FORVIS

What Is Missing in the SOC Examination Reports You Receive?

TPRM Madness

TO RECEIVE CPE CREDIT

- **You must respond to at least 3 of the 4 polling questions per CPE hour**
- **You must be logged in for a minimum of 50 minutes per every CPE hour in order to receive CPE credit**

FORVIS

Meet the Presenters

Jennifer Jones
National Practice Leader, SOC and HITRUST

919.610.4658
jennifer.jones@forvis.com

Ryan Boggs
Principal, SOC and HITRUST

828.989.3176
ryan.boggs@forvis.com

FORVIS

FORVIS

What Is Missing in the SOC Examination Reports You Receive?

TPRM Madness

Agenda

- Introductions
- SOC Suite of Services
- What is Missing in the SOC Examination Reports You Receive?
- Closing

Polling Question 1

What do you seek to learn from today's presentation?

A / I am part of the vendor management team or another team responsible for reviewing SOC reports from our vendors and wish to learn how to more efficiently and effectively read and understand those SOC reports.

B / I am a part of the team at my company responsible for issuing our own SOC report to our users and wish to learn ways to enhance our current reports.

C / I am neither part of the vendor management team nor responsible for my company's own SOC report but want to understand more about the SOC suite of services.

FORVIS

SOC Suite of Services

A Recap on the Basics

FORVIS

What are SOC Reports?

- System and Organization Controls (SOC) for Service Organizations
  - SOC for Service Organizations Reports are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address risks associated with an outsourced service.
- Why SOC Reporting?
  - As more and more companies use third-party service providers, there is more demand for a detailed understanding of the processes and controls of these third-party service providers (referred to as service organizations).
  - Service organizations need to show their customers (referred to as user organizations) or prospective customers what processes and controls they have in place around internal controls over financial reporting and/or information security controls around the systems or services they provide.

For CPAs

Provides information to user auditors and service auditors on understanding and performing SOC for Service Organizations Reports

For Users & User Entities

Provides information to user entities on how to mitigate the risks associated with outsourcing services

For Service Organizations

Provides information to service organizations that they can use to build trust and confidence in their systems

FORVIS

SOC Reporting Basics – Key Terms

- **Service Organization or Service Provider**
  - Organization providing the outsourced service
- **Subservice Organization**
  - Organization used by the service organization to provide third-party services to the service organization
- **User Organization or User Entity**
  - Organization receiving the outsourced service
- **Service Auditor**
  - Auditor performing SOC examination of the service organization's controls
- **User Auditors**
  - External auditors of the user organization/entity

FORVIS

SOC Suite of Services

SOC 1

These attestation reports are specifically intended to meet the needs of entities that use service organizations (user entities) as their financial statement auditors (user auditors) use these reports to help evaluate the effect of the controls at the service organization on the user entities' financial statements.

SOC 2

These attestation reports are intended to meet the needs of a broad range of users that need assurance about a service organization's controls as they relate to the security, availability, and processing integrity of the systems the service organization uses to process its users' data and the confidentiality and privacy of the information processed by those systems.

General Examination

These attestation reports are reports on which the Service Auditor issues an opinion about whether a subject matter is in accordance with (or based on) the criteria or the assertion is fairly stated, in all material respects. This type of report is highly customizable to whatever a service organization's needs may be and is intended to provide a service organization's user entities with reasonable assurance over a subject matter.

SOC 3

SOC 3 reports are designed to meet the needs of users who need assurance about the controls at a service organization relevant to security, availability, processing integrity, confidentiality, and/or privacy but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report. Since they are general use reports, SOC 3® reports can be freely distributed.

SOC for Cybersecurity

The AICPA's cybersecurity risk management reporting framework helps organizations communicate about the effectiveness of their cybersecurity risk management programs.

FORVIS

SOC Reporting Basics

	SOC 1	SOC 2
What is Covered by the Report?	Controls related to financial reporting for user organizations	Controls relevant to security, availability, confidentiality, processing integrity, and/or privacy
Intended Audience	Auditors and management of user organizations ("auditor-to-auditor communication")	Auditors, stakeholders (e.g., management, business partners, customers), regulators
Report Format	Long form which includes a detailed description of the system and controls	Long form which includes a detailed description of the system and controls

- SOC 1 and SOC 2 reports are the most common and most useful for vendor risk management purposes.

FORVIS

SOC Reporting Basics – Key Terms (Continued)

- **Type 1**
  - Not to be confused with a SOC 1, a Type 1 report signifies that the report is only as of a specific point in time
  - This type of report includes design and implementation but does not include operating effectiveness of controls
  - Example: SOC 1 Type 1 or SOC 2 Type 1
- **Type 2**
  - Not to be confused with a SOC 2, a Type 2 report signifies that the report covers the operations of controls over a specified period of time
  - This type of report includes design, implementation, and operating effectiveness of controls
  - Example: SOC 1 Type 2 or SOC 2 Type 2

FORVIS

What Is Missing in the SOC Examination Reports You Receive?

FORVIS

Understanding What Might Be Missing

- **There are some preliminary questions to ask yourself before you even dig into the SOC report you received**
  - Do you have the right report for your needs?
    - A SOC 1 Report covers internal controls at the service organization that are relevant to your own internal controls over financial reporting. It will likely not have detailed descriptions of controls relevant to information security, availability, confidentiality, processing integrity, and/or privacy
    - A SOC 2 Report covers internal controls at the service organization that are relevant to information security, availability, confidentiality, processing integrity, and/or privacy. It will likely not have any information relevant to your own internal controls over financial reporting.
  - Is the service auditor reputable?
- **To be able to understand what is missing, you must first understand how to evaluate a SOC report**
- **Our approach for evaluation of a SOC report as an audit firm is presented on the following slides**

FORVIS

How to Evaluate a SOC Report – Initial Questions

- **User to Service Provider(s)**
  - What do you as the User (the company) outsource and to whom?
  - How does that compare to the scope of the SOC report(s) received from those Service Providers?
    - Nature/type of services
    - Applications covered/not covered
    - Geographies/processing centers covered/not covered
    - Period covered by the scope of the report
- **Subservice Organization to Service Provider**
  - Is there anything that the Service Provider outsources to a third party?
  - If so, how is this handled in the opinion?

FORVIS

How to Evaluate a SOC Report – Anatomy

- **Section 1: Report of Independent Service Auditors**
  - The "opinion"
- **Section 2: Management's Written Assertion**
  - May also include a subservice organization's assertion
- **Section 3: Management's Description of the System**
  - Provided by the service organization to describe the overall control environment and the control objectives and control activities related to the system being examined
- **Section 4: Control Objectives and Control Activities**
  - Independent Service Auditor's tests of controls and results of those tests included in a Type II
- **Section 5 (optional): Supplemental Material Provided by the Service Organization**

FORVIS

How to Evaluate a SOC Report – What to Look For

- **Section 1: Report of Independent Service Auditors (the "Opinion")**
  - Was the auditor's opinion qualified or not? If qualified, why was it qualified?
  - Were there any opinion modifications or scope limitations?
  - Is the period of time covered by the report appropriate?
- **Section 2: Management's Written Assertion**
  - This section generally contains the same information as the opinion
- **Section 3: Management's Description of the System**
  - Review the scope of description to identify systems and applications covered and verify the correct systems are covered
  - Evaluate subservice organizations and potentially obtain SOC reports for any significant subservice organizations relevant to financial reporting
  - Evaluate complementary user entity controls and verify these controls are within your environment
- **Section 4: Control Objectives and Control Activities**
  - This section includes tests and results, and it is important to identify any issues noted by the Service Auditor and how they might impact your own control environment
  - Important to evaluate whether or not tests are sufficient for your needs – Inquiry alone is never sufficient
- **Section 5: Optional Section (May include management's responses to testing exceptions)**
  - Management can provide responses to testing exceptions here, which can be useful in determining impact to your own control environment

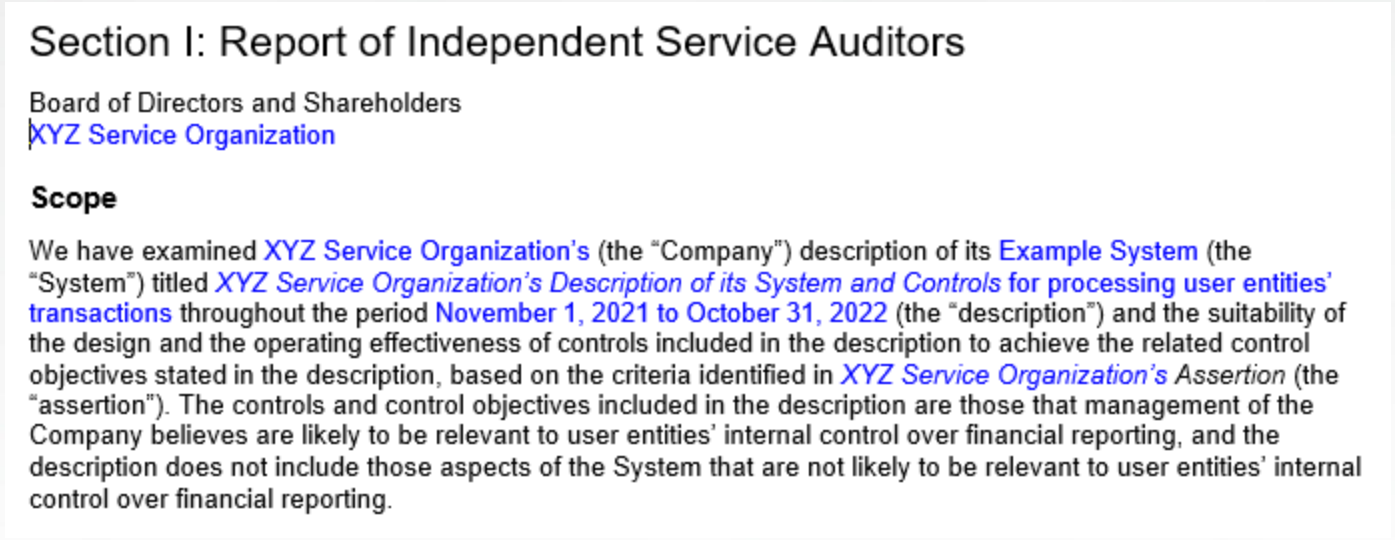
FORVIS

Section 1

FORVIS

Section 1: SOC 1 Type 2 Opinion

- The first paragraph of the Service Auditor's opinion identifies the scope of the report.
- In this example, the scope of the report is the Example System for the period of November 1, 2021 to October 31, 2022.
- If the reporting period doesn't align to your needs, you may want to consider requesting when the next report will be available and request a Bridge Letter (to be discussed later) in the interim period.



Section I: Report of Independent Service Auditors

Board of Directors and Shareholders
XYZ Service Organization

Scope

We have examined XYZ Service Organization's (the "Company") description of its Example System (the "System") titled *XYZ Service Organization's Description of its System and Controls* for processing user entities' transactions throughout the period November 1, 2021 to October 31, 2022 (the "description") and the suitability of the design and the operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in *XYZ Service Organization's Assertion* (the "assertion"). The controls and control objectives included in the description are those that management of the Company believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

FORVIS

Section 1: SOC 1 Type 2 Opinion (Continued)

- Additional paragraphs may appear below the first paragraph of the opinion within the Scope section.
- These are the most common:
  - A Carve-Out for Complementary Subservice Organization Controls
  - A Carve-Out for Complementary User Entity Controls
  - A Carve-Out for controls that did not operate because the circumstances that warranted operation did not occur (Non-Occurrence)

FORVIS

Section 1: SOC 1 Type 2 Opinion (Continued)

- Carve-Out for Complementary Subservice Organization Controls

The Company uses Computer Subservice Organization, a subservice organization, to process and store customers' personal information or The Company uses the subservice organizations listed in the *Subservice Organizations* table in Section III of this report. The description in Section III of this report includes only the control objectives and related controls of the Company and excludes the control objectives and related controls of the subservice organization(s). The description also indicates that certain control objectives specified by the Company can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. Our examination did not extend to controls of the subservice organization(s), and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

FORVIS

Section 1: SOC 1 Type 2 Opinion (Continued)

- When a **Carve-Out for Complementary Subservice Organization Controls** appears within the opinion, you should look for the following when reviewing Section III of the report:
  - The nature of the services performed by the subservice organization and controls assumed in the design of the service organization's controls
  - The monitoring controls at the service organization in place to monitor the subservice organization
- Based on the nature of the subservice organization, you might want to obtain and evaluate the SOC report of the subservice organization as well (if available)

FORVIS

Example Subservice Organization Description

G. Subservice Organizations

The Company utilizes subservice organizations to perform certain functions. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organization.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organization and are necessary to achieve specific control objectives, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organization. Each user entity's internal control over financial reporting must be evaluated in conjunction with the Company's controls and the related tests and results described in Section IV of this report, considering the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Subservice Organization	Service(s) Provided and Monitoring Controls	Relevant Control Objectives
ABC Services, Inc.	The Company uses ABC Services for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control areas are critical to achieving the applicable control objectives:	Control Objective 2*
	• Controls around the physical security of the Data Centers hosting the in-scope applications, and • Controls around the backup processes of servers hosting the in-scope applications to support disaster recovery processes.	
	In addition, the Company has identified the following controls to help monitor the subservice organization:	
	• On an annual basis, management evaluates the third parties that have access to confidential data and/or that perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management performs the following to help monitor the third party: ○ Performs a vendor security assessment of the third party which includes reviewing the complementary subservice organization controls which	

Consider whether or not the monitoring control activity described is to the sufficient level of precision based on the nature of the services

Example Subservice Organization Complementary Control Areas

Example Monitoring Control Activity (Control performed by the service organization to monitor the performance of the subservice organization)

FORVIS

Polling Question 2

Which factor below is most critical when evaluating a SOC report?

A / Exceptions

B / Scope of Report

C / Complementary Subservice Organization Controls

FORVIS

Section 1: SOC 1 Type 2 Opinion (Continued)

- Carve-Out for Complementary User Entity Controls

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

FORVIS

Section 1: SOC 1 Type 2 Opinion (Continued)

- When a **Carve-Out for Complementary User Entity Controls** appears within the opinion, you should consider the following when reviewing **Section III of the report**:
  - The Complementary User Entity Controls descriptions (usually located at the end of the description of the system)
  - Where or how each applicable Complementary User Entity Control is being addressed in your own control environment as a user of the report
  - This section is extremely important and often overlooked; if this is missing from the SOC report you are reviewing or the service organization didn't include any complementary user entity controls, you should consider following up with the service provider to confirm your responsibilities

FORVIS

Example Complementary User Entity Control Description

H. User Entity Controls

XYZ Service Organization's controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company's system. It is not feasible for the control objectives to be solely achieved by the Company. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with the Company's controls and related testing detailed in Section IV of this report, taking into account the related complementary user entity controls identified in the table below, where applicable. Complementary user entity controls and their associated control objective(s) are included within the table below.

In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine if the identified complementary user entity controls have been implemented and are operating effectively.

User Entity Controls	Related Control Objectives
Each user organization is responsible for helping to ensure the confidentiality of any user IDs and passwords assigned to it for use with XYZ Service Organization 's systems.	Control Objective 3*
Each user organization is responsible for performing annual user access reviews for access to XYZ Service Organization's systems.	Control Objective 3*
Each user organization is responsible for provisioning and deprovisioning access to its Example System environment.	Control Objective 3*
Each user organization and XYZ Service Organization will mutually agree upon the timing of invoice schedules. Each user organization is responsible for communicating changes to the approved invoice schedule.	Control Objective 4*

These are the controls that users of the report are responsible for helping to ensure are implemented and operating in their own environments

Have you implemented controls to address these responsibilities in your own environment?

FORVIS

Section 1: SOC 1 Type 2 Opinion (Continued)

- When controls did not operate to achieve a control objective, in part or in full, because the circumstances that warranted operation of the related controls did not occur, a "Non-Occurrence" Paragraph should be added to the Scope paragraph of the Service Auditor's Opinion

As indicated on page [*nn*] of XYZ Service Organization's description of its Trust System, no new accounts were established for the ABC application during the period January 1, 201X, to September 30, 201X; therefore, we did not perform any tests of the design or operating effectiveness of controls related to the control objective 2, *Controls provide reasonable assurance that new accounts are authorized and set up on the system in a complete, accurate, and timely manner.*

- A "Non-Occurrence" Paragraph is not necessarily a negative item – it just means the Service Auditor determined that the circumstances that warranted operation of specific controls noted within the description of the system did not occur, so it could not be tested for design or operating effectiveness

FORVIS

Section 1: SOC 1 Type 2 Opinion (Continued)

Service Organization's Responsibilities

In Section II of this report, the Company has provided an assertion about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The Company is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; selecting the criteria stated in the assertion; and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period November 1, 2021 to October 31, 2022. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion;
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- Evaluating the overall presentation of the description, the suitability of the control objectives stated in the description, and the suitability of the criteria specified by the service organization in its assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions or identify the function performed by the System. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

- Following the Scope section are the Service Organization's Responsibilities, the Service Auditor's Responsibilities, and Inherent Limitations
- These sections do not typically provide useful information for purposes of evaluating a control environment and only contain standard language explaining the limitations and responsibilities of the different parties preparing the report

FORVIS

Section 1: SOC 1 Type 2 Opinion (Continued)

- **After the Inherent Limitations section is the actual Service Auditor's Opinion**

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in Section IV of this report.

Opinion

In our opinion, in all material respects, based on the criteria described in XYZ Service Organization's assertion,

A. The description fairly presents the System that was designed and implemented throughout the period November 1, 2021 to October 31, 2022.
B. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period November 1, 2021 to October 31, 2022 and if the subservice organization(s) and user entities applied the complementary controls assumed in the design of XYZ Service Organization's controls throughout the period November 1, 2021 to October 31, 2022.
C. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period November 1, 2021 to October 31, 2022 if complementary subservice organization and user entity controls assumed in the design of XYZ Service Organization's controls operated effectively throughout the period November 1, 2021 to October 31, 2022.

This example is what is called an unqualified opinion

This means that the Service Auditor concluded that all of the control objectives identified by the Service Organization were suitably designed and operating effectively (assuming a Type 2 Report)

FORVIS

Section 1: SOC 1 Type 2 Opinion (Continued)

- **Modified Opinion Example**

Basis for Qualified Opinion

The service organization states in its description that it has controls in place to reconcile securities account master files to subsidiary ledgers, to follow up on reconciling items, to perform surprise annual physical counts, and to independently review its reconciliation procedures. However, as noted at page [mn] of the description of tests of controls and results, controls related to the reconciliations and annual physical counts were not performed during the period November 1, 2021 to October 31, 2022. As a result, controls were not operating effectively to achieve control objective 3, *Controls provide reasonable assurance that securities account master files are properly reconciled to subsidiary ledgers and surprise annual physical counts are performed.*

Qualified Opinion

In our opinion, except for the matter referred to in the preceding paragraph, in all material respects, based on the criteria described in XYZ Service Organization's assertion,

A. The description fairly presents the System that was designed and implemented throughout the period November 1, 2021 to October 31, 2022.
B. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period November 1, 2021 to October 31, 2022 and if the subservice organization(s) and user entities applied the complementary controls assumed in the design of XYZ Service Organization's controls throughout the period November 1, 2021 to October 31, 2022.
C. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period November 1, 2021 to October 31, 2022 if complementary subservice organization and user entity controls assumed in the design of XYZ Service Organization's controls operated effectively throughout the period November 1, 2021 to October 31, 2022.

If the opinion is qualified, you should:

- Review the description of test procedures and results in Section IV to understand the nature, timing, and extent of the deviation
- Determine the impact of the failure on your own control environment
- Consider performing additional substantive testing if it is a significant impact or discussing further with the Service Organization
- Review management's responses to exceptions noted (oftentimes found below the exception or in an unaudited section of the report, Section 5)

FORVIS

Section 1: SOC 1 Type 2 Opinion (Continued)

- **Restricted Use Example**

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of the Company, user entities of the Company's System during some or all of the period November 1, 2021 to October 31, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

(Insert Signature Logo)

City, ST

DATE

FORVIS

Section 2

FORVIS

Section 2: SOC 1 Type 2 Assertion

- SOC 1 Type 2 Assertion generally mirrors the SOC 1 Type 2 Opinion from the Service Auditor
- While not useful for obtaining new information, it is important that management does make an assertion

FORVIS

Section 2: SOC 1 Type 2 Assertion (Continued)

XYZ Service Organization Logo

Section II: XYZ Service Organization's Assertion

We have prepared the description of XYZ Service Organization's (the "Company") Example System (the "System") entitled *XYZ Service Organization's Description of its System and Controls* for processing user entities' transactions throughout the period November 1, 2021 to October 31, 2022 (the "description"), for user entities of the System during some or all of the period November 1, 2021 to October 31, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the subservice organization(s) and user entities of the System themselves, when assessing the risks of material misstatement of the user entities' financial statements.

The Company uses Computer Subservice Organization, a subservice organization, to process and store customers' personal information or The Company uses the subservice organizations listed in the *Subservice Organizations* table in Section III of this report. The description includes only the control objectives and related controls of the Company and excludes the control objectives and related controls of the subservice organization(s). The description also indicates that certain control objectives specified by the Company can be achieved only if the complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. The description does not extend to the controls of the subservice organization(s).

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. The description does not extend to the controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

A. The description fairly presents the System made available to user entities of the System during some or all of the period November 1, 2021 to October 31, 2022 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

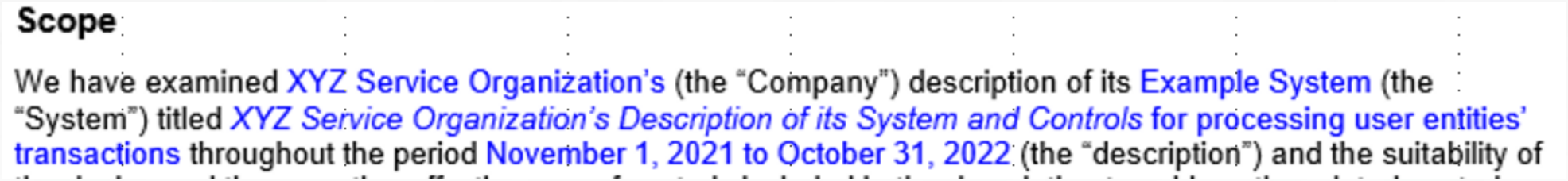
FORVIS

Section 3

FORVIS

Section 3: Management's Description of the System

- The Description of the System follows Management's Assertion and is usually Section 3 of a SOC 1 Type 2 Report
- The Description of the System is the section within a SOC 1 Report that the Service Auditor is opining on:
  - Whether or not the description is fairly presented in accordance with the description criteria identified within management's assertion
  - Whether or not the controls stated in the description were suitably designed
  - Whether or not the controls stated in the description were operating effectively



Scope

We have examined XYZ Service Organization's (the "Company") description of its Example System (the "System") titled *XYZ Service Organization's Description of its System and Controls* for processing user entities' transactions throughout the period November 1, 2021 to October 31, 2022 (the "description") and the suitability of

FORVIS

Section 3: Description of the System (Continued)

- Look for the following key items when evaluating Management's Description of the System:
  - Scope of IT Systems included and their relevance to your own environment; are any systems missing that you expected to be included?
  - Key reports and how they are generated and reviewed for accuracy and completeness
  - Complementary subservice organization controls and monitoring controls
  - Complementary user entity controls

FORVIS

Polling Question 3

Which area of the SOC report is required to have complementary user entity controls described in detail?

A / Section I: Opinion

B / Section II: Assertion

C / Section III: Management's Description of the System

D / Section V: Other Information Provided by Management

FORVIS

Section 4

FORVIS

Section 4: Control Objectives and Control Activities

- Section 4 in a Type 2 Report includes the Control Objectives, Control Activities, Test Procedures performed by the Service Auditor, and Results of Testing
- Obviously one of the items to focus on is whether or not there are any testing exceptions
- Beyond exceptions, it is also important to determine whether or not the **procedures performed were adequate** for your purposes:
  - Did the Service Auditor test all attributes of the control properly?
  - Did the test procedure cover the entire specified period?
  - Were procedures beyond inquiry performed? (Inquiry alone is not sufficient)

FORVIS

Section 4: Control Objectives and Control Activities

- Section 4 Example

Control Objective 1—Defined Contribution Plan Setup

Controls provide reasonable assurance that defined contribution plans set up on the ABC Recordkeeping application are authorized by plan sponsors and completely and accurately processed and recorded in a timely manner.

Controls Specified by Example Service Organization	*Tests of Controls*	*Results of Tests*
1.1 New plans or plans from prior recordkeepers are accepted and entered in the ABC Recordkeeping application only after receipt of a signed and authorized administrative services agreement from the plan sponsor. A member of the service organization's new accounts team uses a new accounts setup checklist to ensure that plans are set up completely and accurately in the ABC Recordkeeping application, based on the information in the supporting document provided by the plan sponsor or prior recordkeeper.	Inspected the administrative services agreement for a sample of new plans to determine that the agreement was signed and authorized by the plan sponsor for each selected plan.	No exceptions noted.
	Inspected the new accounts setup checklist for a sample of plans to determine that the checklist was completed and signed by the new accounts team manager for each selected plan.	No exceptions noted.
	. . .	

FORVIS

AICPA SOC 1 Guide, 2017

Section 5

FORVIS

Section 5: Other Information Provided By Management

- Section 5 is an optional section
- It is often used by management to provide mappings to other control frameworks or to provide more information about exceptions
- Section 5 is an unaudited section, which means management's responses to testing exceptions are **not** included within the Service Auditor's opinion
- If management's response to exceptions noted does not include enough detail, such as actions taken to remediate the issue and prevent issues from occurring in the future, you may want to reach out to the service organization for additional information

FORVIS

Section 5: Other Information Provided By Management

- Section 5 Example

Section V: Other Information Provided by XYZ Service Organization

The information in this section describing activities and controls is presented by the Company to provide additional information to its user entities and is not part of the Company's description of controls that may be relevant to the user entities' internal control as it relates to an audit of financial statements or internal control over financial reporting. The information in Section A, *Disaster Recovery Plan*, and in Section B, *Management's Responses to Testing Exceptions*, have (has) not been subjected to the procedures applied in the examination of the description of the Company's Example System, and accordingly, FORVIS, LLP expresses no opinion on it.

A. Disaster Recovery Plan

The disaster recovery and . . . .

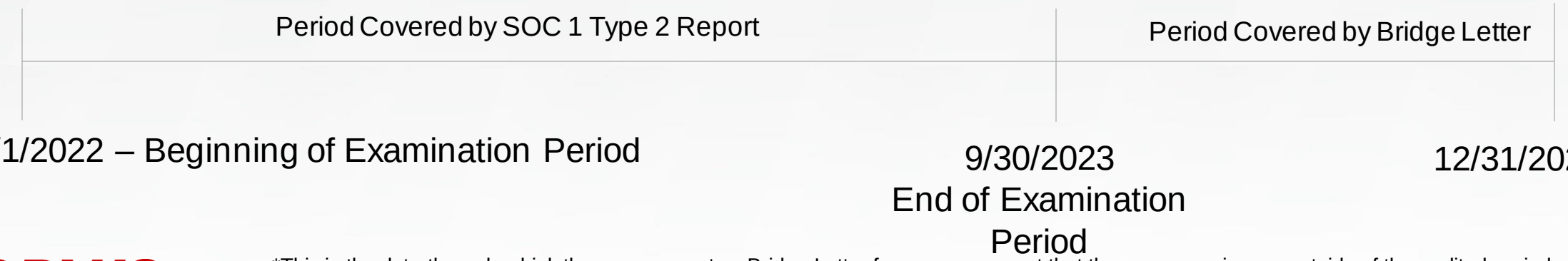
FORVIS

Bridge Letters

FORVIS

SOC Bridge Letters

- Did you receive a **Bridge Letter** along with your SOC reporting package?
- **Bridge Letters** are letters from management of the Service Organization directly to its users to cover the “gap” period between the end of the last specified period of SOC report to whatever time frame is requested by the user.
- The Service Auditor is not involved in the issuance of a Bridge Letter.
- Bridge Letters can be written to cover any period of time since the issuance of the last SOC report; however, common practice is that Bridge Letters covering a **period longer than 90 days are not acceptable** by external auditors that might rely on the SOC Report.



*This is the date through which the user requests a Bridge Letter from management that there were no issues outside of the audited period

FORVIS

Polling Question 4

Which items should you check for when evaluating the strength of a test procedure?

A / Did the Service Auditor test all attributes of the control properly?

B / Did the test procedure cover the entire specified period?

C / Were procedures beyond inquiry performed? (Inquiry alone is not sufficient)

D / All the above.

FORVIS

Brought to You by the FORVIS SOC and HITRUST Practice

- **FORVIS can help with SOC Reporting needs!**
  - **FORVIS** has a **dedicated team** that focuses only on helping third-party providers build trust with their clients and prospects through compliance reporting vehicles such as SOC and HITRUST day-in, day-out
  - Transparent, **proven** methodologies
  - **Innovative technology** and tools that drive more efficient and effective engagements
  - **Quality and credibility** you can trust
  - **Future-focused** approach

As a user, if you come across third parties from which you have asked for a SOC report and they don't have one, feel free to refer us!

FORVIS

Questions

FORVIS

CONTINUING PROFESSIONAL EDUCATION (CPE) CREDIT

FORVIS, LLP is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

FORVIS

CPE CREDIT

- CPE credit may be awarded upon verification of participant attendance
- For questions, concerns, or comments regarding CPE credit, please email FORVIS at cpecompliance@forvis.com

FORVIS

Thank you!

forvis.com

FORVIS

Assurance / Tax / Advisory