LETICIA SAIID

Common Mistakes When Reviewing SOC Reports

KEYS CONFERENCE

1

Disclaimer

A FEW THINGS FIRST

This presentation is for information only.
Evaluate risks before acting based on ideas from this presentation.

This presentation contains opinions of the presenters.
Opinions may not reflect the opinions of Tandem.

This presentation is proprietary.
Unauthorized release of this information is prohibited.

KEYS CONFERENCE

2

Leticia Saiid

Security+, Chief of Staff

KEYS CONFERENCE

3

4

Agenda

HERE'S THE PLAN

- Gathering Methods
- History of SOC
- Structure of SOC
- Review Items for SOC
- Reporting to the Board

Pointing out mistakes along the way

KEYS CONFERENCE

5

Gathering Methods

KEYS CONFERENCE

6

How do you know which vendors need to provide which documents?

KEYS CONFERENCE

7

STOP USING THE BUCKET METHOD

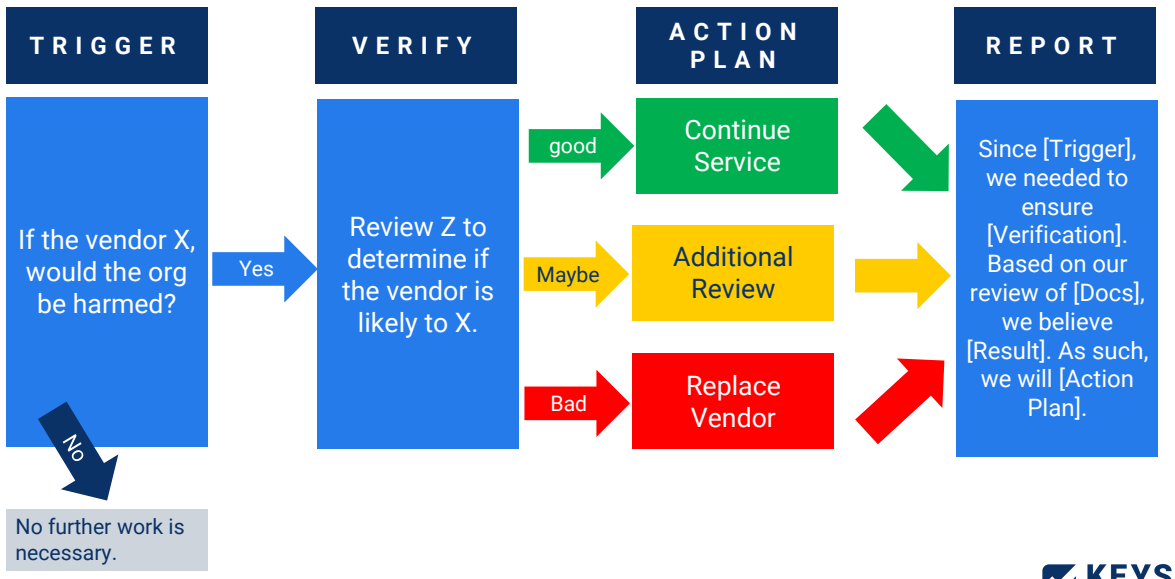
#emptythebucket

Problems created by this method:

1. Unnecessary document exceptions
2. Missed relevant documents

KEYS CONFERENCE

8

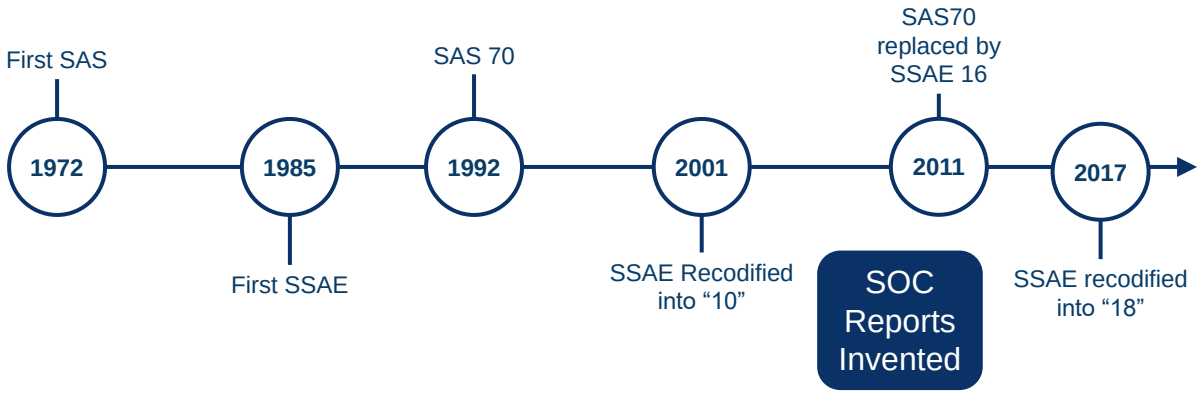


https://tandem.app/blog/a-more-accurate-method-for-collecting-due-diligence-documents-from-third-parties

9

10

SOC REPORT HISTORY



AICPA: American Institute of Certified Public Accountants
ASB: Auditing Standards Board
SAS: Statements on Auditing Standards
SSAE: Statements on Standards for Attestation Engagement

KEYS CONFERENCE

11

Attestation

NOUN

- evidence or proof of something.
- a declaration that something exists or is the case.
- the action of being a witness to or formally certifying something.

KEYS CONFERENCE

12

Structure

System and Organization Controls

Report on Controls at a Service Organization
Relevant to User Entities'
Internal Control over Financial Reporting

**Report on Vendor's Controls
That Could Affect Your
Efforts for Business Performance**

KEYS CONFERENCE

13

Structure

Guidelines	Report	Type	Report Description
SSAE 18	SOC 1	Type 1	Internal Controls Over Financial Reporting (ICFR)
		Type 2	ICFR + Opinion of controls operating effectiveness
	SOC 2	Type 1	Trust Services Criteria
		Type 2	TSC + Opinion of controls operating effectiveness
	SOC 3	TSC with no testing details Freely distributed version for marketing	

KEYS CONFERENCE

14

SOC Quiz

Which kind of SOC Report includes tested controls over a period of time?

A SOC 1 - Type 1

B SOC 1 - Type 2

C SOC 2 – Type 1

D SOC 2 – Type 2

KEYS CONFERENCE

15

Cover Page

What is being reviewed
SOC # and Type #

The company being reviewed

The auditing firm

Table of Contents

Section 1 - Auditor's Report
Section 2 - Management's Assertion
Section 3 - Description of the System
Section 4 - Test Results (Type 2 only)
Section 5 - Other Info

KEYS CONFERENCE

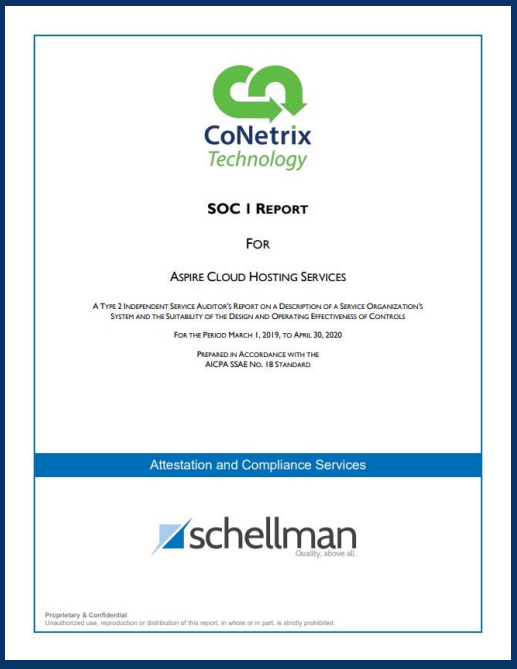
16

TABLE OF CONTENTS

2

KEYS CONFERENCE

17



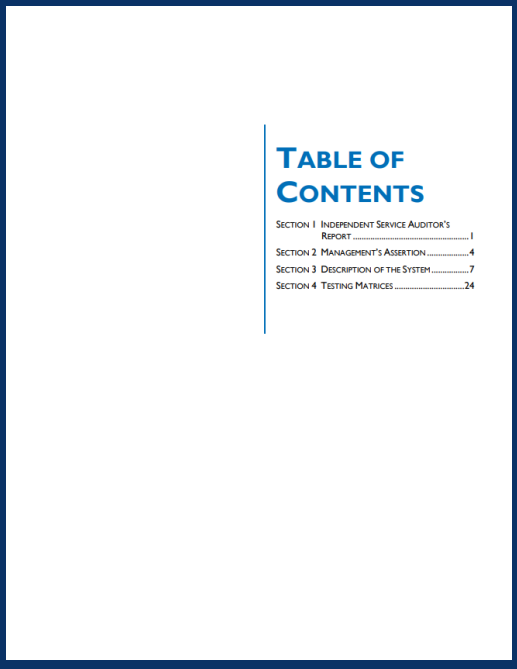


TABLE OF CONTENTS

KEYS CONFERENCE

18

Auditor's Report

SCOPE
We have examined the description of the system over N-M timeframe and the suitability of the controls to meet the objectives in the description. The description says these can only be achieved if the noted complementary user entity controls are employed / noted subservice provider controls are employed. We did not review those controls.
.. the ability to meet the Trust Service Principles (for SOC 2) …current/subsequent significant events were X.

VENDOR RESPONSIBILITY
To provide an assertion and the "description" in a fair, accurate, and complete fashion, including controls.

AUDITOR RESPONSIBILITY
To verify the accuracy of what this vendor says in the description and assertion. We follow the AICPA SSAE guidelines to conduct our audit. "We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis of our opinion."

LIMITATIONS
This is for a broad range of people and may not cover every aspect of the system. Controls cannot be expected to prevent, detect, and correct every possible misstatement, and controls that worked when we reviewed this could become ineffective.
We also ran in to the following limitations: A, B, C.

DESCRIPTION OF TESTED CONTROLS
(*Type 2 only*).
We tested the controls, and you can read about that testing in section 4.

OPINION
Here are the issues we found, if any: one, two.
In our opinion, other than the above statement, (1) the description fairly represents the system, (2) the controls are suitably designed, and (3) the controls tested operate effectively (*Type 2 only*).

RESTRICTED USE
This is to be used by the company and the people they give it to. ☺

Signature
mm/dd/yyyy

KEYS CONFERENCE

19

schellman

INDEPENDENT SERVICE AUDITOR'S REPORT

SCOPE

Scope

We have examined CoNetrix Technology LLC's ("CoNetrix Technology" or "service organization") description of its Aspire Cloud Hosting Services system throughout the period March 1, 2019, to April 30, 2020 (the "description"), and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on criteria identified in "Management's Assertion" in Section 2 (the "assertion"). The controls and control objectives included in the description are those that management of CoNetrix Technology believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Aspire Cloud Hosting Services system that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates whether certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of CoNetrix Technology'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, as applicable, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

CoNetrix Technology uses a subservice organization for data center colocation services. The description includes only the control objectives and related controls of CoNetrix Technology and excludes the control objectives and related controls of the subservice organization. The description also indicates whether certain control objectives specified by CoNetrix Technology can be achieved only if complementary subservice organization controls assumed in the design of CoNetrix Technology's controls are suitably designed and operating effectively, along with the related controls at CoNetrix Technology. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such

VENDOR RESPONSIBILITY

assertion, including the completeness, accuracy, and method of presentation of the description and the 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

AUDITOR RESPONSIBILITY

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 March 1, 2019, to April 30, 2020. 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:

2

- 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
-

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 the Aspire Cloud

DESC. OF TESTED CONTROLS

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4 (the "Testing Matrices").

OPINION

a.

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 March 1, 2019, to April 30, 2020, and as applicable, subservice organizations and user entities applied the complementary controls assumed in the design of CoNetrix Technology's controls throughout the period March 1, 2019, to April 30, 2020; and

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period March 1, 2019, to April 30, 2020, if, as applicable, complementary subservice organization and user entity controls assumed in the design of CoNetrix

RESTRICTED USE

Aspire Cloud Hosting Services system during some or all of the period March 1, 2019, to April 30, 2020, 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 the specified parties.

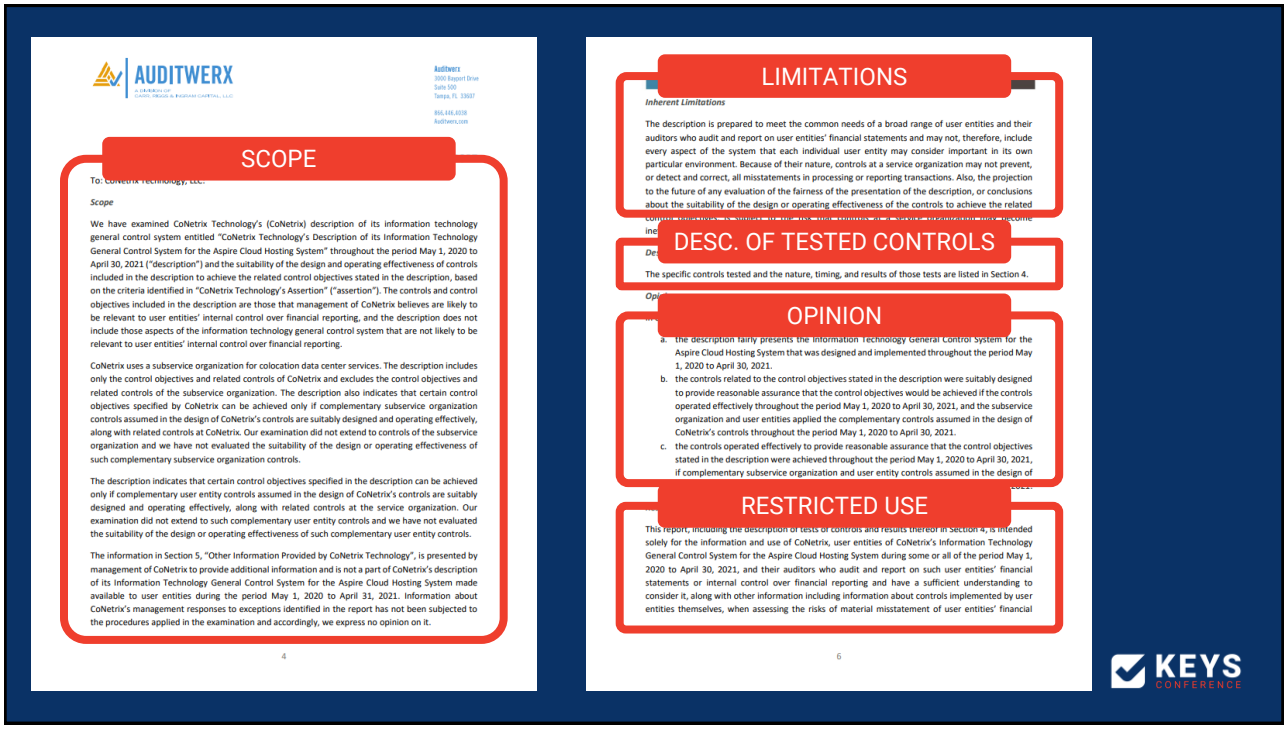
Schellman & Company, LLC
Irving, Texas
June 2, 2020

SIGNATURE & DATE

3

KEYS CONFERENCE

20



21

Assertions of XYZ Co.

We wrote a description about our system.

To the best of our knowledge that description (1) fairly presents the system and controls, (2) includes relevant details of changes during the timeframe, (3) the controls were suitably designed and operated effectively during this time.

We admit we had two exceptions: issue 1, issue 2.

We assert that (1) risks were identified by management, (2) controls working correctly provide reasonable assurance those risks don't hinder our objectives, (3) the controls were consistently applied as designed, including manual application as needed by qualified persons.

Description of System

Here is the description of our system and the controls we have in place.

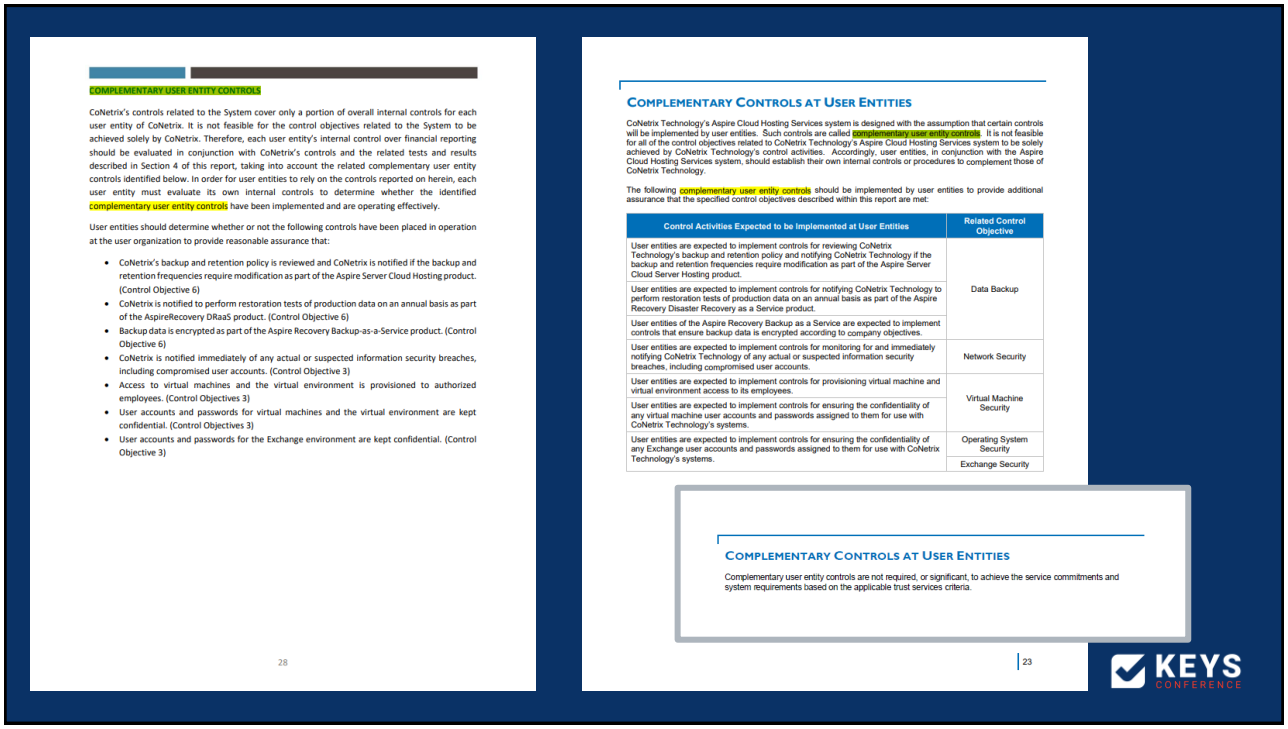
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Complementary User Entity Controls
Our system is designed such that the user must implement some CUECs. The ones you need to implement are: A, B, and C.

Subservice Organization Monitoring
Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

KEYS CONFERENCE

22



COMPLEMENTARY USER ENTITY CONTROLS

CoNetrix's controls related to the System cover only a portion of overall internal controls for each user entity of CoNetrix. It is not feasible for the control objectives related to the System to be achieved solely by CoNetrix. Therefore, each user entity's internal control over financial reporting should be evaluated in conjunction with CoNetrix's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary user entity controls identified below. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal controls to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

User entities should determine whether or not the following controls have been placed in operation at the user organization to provide reasonable assurance that:

- CoNetrix's backup and retention policy is reviewed and CoNetrix is notified if the backup and retention frequencies require modification as part of the Aspire Server Cloud Hosting product. (Control Objective 6)
- CoNetrix is notified to perform restoration tests of production data on an annual basis as part of the AspireRecovery DRaaS product. (Control Objective 6)
- Backup data is encrypted as part of the Aspire Recovery Backup-as-a-Service product. (Control Objective 6)
- CoNetrix is notified immediately of any actual or suspected information security breaches, including compromised user accounts. (Control Objective 3)
- Access to virtual machines and the virtual environment is provisioned to authorized employees. (Control Objectives 3)
- User accounts and passwords for virtual machines and the virtual environment are kept confidential. (Control Objectives 3)
- User accounts and passwords for the Exchange environment are kept confidential. (Control Objective 3)

28

COMPLEMENTARY CONTROLS AT USER ENTITIES

CoNetrix Technology's Aspire Cloud Hosting Services system is designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the control objectives related to CoNetrix Technology's Aspire Cloud Hosting Services system to be solely achieved by CoNetrix Technology's control activities. Accordingly, user entities, in conjunction with the Aspire Cloud Hosting Services system, should establish their own internal controls or procedures to complement those of CoNetrix Technology.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the specified control objectives described within this report are met:

Control Activities Expected to be Implemented at User Entities	Related Control Objective
User entities are expected to implement controls for reviewing CoNetrix Technology's backup and retention policy and notifying CoNetrix Technology if the backup and retention frequencies require modification as part of the Aspire Server Cloud Server Hosting product.	Data Backup
User entities are expected to implement controls for notifying CoNetrix Technology to perform restoration tests of production data on an annual basis as part of the Aspire Recovery Disaster Recovery as a Service product.	
User entities of the Aspire Recovery Backup as a Service are expected to implement controls that ensure backup data is encrypted according to company objectives.	
User entities are expected to implement controls for monitoring for and immediately notifying CoNetrix Technology of any actual or suspected information security breaches, including compromised user accounts.	Network Security
User entities are expected to implement controls for provisioning virtual machine and virtual environment access to its employees.	Virtual Machine Security
User entities are expected to implement controls for ensuring the confidentiality of any virtual machine user accounts and passwords assigned to them for use with CoNetrix Technology's systems.	
User entities are expected to implement controls for ensuring the confidentiality of any Exchange user accounts and passwords assigned to them for use with CoNetrix Technology's systems.	Operating System Security
	Exchange Security

COMPLEMENTARY CONTROLS AT USER ENTITIES

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

23

KEYS CONFERENCE

23

Test Results

Control	Test Process	Results
Blah blah blah	Yata ya	No Exception found.
Blah blah blah	Yata ya	When we tested this, here's what happened. It wasn't so good.
Blah blah blah	Yata ya	No Exception found.

Other Info

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

We did have these two exceptions: issue 1, issue 2. We have made such and such changes so they don't happen again.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

KEYS CONFERENCE

24

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Server Room		
1.07	Visitors are required to be escorted by authorized personnel when accessing the server room.	Inquired of the network engineer manager regarding visitor access into the server room to determine that visitors were required to be escorted by authorized personnel when accessing the server room.	No exceptions noted.
		Observed authorized personnel escorting visitors in the server room with the assistance of the network engineer manager to determine that visitors were required to be escorted by authorized personnel when accessing the server room.	No exceptions noted.
1.08	Access to the server room is controlled through a biometric and keypad smart lock access system with access restricted to authorized personnel.	Inquired of the network engineer manager regarding access to the server room to determine that access to the server room was controlled through a biometric and keypad smart lock access system with access restricted to authorized personnel.	No exceptions noted.
		Observed the server room biometric and keypad door lock to determine that access to the server room could only be accessed by predefined and authorized biometric and keypad access and that the server room door was securely locked.	No exceptions noted.
		Inspected the server room biometric and keypad smart lock system access listing with the assistance of the network engineer manager to determine that access to the server room was restricted to predefined and authorized personnel.	No exceptions noted.
1.09	Administrative access privileges to the biometric and keypad smart lock access system is restricted to user profiles accessible by authorized personnel.	Inspected the administrative access privileges to the biometric and keypad smart lock access system with the assistance of the network engineer manager to determine that administrative access was restricted to user profiles accessible by authorized personnel.	No exceptions noted.

28

PHYSICAL ACCESS

Control Objective 2: Controls provide reasonable assurance that physical access to computer and other resources is restricted to authorized personnel.

#	CONTROL ACTIVITY(IES)	NATURE, TIMING & EXTENT OF TEST(S) PERFORMED	TEST RESULT(S)
2.1	An Access Control System (ACS) and physical key are utilized to restrict access to the Company facility and on-site server room. Administrator access is restricted to the ACS to authorized individuals	Observed the corporate facility and on-site server room ACS Configurations or physical key logs to verify that entry to the facility and on-site server room was controlled by an ACS and physical key.	No exceptions noted.
		Inspected the facility physical key access tracking listing to verify that tracking of keys is monitored.	No exceptions noted.
		Inspected the system-generated list of personnel with administrator access to the keypad code system for entry to the office and inquired with management to verify that, for the period of May 1, 2020 to April 19, 2021, administrator access was authorized.	No exceptions noted.
		Inspected the system-generated list of personnel with administrator access to the Verkada keycard system for entry to the office and inquired with management to verify that, for the period of April 20, 2021 to April 30, 2021, administrator access was authorized.	No exceptions noted.
		Inspected the system-generated list of personnel with administrator access to the biometric keylock system for the on-site server room and inquired with management to verify that administrator access was authorized.	No exceptions noted.

34

KEYS CONFERENCE

25

SOC Quiz

Which section of the Auditor's Report discusses any issues found?

A Scope

B Vendor Responsibility

C Limitations

D Opinion

KEYS CONFERENCE

26

SOC Quiz

Where can you find the details of the Complimentary User Entity Controls?

A Auditor's Report

B Company Assertion

C Description of System

D Scope

KEYS CONFERENCE

27

Review Items

KEYS CONFERENCE

28

Review Items

REPORT PROFILE

Contracted Services Covered – find your service in the doc

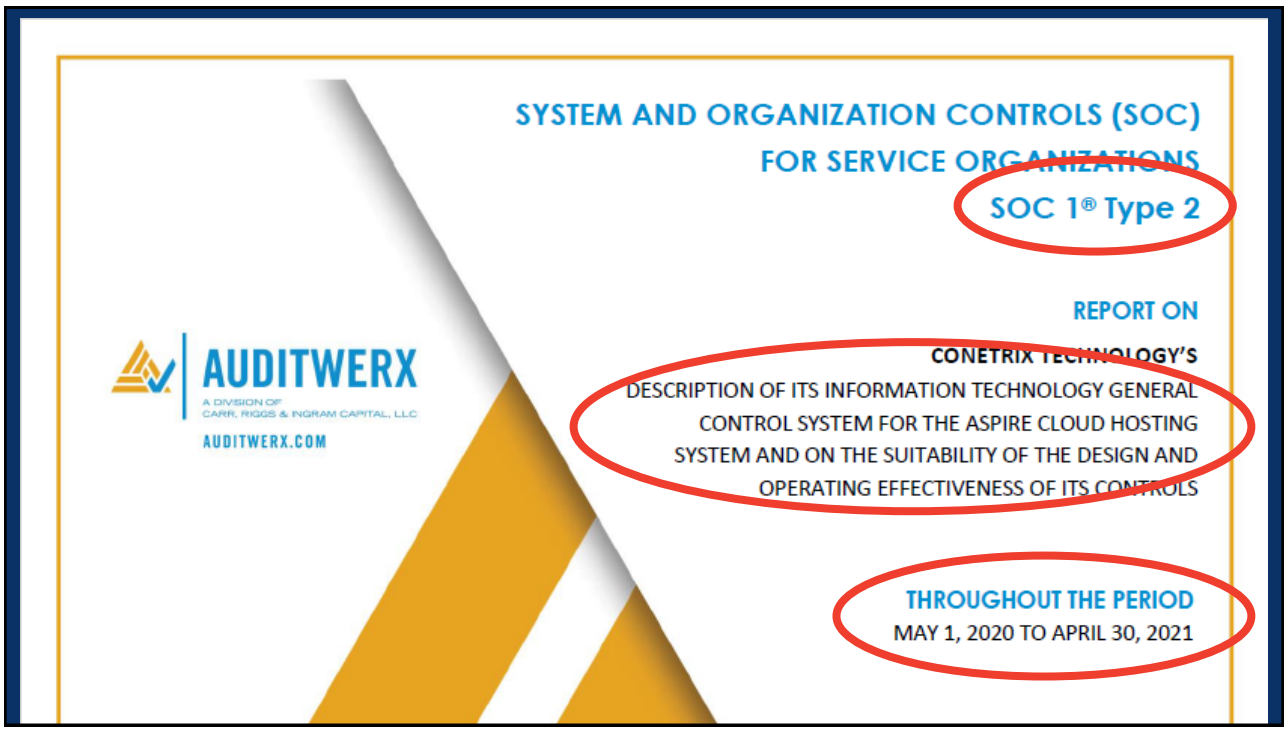
Report Type and Number – a hint to what you can expect

Date of Report – the time of year you can expect to see the next SOC report

Testing Period - the period of the info that was reviewed

KEYS CONFERENCE

29



30

CoNetrix Technology

SOC 1 Report

For

Aspire Cloud Hosting Services

A Type 2 Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

For the Period March 1, 2019, to April 30, 2020

Prepared in Accordance with the AICPA SSAE No. 18 Standard

KEYS CONFERENCE

31

a. the description fairly presents the Aspire Cloud Hosting Services system that was designed and implemented throughout the period March 1, 2019, to April 30, 2020;

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 March 1, 2019, to April 30, 2020, and as applicable, subservice organizations and user entities applied the complementary controls assumed in the design of CoNetrix Technology's controls throughout the period March 1, 2019, to April 30, 2020; and

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period March 1, 2019, to April 30, 2020, if, as applicable, complementary subservice organization and user entity controls assumed in the design of CoNetrix Technology's controls operated effectively throughout the period March 1, 2019, to April 30, 2020.

Restricted Use

This report, including the description of the tests of controls and results thereof in the Testing Matrices, is intended solely for the information and use of management of CoNetrix Technology, user entities of CoNetrix Technology's Aspire Cloud Hosting Services system during some or all of the period March 1, 2019, to April 30, 2020, 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 the specified parties.

Schellman & Company, LLC

Irving, Texas
June 2, 2020

KEYS CONFERENCE

32

statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Auditwerx, LLC

Auditwerx, LLC, a Division of Carr, Riggs & Ingram Capital, LLC

Tampa, Florida
October 29, 2021

KEYS CONFERENCE

33

Review Items

CURRENT OR SUBSEQUENT SIGNIFICANT EVENTS

Does the report, a bridge letter for the report, or any other source identify any **current or subsequent significant events**?

- No. See date of bridge letter, if applicable.
- The report.
- A bridge letter.
- Another source.

These events include anything that happened during or after the audit that could have affected testing or reporting, such as incidents and/or material changes to the controls. See the **Independent Service Auditors Report** section. The **Scope** subsection will identify these events, if any were noted during the report process. A bridge (gap) letter should be available at the end of the calendar year to cover the time between the audit review period and the end of the calendar year.

KEYS CONFERENCE

34

To CoNetrix Technology, LLC:

Scope

We have examined CoNetrix Technology LLC's ("CoNetrix Technology" or "service organization") description of its Aspire Cloud Hosting Services system throughout the period March 1, 2019, to April 30, 2020 (the "description"), and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on criteria identified in "Management's Assertion" in Section 2 (the "assertion"). The controls and control objectives included in the description are those that management of CoNetrix Technology believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Aspire Cloud Hosting Services system that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates whether certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of CoNetrix Technology'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, as applicable, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

CoNetrix Technology uses a subservice organization for data center colocation services. The description includes only the control objectives and related controls of CoNetrix Technology and excludes the control objectives and related controls of the subservice organization. The description also indicates whether certain control objectives specified by CoNetrix Technology can be achieved only if complementary subservice organization controls assumed in the design of CoNetrix Technology's controls are suitably designed and operating effectively, along with the related controls at CoNetrix Technology. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

In Section 2, CoNetrix Technology has provided an assertion about the fairness of the presentation of the

35

Scope

We have examined CoNetrix Technology's (CoNetrix) description of its information technology general control system entitled "CoNetrix Technology's Description of its Information Technology General Control System for the Aspire Cloud Hosting System" throughout the period May 1, 2020 to April 30, 2021 ("description") and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "CoNetrix Technology's Assertion" ("assertion"). The controls and control objectives included in the description are those that management of CoNetrix believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the information technology general control system that are not likely to be relevant to user entities' internal control over financial reporting.

CoNetrix uses a subservice organization for colocation data center services. The description includes only the control objectives and related controls of CoNetrix and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by CoNetrix can be achieved only if complementary subservice organization controls assumed in the design of CoNetrix's controls are suitably designed and operating effectively, along with related controls at CoNetrix. Our examination did not extend to controls of the subservice organization and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization 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 CoNetrix'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.

The information in Section 5, "Other Information Provided by CoNetrix Technology", is presented by management of CoNetrix to provide additional information and is not a part of CoNetrix's description of its Information Technology General Control System for the Aspire Cloud Hosting System made available to user entities during the period May 1, 2020 to April 31, 2021. Information about CoNetrix's management responses to exceptions identified in the report has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

KEYS CONFERENCE

36

Review Items

LIMITATIONS

Does the report contain any **limitations** with regard to documentation of testing of controls?

- No
- Yes

Limitations include anything that could limit the ability for the auditor to document or test a control, such as an area that could not be tested at the time. See the **Independent Service Auditors Report** section. If there are any noteworthy limitations, they will be included in the **Limitations** subsection in addition to the standard two-sentence limitations clause.

KEYS CONFERENCE

37

Review Items

COMPLEMENTARY USER ENTITY CONTROLS

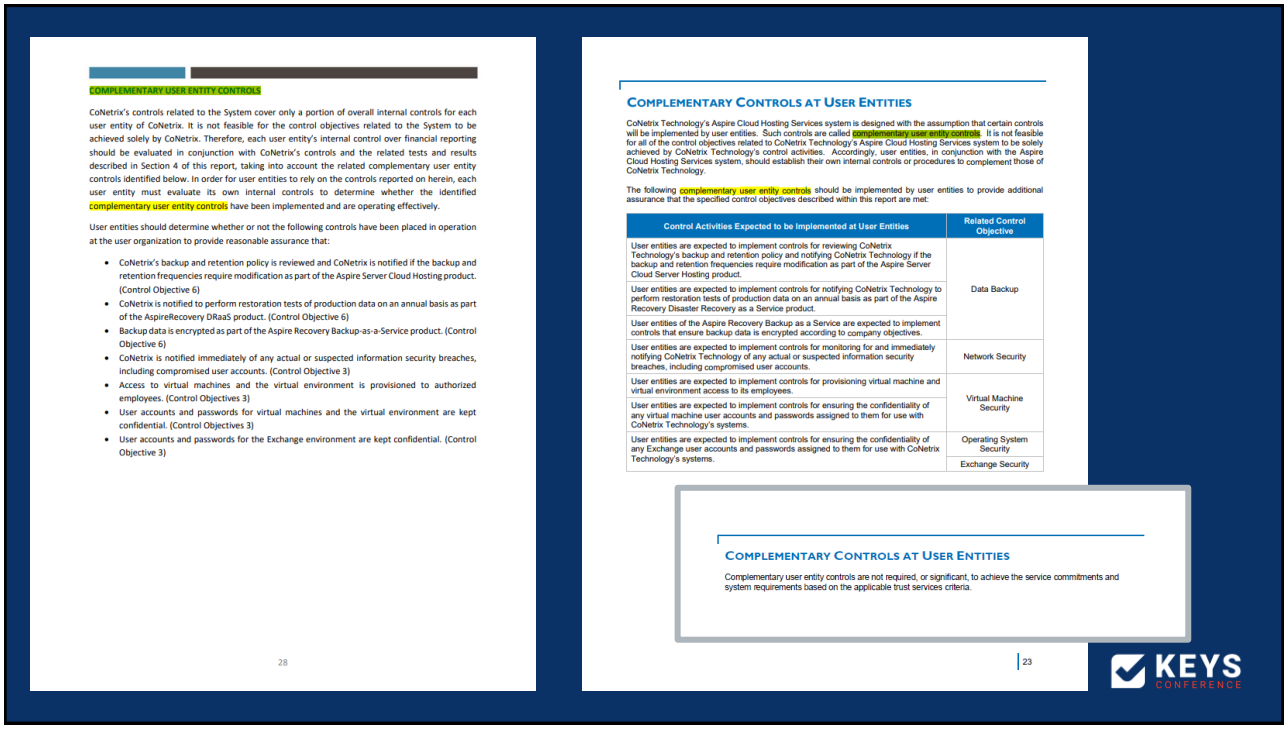
Are **complementary user entity controls** necessary to achieve the control objective?

- No.
- Yes, and we have implemented.
- Yes, but we have not implemented.

See the **Independent Service Auditors Report** section. The **Scope** subsection will identify the necessity of "complementary user entity" controls, if any. If there are any, refer to the section called **Description of Controls** (or similar) in the System Description for a list. In the comments, list the controls and describe how you have implemented each.

KEYS CONFERENCE

38



COMPLEMENTARY USER ENTITY CONTROLS

CoNetrix's controls related to the System cover only a portion of overall internal controls for each user entity of CoNetrix. It is not feasible for the control objectives related to the System to be achieved solely by CoNetrix. Therefore, each user entity's internal control over financial reporting should be evaluated in conjunction with CoNetrix's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary user entity controls identified below. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal controls to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

User entities should determine whether or not the following controls have been placed in operation at the user organization to provide reasonable assurance that:

- CoNetrix's backup and retention policy is reviewed and CoNetrix is notified if the backup and retention frequencies require modification as part of the Aspire Server Cloud Hosting product. (Control Objective 6)
- CoNetrix is notified to perform restoration tests of production data on an annual basis as part of the AspireRecovery DRaaS product. (Control Objective 6)
- Backup data is encrypted as part of the Aspire Recovery Backup-as-a-Service product. (Control Objective 6)
- CoNetrix is notified immediately of any actual or suspected information security breaches, including compromised user accounts. (Control Objective 3)
- Access to virtual machines and the virtual environment is provisioned to authorized employees. (Control Objectives 3)
- User accounts and passwords for virtual machines and the virtual environment are kept confidential. (Control Objectives 3)
- User accounts and passwords for the Exchange environment are kept confidential. (Control Objective 3)

28

COMPLEMENTARY CONTROLS AT USER ENTITIES

CoNetrix Technology's Aspire Cloud Hosting Services system is designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the control objectives related to CoNetrix Technology's Aspire Cloud Hosting Services system to be solely achieved by CoNetrix Technology's control activities. Accordingly, user entities, in conjunction with the Aspire Cloud Hosting Services system, should establish their own internal controls or procedures to complement those of CoNetrix Technology.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the specified control objectives described within this report are met:

Control Activities Expected to be Implemented at User Entities	Related Control Objective
User entities are expected to implement controls for reviewing CoNetrix Technology's backup and retention policy and notifying CoNetrix Technology if the backup and retention frequencies require modification as part of the Aspire Server Cloud Server Hosting product.	Data Backup
User entities are expected to implement controls for notifying CoNetrix Technology to perform restoration tests of production data on an annual basis as part of the Aspire Recovery Disaster Recovery as a Service product.	
User entities of the Aspire Recovery Backup as a Service are expected to implement controls that ensure backup data is encrypted according to company objectives.	
User entities are expected to implement controls for monitoring for and immediately notifying CoNetrix Technology of any actual or suspected information security breaches, including compromised user accounts.	Network Security
User entities are expected to implement controls for provisioning virtual machine and virtual environment access to its employees.	Virtual Machine Security
User entities are expected to implement controls for ensuring the confidentiality of any virtual machine user accounts and passwords assigned to them for use with CoNetrix Technology's systems.	
User entities are expected to implement controls for ensuring the confidentiality of any Exchange user accounts and passwords assigned to them for use with CoNetrix Technology's systems.	Operating System Security
	Exchange Security

COMPLEMENTARY CONTROLS AT USER ENTITIES

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

23

KEYS CONFERENCE

39

Review Items

OPINION

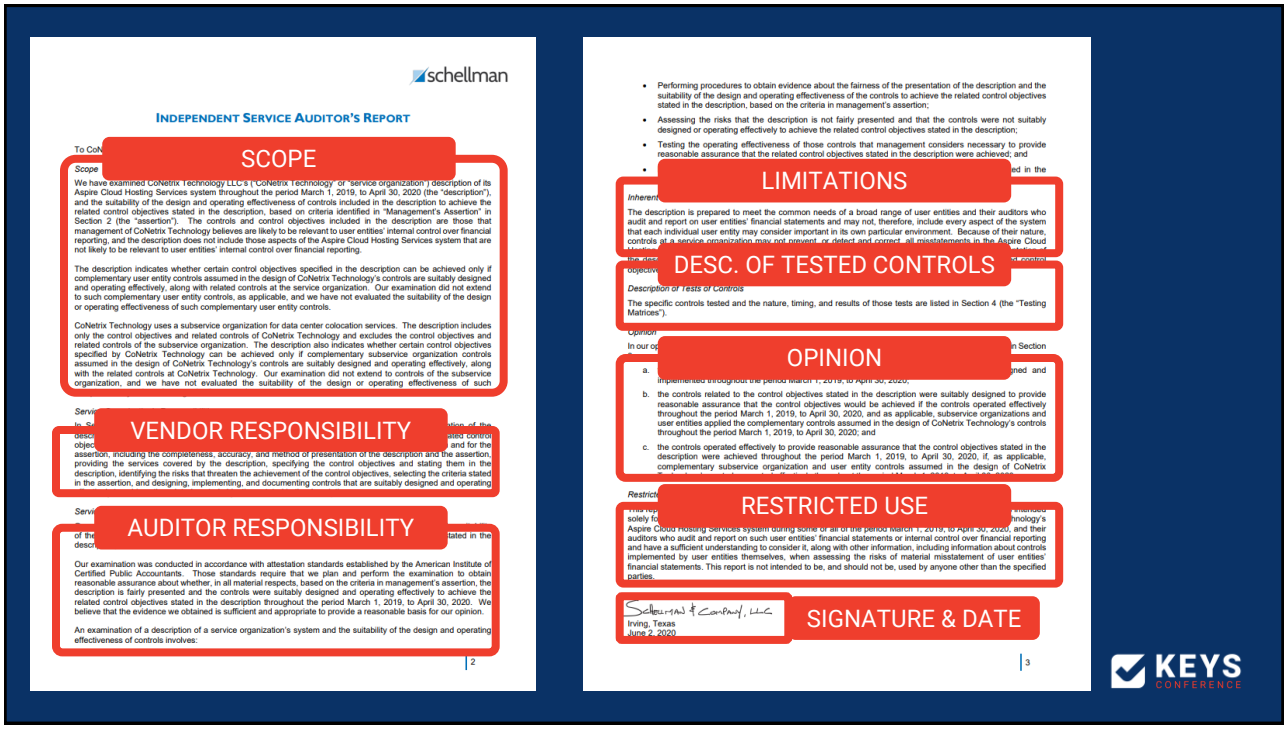
What was the auditor's opinion of the organization's assertion?

- Good (a.k.a., "unqualified").
- Not Good (a.k.a., "qualified").
- Can't say.

See the **Independent Service Auditors Report** section. In the **Opinion** subsection, the auditor's opinion should assert that the service organization's controls are (1) described fairly, (2) designed effectively, and for *Type 2* reports (3) operating effectively over a specified period of time. This wording is standardized in all SOC Reports. Significant exceptions will be identified in the **Opinion** subsection and should be documented. Responses to significant exceptions are often identified in the **Management Assertion** or an **Other** section. Both the organization's response and your management's stance on the exceptions/response should be documented.

KEYS CONFERENCE

40



41

Opinion

In our opinion, in all material respects, based on the criteria described in CoNetrix Technology's assertion in Section 2,

a. the description fairly presents the Aspire Cloud Hosting Services system that was designed and implemented throughout the period March 1, 2019, to April 30, 2020;

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 March 1, 2019, to April 30, 2020, and as applicable, subservice organizations and user entities applied the complementary controls assumed in the design of CoNetrix Technology's controls throughout the period March 1, 2019, to April 30, 2020; and

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period March 1, 2019, to April 30, 2020, if, as applicable, complementary subservice organization and user entity controls assumed in the design of CoNetrix Technology's controls operated effectively throughout the period March 1, 2019, to April 30, 2020.

Restricted Use

This report, including the description of the tests of controls and results thereof in the Testing Matrices, is intended solely for the information and use of management of CoNetrix Technology, user entities of CoNetrix Technology's Aspire Cloud Hosting Services system during some or all of the period March 1, 2019, to April 30, 2020, 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 the specified parties.

42

Review Items

WEAKNESS

Did the auditor identify weaknesses in the controls?

- N/A (Type 1)
- No.
- Yes, and the company responded.

See the section called **Test Results** (or similar) for any exceptions. The final table column, **Results**, will most commonly display "No exceptions found." If other results exist, the exception is considered a weakness for the control.

KEYS CONFERENCE

43

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Server Room		
1.07	Visitors are required to be escorted by authorized personnel when accessing the server room.	Inquired of the network engineer manager regarding visitor access into the server room to determine that visitors were required to be escorted by authorized personnel when accessing the server room.	No exceptions noted.
		Observed authorized personnel escorting visitors in the server room with the assistance of the network engineer manager to determine that visitors were required to be escorted by authorized personnel when accessing the server room.	No exceptions noted.
1.08	Access to the server room is controlled through a biometric and keypad smart lock access system with access restricted to authorized personnel.	Inquired of the network engineer manager regarding access to the server room to determine that access to the server room was controlled through a biometric and keypad smart lock access system with access restricted to authorized personnel.	No exceptions noted.
		Observed the server room biometric and keypad door lock to determine that access to the server room could only be accessed by predefined and authorized biometric and keypad access and that the server room door was securely locked.	No exceptions noted.
		Inspected the server room biometric and keypad smart lock system access listing with the assistance of the network engineer manager to determine that access to the server room was restricted to predefined and authorized personnel.	No exceptions noted.
1.09	Administrative access privileges to the biometric and keypad smart lock access system is restricted to user profiles accessible by authorized personnel.	Inspected the administrative access privileges to the biometric and keypad smart lock access system with the assistance of the network engineer manager to determine that administrative access was restricted to user profiles accessible by authorized personnel.	No exceptions noted.

28

PHYSICAL ACCESS

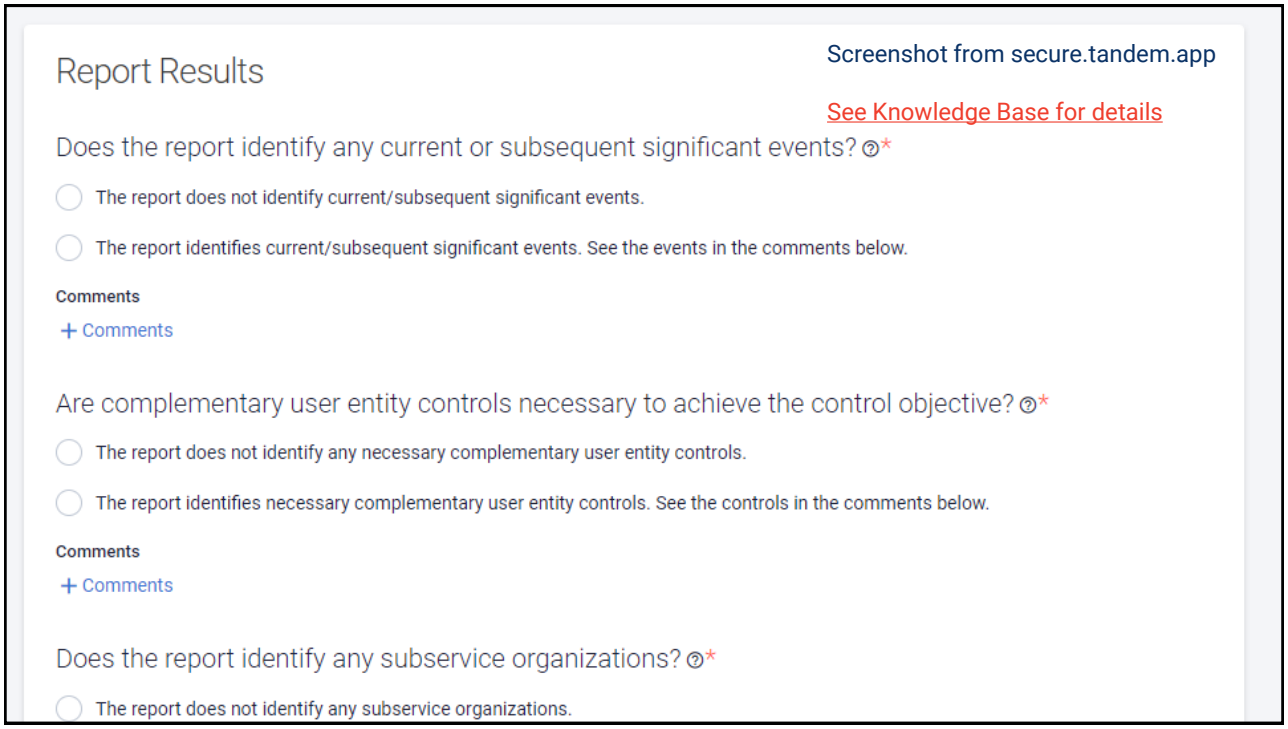
Control Objective 2: Controls provide reasonable assurance that physical access to computer and other resources is restricted to authorized personnel.

#	CONTROL ACTIVITY(IES)	NATURE, TIMING & EXTENT OF TEST(S) PERFORMED	TEST RESULT(S)
2.1	An Access Control System (ACS) and physical key are utilized to restrict access to the Company facility and on-site server room. Administrator access is restricted to the ACS to authorized individuals	Observed the corporate facility and on-site server room ACS Configurations or physical key logs to verify that entry to the facility and on-site server room was controlled by an ACS and physical key.	No exceptions noted.
		Inspected the facility physical key access tracking listing to verify that tracking of keys is monitored.	No exceptions noted.
		Inspected the system-generated list of personnel with administrator access to the keypad code system for entry to the office and inquired with management to verify that, for the period of May 1, 2020 to April 19, 2021, administrator access was authorized.	No exceptions noted.
		Inspected the system-generated list of personnel with administrator access to the Verkada keycard system for entry to the office and inquired with management to verify that, for the period of April 20, 2021 to April 30, 2021, administrator access was authorized.	No exceptions noted.
		Inspected the system-generated list of personnel with administrator access to the biometric keylock system for the on-site server room and inquired with management to verify that administrator access was authorized.	No exceptions noted.

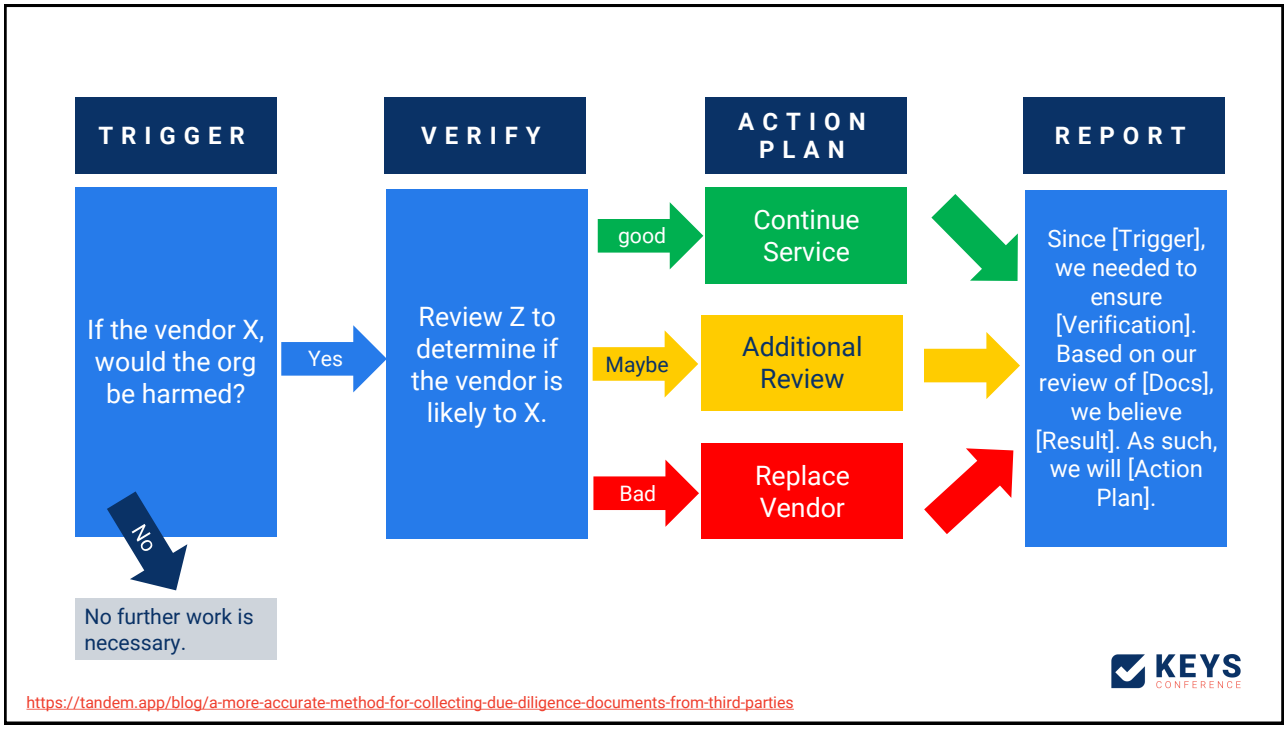
34

KEYS CONFERENCE

44


Report Results
Screenshot from secure.tandem.app
See Knowledge Base for details
Does the report identify any current or subsequent significant events? *
The report does not identify current/subsequent significant events.
The report identifies current/subsequent significant events. See the events in the comments below.
Comments
+ Comments
Are complementary user entity controls necessary to achieve the control objective? *
The report does not identify any necessary complementary user entity controls.
The report identifies necessary complementary user entity controls. See the controls in the comments below.
Comments
+ Comments
Does the report identify any subservice organizations? *
The report does not identify any subservice organizations.

45


TRIGGER
VERIFY
ACTION PLAN
REPORT
If the vendor X, would the org be harmed?
Yes
No
No further work is necessary.
Review Z to determine if the vendor is likely to X.
good
Maybe
Bad
Continue Service
Additional Review
Replace Vendor
Since [Trigger], we needed to ensure [Verification]. Based on our review of [Docs], we believe [Result]. As such, we will [Action Plan].
KEYS CONFERENCE
https://tandem.app/blog/a-more-accurate-method-for-collecting-due-diligence-documents-from-third-parties

46

TRIGGER QUESTION

If the vendor lost/exposed our data they store, would the organization be significantly affected?

VERIFICATION

Review **the SOC Report** to determine if the vendor has any security issues or requires any CUECs.

ACTION PLAN

Continue Service	Additional Review	Replace Vendor

REPORT TO MANAGEMENT

Since the vendor stores our customer information, we needed to ensure the vendor has no security issues and all CEUCs have been implemented by the bank. Based on our review of their SOC Report, we believe they are secure. As such, we will continue service as-is. Also, based on our review, we believe there are 5 CUECs and all have been implemented.

KEYS CONFERENCE

47

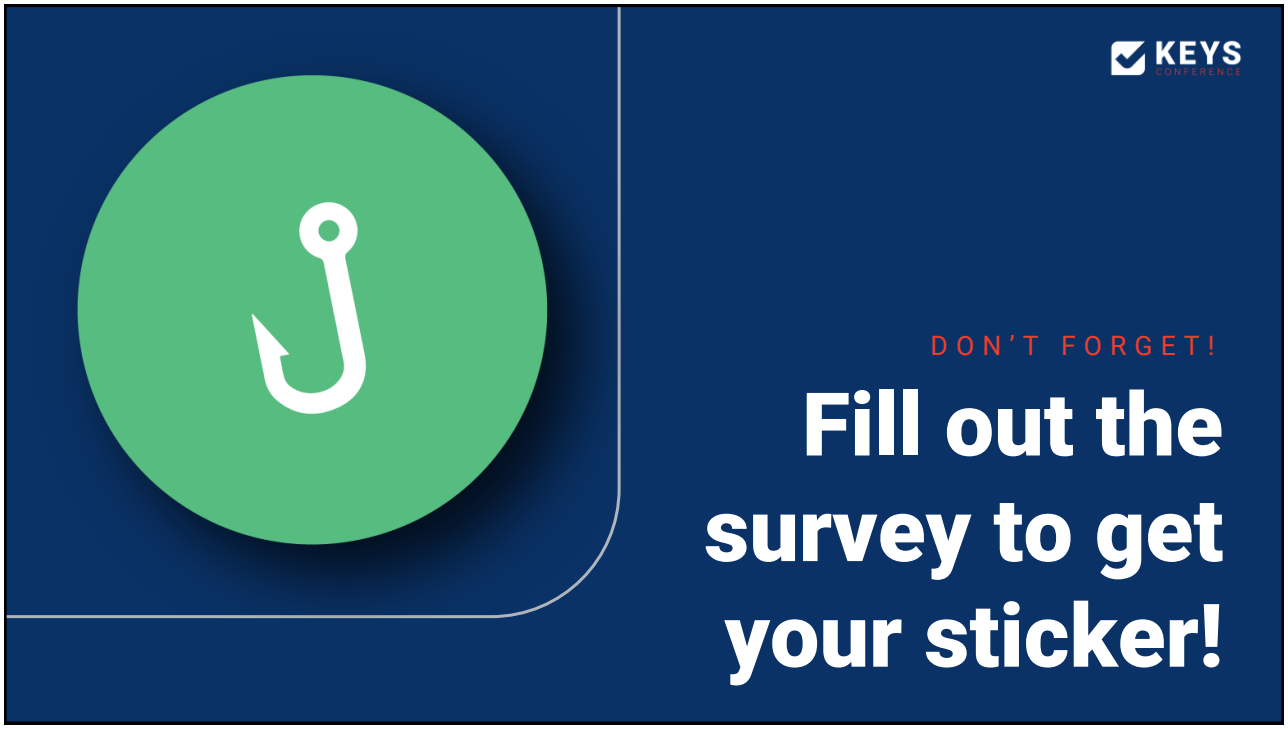
Recap

WHAT WE DID

- Gathering Methods
- History of SOC
- Structure of SOC
- Review Items for SOC
- Reporting to the Board

KEYS CONFERENCE

48



49

Upcoming Sessions

TANDEM

Up and Running with Audit Management Pro

Christopher Hidalgo, CoNetrix Security

RISK & COMPLIANCE

How to Write a Policy

Alyssa Pugh, Tandem

CYBERSECURITY

Best Practices for Mitigating Risks of a Digital Experience Platform

Brad Hunt & Dusty Ellis, Smooth Fusion

KEYS CONFERENCE

50


KEYS
CONFERENCE
THANKS FOR JOINING!
Common Mistakes When Reviewing SOC Reports
Leticia Saiid
Security+, Chief of Staff

51