How to perform proper vendor management and third-party risk assessment reviews

Contents

Introduction

Vendor management, a component of third-party risk management, focuses specifically on evaluating and managing the risks of doing business with external vendors or suppliers. A vendor management program is critical for any organization that relies on third-party services to achieve its business objectives. By establishing a comprehensive program, an organization can identify, assess, and mitigate the risks associated with its third-party relationships. A vendor management program also enables an organization to improve its vendor selection, monitoring, and evaluation processes, ensuring that it receives the expected service and commitments from its third-party providers.

The purpose of this document is to highlight the critical elements of a vendor management process and, when applicable, discuss how the SOC 2® report[1] aligns with that process. The first intended audience for this document is an organization that is looking to implement (or improve) a vendor management program and would use this document as a best practice framework. This document is also intended to be used by auditors and other third-party program assessors who are reviewing controls and processes around a vendor management program to make sure all expected areas have been designed, implemented, and operating as expected.

SOC 2 reports that have a detailed description and documented controls around the security[2] of information and data are the preferred reports needed for review of potential risks or mitigated risks when outsourcing processes and procedures to third-party entities.

The key areas of an effective vendor management program are as follows:

- Governance
- Policy
- Third-party risk assessment reviews
- Due diligence procedures
- Evaluation of vendor contracts
- Ongoing monitoring

1 SOC is a suite of service offerings CPAs may provide in connection with system-level controls of a service organization or entity-level controls of other organizations. There are a variety of SOC services available (for example, SOC 1, SOC 2, SOC 3, SOC for Cybersecurity, and SOC for Supply Chain); however, this paper focuses primarily on SOC 2 reports as they provide insights into how vendors manage user data.

2 Security is only one of the trust services criteria that can be included in SOC 2 reports. The others include Availability, Confidentiality, Processing Integrity, and Privacy.

Governance

A vendor management committee (committee) is a group of designated personnel that oversees the vendor management program and provides guidance and oversight to the business units or departments that work with third-party providers. The committee would also ensure that the vendor management program is aligned with the organization's objectives, values, and culture.

The purpose of the vendor management committee is to

- establish and communicate the vision, mission, and goals of the vendor management program.
- define and implement the vendor management governance structure, roles, and responsibilities.
- develop and maintain the vendor management policies, standards, and procedures.
- ensure compliance with the applicable laws, regulations, and contractual obligations.
- identify and manage the risks and opportunities associated with the vendor relationships.
- monitor and evaluate the performance and value of the vendor relationships.
- facilitate communication and collaboration among the stakeholders involved in the vendor management process.
- promote a culture of continuous improvement and innovation in the vendor management program.
- report on the vendor management program to senior management and the board of directors.

The vendor management committee would consist of representatives from different functions and levels of the organization, depending on the size, complexity, and nature of the vendor relationships. The committee may include the following roles:

- A member of management who serves as the chair of the committee and provides strategic direction and leadership
- A small number of staff members from the related business units or departments who will be working with the third-party providers; and who serve as the business owners and primary contacts for the vendor relationships
- IT personnel and information security personnel, who provide technical support and guidance for vendor relationships
- Compliance personnel, who ensure that vendor relationships comply with the regulatory and contractual requirements
- Procurement or supply chain personnel, who are usually responsible for managing the supply chain or vendor relationships with the entity

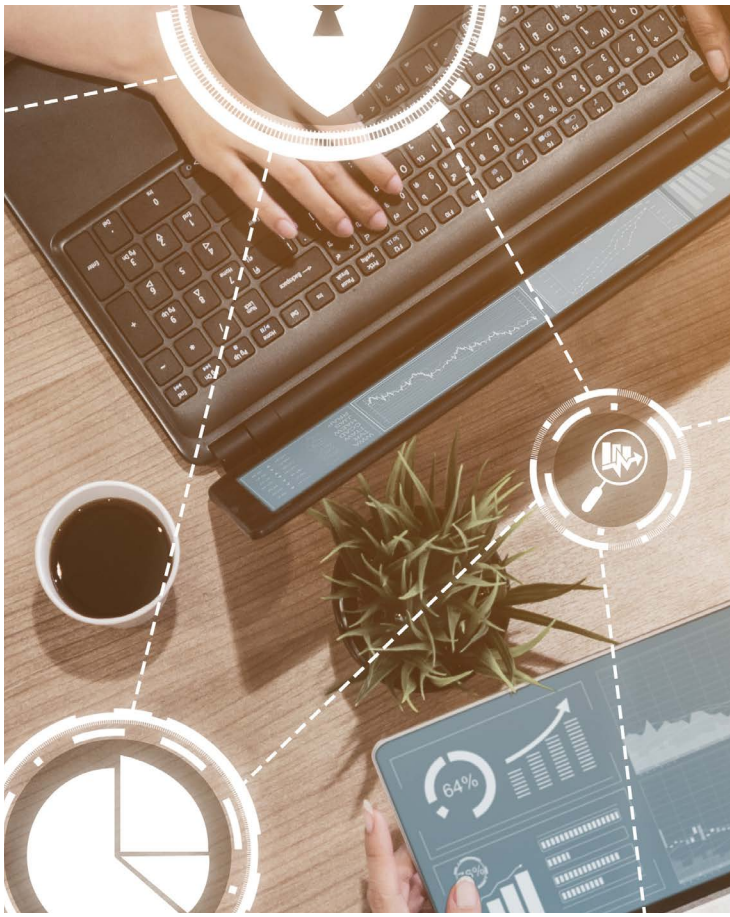
Policy

The policy for a vendor management program defines the objectives, scope, roles and responsibilities, processes, and reporting requirements for managing the organization's third-party relationships. The policy would apply to all vendors that provide goods or services to the organization, or that have access to the organization's data, systems, or facilities. The policy also applies to all employees, contractors, and agents of the organization who are involved in the selection, contracting, monitoring, or termination of vendor relationships.

The policy would aim to

- align the vendor management activities with the organization's strategic goals and risk management objectives.
- establish a consistent and structured approach for selecting, contracting, monitoring, and terminating vendor relationships.
- promote collaboration and communication among the stakeholders involved in the vendor management process.
- foster a culture of accountability and continuous improvement in the vendor management program.

The policy would be reviewed at least annually and updated (with changes or revisions to the policy noted and communicated to those to whom it applies).



Third-party risk assessment reviews

One of the key aspects of vendor management is conducting regular risk assessment reviews of both new and existing third-party vendors. A risk assessment review helps to identify the level of risk exposure, the adequacy of the vendor's controls, and the need for any corrective actions or improvements. A risk assessment review also helps to ensure that the vendor is complying with the contractual obligations, regulatory requirements, and industry best practices.

A risk assessment consists of the following steps:

1. **Define the vendor management program scope.** Not all vendor services are equal regarding their significance and potential impact to the organization, including the system of internal control. Certain vendors may have little inherent risk when compared to other vendors (for example, cleaning crews and janitorial service, landscaping services, document delivery, or courier services). As a result, management would define the criteria against which vendors will be evaluated to determine the nature and extent to which vendor management procedures are necessary and appropriate in the circumstances and in the context of the organization. This would be based on risk factors defined by management (such as sensitivity and access to the data stored, processed, or transmitted; the geography or jurisdiction in which the vendor operates; or the reputation risk posed by the vendor).

2. **Perform an inventory of vendors (identifying and classifying vendors).** This involves identifying all vendors that provide or are likely to provide services and goods (including commercial off-the-shelf software, security appliances, Internet of things [IoT] devices, and other goods and services). Vendors would then be evaluated for applicability against the predefined criteria established in preceding step 1. Vendors that do not pose a material inherent risk may be exempt from extended vendor management assessment procedures, provided those justifications are documented, approved by management, and reviewed on an annual basis. This process allows for the creation of a formal vendor inventory system and for management to ensure the efficient allocation of resources toward material risk areas.

3. **Define the scope and objectives of the applicable vendor assessment process.** This involves determining the scope of the applicable vendor's activities, processes, systems, and controls that are relevant to the organization's objectives, data, and operations. It also involves defining the objectives and criteria of the assessment, such as the regulatory requirements, contractual obligations, acceptable artifacts, certifications, and additional forms of documentation to be provided by vendors, industry best practices, and internal policies and standards with which the vendor would comply.

4. **Prepare for the assessment.** This involves identifying the key stakeholders, roles, and responsibilities of the review team. It also involves developing a review plan that outlines the timeline, methodology, resources, tools, and deliverables of the review. The review plan would include a communication plan that specifies how and when the review team will communicate with the vendor and other parties involved. Part of this preparation would include ensuring the assessment team members have the requisite knowledge, skills, and competencies to execute the review. Reviewers need to understand the methodology, including the evaluation of the artifacts and various forms of assurance provided by existing or potential vendors, and receive ongoing training to ensure continuous improvement and effective decision making. For example, if SOC 2 reports or other forms of documentation are received from existing or potential vendors, the review team personnel would include individuals that are competent and capable of evaluating those forms of documentation for appropriateness and identifying the information necessary to determine the risk impact posed by the vendor.

5. **Conduct the assessment.** This involves collecting and analyzing the appropriate information and evidence from the vendor and other sources, such as the contract, the service level agreement, the vendor's policies and procedures, the vendor's audit or examination reports, the vendor's self-assessment questionnaires, the vendor's performance metrics, as predefined in **step 3**, as well as any feedback from the organization's staff and customers who interact with the vendor. The review team would use various methods and techniques to gather and evaluate the information and evidence based on their knowledge and training, as described in **step 4**. The review team would document the findings and observations of their review, such as (1) the level of inherent risk, (2) the likelihood and impact of the vendor's risk factors based on the vendor's activities, processes, systems, and controls; the gaps and deficiencies in the vendor's compliance with the objectives; and criteria of the review, and (3) the risks and impacts of the vendor's activities, processes, systems, and controls on the organization's objectives, data, and operations. The resulting risk rating or scoring would be documented in accordance with the documentation requirements established in **step 3**.

6. **Reporting and communication.** This involves preparing and presenting a risk assessment review report that summarizes the scope, objectives, methodology, findings, observations, conclusions, and recommendations of the review, consistent with the documentation requirements established in **step 3** and **step 4**. The report would include a risk matrix that shows the overall risk rating of the vendor based on the likelihood and impact of the objectives not being met (an example risk matrix is found in appendix A). The report would also include an action plan and a follow-up template that specifies the corrective actions or improvements that the vendor and the organization would take to address the gaps and deficiencies identified in the review, the responsible parties, the target dates, and the expected outcomes. The report would be communicated to the vendor and other relevant parties, such as senior management, the board of directors, regulators, and service auditors, in a timely and appropriate manner, as applicable.

7. **Revised impact to the assessed level of risk.** This involves formally incorporating the effect of the vendor risk assessment and review procedures into the broader enterprise or organizational risk management program. This ensures that acceptable or unresolved vendor risk factors are not considered separate from the context of the broader organizational goals and risk management objectives. For example, if a vendor receives an audit deficiency or unfavorable security assessment, the effect of that determination, and any necessary remediation determined in **step 6**, may cause prior assessed levels of risk to organizational risk objectives to be higher than previously assessed. Consider a scenario in which the risk of unauthorized disclosure of customer information was assessed to be at an acceptable risk level based on the use of a particular vendor. Then, after that vendor's risk assessment, including a review of that vendor's SOC 2 audit findings, which described the vendor's ineffective system of internal control and data management practices, the previously assessed level of risk of unauthorized disclosure would be reevaluated and may be determined to be unacceptably high, based on the new information. In this event, additional risk treatment decisions and actions may be warranted to bring the risk down to an acceptable level.

Due diligence procedures

Due diligence refers to the process of investigating, assessing, and evaluating new or existing vendors to ensure that they are capable of fulfilling their contractual obligations. These procedures are essential for ensuring that vendors meet an organization's requirements and standards. Due diligence procedures may include the following:

1. **Prepare for the review**

   This part of the due diligence process is a fact-gathering exercise to understand the different aspects and elements of the vendor relationship with the organization. This is where the information gathered will be used in the calculation of risk and determination of any acceptable or countered risk profile of the vendor.

   The scope of the vendor management review covers the following aspects of the vendor relationship:

   - The nature and scope of the services or products provided by the vendor and how they align with the organization's strategic goals and objectives
   - The contractual terms and conditions, including service level agreements, performance metrics, reporting requirements, and dispute resolution mechanisms
   - The compliance status of the vendor regarding applicable laws, regulations, standards, and best practices in the industry
   - The risk profile of the vendor, including financial, operational, reputational, security, and privacy risks that may affect the organization or its customers

   The frequency and nature of a vendor review would be commensurate with the risks and significance of the services provided by a given vendor. Vendors who have access to an organization's sensitive data, for example, would be subjected to more frequent and thorough reviews than would be applied to a vendor who performs custodial services for an office suite. The categorization of the vendor would be based on the following criteria (and performed in connection with the risk assessment review matrix in the preceding section ***Third-party risk assessment reviews***):

   - The criticality of the services or products provided by the vendor, and the impact of their failure or disruption on the organization's operations, reputation, and customer satisfaction
   - The complexity of the services or products provided by the vendor, and the degree of integration, interdependence, and customization required by the organization
   - The sensitivity of the data shared or accessed by the vendor, and the potential exposure of the organization or its customers to data breaches, identity theft, fraud, or other cyberattacks

   A process would be in place to address and resolve vendor issues and incidents. *Vendor issues and incidents* are defined as any events or situations that may adversely affect the quality, timeliness, or security of the vendor services, or cause harm to the organization or its customers. Examples of vendor issues include service outages, data breaches, noncompliance, or poor performance. Organizations would have clear policies and procedures for identifying, reporting, escalating, investigating, and resolving vendor issues and incidents, and holding the vendors accountable for remediation and restitution.

The boundaries of the vendor's access to (or processing of) the user data would be clearly defined and documented, and would include the following information:

- The type, format, sensitivity, source, destination, and frequency of the data exchanged or processed by the vendor
- The ownership, custody, and control of the data, and the roles and responsibilities of the parties involved in the data life cycle
- The data retention, disposal, and back-up policies and procedures, and the security measures and controls implemented by the vendor to protect the data
- The data breach notification and incident response protocols, and the remediation and recovery plans in case of a data compromise

2. Review of vendor financial statements

The review of the vendor's financials would include the following steps:

- Requesting and obtaining the vendor's audited financial statements, including the balance sheet, income statement, cash flow statement, and notes to the financial statements, for the past three years
- Analyzing the vendor's financial performance, liquidity, solvency, profitability, and growth using relevant financial ratios and indicators
- Comparing the vendor's financial results with the industry benchmarks and peer groups and identifying any significant deviations or trends
- Evaluating the vendor's financial stability and viability and assessing the potential impact of any financial distress or insolvency on the organization and its customers
- Documenting the findings, conclusions, and recommendations of the financial review, and reporting any material issues or risks to senior management and the vendor relationship manager

3. Review of vendor reputation

The review of the vendor may also include the following:

- Conducting a background check on the vendor and verifying the vendor's legal name, address, contact information, registration, and licensing
- Searching for any public records or reports on the vendor, such as lawsuits, complaints, investigations, sanctions, or penalties, and evaluating the nature and severity of the issues or incidents
- Searching for any online reviews, ratings, feedback, or testimonials on the vendor, and analyzing the positive and negative aspects of the vendor's services or products, customer service, and overall satisfaction
- Consulting with the industry associations, peers, or experts and obtaining their opinions, insights, or recommendations on the vendor
- Documenting the findings, conclusions, and recommendations of the reputation research and reporting any material issues or risks to senior management and the vendor relationship manager

4. **Review of vendor's SOC 2 report**

A SOC 2 report provides a comprehensive and detailed assessment of an organization's controls related to security, availability, processing integrity, confidentiality, and privacy. Unlike other certifications or assessments that may only offer a high-level confirmation of compliance, a SOC 2 report includes in-depth information about the test procedures and results. This level of detail allows stakeholders to gain a deeper understanding of the effectiveness of the organization's controls and the specific measures taken to protect sensitive data. These reports are conducted in accordance with the AICPA's attestation standards, which are developed by accredited bodies that subject the standards to due process procedures. By providing transparency and thorough documentation, a SOC 2 report helps build trust and confidence among clients, partners, and regulators, making it a valuable tool for demonstrating a commitment to robust security practices.

The review of the vendor's SOC 2 report will include the following steps:

- **Identify the internal personnel who have sufficient knowledge to review the SOC 2 report.** A SOC 2 report is intended to be used by those who have sufficient knowledge and understanding of the service organization, the services it provides, and the system used to provide those services. Without this knowledge, users are likely to misunderstand the content of the SOC 2 report, the assertions made by management, and the service auditor's opinion. Sufficient knowledge ordinarily includes an understanding of the following:
  - The intent and purpose of the SOC 2 report. A SOC 2 examination is a report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy. SOC 2 reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.
  - The nature of the service provided by the vendor.
  - How the vendor's system interacts with user entities, business partners, subservice organizations, and other parties.
  - Internal control and its limitations.
  - Complementary user entity controls and complementary subservice organizations controls and how those controls interact with the controls at the vendor to achieve service commitments and system requirements.
  - User entity responsibilities and how they may affect the user entities' ability to effectively use the vendor's services.
  - The applicable trust services criteria.
  - The risks that may threaten the achievement of the vendor's service commitments and system requirements, and how controls address those risks.

- **Review the vendor's SOC 2 report[3] and understand the following items to ensure that the report is fit for purpose:**
  - General information:
    - The type of examination and related report. Because the informational needs of users vary, there are two types of reports for a SOC 2 engagement:

      Type 1 - An examination of whether a service organization's description presents the system that was designed and implemented at a point in time in accordance with the description criteria, and controls were suitably designed at a point in time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria if controls operated effectively.

      Type 2 - An examination that also addresses the description of the system and the suitability of design of controls and additional evaluation criteria, whether controls operated effectively throughout a period of time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
    - The system, processes, and locations covered by the SOC 2 report (consider if this is the system the organization is using).
    - The report period ("as of" for type 1 and "period" for type 2; also consider if it is recent enough to be useful) and whether there was a gap in time since the prior report period.
    - The scope (that is, the trust services categories: security, availability, confidentiality, processing integrity, or privacy) and whether it is sufficient to meet the needs of the organization.
    - The service commitments and system requirements identified in the system description and whether they are sufficient to address users' needs.
    - The service auditor's opinion on the vendor's description of its system and design, implementation, and operation of the vendor's controls, as applicable.
  - Service auditor information:
    - Who the report was issued by and whether there has been a change in CPA firm since the prior report. Ensuring that the report was issued by a licensed independent CPA or CPA firm (through review of AICPA and other accounting industry websites) is crucial. Objectivity, credibility, and integrity are qualities valued most in assurance providers. These core qualities, in addition to independence, professional skepticism, and commitment to quality, are what consistently guide the judgment and performance of a CPA's work, as required by professional standards. A current CPA license demonstrates commitment to these qualities and is required to issue a SOC 2 report.

3 The AICPA's SOC 2 *Report Walkthrough* video and template provide guidance to those charged with reviewing and evaluating a vendor's SOC 2 report, or for organizations who rely on a third-party risk management solution.

- Additional information to consider:
  - The adequacy of the governance-related controls.
  - The vendor's assertion on the suitability of design and operating effectiveness of its controls relevant to the services provided, as evaluated based on the Trust Services Criteria.
  - The service auditor's testing procedures (which include observation, inspection, and reperformance and do not solely rely on inquiry) and results, and any deviations, exceptions, or deficiencies identified in the vendor's system description or controls relevant to the services or goods provided. Reports with operating effectiveness results (type 2) offer a higher level of comfort than reports that only focus on design and implementation (type 1).
  - Any subservice organizations that provide services on behalf of the vendor and whether they have been included in the scope of the SOC 2 report or excluded. If excluded, the organization would evaluate whether it is necessary to obtain a SOC 2 report from the subservice organization or if there is sufficient information in the vendor's SOC 2 report to provide comfort that risk associated with those subservice organizations are properly managed.
  - The vendor's complementary subservice organization controls (CSOCs), which are the controls at the subservice organization that the vendor depends on in order to deliver the services or goods to the organization.
  - The vendor's complementary user entity controls (CUECs), which are the controls that the organization may need to implement to complement the vendor's controls relevant to the services or goods provided.

    The documentation of the CUECs would include the following steps:

    1. Identifying and documenting the CUECs that are relevant and applicable to the organization based on the vendor's SOC 2 report and the organization's policies and procedures
    2. Implementing and monitoring the CUECs and ensuring that they are operating effectively and consistently
    3. Documenting the evidence of the CUECs, such as policies, procedures, manuals, checklists, logs, reports, or screenshots
    4. Reviewing and updating the CUECs periodically and addressing any changes or gaps in the vendor's system or the organization's requirements

- **Document the findings, conclusions, and recommendations of the SOC 2 report review, and report any material issues or risks to the vendor management stakeholders established in the section *Third-party risk assessment reviews*.**

5. **Alternative procedures for vendors without SOC 2 reports or other third-party assessment reports**

   Because there is an auditor's opinion in relation to the design, implementation, and operating effectiveness (with a type 2 report) of the controls in place, a SOC 2 report gives the most assurance to the control environment. However, if the vendor does not have a SOC 2 report or other third-party assessment report, the following alternative procedures would be followed:

   - Requesting and obtaining a detailed questionnaire from the vendor, which will cover the following topics:
     - The vendor's background, history, ownership, and organizational structure
     - The vendor's services or products, and how they are delivered, supported, and maintained
     - The vendor's internal controls, policies, and procedures, and how they are designed, implemented, and monitored
     - The vendor's compliance status, certifications, and accreditations, and how they are verified and validated
     - The vendor's risk management, incident response, and business continuity plans, and how they are tested and updated
   - Reviewing and evaluating the vendor's questionnaire responses and ensuring the accuracy and completeness of the information provided by requesting and obtaining additional documentation or evidence from the vendor, such as policies, procedures, manuals, checklists, logs, reports, or screenshots. **NOTE:** A self-assessment or catalog of questionnaire responses would be considered to provide a basis of understanding of the internal control framework, and any vendor without an independent assessment would be strongly encouraged to undergo and provide the results of an independent assessment within a period of no more than 24 months.

6. **Periodic on-site visits**

   Periodic on-site visits to the vendor's premises would include the following steps:

   - Planning and scheduling the on-site visit, and communicating the objectives, scope, and agenda of the visit to the vendor.
   - Conducting the on-site visit and observing, inspecting, and interviewing the vendor's personnel, processes, and facilities. Contracts with vendors might require a right-to-audit clause (as noted in item 5 that follows) for these visits.
   - Identifying and documenting any issues, discrepancies, or gaps in the vendor's system, services, or products, and evaluating their impact and risk.
   - Documenting the findings, conclusions, and recommendations of the on-site visit, and reporting any material issues or risks to senior management and the vendor relationship manager.
   - Following up with the vendor on the resolution of the issues or gaps and monitoring the vendor's progress and performance.

Evaluation of vendor contracts

Reviewing and evaluating an organization's contracts with its vendors is an important process in a successful vendor management program. This process begins in the early stages of procurement and requires detailed review from multiple members of the organization to ensure the contract aligns with the applicable objectives and risks.

The first step is to obtain the draft contract and review for completeness, accuracy, and compliance. The contract would state the service commitments and pricing clearly and accurately. It would also specify the performance metrics, service level agreements, and reporting requirements. (If the vendor undergoes a SOC 2 examination, these items may be laid out in the vendor's SOC 2 report, as well). Other critical details to review are as follows:

- Business continuity/disaster recovery requirements and procedures
- Breach notification and incident response requirements and procedures
- Confidentiality or security requirements and commitments for both parties
- Data protection and ownership clauses
- Right-to-audit clauses
- Indemnification and limitations of liability clauses for both parties
- Termination clauses
- Any other relevant terms and conditions

The second step is to compare the contracts with the actual services expected to be delivered by the vendor and identify any gaps, risks, or issues in which the contractual provisions and the expected services are misaligned. Any area of misalignment would be marked and negotiated with the vendor. Once the final contract has been executed, evergreen contracts would be periodically re-reviewed using similar metrics as used in the initial review to ensure the contract is still appropriate as technology, risks, threats, best practices, and organizational objectives mature and evolve. It is good practice to have a legal representative involved in the contract process to ensure regulatory and compliance issues are addressed.

Ongoing monitoring

Once implemented, the vendor management program would be continuously monitored to ensure that it remains effective and aligned with the organization's needs and business objectives. Regular monitoring of the program's effectiveness, incorporating feedback, and implementing changes helps to identify emerging risks before they escalate into significant issues. This also ensures that vendors consistently meet the organization's standards and are delivering value.

Implementing an effective vendor management process ensures that vendor relationships are well-managed, risks are identified and addressed in a timely manner, and business objectives are being met. A robust program allows organizations to proactively address potential issues, optimize vendor performance, and protect sensitive data. SOC 2 engagements play a major role in this process by providing a reliable means to assess and ensure that vendors are maintaining effective controls to protect the privacy and confidentiality of users' data as well as the security, availability, and processing integrity of their systems. SOC 2 reports include valuable information that can add credibility and trust to the information users need to manage the risks associated with outsourced service providers. For additional information on the SOC suite of services and resources available, please visit https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services.

Appendix A — Example risk assessment matrix

The following chart illustrates a *risk matrix,* a tool used to assess and prioritize potential risks associated with third-party vendors. It presents the vendor's overall risk rating based on the likelihood and impact of unmet objectives.

	Third-Party Relationship/Vendor	Description of Services Provided	Employee Assigned to Vendor (e.g., business owner or primary contact for the vendor relationship)	Date of Initial Contract/Renewal Date	Contract Expiration Date, if applicable
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					

	Access Need	Scope of Data	Alter/Modify Data	Level of Access Control	Overall Risk Rating
	15%	**30%**	**20%**	**35%**	
	Requires access to Company or data? 1 - No 3 - May require 5 - Does require	1 - Basic personal information (i.e., name, contact) 2 - Basic transactional (i.e., isolated and particular transactions) 3 - Detailed personal information (i.e., type, number, etc.) 4 - Detailed transactional (i.e., balance history, credit limits)	1 - Read-only 5 - Change/edit transactions	1 - Provided by Company, on-site access 2 - Electronic access to Company systems, permission required w/Company monitoring 3 - Provided by Company, off-site access 4 - Electronic access to Company systems, permission required w/o Company monitoring 5 - Electronic access to Company systems, "always-on" connection	If overall risk <= 2.00, **Tier III** required. If overall risk between 2.01 and 3.99, **Tiers II & III** required. If overall risk >= 4.00, **Tiers I, II, & III** required.
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					

	Tier 1	Tier 2	Tier 3
	1 - Review of system access rights 2 - Financials 3 - SOC 2® report	1 - Review of system access rights 2 - Contract review	1 - Review of associated risks
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			

	Obtained and Reviewed SOC 2 Report Y/N/NA?	Conducted On-Site Visit of Vendor Y/N? (This would be necessary when physical security concerns cannot be obtained through documentation)	Comments	Completed Date
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

aicpa-cima.com

Founded by AICPA and CIMA, the Association of International Certified Professional Accountants powers leaders in accounting and finance around the globe.