

VENDOR RISK ASSESSMENT CHECKLIST

Try Smartsheet for FREE

REFERENCES

Who are your references? Please provide individual names and contact information.

What is the evidence of financial solvency that can be provided, including recent financial statements?

PERFORMANCE

What is your percentage of on-time delivery?

What contract stipulations, including terms, renewal and notification requirements, and required service levels, can you meet?

What are your client and internal communication protocols?

What project management process documentation will be provided for review?

COMPLIANCE

When can we review your liability insurance to ensure that it's up to date?

What is your ability for verifying necessary licensing and regulatory compliance, such as governmental security clearance, financial regulatory compliance, or HIPAA training?

When can we obtain criminal and background checks, including any history from lawsuits, complaints to the state attorney general, or Better Business Bureau records, to demonstrate a history of compliance?

DISASTER PREPAREDNESS

What is your readiness strategy for business continuity in the event of a widespread outbreak of disease?

What are your disaster recovery processes, policies, and procedures for recovery or technology infrastructure continuation after a human-made or natural emergency?

SECURITY PROCESSES

Do you have incident security breach management practices in place?

What is your organizational security process? Can we review any relevant documentation?

Who is in charge, and who receives training in the handling and safeguarding of customer information and procedural breaches?

What are the physical security procedures that define security for offices and data centers? How do you handle visitors, access to premises, and surveillance?

What is the asset management process of operating, maintaining, upgrading, and disposing of digital assets or other valuables?

CYBERTHREAT GOVERNANCE AND ORGANIZATIONAL STRUCTURE

Who is responsible for security and cybersecurity within the organization?

Who is the chief information security officer or chief information officer?

What can you tell us about any teams or committees that meet regularly on cybersecurity issues?

What cybersecurity policies do you employ?
Where do you outsource IT or IT security functions?
When and how frequently do you train employees on your IT security policies? Do you automate assessments?
Who on your senior executive team participates in cybersecurity exercises?
What is your prioritization process to protect your critical assets?
What standards do you use to protect customer information?
What has been your most significant cybersecurity incident?
SECURITY CONTROLS AND TECHNOLOGY
Who is in charge and how do you use cyber vulnerability and cyberthreat information?
When and how do you perform inventory on authorized and unauthorized software and devices?
What practices have you developed to secure configurations for hardware and software?
What do you use to assess the security of the software that you develop and acquire?
What processes do you use to monitor the security of your wireless networks?
What are your data recovery capabilities?
What automated tools do you use to continuously monitor for malware? What processes and tools do you use to reduce and control administrative privileges?
What processes do you have in place to prevent sensitive data exfiltration?
What are your cybersecurity incident plans and preparations?
What processes do you have in place to respond to an incident? Do you regularly practice those processes?
When do you conduct external and internal tests to identify vulnerabilities and attack vectors?
What do you use to manage remote access to your corporate network?
What are your removable media policies and controls?
When and how do you monitor for unauthorized connections, devices, personnel, and software?
What is the process you have in place to communicate security incidents affecting our data?

DISCLAIMER

Any articles, templates, or information provided by Smartsheet on the website are for reference only. While we strive to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the website or the information, articles, templates, or related graphics contained on the website. Any reliance you place on such information is therefore strictly at your own risk.