BITSIGHT

EBOOK

40 Questions You Should Have In Your Vendor Risk Assessment

Table of Contents

01

Introduction

01 Introduction

Third parties, often referred to as vendors, are essential to helping businesses grow and stay competitive. But failure to conduct thorough due diligence and vendor risk assessments can also make them a weak link in the digital supply chain and introduce unwanted cyber risk.

By asking the right questions and evaluating the security practices of their vendors, organizations can proactively identify and address potential risks, strengthening their overall cyber resilience. And by continuously monitoring performance, they can ensure that vendor cybersecurity measures align with the organization's expectations—even as AI-generated threats, regulatory complexity, and global supply chain attacks continue to evolve.

This comprehensive guide will assist security teams in navigating the intricate landscape of vendor risk management (VRM). It provides a detailed framework of 40 key questions and considerations to incorporate into the vendor risk assessment process.

Each question serves a critical purpose—to uncover potential vulnerabilities, assess security controls, evaluate incident response capabilities, and ascertain the level of due diligence exercised by third-party vendors. From technical safeguards and access controls to data protection practices and supply chain security, these questions delve deep into the core aspects that can make or break a vendor's security posture.

You will learn about:

The top three frameworks you should examine

40 questions you may want to consider (and why)

Tips and best practices to enhance your VRM program

02

Top Three Security Assessment Frameworks

02 Top Three Security Assessment Frameworks

Every organization—and every vendor—is unique, warranting the creation of customized risk assessments. Subjecting all vendors to the same set of questions would be impractical, as requirements might be too stringent or lenient for their involvement with the organization. But resources are often stretched and security teams face intense pressure from management to complete security assessments quickly and avoid bottlenecks.

So how can security leaders conduct flexible assessments without starting from scratch every time?

Industry-accepted frameworks and their proven methodologies serve as a starting point, and they also bring a sense of standardization and consistency to the process that allows organizations to compare their findings with industry benchmarks. They also provide alignment with regulatory requirements and compliance standards such as GDPR, PCI DSS, NIS 2.0 or HIPAA. This ultimately enhances the organization's overall cybersecurity posture.

There are three industry-standard methodologies that teams can leverage and customize:

1 CIS Critical Security Controls (CIS Controls)

Formerly called SANS Critical Security Controls (SANS Top 20), CIS Controls is a list of 18 controls developed by security experts based on practices that are known to be effective in reducing cyber risk. The framework is periodically updated to reflect evolving technology, threats, and workplaces.

2 NIST Cybersecurity Framework

The NIST Cybersecurity Framework is a voluntary risk management framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. Its latest version includes a new section on self-assessment, expanded use cases for cyber supply chain risk management, and refinements to better account for authentication, authorization, and identity proofing. The latest version added a Govern function, which places greater emphasis on governance, supply chain risk management, and continuous improvement.

3 Standardized Information Gathering Questionnaire (SIG)

Developed by Shared Assessments, the SIG Questionnaire spans 19 risk domains assessing cybersecurity, IT, privacy, data governance, and business resiliency. The SIG Lite version contains 126 questions, and is recommended for lowerrisk third parties. The SIG Core version contains 855 questions that allow for a deeper scope, typically used for vendorswho manage highly sensitive or regulated information, or perform critical business functions.

Among these methodologies, there are thousands of questions to use, and even more combinations of question sets. However, the most successful risk assessments show consistency across certain domains. In the next section, we've compiled 40 of the most important questions to ask your vendors.

03

40 Critical Questions For Vendor Risk Assessments

03 40 Critical Questions For Vendor Risk Assessments

About Governance

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 foryour 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 the security strategy.

3. Is there a cross-organizational committee that meets regularly on cybersecurity issues?
More and more companies are realizing that cyber risk is business risk. Organizations that involve multiple perspectives are likely to have a more sophisticated approach to managing cyber risk.

4. Describe the experience and expertise of your IT security staff.
Experienced professionals are more likely to be up-to-date with emerging threats, compliance requirements, and incident response techniques. This answer will provide you with valuable insights into their ability to handle security challenges, protect sensitive data, and effectively mitigate risks.

5. 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 or fourth parties that may be able to gain access to your sensitive information.

6. Have you participated in a cybersecurity exercise with your senior executives?
Running tabletop drills can help an organization nail down a quick response time.

7. How frequently are your employees trained on your IT security policies, and do you use automated assessments?
Just like employees at your company are your first line of defense, so are the employees at your third-party vendors.
60 percent of breaches include the human element[1], but people are much more likely to avoid behaviors that could affect your data if they have been trained properly.

[1] 2025 Data Breach Investigations Report, Verizon

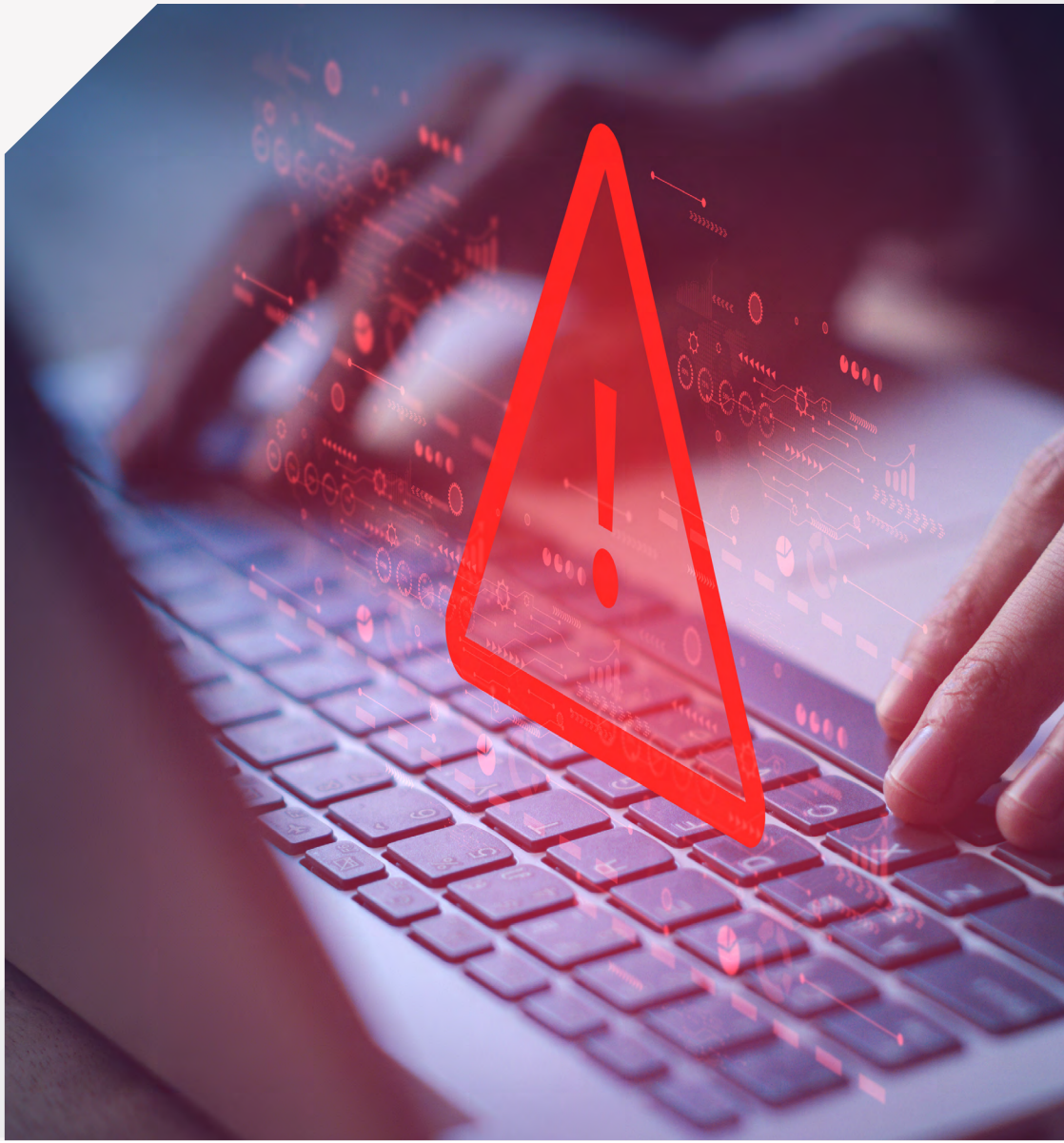
About Security Performance

8. When was the 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.

9. What were the results of your most recent vulnerability assessment or penetration test?
Look for details of the actual tests or assessments and the descriptions of the outcomes and remediation plans. Typical findings include weak password policies, outdated or unpatched software, insufficient network segmentation, and inadequate access controls.

10. Have you ever experienced a significant cybersecurity incident? Please define and describe it.
The description of any significant incident they could have experienced will be quite telling—pay closeattention to how (and how quickly) the matter was resolved.

11. How do you plan 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.



About Processes

12. 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 their implementation—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.

13. 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.

14. 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.

15. Do you have a data recovery capability?
A good data recovery capability combines proactive planning, technical expertise, comprehensive processes,and continuous improvement to minimize data loss and expedite recovery in the event of a data incident.

16. What processes do you have in place to prevent the exfiltration of sensitive data, particularly sensitive customer data?
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.

17. 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?

18. How are cybersecurity incidents reported?
You likely will want to see the incident escalation document showing how incidents are classified or prioritized, and how everyone—from the IT security staff up through the senior executive team—becomes involved as a significant incident escales.

19. Describe the process you have in place to communicate to us security incidents affecting our data.
You want to understand clearly when and how your vendor will communicate to you regarding a security incident affecting their network and your data.

20. Have you developed secure configurations for hardware and software?
This can include encryption settings, firewall rules, intrusion detection and prevention systems, antivirus configurations, version control, change management, and other security-related settings. Make sure your IT security department is involved in checking these onfigurations as well.

21. How do you securely configure your network infrastructure?
Check for hardened network devices, network segmentation into virtual LANs (VLANs), logging mechanisms, and an overall robust network security policy.

22. What processes do you use to monitor the security of your wireless networks?
Look for robust firewall configurations, intrusion detection and prevention software, VPN usage, content filtering, encryption, and authentication mechanisms. Network devices, such as wireless access points, should not be using default administrator passwords—those are easily available to obtain online.

23. 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 potential risks and reduce shadow IT—the use of hardware, software, or cloud services without approval from the IT security team.

24. 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. Network access controls need to be paired with endpoint security, asset management, access control, vulnerability management, and security awareness.

25. How do you assess the security of the software that you develop and acquire?
Check that security is integrated into every step of a vendor's software development and implementation processes.
Pay particular attention to how often they perform code reviews, penetration testing, vulnerability scanning, and risk assessments.

26. Do you have automated tools that continuously monitor to ensure malicious software is not deployed?
Continuous monitoring allows for the prompt identification of anomalies, including suspicious network traffic, unauthorized code modifications, or unexpected behaviors within software components.
Ensure your vendor can quickly respond to potential threats.

27. 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.

28. 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.

29. Do you build lists for blocked and allowed communications?
This process shows the vendor is taking the initiative toward categorizing good and bad internet communications.

30. 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.

31. How do you employ network separation?
Network segmentation involves breaking down the organization's network into smaller networks, while network separation involves utilizing various access controls to enable connections across these smaller networks. Your vendor's strategy should clearly outline the criteria and techniques for both approaches.

32. How do you monitor your network to alert you to cybersecurity events?
Ask your vendor to clearly describe their network monitoring—including technology. Common solutions include Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and User and Entity Behavior Analytics (UEBA) tools.

33. 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?

34. 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 detecting gaps in an organization's defenses and adjusting them. This improves cyber resiliency that creates a robust and adaptive security posture that can withstand attacks, limit the damage caused, and recover swiftly.

35. How do you analyze security logging information?
Check specifically how these processes are automated or if they even are being completed at all.

36. Do you have a disaster recovery plan? Describe it.
A disaster recovery plan (DRP) is a crucial component of business continuity planning, focusing on the recovery of IT systems and data in the event of a major disruption or disaster. You'll want to know whether your vendor has the proper protocols in place.

37. 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.

38. 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 in a distributed, work-from-anywhere workforce, it's easy to forget that sometimes physical access can be the entry point for a threat actor.

39. Have you identified any third parties who have access to your network or data? How do youoversee their security initiatives?
Essentially you're asking your vendor if they have a vendor risk management (VRM) program in place to ensure their vendors meet the organization's security, compliance, and operational standards, and that potential risks arising from those relationships are identified and effectively managed.

40. 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?

04

Vendor Risk Management Tips and Best Practices

04 Vendor Risk Management Tips and Best Practices

The cybersecurity threat posed by third parties is on the rise. That risk grows commensurate with the number of businesses your company works with—73 percent of organizations have experienced at least one significant disruption caused by a third party[2].

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

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

Faced with these challenges, 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.

As such, you may spend more time than necessary performing assessments, which can undercut your business's and growth 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 following these steps:

1. Automate manual processes

69 percent of businesses rely on manual processes involving emails and spreadsheets[3]. Bitsight Vendor Risk Management[4] automates risk assessments and related tasks, such as triggering documentation requests based on tiering, or reassessing existing vendors, allowing teams to focus on higher value activities.

2. Tier vendors by criticality

Prioritizing your vendor inventory will help you determine whether a vendor needs a more in-depth assessment or not, and what requirements to include in it. Take into account their handling of sensitive data (or lack thereof) and their criticality to your business.

[2] Third-Party Risk Management Outlook 2022, KPMG
[3] The Forrester Wave™: Third-Party Risk Management Platforms, Q2 2022, Forrester
[4] www.bitsight.com/vendor-risk-management

3. Leverage Risk Data to Expedite Decisions

Questionnaires are a great tool to assess vendors, but they are self-assessments. Complement them with objectiveevidence and data to validate their responses. For instance, Bitsight surfaces unparalleled data and insights, operating one of the largest risk datasets in the world. Make quicker vendor decisions by bridging subjective and objective assessments and data.

4. Establish acceptable risk thresholds

Use analytics to set a baseline for acceptable risk and ensure that your vendors continue to maintain acceptable security postures. If a vendor falls below your threshold, you can take immediate action to reach out to the vendor in question to inquire about particular areas of risk and remediation.

5. Integrate new technologies into your workflows

Technology is moving faster than most organizations can keep up and AI is the latest to tool that can be leveraged to make substantial process improvements. At Bitsight, Instant Insights for SOC 2 - powered by AI - helps analyze and summarize SOC 2 reports to help organizations review reports more quickly - ultimately accelerating the onboarding and assessment process.

Bitsight

Bitsight Vendor Risk Management can scale your risk assessment and onboarding processes to drive strategic decisions and collaborate confidently with your vendors. Powered by the global leader in cyber risk intelligence, Bitsight VRM offers automated workflows, pre-populated vendor profiles, and objective data that allows organizations to save time and resources, reduce program risk, and increase business value.

Contact Bitsight, to scale vendor management

sales@bitsight.com

BOSTON (HQ)
RALEIGH
NEW YORK
LISBON
SINGAPORE

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BITSIGHT