Scrut Automation

Put your best foot forward:

Step-by-Step Guide To Acing Enterprise RFP Security Questionnaires

Scrut Automation

Content

Introduction

Do you have a spare $202 million?

If not, be grateful you weren't in the position of retail giant Target. That amount constitutes the overall cost of their 2013 data breach.

Did you know?

In the Target 2013 data breach, the payment information of an estimated 40 million customers, and personal information of an estimated 70 million customers, was stolen by hackers.

The culprit? An employee of Fazio Mechanical, one of Target's third-party vendors, was duped by a phishing email. Worse yet, the Trojan horse virus in question was nothing new and could be detected by most malware detection programs - but not the one used by this particular vendor.

Fazio "lacked the massive security infrastructure that Target had, allowing the malware to remain undetected on the Fazio computers. Through the Trojan horse, the hackers obtained Fazio's log-in credentials for Target's system."

The data breach was a severe blow to the company financially and reputation-wise. In the wake of the breach, Target has made several changes to its security protocols, but it remains to be seen if these changes will be enough to prevent another breach.

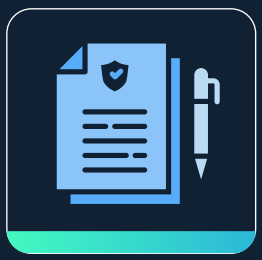
Target's experience has become a cautionary tale of what happens if a business fails to **thoroughly and annually vet the information security practices of third-party vendors.** Situations like Target's are why companies soliciting the services of third-party vendors via RFPs ask those potential vendors to fill out a security questionnaire.

What is an RFP security questionnaire?

A security questionnaire is a document used to **collect information about an organization's security posture.**

The RFP security questionnaire delves into a vendor's

Security policies



Security procedures

Security practices

Incident response plans

Security certifications.

It also collects information about that business's security infrastructure, including its network, servers, and applications.

Why do you need to complete an RFP security questionnaire?

The security questionnaire can **help to identify potential security risks and weaknesses**. It provides businesses with the information they need to select a vendor who is least likely to risk their company's data and reputation with inferior cybersecurity practices.

By completing a security questionnaire, you can assist potential clients as they evaluate the security capabilities of your business to ensure that you can meet their specific security requirements.

The questions will help your customer to understand **how you can protect their company's data and assets** and whether or not you have the necessary experience and expertise to do so.

Completing a security questionnaire can be a formidable task. Still, it is essential to prove to potential clients that they can trust your business to keep their data and systems as safe and secure as possible.

This guide will walk you through completing a security questionnaire, from gathering the necessary information to responding to the questions.

The Security Questionnaire: What to Expect

The questionnaire will request specific details about your **company's security procedures and protocols.**
Typically, the questionnaires contain **hundreds of questions** and take **approximately 20-24 hours** to complete, spread over weeks. Filling out the security questionnaire requires weeks of back and forth between customer stakeholders, sales teams, and engineering and compliance teams, delaying those **precious high value deals**
by weeks, often months. Moreover, the length and time investment required may vary as it depends on several factors: the size of both the prospective client and the vendor, the complexity of the products or services under evaluation, and so on.

The security assessment questionnaire may include any or all of the following categories and questions:

Business Continuity

- What is your company's incident response plan?
- How often is this plan tested?

Change Management

- Do you have procedures in place to detect security defects in source code?
- Do you have documentation about your procedures for ensuring all network equipment is regularly updated with the most recent patches and updates?

Support

- How do employees, customers, and clients report security incidents to your team?
- Describe the degree(s) of technical support incorporated into your license agreements.

Change Management

- Do you have procedures in place to detect security defects in source code?
- Do you have documentation about your procedures for ensuring all network equipment is regularly updated with the most recent patches and updates?

Data

- Do you keep any physical copies of confidential data?
- If yes to the above, what is your procedure for securely disposing physical copies containing confidential data?

Governance

- How often does your company conduct a comprehensive risk assessment?
- Do you have a governance committee? If yes, please provide their names, titles, and relevant credentials.

Human Resources

- Describe the identity and access management protocols in place for all employees.
- When employees change their passwords, how do you test for password strength?

Mobile Security

- Do you permit employees to use personal devices for business purposes?
- Do you require malware detection software on all mobile devices used for business purposes?

Network Security

- What solutions does your IT team provide for network intrusion detection and intrusion protection?
- What firewall system(s) do you use to monitor and control incoming and outgoing network traffic?

Physical Security

- What security procedures do you have in place at your physical offices?
- What is your process for securing the disposal of obsolete electronic devices such as desktop computers, laptops, tablets, mobile phones etc.?

Platform

- Do you regularly review user behaviour logs? If yes, who is responsible for doing so, and how often are audits performed?
- Do you have a system in place for two-factor authentication?

Policies

- How do you provide customers with your privacy policy/privacy notices? If available online, please provide the URL.
- How often are your employees trained on cybersecurity topics such as password protocols and phishing scam detection?

Vulnerabilities

- Has your organization ever been the victim of a cybercrime?
- Do you keep abreast of cybercrime activity and news that may affect your product? If yes, how?

These questions represent only a tiny sampling of what may be included in an RFP security questionnaire.

Occasionally a business compiling an RFP will construct their own security questionnaire, but they are more likely to utilize one from security and compliance oversight professional organizations.

Did you know?

- Three of the more well-known security and compliance oversight professional organizations are:
- Cloud Security Alliance - Cloud Controls Matrix
- Shared Assessments Group - Standardized Information Gathering Questionnaire (SIG / SIG-Lite)
- Vendor Security Alliance - Questionnaire (VSA-Full / VSA Core)

Some questionnaires are specific to certain types of organizations or industries. For example, the Higher Education Community Vendor Assessment Tool (HECVAT / HECVAT Lite) questionnaire is specific to higher education.

Another example is the Payment Card Industry Data Security Standards (PCI DSS) questionnaire for organizations that handle credit cards from major credit card companies.
Now that you know what to expect from an RFP security questionnaire let's discuss how best to respond.

How to Craft a Comprehensive & Compliant Response

Your responses must be as detailed as possible to give the RFP committee **a clear and forthright picture of your company's security capabilities.**

The acronym RFP WINS represents the seven steps to crafting a comprehensive and compliant response:

Read through the questionnaire

Formulate a plan for answering

Procure all necessary information

Write with thoroughness and accuracy

Inspect each finished section for typos, errors, inconsistencies, and formatting

Note your responses and document them for future questionnaires

Submit the questionnaire to the appropriate parties

1. Read through the questionnaire

Read through the questionnaire thoroughly and make sure you fully comprehend all of the questions. If you are unsure how to answer a particular question or are uncertain what type of response is required, **ask for clarification or assistance** from the person conducting the questionnaire.

2. Formulate a plan for answering

After reviewing the questionnaire, create an action plan for answering it. This plan should include who will be responsible for each section, as well as deadlines for completion and a timeline that provides for different stages of the process and mechanisms for follow-up.

If data from other entities need to be collected, assign a specific person responsible for procuring that data, and build regular check-ins into your timeline.

Remember, it's not enough to have a plan. You need to ensure **you have the right people to execute it.** Identify the people who will be responsible for each step of the project. Make sure they understand their roles and the necessary deadlines.

Also, **build contingency plans.** For example, if one of the responsible parties goes on unexpected medical leave, ensure there is a backup person who knows both the process and the data and can step into their shoes. Deadlines can be tight, and sometimes no delays are possible. person who knows both the process and the data and can step into their shoes. Deadlines can be tight, and sometimes no delays are possible.

3. Procure all necessary information

Gather all of the information and documentation needed to answer the questions. This data includes, but is not limited to:

- Company policies
- Cybersecurity policies
- General security policies

- Security compliance certificates
- Network diagrams
- Employee training records
- Organization charts
- IT risk and mitigation controls
- Previous security audits

4. Write with thoroughness and accuracy

When answering an information security questionnaire, it is vital to be as detailed and honest as possible. Take your time to answer the questions **thoroughly and accurately.** This will help ensure that the person or company conducting the questionnaire clearly understands your current security measures and can make appropriate recommendations.

5. Inspect each finished section for typos, errors, inconsistencies,

Go over the first draft multiple times, and ensure they're thorough. If possible, have someone who has not been involved in the writing process also read it. A fresh set of eyes can often spot errors that others may overlook.

Proofreading can be tedious, but it is essential to produce quality writing. A single typo can change the meaning of a sentence, and multiple typos can make a response very difficult to understand. Grammatical errors, such as using the wrong verb tense or pronoun, can also be detrimental.

Also, check to ensure that your RFP is in the correct format and file type. If the issuer wants your response in an Excel spreadsheet and you submit a Word document, it's doubtful you'll win the bid.

6. Note your responses and document them for future questionnairesand formatting

If this is your first time responding to an RFP, carefully saving all of your work will save you significant time with your next one. Building up a knowledge base of your information and data security practices will primarily benefit your organization in the long run, whether or not you respond to additional questionnaires.

Suppose you recognize that your company may not be the best fit for the RFP during the project. In that case, it's entirely reasonable to withdraw your candidacy or decline to continue the process.

Think of the RFP like a job interview - not only is the issuer interviewing you to explore if you are a good fit for their organization, you are interviewing them to find out the same. If you conclude that you aren't a good fit or vice versa, focusing your energies on more productive endeavours is preferable.

Regardless, even if you decide to withdraw from an RFP process, save the work you have already done, as it may come in handy in the future.

7. Submit the questionnaire to the appropriate parties

Once you have crafted a comprehensive and compliant response to the security questionnaire, it has been compiled, proofread, and documented in the correct format and file type specified by the RFP; the final step is to submit. Then the waiting begins.

If you win the bid, celebrate!

If you don't, count the process as a valuable learning experience for future questionnaires. The more you complete, the faster and easier the process becomes.

Scrut Automation

Putting Your Best Foot Forward: Do's And Don'ts During The Process

When responding to an information security questionnaire, a few Do's and Don'ts must be kept in mind.

Do's

Take your time in responding

Be as detailed as possible

Provide statistics and give examples

You want to be part of their solutions

Dont's

Disrespect the time of the RFP evaluators

Overlook the details

Provide false, misleading, or incomplete information

Treat the questionnaire as a compliance exercise

Do:

- **Take your time in responding.** Rushing the process can lead to mistakes. Allow your team as much time as possible to plan and prepare.
- **Be as detailed as possible** in your responses- the more information you can provide, the better. Remember to show and not just tell. Instead of "XYZ Company is experienced at preventing DDoS attacks," with no elaboration, try "XYZ Company employs the following measures to prevent DDoS attacks..."
- Use the opportunity to showcase your company's security procedures and protocols. **Provide statistics and give examples** that demonstrate your understanding in your field as well as in cybersecurity.
- Show how your company can best solve the problem posed in the RFP. Your response should indicate that **you want to be part of their solutions** and how your security measures can help accomplish their goals.

Dont's:

- **Disrespect the time of the RFP evaluators.** The issuers likely have quite a few questionnaires to go through. Your questionnaire will represent a frustrating time sink if your answers are too long, too short, rambling, indirect, evasive, etc. That isn't the reputation you want for your company.
- **Overlook the details.** All questions should be carefully considered, and all supporting documentation should be provided. Pay close attention to all formatting instructions also.
- **Provide false, misleading, or incomplete information.** This approach will only hurt your company in the long run. Winning the RFP is a short-term victory, and the eventual reputation loss that can occur if you've oversold your abilities is incalculable.
- **Treat the questionnaire as a compliance exercise.** While compliance is essential, the questionnaire should assess your company's security posture and identify potential vulnerabilities. The questionnaire should be used as a starting point for a conversation about security, not as a way to check a box for compliance.

By taking the time to understand the RFP process and preparing your responses carefully, you can increase your chances of getting the attention of the right decision-makers and being selected for the project.

With these tips in mind, you should be able to approach an RFP security questionnaire with confidence, knowing that you have the experience and understanding to put your best foot forward and give the optimal answers.

Trust Vault:
Automating Responses for Best Results

What if there was a way to make responding to RFP security questionnaires systematized, streamlined, and efficient?

If you think it sounds too good to be true, think again.

Scrut Automation has done just that with our Trust Vault solution.

Trust Vault is the single window to help you incorporate automation into security certification and report requests.

Our technology can help you showcase your security protocols, build real-time visibility into your security and compliance posture, and keep your customers informed about the measures you take to ensure the security and protection of their data.

With Trust Vault, you can:

- Build and share an auto-populated company-branded security page to demonstrate your business' information security posture;

- Proactively display all your compliance certifications,attestations, and reports in one convenient location;

- Equip yourself with viewer engagement insights to identify your prospect's top concerns for a sea- mless deal cycle; and

- Address security con- cerns and answer questions before they are asked using your customized searchable security knowledge database.

Additionally, you can share detailed certificates, attestations, and reports instantly without worrying about sensitive data leaks.

With Trust Vault, you can manage who can access these reports through admin-managed gated access, backed with auto-populated two-way Non-Disclosure Agreements (NDAs).Are you interested in learning more? Visit our website at https://www.scrut.io/trustvault, or click here to see Trust Vault in action!