.

To save time and money later, spend some time defining a standard for determining the importance of an asset. Most organizations include asset value, legal standing and business importance. Once the standard is formally incorporated into the organization's information risk management policy, use it to classify each asset as critical, major or minor.

There are many questions you can ask to determine value:

- Are there financial or legal penalties associated with exposing or losing this information?
- How valuable is this information to a competitor?
- Could we recreate this information from scratch? How long would it take and what would be the associated costs?
- Would losing this information have an impact on revenue or profitability?
- Would losing this data impact day-to-day business operations? Could your staff work without it?
- What would be the reputational damage of this data being leaked?
Step 3

Identify all potential cyber threats

A cyber threat is any vulnerability that could be exploited to breach security to cause harm or steal data from your organization. While hackers, malware, and other IT security risks leap to mind, there are many other threats:

<table>
<thead>
<tr>
<th>Natural disasters</th>
<th>Floods, hurricanes, earthquakes, lightning, and fire can destroy as much as any cyber attacker. You can not only lose data but servers too. When deciding between on-premise and cloud-based servers, think about the chance of natural disasters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>System failure</td>
<td>Are your most critical systems running on high-quality equipment? Do they have good support?</td>
</tr>
<tr>
<td>Human error</td>
<td>Are your S3 buckets holding sensitive information properly configured? Does your organization have proper education around malware, phishing and social engineering?</td>
</tr>
<tr>
<td></td>
<td>Anyone can accidentally click a malware link or enter their credentials into a phishing scam. You need to have strong IT security controls including regular data backups, password managers, etc.</td>
</tr>
<tr>
<td>Adversarial threats</td>
<td>Third party vendors, insiders, trusted insiders, privileged insiders, established hacker collectives, ad hoc groups, corporate espionage, suppliers, nation-states.</td>
</tr>
</tbody>
</table>
Some common threats that affect every organization include:

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access</td>
<td>Both from attackers, malware, employee error.</td>
</tr>
<tr>
<td>Misuse of information by authorized users</td>
<td>Typically an insider threat where data is altered, deleted or used without approval.</td>
</tr>
<tr>
<td>Data leaks</td>
<td>Personally identifiable information (PII) and other sensitive data, by attackers or via poor configuration of cloud services.</td>
</tr>
<tr>
<td>Loss of data</td>
<td>Organization loses or accidentally deleted data as part of poor backup or replication.</td>
</tr>
<tr>
<td>Service destruction</td>
<td>Loss of revenue or reputational damage due to downtime.</td>
</tr>
</tbody>
</table>

After you've identified the threats facing your organization, you'll need to assess their impact.
Step 4

Identify all vulnerabilities

Now it's time to move from what "could" happen to what has a chance of happening. A vulnerability is a weakness that a threat can exploit to breach security, harm your organization, or steal sensitive data.

Vulnerabilities are found through vulnerability analysis, audit reports, the National Institute for Standards and Technology (NIST) vulnerability database, vendor data, incident response teams, and software security analysis.

You can reduce organizational software-based vulnerabilities with proper patch management via automatic forced updates. But don't forget physical vulnerabilities, the chance of someone gaining access to an organization's computing system is reduced by having keycard access.

Step 5

Analyze controls and implement new controls

Analyze controls that are in place to minimize or eliminate the probability of a threat or vulnerability. Controls can be implemented through technical means, such as hardware or software, encryption, intrusion detection mechanisms, two-factor authentication, automatic updates, continuous data leak detection or through nontechnical means like security policies and physical mechanisms like locks or keycard access.

Controls should be classified as preventative or detective controls. Preventative controls attempt to stop attacks like encryption, antivirus or continuous security monitoring, detective controls try to discover when an attack has occurred like continuous data exposure detection.
Step 6

Calculate the likelihood and impact of various scenarios on a per-year basis

Now you know the information value, threats, vulnerabilities and controls, the next step is to identify how likely these cyber risks are to occur and their impact if they happen. It's not just whether you might face one of these events at some point, but what it's potential for success could be. You can then use these inputs to determine how much to spend to mitigate each of your identified cyber risks.

Imagine you have a database that stores all your company's most sensitive information and that information is valued at $100 million based on your estimates.

You estimate that in the event of a breach, at least half of your data would be exposed before it could be contained. This results in an estimated loss of $50 million. But you expect that this is unlikely to occur, say a one in fifty-year occurrence. Resulting in an estimated loss of $50m every 50 years or in annual terms, $1 million every year.
Step 7

Prioritize risks based on the cost of prevention vs information value

Use risk level as a basis and determine actions for senior management or other responsible individuals to mitigate the risk. Here are some general guidelines:

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Corrective measures to be developed as soon as possible.</td>
</tr>
<tr>
<td>Medium</td>
<td>Correct measures developed within a reasonable period of time.</td>
</tr>
<tr>
<td>Low</td>
<td>Decide whether to accept the risk or mitigate.</td>
</tr>
</tbody>
</table>

Remember, you have now determined the value of the asset and how much you could spend to protect it. The next step is easy: if it costs more to protect the asset than it's worth, it may not make sense to use a preventative control to protect it. That said, remember there could be reputational impact not just financial impact so it is important to factor that in too.

- Organizational policies
- Reputational damage
- Feasibility
- Regulations
- Effectiveness of controls
- Safety
- Reliability
- Organizational attitude towards risk
- Tolerance for uncertainty regarding risk factors
- The organizational weighting of risk factors
### Step 8

**Send security questionnaires**

With the details of all third-party risks outlined, you can now send the appropriate security questionnaire to each of your vendors.

The UpGuard platform enables users to select from 18 different questionnaires (outlined below) many of which map directly to cybersecurity risk frameworks. Some questionnaires are mandatory for specific industries, but organizations are free to use any questionnaire that best meets the protection requirements identified through the preceding steps.

<table>
<thead>
<tr>
<th>Questionnaire</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CyberRisk Questionnaire</strong></td>
<td>Provides a comprehensive assessment of an organization's security posture, from their policy framework right down to their technical controls. It comprises four sections: Security and Privacy Programs, Physical and Data Center, Infrastructure, and Web Application.</td>
</tr>
<tr>
<td><strong>ISO 27001 Questionnaire</strong></td>
<td>Assesses an organization's security posture against the ISO 27001 standard with risks mapped against ISO 27001 domains. It is also suitable for the assessment of APRA CPS 234 requirements.</td>
</tr>
<tr>
<td><strong>Short Form Questionnaire</strong></td>
<td>A condensed version of the CyberRisk Questionnaire, designed to be sent to smaller organizations. It focuses on the information security risks smaller organizations are typically exposed to, such as their back up process and email security concerns, while avoiding areas where small organizations are typically less mature (such as their information security policy framework).</td>
</tr>
<tr>
<td>Questionnaire</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NIST Cybersecurity Framework Questionnaire</td>
<td>Assesses an organization's security posture against the NIST Cybersecurity Framework.</td>
</tr>
<tr>
<td>PCI DSS Questionnaire</td>
<td>Assess an organization's adherence to the twelve requirements of PCI DSS.</td>
</tr>
<tr>
<td>California Consumer Privacy Act (CCPA) Questionnaire</td>
<td>Assesses whether a vendor is compliant with the personal information disclosure requirements outlined in CCPA.</td>
</tr>
<tr>
<td>COBIT 5 Security Standard Questionnaire</td>
<td>Assesses compliance against the Control Objectives for Information and Related Technologies Framework created by ISACA.</td>
</tr>
<tr>
<td>ISA 62443-3-3:2013 Security Standard Questionnaire</td>
<td>Assesses compliance against technical control system requirements associated with the seven foundational requirements (FRs) described in IEC 62443-1-1.</td>
</tr>
<tr>
<td>GDPR Security Standard Questionnaire</td>
<td>Assesses compliance against the personal information disclosure requirements outlined in the European Union’s General Data Protection Regulation (GPDR).</td>
</tr>
<tr>
<td>Questionnaire</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>CIS Controls 7.1 Security Standard Questionnaire</strong></td>
<td>Assesses whether the vendor follows the best practice guidelines for cybersecurity outlined in 20 CIS Controls.</td>
</tr>
<tr>
<td><strong>NIST SP 800-53 Rev. 4 Security Standard Questionnaire</strong></td>
<td>Assesses compliance against the security and privacy controls required for all U.S. federal information systems except those related to national security.</td>
</tr>
<tr>
<td><strong>Modern Slavery Questionnaire</strong></td>
<td>Designed to identify modern slavery risks, address identified risks, and highlight areas requiring further due diligence.</td>
</tr>
<tr>
<td><strong>Pandemic Questionnaire</strong></td>
<td>Designed to help you assess the impact of any current or future pandemics.</td>
</tr>
<tr>
<td><strong>Security and Privacy Program Questionnaire</strong></td>
<td>Focuses solely on an organization's security and privacy program.</td>
</tr>
<tr>
<td><strong>Web Application Security Questionnaire</strong></td>
<td>Focuses solely on an organization's web application security controls.</td>
</tr>
<tr>
<td><strong>Infrastructure Security Questionnaire</strong></td>
<td>Focuses solely on an organization's infrastructure security controls.</td>
</tr>
<tr>
<td><strong>Physical and Data Centre Security Questionnaire</strong></td>
<td>Focuses solely on an organization's physical and data center security controls.</td>
</tr>
</tbody>
</table>
Whether you are a small business or multinational enterprise, information risk management is at the heart of cybersecurity. These processes help establish rules and guidelines that provide answers to what threats and vulnerabilities can cause financial and reputational damage to your business and how they are mitigated.

Ideally, as your security implementations improve and you react to the contents of your current assessment, your cybersecurity score should improve.
Limitations of security questionnaires

Security questionnaires prevent third-party breaches and help heavily regulated industries maintain compliance. These benefits, however, are often eclipsed by two concerning limitations to conventional methods of managing risk assessments.

1. Logistical difficulties

Creating, administering, and reviewing security questionnaires is notoriously labor-intensive. This difficulty is compounded as the number of vendors multiplies.

Once a company has more than a handful of vendors, sending questionnaires through email, tracking responses in spreadsheets and validating responses by hand, becomes a logistical nightmare.

2. Third-party risks are no longer compartmentalized

The acceleration of digital transformation has carved highly detailed mutations across the third-party attack landscape. As a result, risk assessment requirements have outgrown discovery mechanisms offered by current, standardised questionnaire frameworks.

These limitations make sending highly-targeted security questionnaires a challenge. Maintaining accuracy requires increased administrative effort which further adds to the logistical difficulties of managing each questionnaire.
The future of security questionnaires

To keep up with rapidly developing third-party risks in an age of accelerated digital transformation, a reformation of conventional risk assessment methods is required.

A reformative solution is one that addresses the two current limitations of security questionnaire management.

Digital risk assessment management

Rudimentary reliance upon spreadsheets and emails should be replaced by a digital platform that manages the complete lifecycle of security questionnaires from creation to administration, tracking, and review.

Customizable questionnaires

To extend the usefulness of automated security questionnaires, they must become customizable.

Third-party risk requirements differ across organizations. To efficiently manage each unique risk, organizations must be empowered to design their own custom questionnaires for every use case.
UpGuard: The future of security questionnaires

The accelerating expansion of the third-party attack surface is creating new exposures across the vendor attack surface. These exposures are further complicating third-party risk detection beyond the scope of conventional detection methodologies.

To revive the accuracy of third-party risk evaluation, security questionnaires need to be capable of conforming to every congruence along the attack surface. This can only be achieved through customization.
UpGuard: The future of security questionnaires

Customizable security questionnaires

UpGuard has broken free from the outdated risk assessment methods currently restricting the cybersecurity industry. Now, organizations have the ability to create their own custom questionnaires, either from a blank canvas or by modifying existing frameworks from a library of standardized questionnaires that align to cybersecurity frameworks.
UpGuard: The future of security questionnaires

Digital risk assessment management

The UpGuard platform contains an end-to-end workflow to accelerate each step of the questionnaire process from creation to administration and review.

<table>
<thead>
<tr>
<th>Creation</th>
<th>Create your own custom questionnaire or select a pre-designed framework from a growing library of questionnaires curated by cybersecurity experts.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>A robust workflow empowers organizations to send questionnaires, track progress, and ask for revisions as required. Set deadlines, track the status of outgoing questionnaires, and ask and respond to questions all from a single, clean interface.</td>
</tr>
<tr>
<td>Review</td>
<td>Automatically store, review, identify risks, and assign severity based on questionnaire responses. Completed questionnaires are stored in the UpGuard platform and available for audit or review at any time.</td>
</tr>
</tbody>
</table>
UpGuard: The future of security questionnaires

How to perform risk assessments with a custom security questionnaire

Preparing security questionnaires with an easy-to-use questionnaire builder is a much faster and more streamlined alternative to the conventional 8 step manual process outlined on page 6.

With UpGuard, a questionnaire can either be created from an existing template or from a blank canvas.

1. **To create a custom questionnaire from an existing template, simply duplicate your selected template, and then begin modifying its contents.**
2. To create a completely personalized questionnaire from a blank canvas, select the “Create Custom Questionnaire” option from the questionnaire library view.
UpGuard: The future of security questionnaires

Question styles

UpGuard’s questionnaire builder supports six different question styles to support highly-targeted third-party risk evaluations.

1. **Sections**
   - Sections are a simple tool to create a group with sub-questions inside.

2. **Single-select questions**
   - Allows respondents to choose a single option from a predefined set of mutually exclusive answers.

3. **Multi-select questions**
   - Allows respondents to choose as many options as they wish from a predefined set of answers.

4. **Text questions**
   - Give respondents a free-form text field to answer as they see fit.

5. **File uploads**
   - Allows respondents to upload pdf, doc, docx, jpg, png, xlsx, csv, or pptx documents. Each document can be up to 10 MB.

6. **Identified risks**
   - Identified risks allow you to automatically raise a risk based on an answer to a question or multiple questions. To do this, you’ll need to add conditional visibility to the risk. If the identified risk has a potential compensating control, you can provide the respondent with the chance to provide additional information on how they mitigate it.
Once you’re ready to go, you can incorporate your new security questionnaire/s in UpGuard’s risk assessment workflow. Risk assessments capture the end-to-end process of assessing a vendor’s cybersecurity performance, including:

- The result of security questionnaires
- The risks surfaced by automated scanning, in the form of security ratings
- Continuous monitoring and assessment of an organization’s data leaks, and other threats

UpGuard makes it easy for organizations to conduct regular risk assessments with third-parties, remediate the identified risks, and measure vendor performance over time.

For a free trial of UpGuard’s custom questionnaire builder, visit:

www.upguard.com/demo
Questions? We have answers
We're here to help, shoot us an email at sales@upguard.com

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.

Contact sales  Free demo →