QorusDocs

The QorusDocs *"Everything-you've-ever-wanted-to-know-and-more"* Guide to Security Questionnaires

www.qorusdocs.com

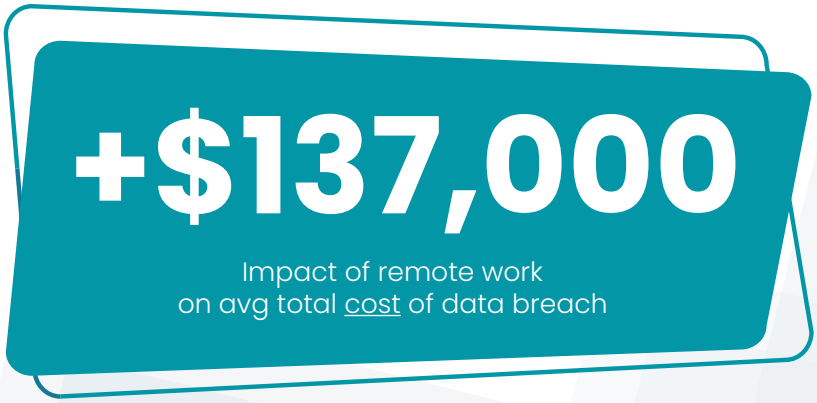
This ain't your mama's InfoSec.

Remember the days when companies could throw up a firewall and install some anti-virus software and feel protected? Neither do we—that era is long gone. Today, cloud-based computing services enable employees to access software applications, data storage, and other services remotely via wireless connections, creating a new digital ecosystem rife with information security (InfoSec) complexities.

Adding fuel to the cyberthreat fire, the global pandemic has accelerated the digital transformation of the corporate world, with millions of workers moving online to facilitate remote working. Pre-COVID, only 19% of organizations had more than half of their workforce working remotely, compared to 62% now, according to a recent Cisco report.

As companies digitize their processes—including the transfer, storage, and processing of important and sensitive data and communications—and grapple with the challenge of securing both legacy and cloud systems, security and compliance professionals are in a race to keep pace with the intensifying scale and sophistication of cyberattacks.

Indeed, with the surge of people working remotely, costly data breaches, phishing, and ransomware threats are on the rise. According to Cisco's Future of Secure Remote Work Report, 61% of companies surveyed reported a 25% or greater increase in cyberthreats since the beginning of the pandemic in March 2020. Similarly, a report by Accenture found that 68% of business leaders feel their cybersecurity risks are increasing.



Stranger Danger

InfoSec has taken on a new sense of urgency and importance in today's business environment as companies start to rely more heavily on third parties to manage their organization (e.g., professional services firms, SaaS vendors, cloud infrastructure). Today, the greatest risk to the enterprise may come from outside the organization.

Case in point: a 2019 Deloitte poll revealed that 70% of businesses rate their reliance on outside vendors as moderate to high, with nearly half (47%) experiencing a risk incident involving the use of an external entity in the last three years.

A 2021 Gartner report noted that "digital business has created a new ecosystem, one in which **partners add new business capabilities and security complexities**. The…vision for risk and security must be based on an ecosystem that enables trust and resilience."

56%

of organizations have experienced a data breach caused by one of their vendors or third parties

Risky Business

While the digitization of business processes has helped organizations reduce operational costs and increase efficiency, cybercriminals are now more able to exploit system vulnerabilities and gain access to sensitive data. The following risk factors may play a role in threatening the security of an organization:

- The nature of the company's operations
- The environment in which an organization operates
- Responsibilities entailed in operating and maintaining the company's systems and processes

60%

of breaches in 2019 involved unpatched vulnerabilities

- The types of information generated, used, or stored by the entity
- The types of commitments made to customers and other third parties
- The technologies, connection types, and delivery channels used by the organization

- The **use of third parties**, such as service providers and suppliers, who have access to the company's system in order to provide them with critical raw materials or components, or operate controls that are necessary (in combination with the company's controls) to achieve the system's objectives
- Changes to the following:
  - System operations and related controls
  - Processing volume
  - Key management personnel of a business unit, supporting IT, or related personnel
  - Legal and regulatory requirements with which the entity needs to comply
- Introduction of new services, products, or technologies

This lengthy list of potential risk factors, in conjunction with the digital transformation that is driving migration to cloud data centers and SaaS applications, is a testament to the growing interest of companies in upping their InfoSec and vendor risk management (VRM) game. Indeed, 84% of Canadian companies said that cybersecurity is now extremely important or more important than before COVID-19.

It's no surprise that organizations are placing such high value on information security. The cost of cyberattacks can be immense for companies, with lost business the largest contributing cost factor. According to a 2020 IBM Security report, lost business costs accounted for nearly 40% of the average total cost of a data breach, increasing from $1.42 million in 2019 to $1.52 million in 2020. Lost business costs include increased customer turnover, lost revenue due to system downtime, and the increasing cost of acquiring new business due to diminished reputation.

In 2020, the average total cost of a data break was $3.86 million and took 280 days to identify and contain.

The Basics

What is information security?

InfoSec is all about protecting information from unauthorized access and involves preventing or reducing the probability of unauthorized access, use, disclosure, disruption, deletion, corruption, modification, inspect, or recording.[1]

What is an information security policy (ISP)?

An ISP is a set of rules, policies, and procedures designed to ensure all users and networks within an organization meet minimum IT security and data protection security requirements. ISPs should address all data, programs, systems, facilities, infrastructure, users, third-parties, and fourth-parties of an organization[2]—essentially everything but the kitchen sink.

What is vendor risk management?

Vendor risk management includes a set of proactive actions that help the organization identify, manage, and monitor of risks resulting from third-party vendors and suppliers of IT products and services. VRM programs are concerned with ensuring third-party products, IT vendors, and service providers do not result in business disruption or financial and reputational damage.[3]

What is a security questionnaire?

Forming part of a company's vendor risk management program, a security questionnaire (also called a vendor risk assessment questionnaire or IT risk assessment questionnaire) is a tool that an organization circulates to a prospective product vendor or service provider to evaluate and validate their security practices before choosing to do business with that organization.

Mitigating Risk By Asking the Right Questions

Potential customers and business partners want peace of mind that you can be trusted with their data. The security questionnaire is their avenue for gleaning the specific information about your organization that they need to feel secure in doing business with you. And it is your opportunity to demonstrate clearly and concisely the foundational role information security plays within your company's digital ecosystem.

Even if an organization has tight security controls and a best-in-class ISP, vendor risk management must be at the heart of any effective InfoSec program. Security questionnaires are an integral piece of the VRM program and are designed to help an organization identify potential weaknesses among its third-party vendors and partners that could result in a data breach, data leak, or another type of cyberattack.

At a high level, companies will need to evaluate potential third-party vendors' or business partners' control over security, availability, processing integrity, confidentiality, and privacy. To this end, security questionnaires are designed around the following **five trust principles:**

1. **Security**

   Organizations want to ensure information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information.

2. **Availability**

   Companies evaluate controls to ensure information and systems are available for operation and use to meet their objectives. They want to measure whether systems include controls to support accessibility for operation, monitoring, and maintenance.

3. **Processing integrity**

   Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation.

4. **Confidentiality**

   Confidentiality addresses the ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control. It's important to note that confidentiality is not the same as privacy. Privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information.

5. **Privacy**

   Companies deciding whether to do business with a potential vendor use the security questionnaire to evaluate controls about the collection, usage, retention, disclosure, and disposal of personal information.

Mitigating Risk By Asking the Right Questions

Let's dive into the nitty gritty details of completing InfoSec questionnaires to help your organization give peace of mind to potential customers—and help you close more business.

Who, What, Where, When?

You may receive security questionnaires from **prospective customers**, as well as **existing clients**. Prospective clients send their security questionnaire at one of these points in the sales process:

- fairly early on as part of an RFP document or process; or
- later on in the opportunity (at contract negotiation), once internal procurement teams start getting approvals from across their business, including their Security & Operations team or Compliance team.

Existing clients who maintain vendor risk management as part of their security and compliance program will send you security questionnaires to evaluate potential changes in your security posture.

How many questions?

While under 20% of programs leverage an industry-standard question set, the majority of the questionnaires designed by a company's Security and Compliance team are usually between 100 and 150 questions in length—but some questionnaires can exceed 400 questions!

Team effort

Whether it's the sales, proposal, or security and compliance team spearheading completion of the questionnaire, responding to an InfoSec questionnaire is not a one-man show. Many questionnaires contain questions that delve into low-level particulars of specific domains which require collaboration with subject matter experts from across the business. IT Operations, Engineering, Product Management, HR, and Legal may all be part of the process.

Supporting cast

Many organizations are innovating away from sole reliance on questionnaires. Instead, vendors are using a combination of security questionnaires, documentation review, and remote assessments to round out their VRM programs.

Documents commonly requested to support a security questionnaire response include:

- Software and Infrastructure Architecture & Security document
- Organization Information Security Policy
- Information Security Incident Management Procedure
- Business Continuity Policy
- Disaster Management Policy
- Privacy Policy

Preference is often given to vendors who maintain a compliance program and hold a certificate/report, e.g., SOC 2 Type II or ISO 27001. Popular compliance frameworks include SOC 2 Type II, ISO 27001, and the Cloud Controls Matrix (CCM) from Cloud Security Alliance.

It may be unsafe to share the details of policies and procedures like the Disaster Management policy or Information Security Incident Management Procedure outside of the organization. The best course of action is to share only enough information to provide reassurance that adequate controls have been implemented and are being maintained, i.e., share an executive summary and table of contents of these documents.

Time commitment

As part of the end-to-end sales cycle, an organization must provide quick, accurate, and quality responses to security questionnaires to ensure a sustainable competitive advantage. However, receiving swift feedback on complex topics from key stakeholders—who already have their own workload and jam-packed schedules—can be a challenge that directly impacts the expediency of the process.

While security questionnaires have a bad reputation for being tedious and time-consuming—even painful—they vary in length and complexity. Responding can take hours, days, or up to a week, depending on various factors, most notably whether you're tacking the questionnaire manually or using an automated tool, like QorusDocs, to streamline the process via task assignment, progress tracking, and access to high-value reusable content.

Approval process

The Security and Compliance Director typically performs a final review of the security questionnaire before it's returned to the prospect or customer. Complex questions are discussed with the Chief Technology Officer (CTO) and any liability clauses contained in documents relating to the response (e.g., Data Protection Agreement or Standard Contractual Clauses) are signed by an officer of the company.

The Expert Weighs In

While responding to an InfoSec questionnaire may seem like a daunting task, there are ways to make the process not only simpler and speedier, but a valuable piece of your sales and RFP process that fosters trust and loyalty amongst prospective and existing customers and partners. Johan Olivier, Security and Compliance Director at QorusDocs, shares some tips and tricks to get you started:

1. **Appreciate the need for vendor risk management**

   Customers and business partners want peace of mind that you can be trusted with their data. You must go beyond simply answering a set of questions: make an effort to listen to stakeholders and ensure you interpret each question accurately so that you can get behind what is truly being asked.

   Support your responses with quality documentation and offer to engage in Q&A sessions to clarify uncertainties and answer questions. If you do this, the entire exercise will be more valuable, accurate, and rewarding to all parties.

2. **Identify the 'Value Add' for your organization**

   With the right approach, different business areas within your organization can benefit immensely from responding to security questionnaires. Security questionnaires provide direct feedback from the industry in terms of highlighting which aspects of security and organizational resilience are important.

   Aggregate data from multiple questionnaires and use the most common topics as a yardstick to measure your own organization's security posture across divisions (HR, Engineering, IT Operations, etc.). This exercise is incredibly valuable in terms of aligning and improving your organization's security and resilience.

   And remember, the fact that you've been asked to respond to a security questionnaire is a good thing! It's sign that you're succeeding, that you're of interest to prospects, and are on the path to closing more sales.

3. **Show customers you're serious about compliance**

   The importance of complying with industry standards and regulatory requirements must be recognized and appreciated at the C-suite level. A top-down effort dedicating personnel and resources towards running and maintaining a compliance program and providing security assurance, like answering security questionnaires, is essential.

   With the exponential increase in InfoSec threats, conducting vendor risk assessments has become an essential step in the sales process. Responding to security questionnaires is not an activity that should be a minor responsibility of the IT department or Engineering team. SaaS companies should establish a dedicated security team and implement and maintain a proper compliance program.

4. **Maintain continuous compliance**

   Use a well-designed security program to maintain your organization's controls, policies, and procedures. Automate as many of the compliance elements as possible to lessen the workload. Ensure that policies and procedures are reviewed frequently and that internal control audits (checking the effectiveness of controls) are done on a set schedule to ensure continuous compliance.

   Continuous compliance improves your organization's ability to respond to changes in the environment, workforce, industry, etc., without exposing your organization to risk. It also ensures you always have access to updated policies, procedures, and controls, making it easier to supplement your responses to questionnaires with up-to-date supporting documents.

5. **Simplify the task: work smarter, not harder**

   Most of the time, security questionnaires cannot be completed without the need to collaborate across departments. It is critical to streamline collaboration and improve efficiency on complex questionnaires.

6. **Collaborate in your everyday applications**

   Simplify collaboration across the organization by using tools and applications that contributors are familiar with, such as Microsoft Word, Excel, etc.

7. **Build a Knowledge Library of high-quality reusable resources**

   Capture questions and answers into a knowledge base for reuse. Maintain a repository of high-quality, accurate, and up-to-date supporting documentation.

8. **Automate the process**

   Make life easier by taking advantage of software that automates the response process. For example, the QorusDocs Auto Answer capability uses an intelligent response engine to answer questionnaires based on data captured into your knowledge base.

QorusDocs On Your Side

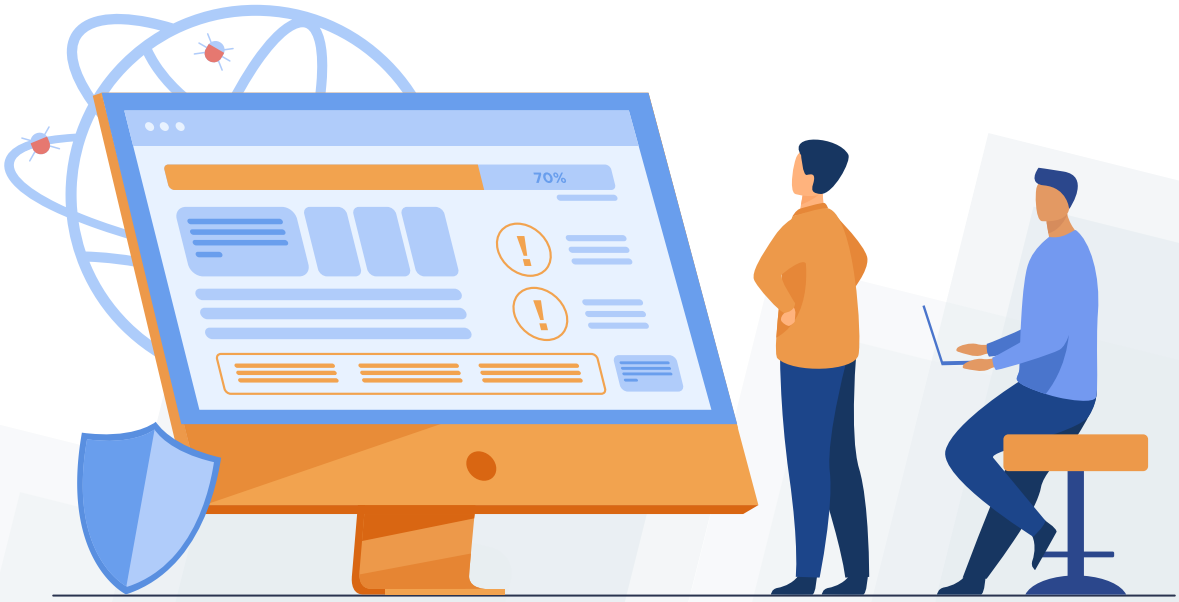
At QorusDocs, we understand that you're faced with the daunting challenge of responding to InfoSec questionnaires at scale. We see the never-ending stream of questionnaires that fills up your inbox and we know the sales team is relying on you to help close their deal.

We appreciate the overwhelming feeling that accompanies those standard 150+ questions, some repeated over and over, and the short notice on turnaround time that stresses you out—especially knowing a simple questionnaire can eat up 16-20 hours of your time.

We're here to help. QorusDocs simplifies the way you respond to security questionnaires in multiple ways, including an intuitive auto-answer capability, task assignment across teams, progress monitoring, and access to up-to-date reusable content.

Complete complex questionnaires 5X faster

QorusDocs can handle anything you throw at it. Use our intuitive software to quickly finish lengthy, intricate security questionnaires while ensuring version control. Our automation software gives you a centralized content hub with the latest pre-approved content, so questionnaire responses are consistent and current no matter how many different stakeholders work on them.

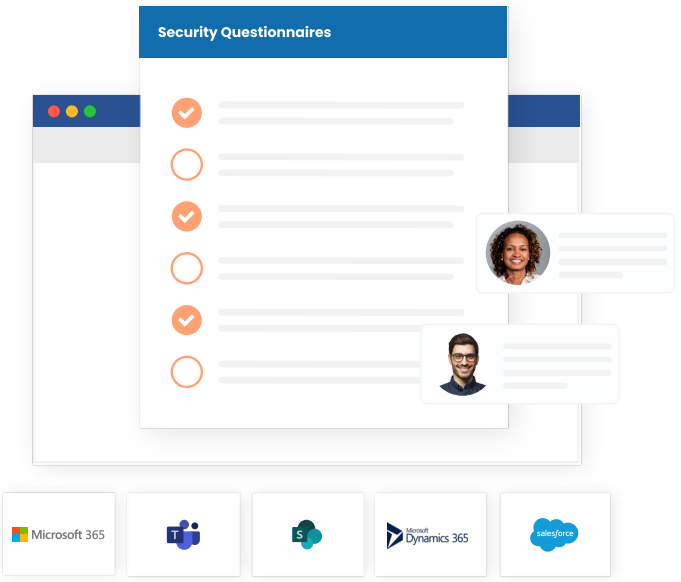


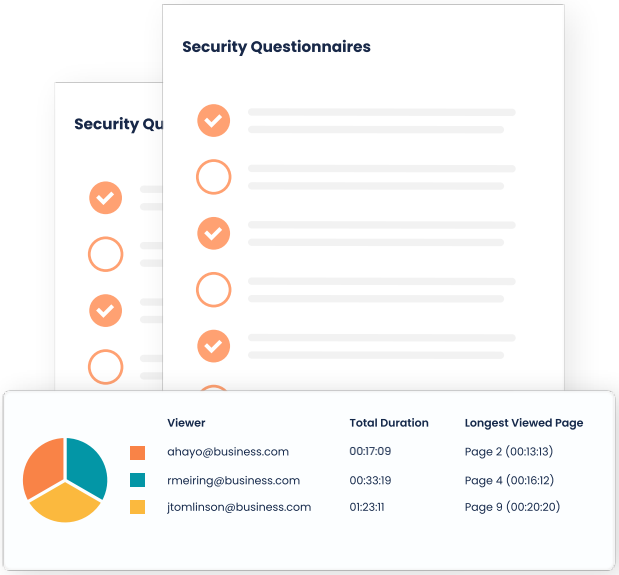
Collaborate in your everyday applications

Keep up with the volume of questionnaires your team has on its plate using the software and applications you already use. Our cloud-based software is purpose-built for Microsoft 365 and popular CRM systems, enabling you to easily share documents from anywhere, assign tasks, and monitor deadlines to keep you ahead of schedule.

Boost productivity with AI-powered content

Leverage the right content for every questionnaire and increase efficiency across your organization. Our automated system gets smarter with each use, putting tailored content recommendations with compliant and up-to-date content at your fingertips. Insert these directly into questionnaires and complete the document in minutes.





Instant questionnaire insight, smarter follow-up

See exactly how a client or prospect is engaging with your completed questionnaire with QorusDocs detailed tracking features. Our built-in measurement tools allow you to see how long a reader stays on each page, what they click on, and what they share. Use these analytics to tailor more personalized follow-up conversations.

Boost the bottom line

QorusDocs secure, cloud-based software enables you to harness your team's potential through streamlined collaboration and improved efficiency. You can respond swiftly and accurately to complex InfoSec questionnaires, giving prospects and potential business partners the peace of mind that their data will be safe—and that assurance translates into more closed deals and more revenue.

If the thought of the number of security questionnaires coming across your desk this quarter fills you with dread, request a demo to learn more about how QorusDocs can help you answer them in a snap!

1, 2, 3. UpGuard Cybersecurity & Risk Management blog. https://www.upguard.com/blog