BITSIGHT®
The Standard in SECURITY RATINGS


EBOOK

# 40 Questions You Should Have in Your Vendor Security Assessment

# Introduction

Third parties are essential to helping businesses grow and stay competitive, but if you're not careful, your trusted partnerships can introduce unwanted cyber risk and overhead into your organization.

BitSight for Third-Party Risk Management can help you gain immediate visibility into cyber risks within potential vendor ecosystems – giving you an instantaneous snapshot of their overall security postures.

With this insight you can prioritize which vendors need the most attention with an in-depth security assessment – such as those with low security ratings, or critical vendors that maintain constant contact with your company's systems.

Assessments are an important part of any third-party risk management (TPRM) program because they provide further context into vendors' security posture and handling of risk.

This helpful guide includes common questions that can help focus your discovery efforts. We'll explain:

- The top three frameworks you should examine;
- Questions you may want to consider (and why);
- And what else to include in your TPRM program.

# Getting Started

Every organization — and every vendor — is unique, warranting the creation of customized security questionnaires.

Resources, however, often are stretched and security teams face intense pressure from management to complete security assessments quickly.

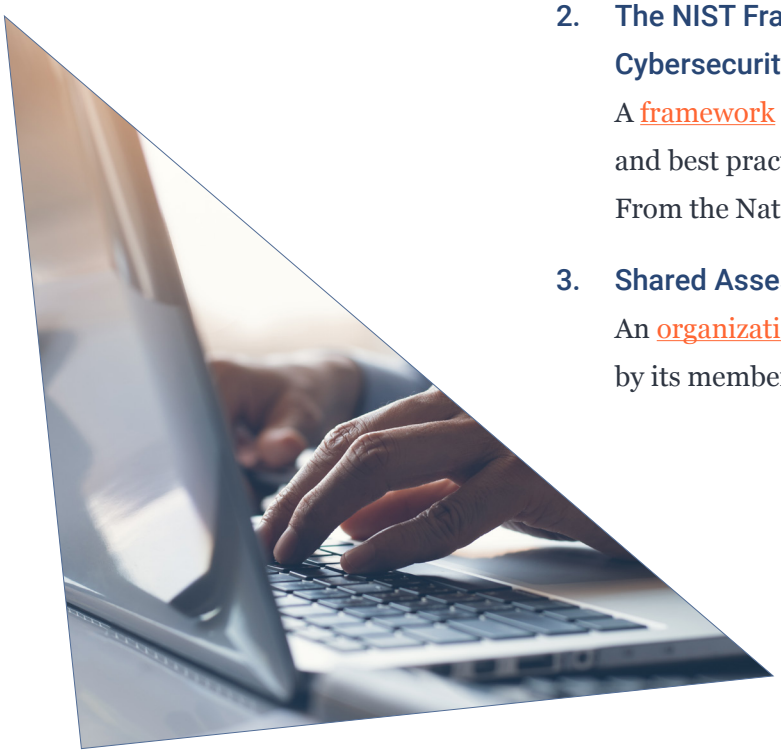
Rather than reinvent the wheel, we suggest relying on the expertise of others for high-level questions and industry-accepted best practices as a starting point for your assessment.

There are three industry-standard security assessment methodologies you can start with:

1. **The SANS Top 20 Critical Security Controls**
   A short list of controls developed by security experts based on practices that are known to be effective in reducing cyber risks. From the System Administration, Networking, and Security Institute (SANS).

2. **The NIST Framework for Improving Critical Infrastructure Cybersecurity**
   A framework that combines a variety of cybersecurity standards and best practices together in one understandable document. From the National Institute of Standards and Technology (NIST).

3. **Shared Assessments**
   An organization that develops assessment questionnaires for use by its members.



## Getting Started (continued)

Among these methodologies, there literally are thousands of questions that you could use.

For instance, if you go to the SANS Top 20 Critical Security Controls page and select “Malware Defenses,” there are 11 items beneath it, each that could represent its own separate questions.

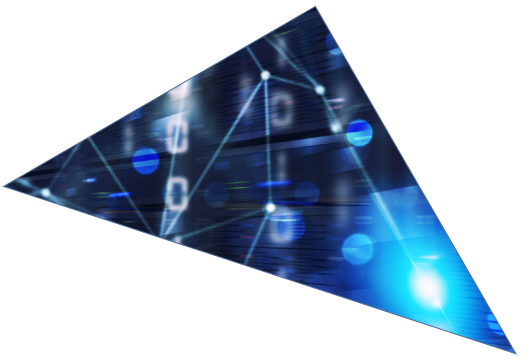
Of course, we can’t fit all of that information here (and we wouldn’t want to even if we could!).

The goal of this guide is to give you an idea of the high-level, critical questions you should consider asking your vendors.

**Let’s take a look.**

**Third parties are essential to helping your business grow and stay competitive. But if you’re not careful, your trusted partnerships can introduce unwanted cyber risk and overhead into your organization.**

# Governance & Organizational Structure Questions



1. **Who is responsible for cybersecurity within the organization?**

   This could be any number of people within the organization, but it's important to have contact points for your vendors.

2. **Is there a chief information security officer (CISO)?**

   You want to verify that the vendor has someone – whether it's a director, vice president, or CISO – in a leadership position responsible for overseeing security strategy.

3. **Is there a cross-organizational committee that meets regularly on cybersecurity issues?**

   Organizations that involve multiple perspectives are likely to have a more sophisticated approach to managing cyber risk.

4. **Have you participated in a cybersecurity exercise with your senior executives?**

   Running tabletop drills can help an organization nail down a quick response time.

5. **How do you prioritize your organization's most critical assets?**

   Understanding what the organization is focused on can give you a sense of where its time and resources are going.

## Governance & Organizational Structure Questions (continued)

### 6. Specifically how do you protect customer information?

When it comes to your data, you want to ask specifically how it is being protected. Is it through encryption, access control, or other mechanisms?

### 7. How are cybersecurity incidents reported?

You likely will want to see the incident escalation document showing how incidents are classified/prioritized, and how everyone – from the IT security staff up through the senior executive team – becomes involved as a significant incident escalates.

### 8. Have you ever experienced a significant cybersecurity incident? Please define and describe it.

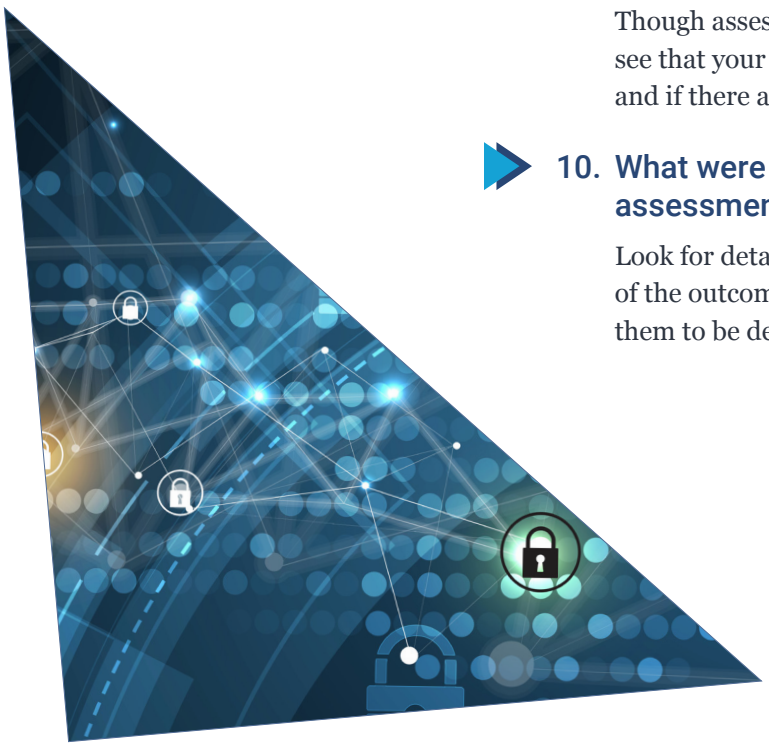
Defining it is one thing, but the description of said significant incident will be quite telling. Pay close attention to how (and how quickly) the matter was resolved.

### 9. When was last time you had a cybersecurity assessment performed by a third-party organization? What were the results of that?

Though assessments only provide a snapshot in time, you'll want to see that your third parties are passing their audits with flying colors – and if there are hiccups, that they're handling them correctly.

### 10. What were the results of your most recent vulnerability assessment or penetration test?

Look for details of the actual tests/assessments and the descriptions of the outcomes and remediation plans. Good or bad, you'll want them to be detailed.



## Governance & Organizational Structure Questions (continued)

### 11. Describe the experience and expertise of your IT security staff.

Experience and expertise are vital.

### 12. Do you outsource any IT or IT security functions to third-party service providers? If so, who are they, what do they do, and what type of access do they have?

You'll want to know this information so you can do your due diligence on any outside sources that may be able to gain access to your sensitive information.

### 13. What types of cybersecurity policies do you have in place in your organization today?

The policies themselves will vary—and what you really care about is the implementation of the policies themselves—but it's important to at least have acceptable use, remote access, and privacy and security policies in place to state the organization's expectations.

### 14. How frequently are your employees trained on your IT security policies, and do you use automated assessments?

Employees are much more likely to avoid downloading malware that could affect your data if they have been trained properly.

# Security Controls & Technology Questions

### 15. How do you inventory authorized and unauthorized devices and software?

Organizations that have an automated process for knowing what's running on their systems will have greater visibility into security incidents.

### 16. Have you developed secure configurations for hardware and software?

The key word here is *secure*; make sure your IT security department is involved in checking these configurations.

### 17. How do you continuously assess and remediate your organization's cyber vulnerabilities?

You want to know that your vendor is making cybersecurity a constant priority and is in tune with the problems that need to be fixed.

### 18. How do you assess the security of the software that you develop and acquire?

Having a mature application security program is a way of reducing the threat landscape inside an organization.

### 19. What processes do you use to monitor the security of your wireless networks?

Seek to understand how they are protecting their network against opportunistic hackers and unauthorized use.

## Security Controls & Technology Questions (continued)

### 20. Do you have a data recovery capability?

This may be the difference between your data being recovered or not.

### 21. How do you securely configure your network infrastructure?

Again, you'll want to involve your IT team to ensure that this long-form response meets their recommendations and requirements.

### 22. Do you have automated tools that continuously monitor to ensure malicious software is not deployed?

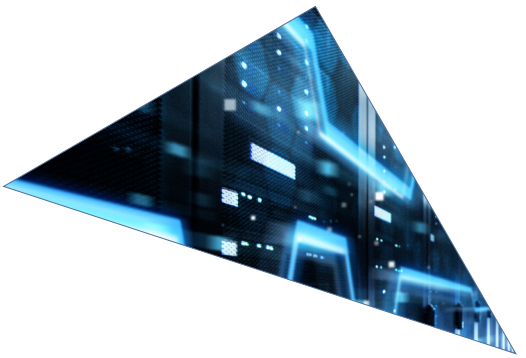
Most attackers are moving their efforts to the endpoint, as this is where your data is located.

### 23. Describe the processes and tools you use to reduce and control administrative privileges.

Not everyone needs administrative access; reducing privileges is an essential element toward creating a more secure ecosystem.

### 24. Do you blacklist or whitelist communications?

This process shows the vendor is taking initiative toward categorizing good and bad internet communications.



## Security Controls & Technology Questions (continued)

### 25. How do you analyze security logging information?

Check specifically how these processes are automated or if they even are being completed at all.

### 26. How do you monitor privileged accounts?

Escalating privileges is a common technique for external attackers, but insider threats can also loom large for your data. Make sure someone is looking at the most sensitive accounts.

### 27. What processes do you have in place to prevent the exfiltration of sensitive data, particularly sensitive customer data like ours?

When configuring a data loss prevention tool, make sure it is programmed to prevent your sensitive data from leaving the environment! Many only configure DLPs to prevent certain classes of data (e.g., personally identifiable information) from leaving.

### 28. How do you plan for and train for a cybersecurity incident? What processes do you have in place to respond to an incident? Do you regularly practice those things?

This multi-part question should provide you with better insight into what may happen in your vendor's organization should there be any security issues or concerns.

### 29. Do you conduct regular external and internal tests to identify vulnerabilities and attack vectors – including penetration testing, red team exercises, or vulnerability scanning?

Having a sophisticated team try to gain access is a way of improving an organization's defenses.

## Security Controls & Technology Questions (continued)

### 30. Do you have a disaster recovery plan? Describe it.

You'll want to know whether your vendor has the proper protocols in place to protect your data or assets in case of an unforeseeable emergency.

### 31. From whom do you receive cyber threat and cyber vulnerability information and how do you ingest that information?

Though threat intelligence can be an important defensive tool, many organizations are not sophisticated enough to do it or do it well.

### 32. What types of physical protection do you have in place to prevent unauthorized access to data or infrastructure assets?

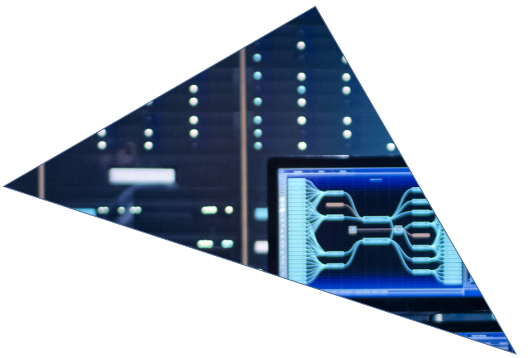
With so much emphasis on cyber threats, it's easy to forget that sometimes physical access can be the entry point for a threat actor.

### 33. How do you manage remote access to your corporate network?

Remote access has become one of the most exploited IT vulnerabilities, so you'll want to evaluate how your third parties control and secure access.

### 34. How do you employ network segregation?

Is sensitive data – particularly sensitive customer data – walled off from other networks?



## Security Controls & Technology Questions (continued)

### 35. Do you have a removable media policy and controls to implement the policy?

Everyone knows how easy it is to walk out of most organizations with a USB full of data; does your vendor allow its employees to do this?

### 36. Have you identified any third parties who have access to your network or data? How do you oversee their security initiatives?

Essentially you're asking your vendor if they have a VRM program in place, which is important.

### 37. How do you monitor your network to alert to cybersecurity events?

Asking your vendors to clearly describe their network monitoring – including technology – is a great way to understand their overall initiatives.

### 38. How do you monitor your third-party service providers?

Having a plan in place for vendor risk management is critical, but how can you be sure that third parties are meeting those efforts?

### 39. How do you monitor for unauthorized personnel, connections, devices, and software?

Monitoring for internal, as well as external, threats is key in securing the infrastructure against attacks.

### 40. Describe the process you have in place to communicate to us security incidents affecting our data.

Again, you want to understand clearly when and how your vendor will communicate to you regarding a security incident affecting their network and your data.

# Optimize Your Vendor Onboarding

The cybersecurity threat posed by third parties is on the rise. That risk grows commensurate with the number of businesses your company works with. According to Gartner, 60% of organizations now work with more than 1,000 third-party vendors – including partners, sub-contractors, and suppliers.[1]

Properly vetting these organizations can be difficult if you don't have all the information you need to evaluate their cyber risk postures effectively.

It's even harder when you're getting pressure from executives to accelerate your vendor onboarding processes and make quick decisions about vendor risk. Hence, you may feel compelled to complete cybersecurity risk assessments too quickly, which could lead to unknown risks entering your organization.

Faced with these pressures, many security managers turn to a "one-size-fits-all" approach to onboarding new vendors, where each third-party is assessed in the same manner. Yet this process is unscalable, creates significant overhead, and fails to take into consideration the variances among different vendors.

**"When onboarding new vendors, it takes the median company an average of 90 days to complete due diligence – 20 days longer than four years ago."**

**-Gartner**[2]
Enable Value and Manage Risk
Through Compendious Supplier Onboarding

1 https://www.gartner.com/smarterwithgartner/a-better-way-to-manage-third-party-risk/

2 https://www.gartner.com/en/documents/3953452/enable-value-and-manage-risk-through-compendious-supplie

As such, you may spend more time than necessary performing assessments, which can undercut your business's efforts at digital transformation and growth acceleration and impede your organization from being able to maximize the value it could receive from these vendors.

But you **can** streamline your assessment process and yield better results by taking several steps.

1. **Group vendors by criticality.**
   This can help you determine whether a vendor needs a more in-depth assessment or not.

2. **Evaluate third-party cyber risk.**
   Use BitSight Security Ratings to evaluate vendors for cyber risk and prioritize which vendors need the most attention.

3. **Establish acceptable risk thresholds.**
   Use security ratings to set a baseline for acceptable risk and ensure that your vendors continue to maintain acceptable security postures.

4. **Monitor your vendors continuously.**
   Implement a continuous monitoring program so you can keep tabs on your vendors' security postures through the life of the partnership. BitSight Security Ratings are updated daily so you easily can track and receive alerts about how a vendor's security performance is changing over time.

Visit www.bitsight.com
to learn how your organization
can save time, reduce costs, and
scale your onboarding process with ease.

BitSight Security Ratings
Deliver Better Data for Better Decisions
About Your Organization's Security

Learn how.
**www.BitSight.com/security-ratings**


BITSIGHT®
The Standard in SECURITY RATINGS

BitSight
111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

## About BitSight

BitSight transforms how organizations manage information cybersecurity risk with objective, verifiable, and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to analyze vast amounts of data on security issues continuously. Seven of the top 10 largest cyber insurers, 25 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks. For more information, please visit www.BitSight.com, read our blog, or follow @BitSight on Twitter.