Introduction

Many times, the deciding factor for choosing a vendor is price. However, other essential factors need to be considered. One significant one is how much risk they can pose to your organization and your ability to provide for your customers.

Through a thorough vendor assessment, your organization can take proactive steps to prevent, mitigate, and lessen the potential impact of selecting vendors that do not meet your organization's requirements by identifying areas of concern with your prospective or current vendors. Vendor assessments are integral to, rather than separate from, ongoing general supply-chain management activities.

Areas assessed include the vendor's ability to reliably deliver their product/service, how well they can protect your data if they meet industry standards, their financial stability, how well they can support their product, and cost.

These factors may be used to compare prospective vendors in determining which one is the most suitable fit for your organization. Or they may be used to decide if using a vendor poses risks that exceed your established level of tolerance.

How to Use

Realize that doing assessments offline, manually via a checklist or spreadsheet is neither enjoyable nor effective.

Visit www.riskwatch.com today, where you can complete an assessment for FREE with a trial of our VendorWatch application. Using our application, you'll be able to automate steps in the assessment, generate a polished report and quickly compare the vendor risk levels across your organization.

How to Calculate a Vendor's Compliance Percentage and Risk Score

Step 1:

Collect information from the vendor that will be needed to answer the survey component of the assessment. You will need to designate one or more individuals from the vendor to be your *Vendor Contacts*. They must have knowledge or access to the vendor's security controls, policies, processes, strategies, and audit results.

Have your *Vendor Contact* refer to the following documents to provide the required information in the *Vendor Survey* found later in this document.

- Organizational Chart
- Security Policies and Procedures
- Proof of compliance with any relevant regulations/standards
- Risk Assessments
- Business Continuity Policies and Procedures
- Incident Response Policies and Procedures
- Coding Practices (if they are providing software)
- Maintenance Plans
- Standard Processes and Procedures

Step 3:

Print out pages 9-26 and answer all the questions in this checklist to the best of your ability using a combination of the information gathered from your Vendor Contacts in step 2 and your own personal research of the vendor.

Step 4

Count and Tally all answers. You will need your totals for Yes, No, and N/A.

Step 5

Subtract your total number of N/A responses from 77 (total number of questions) to **get (X)**

Step 6

Compliance Percentage and Gap Score

Divide your total number of Yes responses by X to calculate the ***Overall Compliance Percentage*.**

Divide your total number of No responses by X to calculate ***Overall Non-compliance Percentage.***

Find the Vendor's ***Gap Score*** in the table below using the overall non-compliance percentage. The Gap Score represents your vulnerability to third-party risk from your vendor.

Gap Score	Vulnerability Level	Compliance Percentage
0	Low	100%
1	Low	81-99%
2	Medium Low	61-80%
3	Medium	41-60%
4	Medium High	21-40%
5	High	0-20%

Step 7

Calculating your Risk Score

1. Determine your ***Threat Level*** value based on the matrix below. This is a rating based on the likelihood that the type of vendor that you are assessing may not be able to provide the products or services that are promised to you. Use the description that most closely relates to the vendor that is being assessed. Use the highest Threat Level of the two columns (Likelihood of being targeted & Reliability).

Threat Level	Likelihood of being targeted	Reliability	Environment
1	This Vendor has a very low likelihood of being targeted by threat actors.	This type of Vendor has a history of very high reliability	This Vendor has a very low likelihood of being affected by a natural disaster or civil unrest.
2	This Vendor has a low likelihood of being targeted by threat actors.	This Vendor has a history of high reliability	This Vendor has a low likelihood of being affected by a natural disaster or civil unrest.
3	This Vendor has a medium likelihood of being targeted by threat actors.	This Vendor has a history of reliability	This Vendor has a medium likelihood of being affected by a natural disaster or civil unrest.
4	This type of Vendor has a medium-high likelihood of being targeted by threat actors.	This Vendor has unpredictable reliability	This type of Vendor has a medium-high likelihood of being affected by a natural disaster or civil unrest.
5	This Vendor has a high likelihood of being targeted by threat actors.	This Vendor has a history of low reliability	This Vendor has a high likelihood of being affected by a natural disaster or civil unrest.

2. Determine your ***Consequence Level*** value based on the matrix below. Use the description that most closely relates to the effects that services or product unavailability could have on your organization. Use the highest Consequence Level of the two columns (Monetary Lose & Effect on critical systems and services).

Consequence Level	Monetary Loss	Effect on critical systems and/or services
1	Services/product unavailability would lead to potential losses (direct & indirect) of less than 1 percent of annual revenue.	Services/product unavailability would lead to minimal critical system and/or services unavailability. No effect to image/reputation.
2	Services/product unavailability would lead to potential losses (direct & indirect) of 1-5 percent of annual revenue.	Services/product unavailability would lead to critical system and/or services unavailable for several hours. Image/reputation affected only minimally.
3	Services/product unavailability would lead to potential losses (direct & indirect) of 5-10 percent of annual revenue.	Services/product unavailability would lead to critical systems and/or services unavailable for 6-12 hours causing significant customer dissatisfaction.
4	Services unavailability would lead to potential losses (direct & indirect) of 10-30 percent of annual revenue.	Services unavailability would lead to critical systems and/or services unavailable for 24 hours causing major customer dissatisfaction. National media coverage of the event.
5	Services unavailability would lead to potential losses (direct & indirect) of more than 30 percent of annual revenue.	Services unavailability would lead to critical systems and/or services unavailable for more than a day causing a disastrous impact to image/reputation. Government intervention highly possible.

3. Determine your ***Criticality Level*** based on the table below. Use the description that most closely reflects the importance of this vendor to your organization.

Criticality Level	Importance of the Vendor
1	This type of vendor has a significantly below average importance to the Organization.
2	This type of vendor has a below average importance to the Organization.
3	This type of vendor has an average importance to the Organization.
4	This type of vendor has an above average importance to the Organization.
5	This type of vendor has an significantly above average importance to the Organization.

4. Use the formula below to determine your ***Vendor Risk Score.*** You can use the resulting value as a comparative data point when assessing other vendors

(Gap Score + Threat Level + Criticality Level)
X
Consequence Level

Step 8

Executive Summary – Optional

Suppose you need to prepare a report for a superior or other stakeholders for later review. In that case, you can complete the *Executive Summary* portion of this worksheet to include with your checklist survey results. Replace the text below that is within the parentheses with the appropriate data.

Executive Summary

Vendor Name: (Enter the Vendor's company name)

Vendor Contact: (Enter your point of contact with the Vendor, including their phone number and email address)

Vendor Website: (Enter the web address of the Vendor's website)

Product: (Enter the product or service that you are receiving from the Vendor)

Compliance Percentage: (Enter your Overall Compliance Percentage from step 6 above)

Risk Score: (Enter your Risk Score from step 7 above)

Introduction:

(Discuss the purpose or objective for performing the assessment)

Background:

(What did you do to prepare for and perform the assessment?)

Findings:

(Summarize the issues/gaps you found through the survey and what should be done to fix them)

Vendor Survey

Some of these questions may not apply to the vendor you are assessing. Mark N/A for those questions.

Category: Vendor Organizational Information Security

THIS CATEGORY COVERS THE VENDOR'S INFORMATION SECURITY POLICIES AND AWARENESS TRAINING.

1. Is there a member of the vendor's organization with dedicated information security duties? If yes, provide their name and contact information.

Yes ☐

No ☐

N/A ☐

Information Security contact:

2. Is a history and background check required for all the vendor's employees accessing and handling your organization's data?

Yes ☐

No ☐

N/A ☐

3. Does the vendor have a documented information security policy that is periodically reviewed and updated? If yes, please upload a copy.

Yes ☐

No ☐

N/A ☐

4. Has the vendor issued its security policy to all employees?

Yes ☐

No ☐

N/A ☐

5. Does the vendor require employees to formally acknowledge adherence to the security policy annually?

Yes ☐

No ☐

N/A ☐

6. Does the vendor have a documented password policy that details the required strength of passwords, length of life, and reuse restrictions? If yes, please list the details in the comments section.

Yes ☐

No ☐

N/A ☐

7. Do all the vendor's employees receive information security awareness training during onboarding and at least annually?

Yes ☐

No ☐

N/A ☐

8. Have the vendor's employees been trained to report suspected security violations and vulnerabilities?

Yes ☐

No ☐

N/A ☐

9. Does the vendor have a documented formal change control process for IT changes?

Yes ☐

No ☐

N/A ☐

10. Does the customer sign off on any changes that the vendor makes that affect the customer?

Yes ☐

No ☐

N/A ☐

11. Does the vendor have a documented procedure for decommissioning old devices that may have contained customer data?

Yes ☐

No ☐

N/A ☐

12. Has the vendor implemented a formal risk analysis process to identify security threats?

Yes ☐

No ☐

N/A ☐

Category: Vendor Compliance

THIS CATEGORY COVERS THE VENDOR'S COMPLIANCE WITH RELEVANT STANDARDS, REGULATIONS, AND BEST PRACTICES.

13. Has the vendor implemented an IT Governance framework such as ITIL or ISO 27001?

Yes ☐

No ☐

N/A ☐

14. If the vendor processes credit cards, are they PCI DSS compliant?

Yes ☐

No ☐

N/A ☐

15. If the vendor processes financial records, are they GLBA compliant?

Yes ☐

No ☐

N/A ☐

16. If the vendor processes medical records or medical insurance data, are they HIPAA compliant?

Yes ☐

No ☐

N/A ☐

17. Does the vendor comply with all applicable standards defined by their industry?

Yes ☐

No ☐

N/A ☐

Category: Vendor General Security

THIS CATEGORY COVERS THE VENDOR'S SECURITY CONTROLS AND PROCESSES

18. Is antivirus software installed and virus definitions regularly updated on the vendor's systems that store or process customer data?

Yes ☐

No ☐

N/A ☐

19. Does the vendor regularly apply system and security patches to systems that store or process customer data?

Yes ☐

No ☐

N/A ☐

20. Does the vendor test system and security patches before implementing them in the production environment?

Yes ☐

No ☐

N/A ☐

21. Do the vendor's employees have a unique log-in ID when accessing customer data?

Yes ☐

No ☐

N/A ☐

22. Does the vendor have security measures for at-rest and in-transit data protection? If yes, please describe them in the comments section.

Yes ☐

No ☐

N/A ☐

Comments:

23. Does the vendor restrict access to systems that contain customer data? Please list controls in place in the comments section.

Yes ☐

No ☐

N/A ☐

Comments:

24. Is physical access to the vendor's data processing equipment restricted? If yes, list the controls in place.

Yes ☐

No ☐

N/A ☐

Controls:

25. Does the vendor have a process for securely disposing of IT equipment and media that have stored or processed customer data? If yes, please describe.

Yes ☐

No ☐

N/A ☐

26. If the Vendor has access to their customer's data, is this access limited to those with a "need to know" and controlled by a specific individual?

Yes ☐

No ☐

N/A ☐

27. Does the vendor share or sell client data to third parties? If yes, in the comments section, identify who the data is shared with or sold to.

Yes ☐

No ☐

N/A ☐

Comments:

28. If the Vendor has access to their customer's data, does the vendor securely delete or return the data when the vendor-client relationship has terminated?

Yes ☐

No ☐

N/A ☐

29. If the vendor stores customer data, is it stored in the same country that the customer resides in?

Yes ☐

No ☐

N/A ☐

30. Does the vender evaluate the security of its third-party vendors?

Yes ☐

No ☐

N/A ☐

Category: Vendor Network Security

THIS CATEGORY COVERS THE VENDOR'S SECURITY CONTROLS RELATED TO THEIR COMPUTER NETWORK.

31. Does the vendor maintain a current network diagram?

Yes ☐

No ☐

N/A ☐

32. Does the vendor use firewalls to protect network boundaries?

Yes ☐

No ☐

N/A ☐

33. Does the vendor have a process to ensure that the firewalls are patched regularly with the latest security updates from the firewall vendor?

Yes ☐

No ☐

N/A ☐

34. Does the vendor regularly perform network vulnerability scanning?

Yes ☐

No ☐

N/A ☐

35. Does the vendor use Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS)? If yes, please describe?

Yes ☐

No ☐

N/A ☐

Description:

36. Are the vendor's employees required to use a VPN when accessing the organization's systems from all remote locations? If no, describe what controls are in place for securing remote access.

Yes ☐

No ☐

N/A ☐

Security controls for remote access:

37. Does the vendor allow wireless access in its organization? If yes, describe how it is protected?

Yes ☐

No ☐

N/A ☐

Wireless protection:

38. Does the vendor monitor the use of privileged accounts?

Yes ☐

No ☐

N/A ☐

Category: Vendor Systems Security

THIS CATEGORY COVERS THE VENDOR'S SECURITY AND AVAILABILITY CONTROLS RELATED TO THE CLIENT DATA THAT THEY STORE.

39. Does the vendor perform regularly scheduled back-ups of its computer systems (servers)?

Yes ☐

No ☐

N/A ☐

40. Has the vendor's backup and recovery process been verified?

Yes ☐

No ☐

N/A ☐

41. Does the vendor store its backups offsite?

Yes ☐

No ☐

N/A ☐

42. Does the vendor encrypt its backups?

Yes ☐

No ☐

N/A ☐

43. Does the vendor verify the integrity of its backups through regular restorations?

Yes ☐

No ☐

N/A ☐

44. Does the vendor replicate data to only locations within the country in which they reside?

Yes ☐

No ☐

N/A ☐

45. Does the vendor refrain from outsourcing data storage? If they do, to whom?

Yes ☐

No ☐

N/A ☐

3rd Party storage:

46. Does the vendor use formal access control to System Administrator privileges?

Yes ☐

No ☐

N/A ☐

47. Are the vendor's servers configured to capture who accessed a system and what changes were made? If no, describe how the vendor determines who accessed the system and what changes were made.

Yes ☐

No ☐

N/A ☐

System access monitoring:

Category: Vendor Application Security

THIS CATEGORY COVERS THE VENDOR'S SECURITY CONTROLS RELATED TO ANY APPLICATIONS THEY PROVIDE TO YOU.

IF THEY ARE NOT PROVIDING SOFTWARE TO YOU, MARK N/A FOR EACH QUESTION.

48. Do the vendor's coding practices address information security during all phases of the SDLC?

Yes ☐

No ☐

N/A ☐

49. Does the vendor perform a security code review during each development phase?

Yes ☐

No ☐

N/A ☐

50. Does the vendor have separate environments for each customer for the development and testing of systems

Yes ☐

No ☐

N/A ☐

Category: Vendor Reliability

THIS CATEGORY COVERS THE VENDOR'S ABILITY TO PROVIDE UNINTERRUPTED SERVICE AND SUPPLY OF PRODUCTS.

51. Does the vendor have an SLA with defined service availability for required services?

Yes ☐

No ☐

N/A ☐

52. Does the vendor have disaster recovery plans for data processing facilities?

Yes ☐

No ☐

N/A ☐

53. Does the vendor have a Business Continuity Plan?

Yes ☐

No ☐

N/A ☐

54. Are the vendor's computer rooms protected against fire and flood?

Yes ☐

No ☐

N/A ☐

55. Does the vendor have a "Hot" recovery site?

Yes ☐

No ☐

N/A ☐

56. Does the vendor conduct periodic drills to verify the effectiveness of its disaster recovery and business continuity plans? If so, how often?

Yes ☐

No ☐

N/A ☐

Indicate how often:

57. Does the vendor provide training to all relevant personnel on backup, recovery, and contingency operating procedures?

Yes ☐

No ☐

N/A ☐

58. Has the vendor operated reliably for at least as long as the proposed service contact?

Yes ☐

No ☐

N/A ☐

59. Is the vendor financially stable with strategic planning in place for the future?

Yes ☐

No ☐

N/A ☐

Category: Vendor Incident Response

THIS CATEGORY COVERS THE VENDOR'S ABILITY TO EFFECTIVELY RECOVER FROM A SECURITY INCIDENT.

60. If there was an information security breach, would the vendor notify the organization? If yes, please note the timeframe below.

Yes ☐

No ☐

N/A ☐

Timeframe to the notification:

61. Does the vendor have a formal Incident Response plan?

Yes ☐

No ☐

N/A ☐

62. Has the vendor experienced an information security breach in the past five years? Please note what information was lost and in what timeframe the clients were notified in the comments section.

Yes ☐

No ☐

N/A ☐

Comments:

63. If the vendor has experienced a breach, have proper measures been put in place to limit the risk of reoccurrence? Give details in the comments section.

Yes ☐

No ☐

N/A ☐

Comments:

64. Does the vendor offer client access to logs after a security event?

Yes ☐

No ☐

N/A ☐

65. Does the vendor carry adequate liability or cyber risk insurance?

Yes ☐

No ☐

N/A ☐

Category: Vendor Auditing

THIS CATEGORY COVERS THE AUDITING OF THE VENDOR'S SECURITY CONTROLS.

66. Does the vendor receive an SSAE-16 SOC Report or a similar third-party audit?

Yes ☐

No ☐

N/A ☐

67. Does the vendor allow clients the right to audit their systems and controls if a third-party audit report is not available?

Yes ☐

No ☐

N/A ☐

Category: Vendor Agreements

THIS CATEGORY COVERS THE CONTRACT BETWEEN YOU AND THE VENDOR.

68. Has both parties signed a contract that establishes the roles and responsibilities of both the vendor and the client?

Yes ☐

No ☐

N/A ☐

69. Can you be released from the contract without excessive penalty if moving to another vendor or in-house becomes necessary?

Yes ☐

No ☐

N/A ☐

70. Has or will the vendor sign a Non-Disclosure Agreement?

Yes ☐

No ☐

N/A ☐

Category: Vendor Product & Support

THIS CATEGORY COVERS THE VENDOR'S ABILITY TO PROVIDE SUPPORT FOR THE PRODUCT.

71. Has the vendor been involved in its industry for more than five years?

Yes ☐

No ☐

N/A ☐

72. Does the vendor provide a support contact that is knowledgeable in the industry? (if yes, enter their name and contact information below)

Yes ☐

No ☐

N/A ☐

Support Contact:

73. Does the vendor provide implementation of their product?

Yes ☐

No ☐

N/A ☐

74. Is support available 24/7?

Yes ☐

No ☐

N/A ☐

75. Have you tested, trialed, or conducted a proof of concept of the products/services offered by the vendor?

Yes ☐

No ☐

N/A ☐

76. Are the vendor's prices equal to or lower than their competitors?

Yes ☐

No ☐

N/A ☐

77. Are there any additional fees that the vendor may require in the future that are not covered in the initial contract?

Yes ☐

No ☐

N/A ☐