LOOPIO'S GUIDE TO RESPONDING TO SECURITY QUESTIONNAIRES

A guide to help Sales teams understand the world of Security Questionnaires and how to respond to them

CONTENTS

INTRODUCTION

A Bit of Background

Companies are increasingly seeking third-party cloud solutions to help support different business processes and initiatives. In fact, a recent AT&T report on Data Security found that "Enterprise cloud services account for 71% of services used by the average organization."

To ensure that their data is secure, companies need to have adequate security controls. These should cover internal processes but also extend to the vendors.

Enter the infamous Security Questionnaire!

WHAT IS A SECURITY QUESTIONNAIRE?

A Security Questionnaire is a technical request that assesses a vendor's internal and external Security policies and procedures.

The size, level of detail, frequency, and types of information asked in these questionnaires varies and usually depends on:

- The type of client data you are hosting or handling
- The type of integrations your solution offers
- The scale of deployment within the client's organization
- The intended use for the solution

For example, if your solution hosts sensitive data, your client may classify it as high risk. Understandably, they will want to know how you are protecting their confidential information and will likely send a more robust Security Questionnaire when assessing your solution. There is also an increased chance that you'll be receiving their Security Questionnaire again after you win the opportunity (e.g. upon renewal).

> ***Companies are currently uploading an average of 18.5 terabytes of data to cloud applications each month, but fewer than 9% of cloud providers have implemented enterprise-grade data security and privacy controls. That's a problem given that nearly 20% of files stored in the cloud contain sensitive data.***
>
> AT&T Cybersecurity Insights: The CEO's Guide to Data Security

Security Questionnaires also differ in format. As an example, you might receive them as:

- An Excel, Word, or PDF document
- An online survey (Google Forms, SurveyMonkey, etc.)
- A set of questions in an email
- A questionnaire hosted in a procurement portal (Ariba, Coupa, etc.)

To make matters even more complicated, there is no consensus on what to call them. Here are a few other names that Security Questionnaires go by:

- Vendor Risk Assessments
- Third-Party Security Assessments
- Compliance and Security Assessments
- Technical RFPs/RFIs

To keep things consistent, we'll refer to them as **Security Questionnaires** throughout this guide.

TYPES OF SECURITY QUESTIONNAIRES

Standardized Security Assessments

VSAQ

Vendor Security Assessment Questionnaire (VSAQ) is a set of self-assessment security questions that Google developed to help evaluate their vendors' security standings. The VSAQ framework is now public.

CAIQ

Consensus Assessments Initiative Questionnaire (CAIQ) was developed by Cloud Security Alliance (CSA) to provide "industry-accepted ways to document what security controls exist in IaaS, PaaS, and SaaS offerings."

SIG and SIG Lite

Standardized Information Gathering Questionnaires (SIG and SIG Lite), developed by Shared Assessments, contain industry standard questions that cover a range of security areas.

VSA

The Vendor Security Alliance questionnaire (VSA) is a relatively new standard assessment that was developed by security leaders at Uber, Atlassian, Square, Twitter, Dropbox, GoDaddy, Palantir, Airbnb, and Docker.

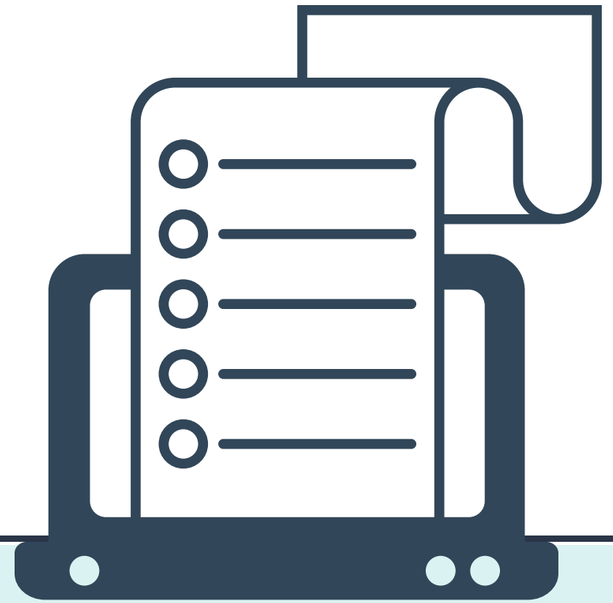
Custom Security Questionnaires

Despite the push by many organizations to standardize Security Questionnaires, many companies still issue custom questionnaires to their vendors. The good thing is, regardless of the type of request you get, a lot of the questions are either the same or similar to those in standardized assessments.

Security Questionnaires Based on Compliance Standards

Sometimes clients will take a compliance standard such as SOC 2 or ISO 27001 and convert it into a Security Questionnaire for vendors. We will go over these and other compliance standards in more detail in the next section.

WHY ARE SECURITY QUESTIONNAIRES ISSUED?



GOVERNMENT REGULATIONS AND INDUSTRY-SPECIFIC SECURITY REQUIREMENTS

Some companies come across industry-specific questionnaires that are enforced either by government regulations or independent authorities, for example:

HIPAA

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), healthcare organizations and their providers (including cloud providers) are required to adhere to national standards of processing health data.

SOX

Sarbanes-Oxley Act of 2002, known as SOX, applies to all publicly traded companies in the United States. It requires them to have controls around secure data storage and transmission in place to protect financial data.

GLBA

The Gramm-Leach-Bliley Act (GLBA) is a US federal law that regulates how financial institutions handle consumer information. The Act requires providers to implement security programs – including Security Assessments – to protect sensitive data.

PCI

The Payment Card Industry Data Security Standard (PCI DSS) sets out security requirements for companies that accept or process payments.

RISK MITIGATION

Security risks, both from internal and external sources, can have potentially devastating effects if not addressed proactively. According to a Cybersecurity Market Report from Cybersecurity Ventures,

“Cybercrime damages will cost the world $6 trillion annually by 2021.”

Many companies are building robust third-party vendor management policies as part of their security management process or security certification requirements (we discuss these certifications on the next page).

Having vendors, both current and potential, complete Security Questionnaires can help companies mitigate risks and minimize the likelihood of exposing their data to breaches.

For those on the receiving end, it means higher volume and complexity of these questionnaires in the future.

CUSTOMER OBLIGATIONS

As part of their obligations to customers, organizations could be required to maintain security controls of their internal infrastructure and also to assess relevant controls and risks of external systems on which they rely. That could mean issuing Security Questionnaires to their current and potential third-party vendors.

THIRD-PARTY CERTIFICATIONS AND STANDARDS

Often companies obtain third-party security and compliance certifications to audit their internal controls and also build trust with their clients. These certifications provide an objective evaluation of their company's security processes while setting a high bar. They often include a mandate to conduct vendor risk assessments. Here are a few of the most common security standards:

SOC

The American Institute of CPAs (AICPA) developed SOC, a reporting framework that companies use to demonstrate their cybersecurity programs. SOC 1 focuses on organization's controls over financial reporting. SOC 2 and SOC 3 focus on organization's controls that relate to Security, Availability, Processing Integrity, Confidentiality, or Privacy.

ISO

The British Standards Institution developed frameworks for information security management (ISO 27001), cloud security management (ISO 27017), and cloud privacy and data protection management (ISO 27018). ISO 27001 is the most popular standard out of the three.

NIST

The National Institute of Standards and Technology developed the NIST Cybersecurity Framework based on different international security standards and incorporated CIS Critical Security Controls into its assessment.

COBIT

Developed by the Information Systems Audit and Control Association (ISACA), COBIT 5 is a global framework for governing and managing enterprise IT systems.

RESPONDING TO SECURITY QUESTIONNAIRES

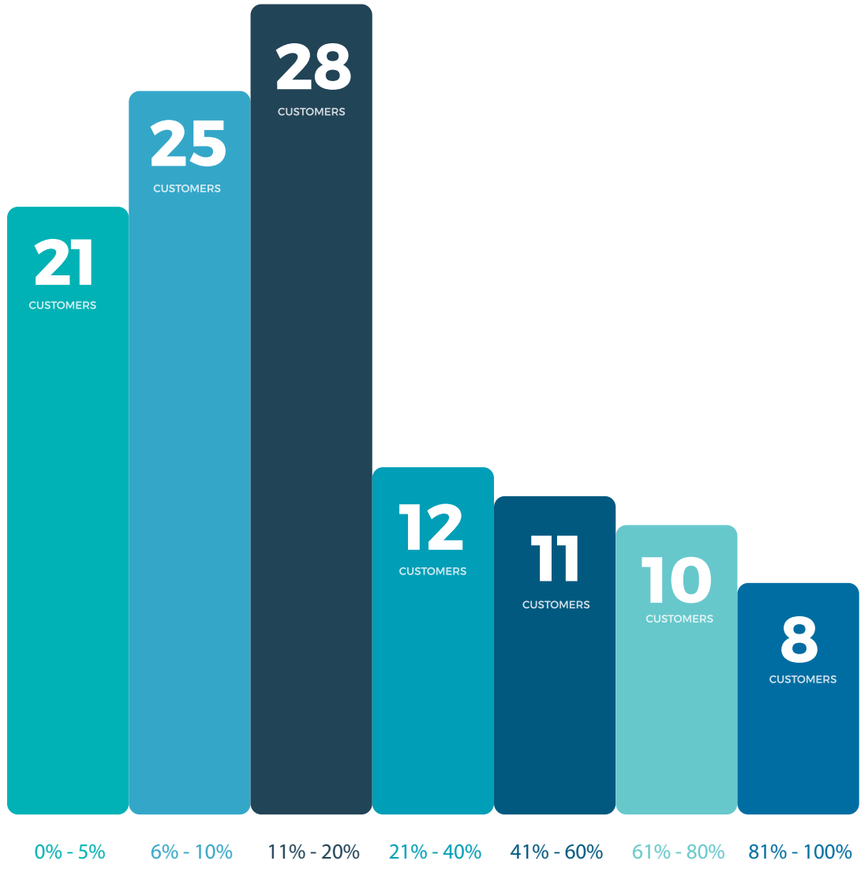
SECURITY QUESTIONNAIRES IN THE SALES CYCLE

Security Questionnaires can land in your inbox at different points in the sales cycle. In fact, you may need to complete one before the conversation with your prospect can even begin.

Other times, Security Questionnaires will come in at the end of a sales cycle, as a final step in the decision-making process. In this case, your prospect has likely chosen your organization as the preferred vendor and is doing their due diligence to mitigate potential risks and ensure that your policies meet their security requirements.

Regardless of when they come in, Security Questionnaires are a crucial part of the sales cycle for many companies.

Here's a snapshot demonstrating the importance of Security Questionnaires among Loopio customers, based on a customer research analysis that we conducted in Q2 2017.



% of Opportunities that Required Completion of a Security Questionnaire

SECURITY QUESTIONNAIRES AND ASSOCIATED RISKS

When responding to Security Questionnaires, you should keep in mind the following:

1 BUSINESS RISKS

If you provide inaccurate information in your response, you may expose your company to risks associated with brand reputation, loss of the deal, and compliance or legal issues.

2 SALES RISKS

Responding takes up a lot of resources and requires input from a wide range of Subject Matter Experts, often at a senior level. Not being able to provide a quick turnaround can prolong the sales cycle or even jeopardize the opportunity.

TIPS FOR RESPONDING TO SECURITY QUESTIONNAIRES

1 Understand What Your Prospect is Looking for

Understanding your prospect's needs is key to successfully responding to Security Questionnaires.

Some requirements in the Security Questionnaire might be a 'must-have' for your prospect, while others might be a 'nice-to-have.' Each company has different levels of business and security risk that are acceptable to them.

The prospect might use a templated or standardized assessment questionnaire, where not all sections or questions apply to your solution. Sometimes, answers to specific questions might trigger follow-up questions or require you to provide evidence.

It's also important to understand who is going to review your responses. Security Questionnaires are different from Requests for Proposals (RFPs) in that they are most often reviewed by technical experts who want to know the facts without having to fish them out of marketing or sales messaging. So, be concise! Also, make sure that you know the context behind every requirement or question. Dig deep into the 'Why?' If necessary, ask your prospect to clarify questions and requirements.

A FEW TIPS

- IDENTIFY 'MUST-HAVE' REQUIREMENTS
- BE CONCISE
- DIG DEEP INTO THE 'WHY?'

2 Be Proactive about Security

Try to be proactive in your efforts to help address prospects' security concerns. One way to do this is to create a Security FAQ. When dealing with large organizations, it likely will not replace a Security Questionnaire. However, by offering this document to prospects early in the sales cycle, you can get a head start and potentially help shape the upcoming Security Questionnaire.

Another effective way to increase your chances of winning the opportunity is to get on the phone! If your prospect has security questions or concerns, ask for their security expert to hop on a call with your Security team. Directly connecting experts who 'speak the same language' can eliminate a lot of back and forth and speed up the response process.

Additionally, a great way for your organization to stay ahead of security requirements is to get a certification like SOC 2 or ISO 27001. Pursuing a certification does take up a lot of resources, but it also provides value in the long run. These third-party standards are widely recognized by organizations and passing such rigorous audits will help you build trust and identify any gaps in your security roadmap.

A FEW TIPS

- CREATE A SECURITY FAQ
- GET ON THE PHONE
- GET A SECURITY CERTIFICATION

3 Share Your Security Roadmap

When it comes to information technology, things are ever-evolving, and so are the security programs and controls your company has in place.

In some instances, it might be sufficient to demonstrate your security action plan. If you don't have the certifications your prospect is asking for but have modeled your controls on them, indicate that in your response. For example, a question asks you about a SOC 2 audit report, but you don't have it yet. Mention the security measures you currently have in place, such as encryption of data, network segmentation, vulnerability testing, etc.

Keep boosting your security and compliance initiatives and let your prospects know what initiatives your Security and IT teams are working on. The procurement process is long and costly, and companies prefer to build long-term relationships with their vendors. That's why prospects want to know where your security is at today and also where it's going to be in the future.

It's also good to ask your prospects for feedback on your security roadmap and to let your Security and IT teams know about any recurring items or significant gaps. This will help them prioritize and, if necessary, adjust their security roadmap.

4 Know Your Contractual Obligations

Beyond asking you to respond to a Security Questionnaire, a prospect can add security-related clauses to your contract. You should carefully review the proposed commitments with the appropriate Subject Matter Experts – someone from Security and Legal teams – to ensure that you can comply with their requirements.

It's important to note that you can have a two-way conversation with your prospect about their requirements. A lot of the time, these conversations will result in mutually-acceptable terms.

5 Understand Different Areas of Security

The types of questions asked in Security Questionnaires vary significantly, but most questions fall into these categories:

- **Change Management:** processes and policies in place to support changes and improvements in the organization
- **Risk Management:** ways you identify and mitigate potential risks
- **Information Security:** processes and policies in place to manage and protect company's information systems
- **Bring Your Own Device (BYOD) and Employee Acceptable Use Policies:** permissions around the use of personal technology for work-related activities and limitations around accessing internal networks
- **Application Security:** measures in place to ensure the security of the software
- **Asset Management:** activities around monitoring and maintaining company's assets
- **Physical Security:** physical and procedural measures in place to ensure the security of staff, facilities, and networks
- **Business Continuity:** processes and policies in place to support main business functions in case of an incident
- **Disaster Recovery:** processes and policies in place to recover the data and systems after an incident
- **Vulnerability Testing:** ways you identify and evaluate security gaps
- **Risk Assessments:** methods of identifying business risk factors
- **Security Certifications:** certifications achieved to help assess company's security standing

Keep in mind that different companies have different ways of categorizing security questions.

6 Make Your Security Content Accessible

Having your security content centralized and organized in a single library kills two birds with one stone – it reduces the need to bug your Subject Matter Experts every time you receive a questionnaire, and it saves you time.

Before you set out to build your content library, determine what areas of security you most often get asked about. You also can get started with this template of 100 Frequently Asked Security Questions.

A lot of Security Questionnaires ask the same question in different ways. A library that allows multiple versions of the same question to be tied to a single answer is an ideal solution for that.

When organizing your information, it's helpful to keep in mind that there can be some confusion around security content. RFPs usually go over product-related questions, whereas Security Questionnaires ask about the company, its processes, and its ability to meet the necessary risk and compliance requirements.

Without clear segmentation and categorization of your content, it's hard to avoid this confusion. For example, if you're a cloud service provider, you'll most likely have content that addresses your internal security policies as well as information about your product security. Can you easily differentiate between content that talks about your internal controls versus content that talks about your hosting provider's controls?

At Loopio, we're no strangers to responding to Security Questionnaires. If you're a Software as a Service company, here's a high-level library structure that we recommend:

- **Organizational Infrastructure and Operations** covers internal systems, policies, and procedures
- **Platform/Product Security** goes over the security aspects of the Loopio Platform
- **Cloud Infrastructure** covers security of our infrastructure and includes information on our hosting providers

7 Keep Your Security Content Fresh

It's important to keep your content up-to-date. As we've mentioned, accidentally providing outdated information in your response can have repercussions and impact your commitments to customers. So, when you find a good home for your security content, figure out a review process to keep it up-to-date.

THE WORLD OF SECURITY

Security is more than just a list of formal policies that the Chief Information Security Officer (CISO) has put together. Threats can come from a variety of sources, both anticipated and not. However, breaches are more likely to occur if people within the company don't understand, support, or follow the necessary security measures and procedures. They are also very likely to occur if you treat security as someone else's responsibility. That's why employee cooperation and partnerships with vendors and clients are important.

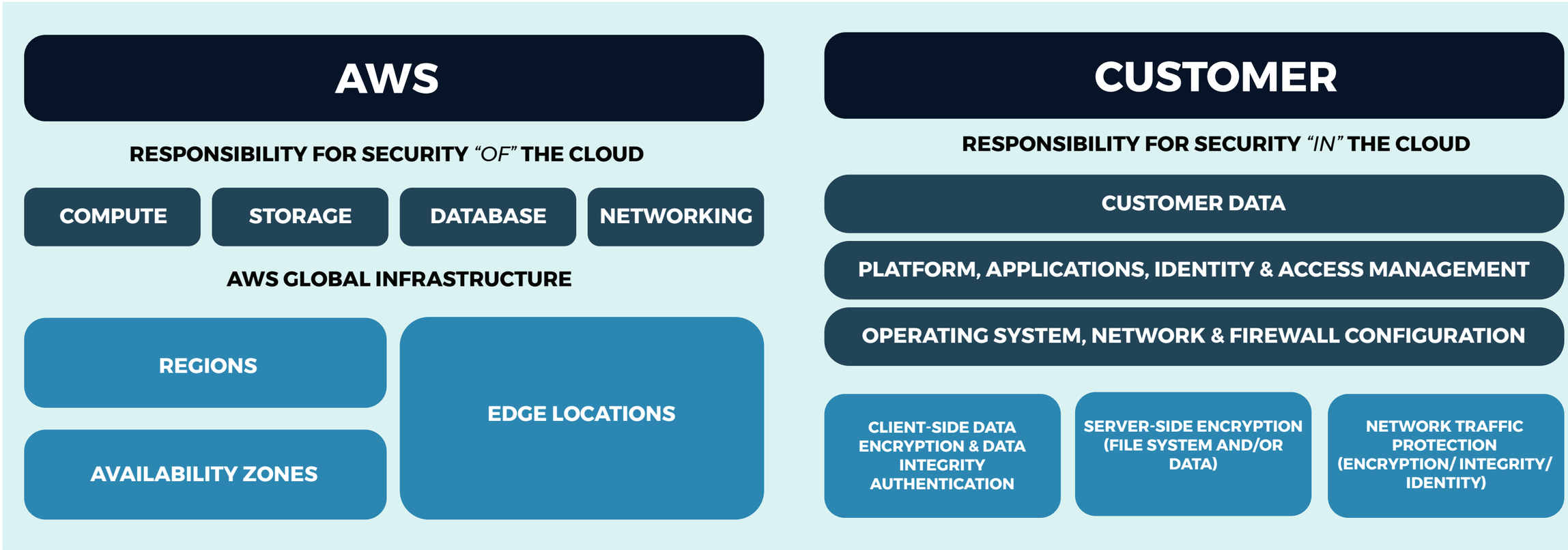
Security is Part of an Organization's Culture

Even if your company has the most robust security policies on paper, at the end of the day, it all comes down to people. For policies to be successful, they need to be supported by employees who live and breathe security.

Security is a Partnership

Security is not one-sided. It requires commitments from different stakeholders, both internal and external, to make it successful.

For example, Amazon Web Services (AWS) developed a Shared Responsibility Model which outlines the difference between security 'in' the cloud (responsibility of the client) and security 'of' the cloud (responsibility of AWS).



Source: Amazon Web Services (AWS)

As part of your response, it's important to indicate to your clients what's possible and set reasonable expectations.

If your solution has integrations and relies on third-party services, this limits your control over external security processes. Your company might have a robust security structure, but if you partner with a service provider who has a fragile security framework that could compromise your ability to protect your client data. After all, security is only as strong as the weakest link.

By regularly assessing your partnerships with vendors, you can identify and eliminate potential vulnerabilities.

SUMMARY

In short, if your company offers solutions that store customer data in the cloud, you can't escape Security Questionnaires! They are technical and time-consuming but also necessary for your client's peace of mind.

The good news is that responding to Security Questionnaires can be easier. The key is to:

- Understand the needs of your prospects
- Stay proactive about your security
- Effectively organize your security content and keep it up-to-date

ABOUT LOOPIO

Loopio's RFP Response Software supercharges the way enterprises respond to RFPs, RFIs, and Security Questionnaires.

Ready to streamline your Security Questionnaire response process?

REQUEST A DEMO