Reviewing and Understanding a

Vendor's SOC Report

venminder

What Is a SOC Report?

A SOC (System and Organization Controls) report is an independent audit report which is performed by a certified public accountant (CPA).

A SOC report provides insight into an organization's internal control environment.

Why Is a SOC Report Important?

Reviewing a SOC report helps organizations in the following ways:

- Verifies the vendor has controls in place to protect their system
- Confirms the controls in place are operating effectively and if there are any control exceptions (Type II)
- Ensures independent testing of controls has been completed
- Provides a detailed overview of the control environment supporting the product or service in scope of the audit
- Assists greatly with the inherent risk and criticality assessment, due diligence and residual risk determination and ongoing monitoring phases of the vendor lifecycle and helps guarantee compliance with regulatory expectations

Understanding SOC 1, 2 and 3

Key differences between the types of SOC reports and what they do.

SOC 1

Designed to review a vendor's internal controls as they relate to your financial reporting, and provides a description of the vendor's system and control environment.

SOC 2

Examination of the vendor's controls over one or more of the 5 Trust Services Criteria (security, availability, processing integrity, confidentiality and privacy) and provides a description of the vendor's system and control environment.

SOC 3

Provides a description of the vendor's system and control environment which comes with a seal of completion and the ability to publicly share the SOC 3 report. It's not as detailed, so a SOC 3 is typically only obtained in vendor vetting.

Type I
(for SOC 1 and SOC 2)

Covers audit controls as of a point in time, or otherwise described as a single date.

Type II
(for SOC 1 and SOC 2)

Covers controls that were in place and operating for a period of time. The Type II assessment is more rigorous, and controls are reviewed for operational effectiveness over a period of time.

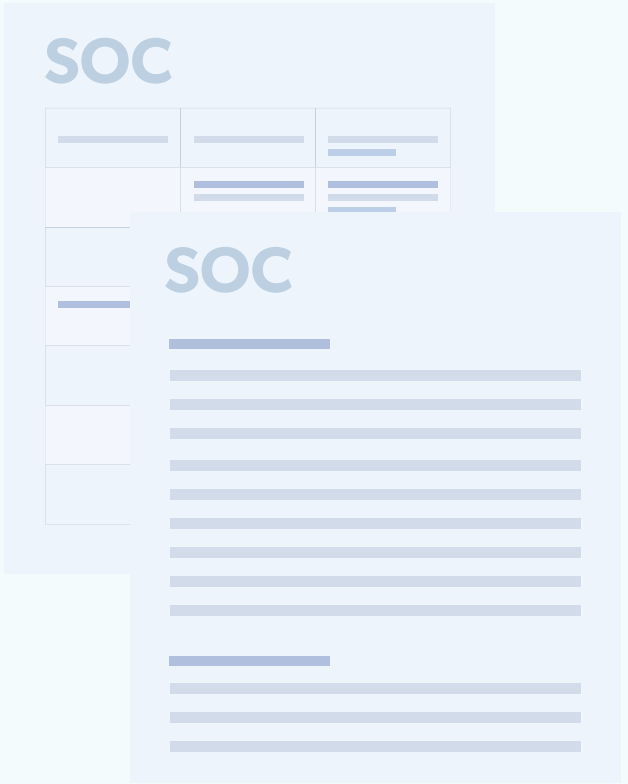
SOC Time Frame

Reporting Period

A SOC report can cover a period of time (Type II), which covers controls that were in place and operating during that time frame, typically six to twelve months; or a SOC report can cover a point in time (Type I), which audits controls on a specific date and includes a review of the suitability of those controls.

You want to ensure the report is the most current available. For Type I reports, verify that they haven't had a Type II report performed, otherwise, request a new report annually. For Type II reports, once a SOC report is as old as the reporting period is long (plus three months), request additional information from your vendor.

Should there be a gap in "coverage" for a SOC report, or an extended amount of time since the completion of the SOC audit, you should request a Bridge/Gap Letter.



A Bridge/Gap Letter should include:

- ☑ The SOC report end date
- ☑ Material changes in the internal control environment (if any)
- ☑ A statement that the service organization isn't aware of any other material changes outside of what is listed in the bridge letter (if any)
- ☑ A reminder that user organizations are responsible for following the complementary user entity controls-sometimes referred to as client control considerations or user control considerations
- ☑ A request for user organizations to read the report
- ☑ A disclaimer that the bridge letter isn't a replacement for the actual SOC report

Reports This Is Found In:
SOC 1
SOC 2
SOC 3

Section 1
Independent Service Auditor's Report

Auditor's Opinion

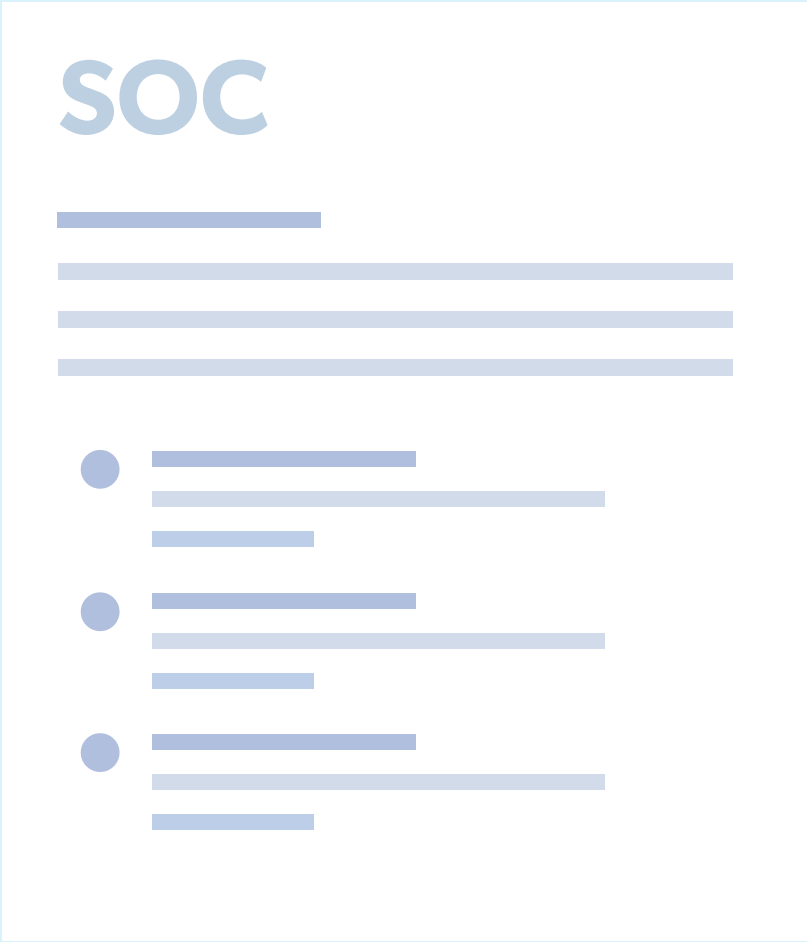
The auditor will notate their overall finding with an opinion of the control environment. Generally, there are four types of opinions you will see in a SOC report: unqualified, qualified, disclaimer and adverse.

An **unqualified opinion**, though sounds bad, is the best news you can hear when discussing SOC report opinions. This should be the standard expectation. You won't necessarily see the words "unqualified opinion" within the report anywhere because it's the baseline state, or normal state of a SOC report. When the auditor feels that the vendor's description fairly represents the system, controls were suitably designed and, in the case of Type II reports, the controls operated effectively, the report is considered unqualified.

A **qualified opinion** is where the vendor had at least one control objective that wasn't implemented or operating effectively. In other words, a qualified report indicates that issues identified in the report were significant enough to deem one or more controls ineffective.

A **disclaimer** is used when there isn't any evidence to prove or disprove that a control wasn't being performed or was in place. This happens often on controls that surround rare occurrences, such as communicating incidents or breaches to clients.

An **adverse opinion** means that the vendor held back or modified information needed to verify controls were either in place or operating effectively. These are very rare, but a red flag.



Disclaimer:
Be aware that the order of Section 1 and Section 2 may be flipped in some SOC reports.

Reports This Is Found In:
SOC 1
SOC 2
SOC 3

Section 2

Management's Assertion Regarding the Effectiveness of Controls

Written Assertion of the Vendor's Management

Management's written assertion should describe the service organization's system to help the auditor perform the upcoming audit with certain reasonable assumptions in mind.

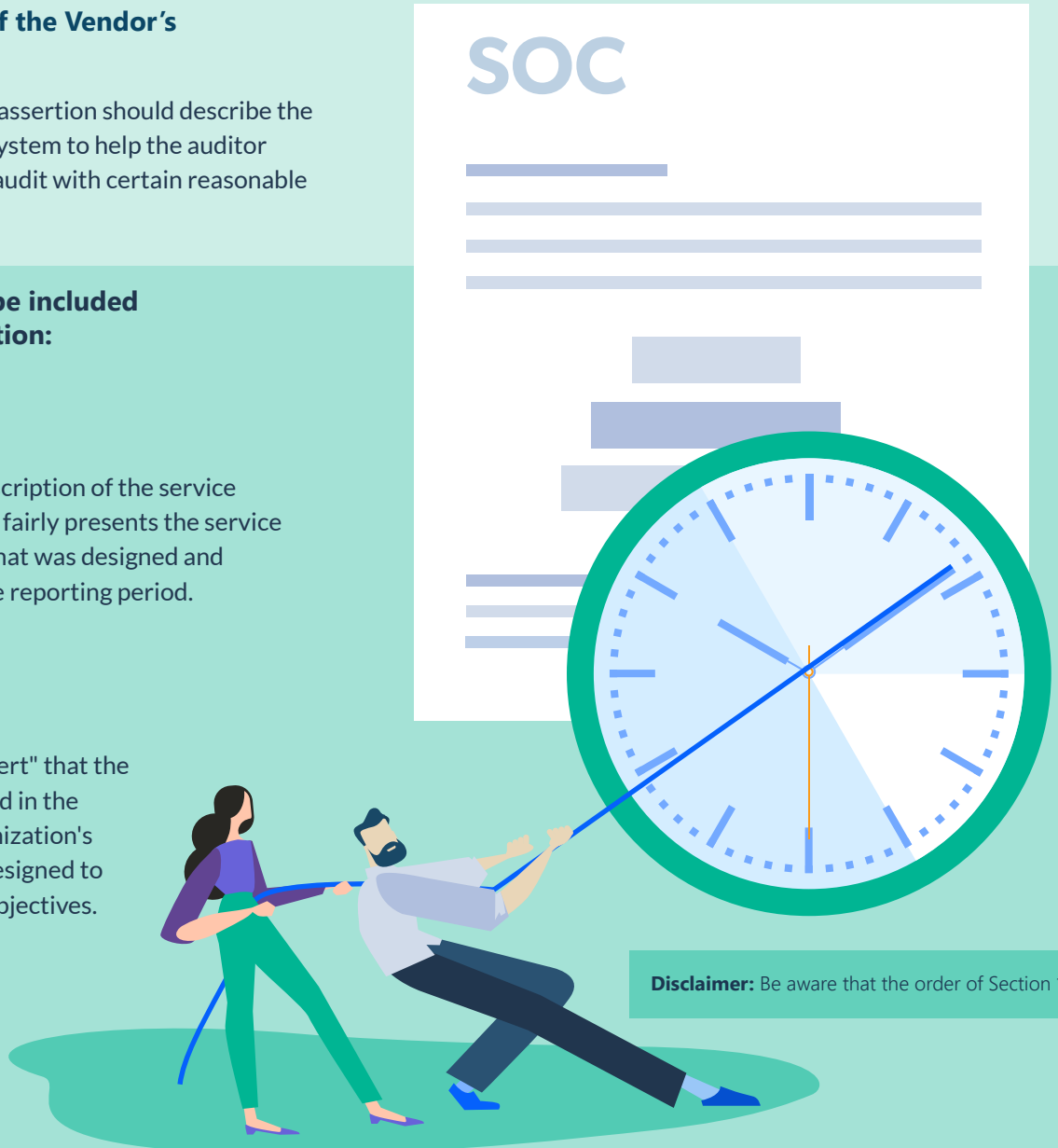
Primary clauses to be included in the written assertion:

1

That management's description of the service organization's "system" fairly presents the service organization's system that was designed and implemented during the reporting period.

2

Management must "assert" that the control objectives stated in the description of the organization's system were suitably designed to achieve those control objectives.



3

Defining the criteria used to effectively make these assertions and, for a Type II report, that the controls were consistently applied.

Disclaimer: Be aware that the order of Section 1 and Section 2 may be flipped in some SOC reports.

Reports This Is Found In:
SOC 1
SOC 2
SOC 3

Section 3

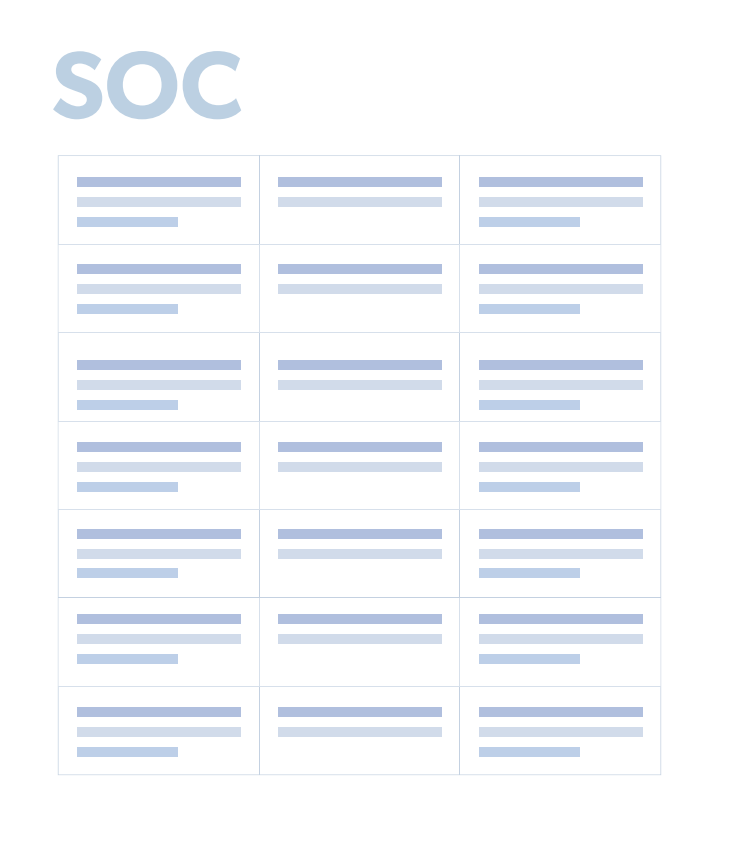
Organization's Description of Its System and Controls

Organization & Administration

This gives you more information about your vendor. It may include when the company was founded, their location, executive and senior management structure and more.

While reviewing this part of a report, you'll want to make sure the following pieces of information are included:

- Tone from the top – Board of director and executive leadership support of risk management
- Security training and policy acknowledgement
- Third-party risk management
- Subservice organizations (aka your fourth parties)



Complementary User Entity Controls (CUEC)

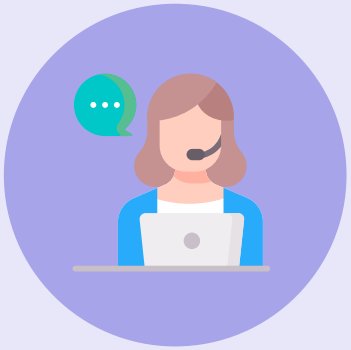
These are the controls the vendor relies on you – the user entity – to implement in order to achieve the vendor's control objectives.

Individual CUECs vary greatly depending on the SOC audit report, service organization and industry. CUECs are critical to understand as they outline what you, the user entity using the product or service, must do to ensure the control objectives are effective. It's putting some responsibility on your organization.

Examples of what a CUEC could say:

- User entities are responsible for controls to provide reasonable assurance that output reports are reviewed by appropriate individuals for completeness and accuracy.
- User entities are responsible for implementing authorization policies and procedures to ensure transactions are appropriately authorized and are secure, timely and complete.

Organization's Description of Its System and Controls



Products and Services

Many vendors have several SOC reports for different products and services and they could all be different.

You may need more than one report for the same product.

Examples:

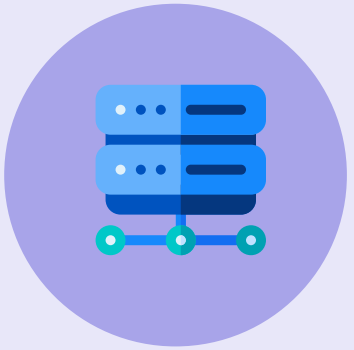
- Information Technology Outsourcing
- Payment Processing
- Call Center Support

The Information System

Understanding what type of information your vendor processes and how they protect it is critical. Your vendor should provide information regarding how they secure servers, networks and computer systems.

Be sure to look at the following areas:

- Server Security
- Network Security
- Access Management
- Vulnerability Management
- System Management



Data Center Information

Understand the access controls, environment and the monitoring of this infrastructure. Data center protections are crucial to protecting information. Look for how your vendor manages their data center and ensures their infrastructure is resilient and available at all times.

Review:

- Physical Access Controls
- Environmental Controls
- Monitoring Controls

Reports This Is Found In:
SOC 1
SOC 2

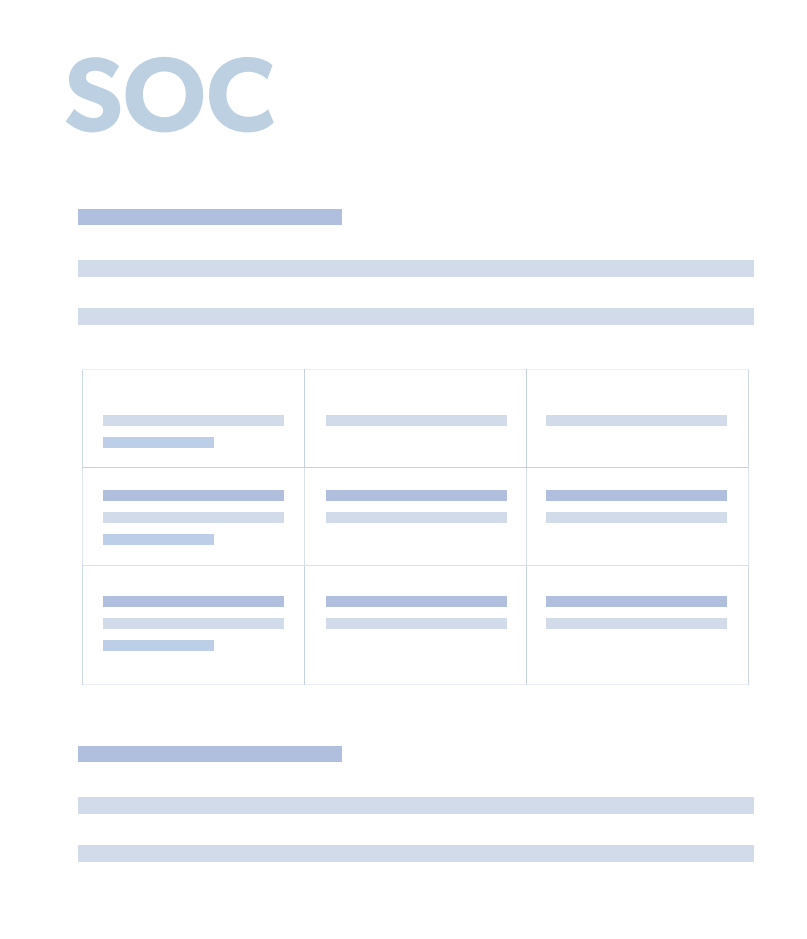
Section 4

Control Objectives, Activities and Tests of Controls

Examination of Control Objectives and Activities

This is where the audit firm can verify and/or test the controls in place and determine if they're in place and operating effectively (Type II).

Identifying audit findings as well as how management responded to those findings are important tools in determining whether the vendor can provide you the service they're contracted to provide.



Reports This Is Found In:
SOC 2

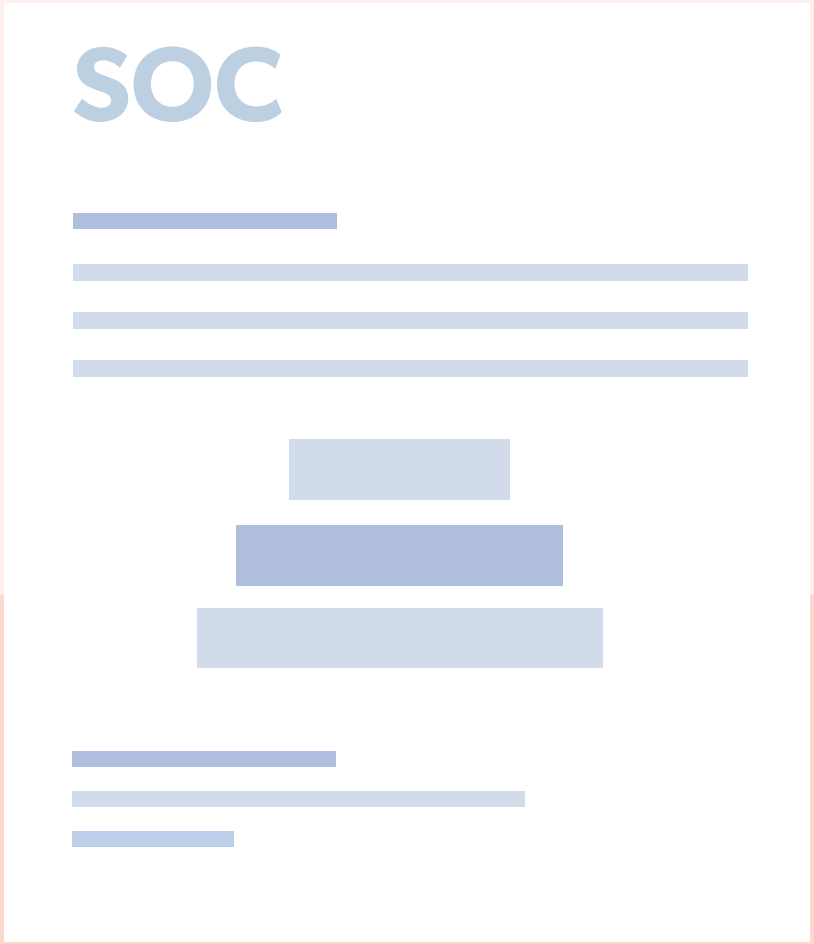
Section 4

Applicable Trust Services Criteria

Review the COSO Principles

In 2019, the COSO 2013 Principles were applied to SOC 2 audits making control requirements more specific. The incorporation of COSO 2013 often overlaps Trust Services Criteria and build upon one another so it's important to consider them during your SOC review.

There are 17 principles falling under 5 main components: Control Environment, Risk Assessment, Control Objectives, Information and Communication and Monitoring.



Think critically as you review the principles and ask yourself questions like the following:

1. Does the vendor have an established code of ethics?
2. Does the vendor make governing policies available to employees?
3. Did the auditors note any exceptions during during control testing?
4. Does the vendor maintain an incident response program?
5. Does the board of directors maintain independence and review the actions of management and operational staff?

Reports This Is Found In:
Case by case basis

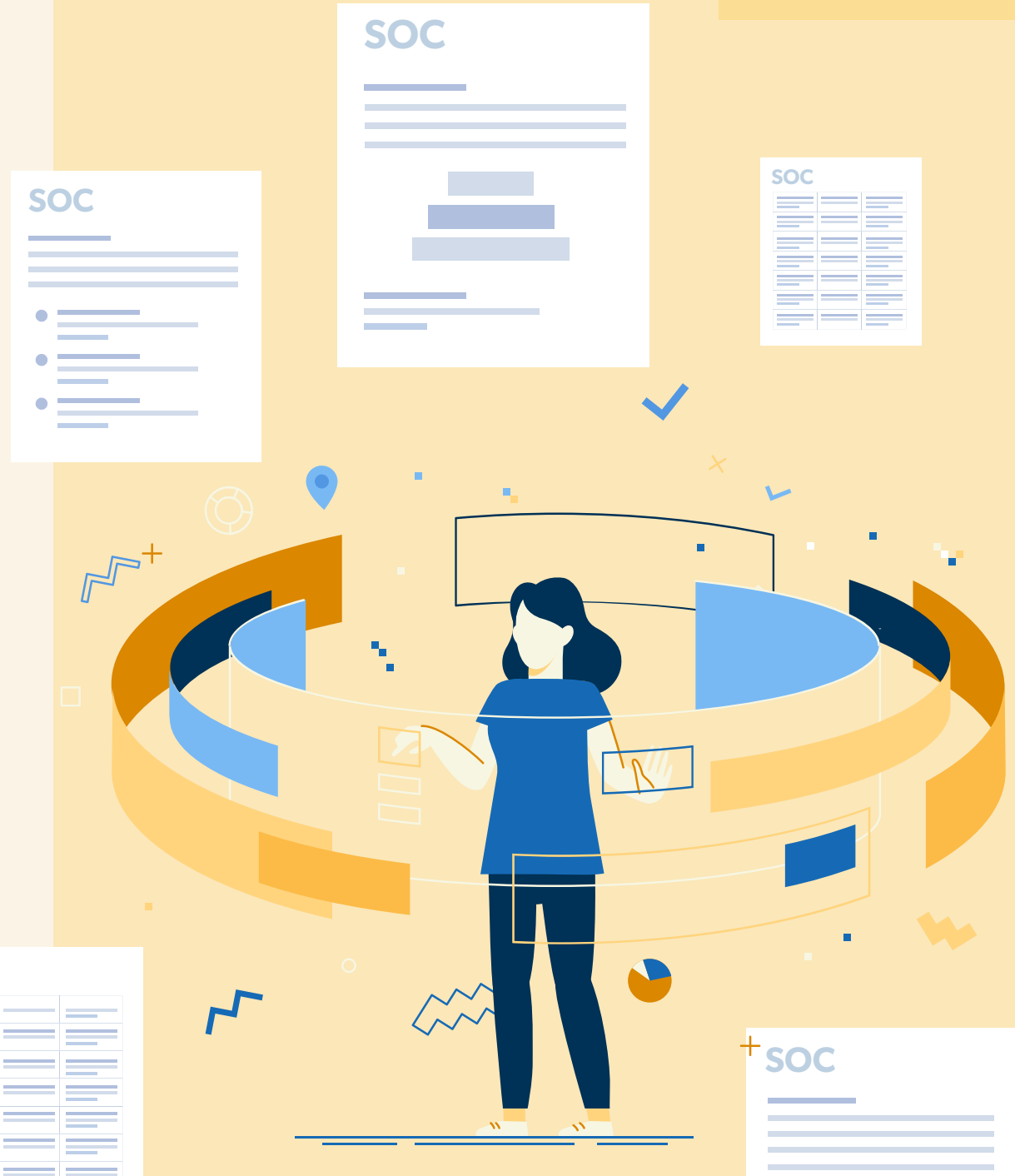
Section 5
Other Information Provided

Additional Vendor Information

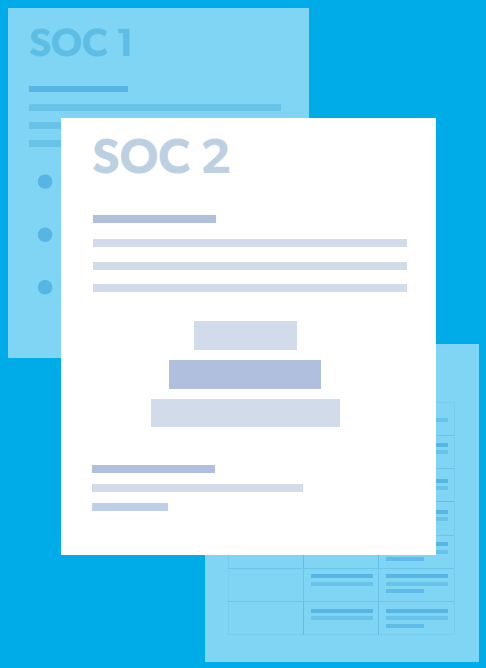
This section is unaudited and provides the vendor an area to share additional information related to the control environment.

Common examples are:

- Management's response to exceptions
- Other details about their control environment



venminder



SOC reports are a great due diligence step when reviewing a vendor as they'll tell you about their internal control environment and how well – or not well – that environment is operating.

Reviewing vendor SOC reports is an integral component of mitigating and reducing vendor risk.

venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

+1 (888) 836-6463 venminder.com

About Venminder

Venminder is an industry recognized leader of third-party risk management solutions. Dedicated to third-party risk, the company is the go-to partner for software, high-quality assessments on vendor controls, certified subject-matter expertise and education.

Venminder's platform provides a centralized location to execute a third-party risk management program. It enables users to store documentation, onboard a vendor, track contracts, manage SLAs, send and manage questionnaires, manage due diligence and oversight, complete risk assessments, create workflows, run reporting and more.

Assessments performed by Venminder's qualified experts, including CISSPs, CPAs, financial risk analysts, paralegals and more, are readily available in an online library. The assessments enable clients to identify possible risks and understand areas of strength on their vendors' information security and privacy standards, SOC reports, financial viability, business continuity/disaster recovery prepared-ness, contractual standards, regulatory compliance and more.

Download a free sample SOC risk assessment and see how Venminder can help reduce your third-party risk management workload.

DOWNLOAD NOW