



SOC REPORTS 101

Heath Peek - CISA
Information Security
Department of Innovation & Technology
heath.peek@illinois.gov



ABOUT SOC

- **Systems & Organization Controls Report**
- **Established by the AICPA (American Institute of Certified Public Accountants)**
- **SSAE No. 18 (Statement on Standards for Attestation Engagement)**



WHAT IS A SOC REPORT?

IN GENERAL

A SOC report is an independent audit report performed by a certified public accountant. The report attests to the existence of a company's controls, policies and procedures, and their operating effectiveness.

BASICALLY

the report should tell you if your vendor has a good base of controls in place to safeguard your data, and whether those safeguards are actually working.

REASONS TO COMMISSION REPORT

CUSTOMER DEMAND

Protecting customer data from malicious activities is important. A SOC report proves your due diligence to your customers

COMPETITIVE ADVANTAGE

Having a SOC report gives your organization an edge over competitors that don't.

REGULATORY COMPLIANCE

SOCs requirements overlap with other frameworks, including the HIPAA and ISO 27001, so attaining certification can speed your organization's overall compliance efforts.

COST-EFFECTIVENESS

Audit costs are high. But, in 2021, the average data breach cost \$4.2 million. And that figure will just keep going up. A SOC audit helps to avoid these security breaches.

PEACE OF MIND

Performing a SOC audit ensures your security posture for your systems and networks.

VALUE

A SOC report provides insights into your risk and security posture, vendor management, internal controls governance, regulatory oversight, and more.

VALUE TO CUSTOMERS

VERIFY CONTROLS

Controls in place have been checked to be valid for the classification of data held by the vendor

INDEPENDENT OPINION

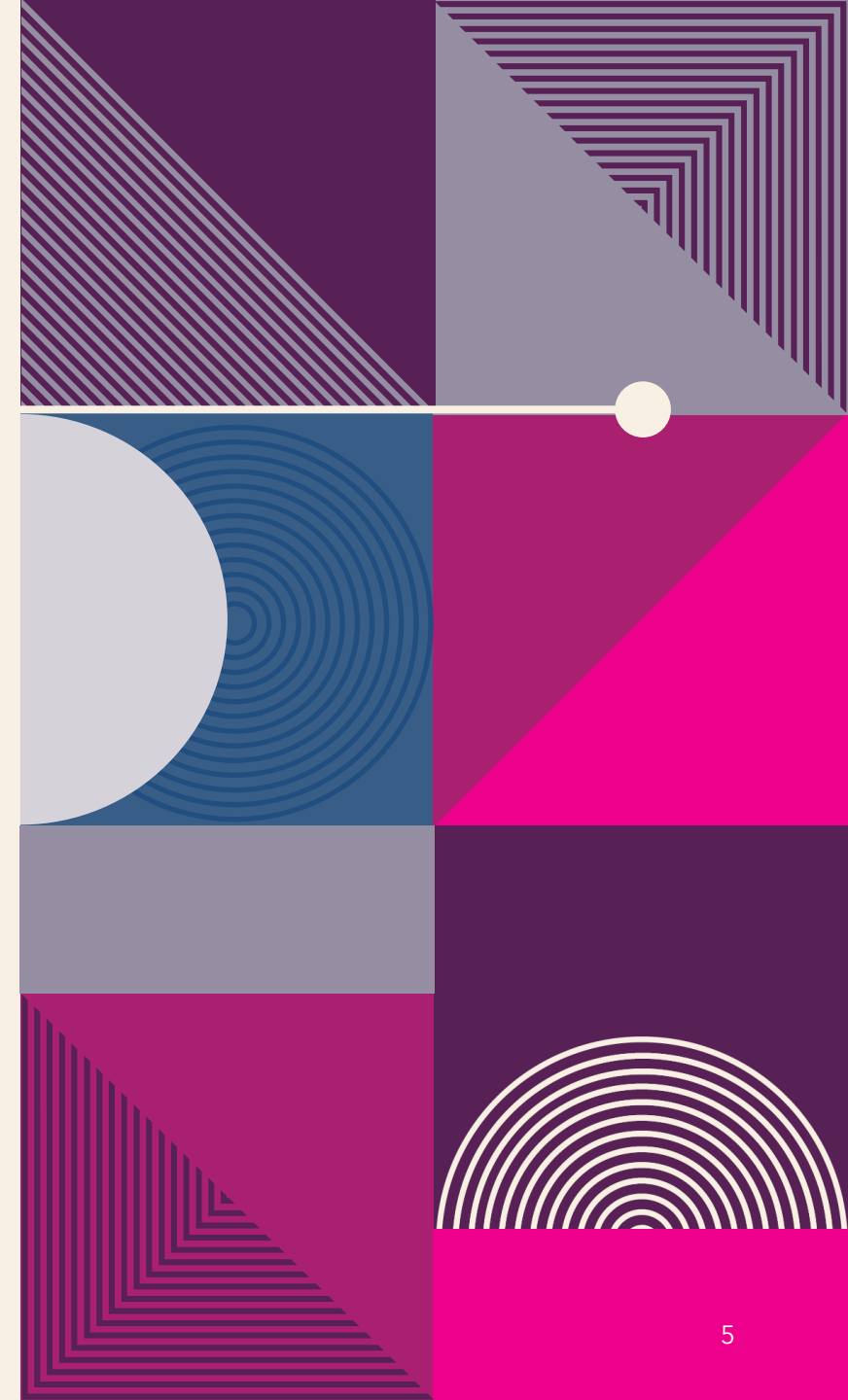
Auditors are an independent third party offering an experienced opinion on the organization's control profile

CONFIRM EFFECTIVENESS

Auditors conduct tests of controls for effectiveness and list any exceptions discovered along with a response detailing how the organization plans to mitigate

DETERMINE COMPLIANCE

Ability to compare Organization controls against contractual obligations



KINDS OF SOC REPORTS

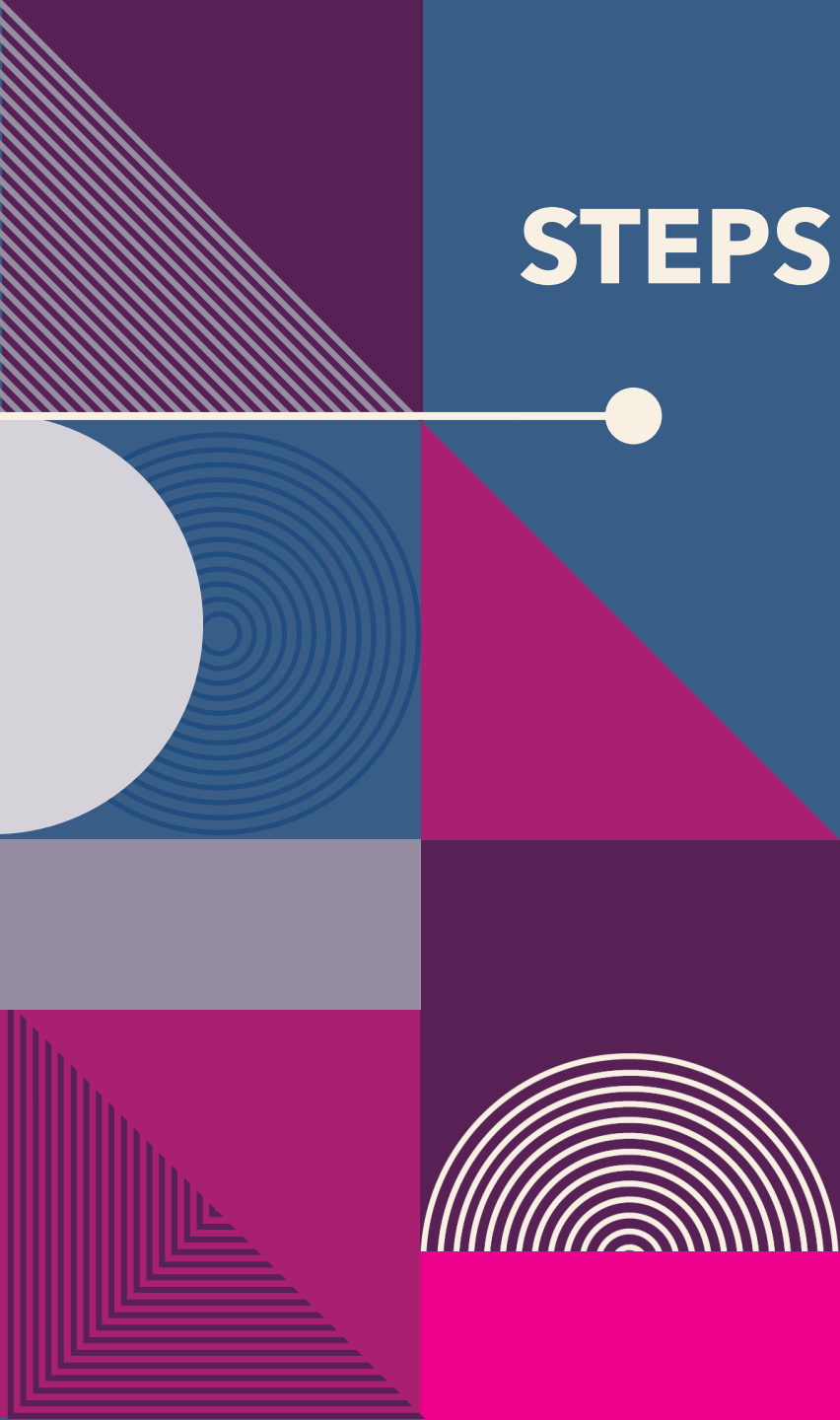
- SOC 1 – Internal controls over financial reporting
- SOC2 – Internal controls over information systems
- SOC3 – A short, non-proprietary version of SOC2

TYPES OF SOC REPORTS

Type I – Describes a service organization's systems and whether the design of specified controls meet the relevant trust principles.

Type II – Addresses the operational effectiveness of the specified controls over a period of time (usually 6 to 12 months).

STEPS TO COMPLETE SOC REPORT

- 
1. Engage with auditor
 2. Classify your data
 3. Determine controls
 4. Write DOS (Description of Service)
 5. Validate controls

This is a type I SOC Report

STEPS TO COMPLETE SOC REPORT



- 6. Auditors test controls
- 7. Final opinion written

This is a type II SOC Report



AUDITOR OPINIONS

UNQUALIFIED

Controls are described in a fair and accurate manner and operate effectively

QUALIFIED

Controls mostly abide by the standards, but fall short in a few areas

ADVERSE

The service organization materially failed one or more of the standards

NO OPINION

Not enough details given to form an opinion

PARTS OF SOC REPORT

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT

This section highlights whether or not the service organization “passed” the assessment, and contains the Auditor’s final opinion

Opinion

In our opinion, in all material respects:

- a. the Description presents the Vendor Services Covered Services system that was designed and implemented throughout the period November 1, 2022, to April 30, 2023, in accordance with the Description Criteria.
- b. the controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively and if the Component and Non-affiliated Subservice Organizations (collectively, Subservice Organizations) applied the controls assumed in the design of Vendor, Inc. s controls throughout the period November 1, 2022, to April 30, 2023.

PARTS OF SOC REPORT

SECTION 2: MANAGEMENT'S ASSERTION

Vendor management assertion that the controls stated in the description were designed, implemented and operated effectively throughout the specified reporting period

Vendor, Inc.'s Management Assertion

We have prepared the accompanying Report on Management's Description of Vendor, Inc.'s Vendor Services' Covered Services System on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality For the Period November 1, 2022 to April 30, 2023 (Description) of Vendor, Inc. (Service Organization) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the Vendor Services' Covered Services system (System) that may be useful when assessing the risks arising from interactions with the System throughout the period November 1, 2022 to April 30, 2023, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

PARTS OF SOC REPORT

SECTION 3: DESCRIPTION OF SERVICES

Organizations write their own descriptions, and it serves as an overview of their systems and controls

Overview of Operations

Vendor, Inc. (Vendor or the Company), headquartered in San Francisco, California, is an enterprise cloud computing company that provides an integrated customer relationship management platform through various products and services. These products and services (Services) include solutions for enhancing customer success through sales, service, marketing, commerce, engagement, integration, analytics, enablement, and productivity, among others.

PARTS OF SOC REPORT

SECTION 3 (CONTINUED): COMPLEMENTARY USER ENTITY CONTROLS

COMPLEMENTARY USER ENTITY CONTROLS

Vendor's services are designed with the assumption that certain controls will be implemented by user entities. It is not feasible for all the Trust Services Criteria related to Vendor's services to be solely achieved by Vendor control procedures. Accordingly, user entities, should establish their own internal controls or procedures to complement those of Vendor's.

1. User entities are responsible for configuring and implementing user access controls.
2. User entities are responsible for ensuring the supervision, management, and control of the use of Vendor services by their personnel.
3. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Vendor services.
4. User entities are responsible for providing Vendor with a list of approvers for security and system configuration changes for data transmission.
5. User entities are responsible for immediately notifying Vendor of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

PARTS OF SOC REPORT

SECTION 3 (CONTINUED): COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

Vendor's services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Vendor services to be solely achieved by Vendor's control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of Vendor.

The following subservice organization controls should be implemented by River Web Services to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization – River Web Services		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.

PARTS OF SOC REPORT

SECTION 4: TEST OF CONTROLS

All auditor tests of controls and the results

Control Description	SOC 2 Criteria Reference	EY's Test Procedures	EY's Test Results
AC-20: Internal Admin Portal logical access is reviewed on a quarterly basis. Accounts identified as not being appropriate are investigated and resolved.	<u>CC6.2</u>	Inspected the access review documentation for a sample quarter to determine that Internal Admin Portal user accounts were reviewed by management quarterly and accounts identified as inappropriate were investigated and resolved.	For the one (1) quarterly review selected for testing related to Vendor.org Internal Admin Portal, determined that while the review was completed, evidence to support the completeness of the review was not retained. No issues noted for the other in-scope access reviews tested.
Management response: Vendor management determined all users' access was appropriate for the impacted review and validated the access review performed in the subsequent quarter within the examination period for the Vendor.org Internal Admin Portal included all required artifacts.			
AC-22a: Vendor provided database accounts are locked, removed or the default password is changed.	<u>CC6.2, CC6.6</u>	Inspected Vendor's Hardening Guide to determine vendor provided (default) database account passwords were required to be locked, or removed, or the default password was required to be changed for accounts that were not needed or being used.	No exceptions noted.

PARTS OF SOC REPORT

SECTION 5: OTHER INFORMATION (OPTIONAL)

Any other additional information relevant to the audit. This section is not verified by the auditor

Other Information Provided by Vendor

The information in this section is presented by Vendor to provide additional information and is not a part of Vendor's description that may be relevant to the user organization's internal control. This information has not been subject to the procedures applied in the examination of the description.

5.1 Health Insurance Portability and Accountability Act (HIPAA)

5.1.1 General Compliance Statement

Vendor has developed and implemented policies and procedures to be in compliance with the regulations promulgated under HIPAA Privacy & Security Rules (effective April 13, 2003), the statutory amendments under the Health Information Technology for Economic and Clinical Health Act (the HITECH Act or the act), and the HIPAA Transaction and Code Sets (effective October 16, 2002).

SOC REPORT IN REVIEW

AUDITOR'S OPINION

- Quick assessment

COMPLEMENTARY USER ENTITY CONTROLS

- In place at your organization?

EXCEPTIONS

- Impact on your organization?

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

- What does the vendor expect from their subservice providers

BRIDGE/GAP LETTER

- Assertion by the service organization that its controls are still in place and operating effectively while waiting for the next audit report
- Not signed by the service auditor



SUMMARY

- Documents the service organization's controls, policies and procedures in a narrative which details not only what they are, but how they interact.
- They are checked for adequacy and effectiveness by a knowledgeable, experienced and accredited professional, independent third party
- Replacement for the survey that typically constitutes the initial phase of a vendor risk assessment



THANK YOU

Heath Peek

217-606-9920

Heath.peek@illinois.gov

doit.illinois.gov/