# System and Organization Control (SOC) Report Discussion

Date Oct. 25, 2021

# Divider Page

# SOC Report Definition

**Definition** - A system and organization controls (SOC) report is a way to verify that an organization is following some specific best practices before you outsource a business function to that organization. These best practices are related to finances, security, processing integrity, privacy, and availability. The reports, which are created and validated by third-party auditors, during their examination of the control environment, are built to provide independent assurance and to help potential customers/partners understand any potential risks involved in working with the organization that was evaluated.

# SOC Report Purpose

**Purpose** - System and Organization Controls (SOC) reports enable companies, agencies, entities to feel confident that service providers, or potential service providers, are operating in an ethical and compliant manner. SOC reports establish credibility and trustworthiness for a service provider.

SOC reports utilize independent, third-party auditors to examine various aspects of a company, such as but not limited to:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy
- Controls related to financial reporting
- Controls related to Cybersecurity

# SOC 1

Reports on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting: SOC 1 reports examine an organization that provides services to user entities when controls are likely to be relevant to a user entity's internal control over financial reporting.

# SOC 2

Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy: Many entities outsource tasks or entire functions to service organizations that operate, collect, process, transmit, store, organize, maintain and dispose of information for user entities. A SOC 2 report is similar to a SOC 1 report, but it also includes a description of the tests performed by the service auditor and the results of those tests. SOC 2 reports specifically address one or more of the following **five key system attributes**:

**Security** – The system is protected against unauthorized access (both physical and logical)

**Availability** – The system is available for operation and use as committed or agreed

**Processing Integrity** – System processing is complete, accurate, timely and authorized

**Confidentiality** – Information designated as confidential is protected as committed or agreed

**Privacy** – Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice, and with criteria set forth in Generally Accepted Privacy Principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants

# SOC Report Types

- **Type 1 –** A Type 1 report details whether it is possible to achieve the related control objectives included in the description as of a specified date.

- **Type 2 –** A Type 2 report tests the related control objectives included in the description over a specified period of time. A Type 2 report provides a more thorough investigation and is a more intensive report to compile.

# BRIDE LETTER

A bridge letter is an essential document issued to you (service organization) to ensure your clients that you are compliant to SOC 1 or SOC 2 requirement even during the interim period between the expiry of previous years SOC report and the release of new SOC report. Typically, SOC 1 and SOC 2 reports cover a time frame of one year. However, an independent third-party auditor may select an examination time frame of less than a full year. In that case, to ensure that your organization has a complete year of coverage for the SOC examination time, a bridge letter is obtained.

The bridge letter or gap letter is issued to your organization from the provider's Chief Executive Officer stating what, if any, controls have changed such the time frame of the SOC examination. If no controls have changed, the bridge letter should simply state that the control environment has not changed since the SOC examination time frame. A SOC examination of a full year is the industry best practice for your clients to gain an understanding and comfort level as to your vendor's control environment.

# Auditing Standard for SOC Reports

SSAE stands for Statement on Standards for Attestation Engagements. Overseen by the American Institute of Certified Public Accountants (AICPA), SSAE 18 governs the way organizations report on their various compliance controls.

These reports usually come in the form of a System and Organization Control (SOC) report, which provides the information needed to accurately evaluate the risks associated with outsourced vendors. When assessing data center certifications, these reports provide the attestations of compliance.

# SOC Report Auditor's Opinion

- **Unqualified -** Controls are described in a fair and accurate manner and operate effectively. Simply, the controls abide by all of the standards.

- **Qualified -** Controls mostly abide by the standards but fall short in a few areas. The auditor will state in specifics where the service organization failed to adhere to the standards. For example, a specific control or objective may have failed the auditors testing and is considered significant enough to be an exception. But for these specific item(s), the auditor believes the control environment is adequate.

- **Adverse -** The adverse opinion is issued to the financial statements where auditors examine and concluded that those financial statements are materially misstated and pervasive.

# DoIT SOC Report

Link to DoIT SOC Reports: https://www.auditor.illinois.gov/Audit-Reports/DoIT.asp

- About the Office
- Audit Reports
- Procurement Bulletin
- Public Documents
- Notices
- Legislative Travel Control Board
- Career Information
- Contact Us
- Audit Related Links
- Search
- Inspector General
- Mobile Device Version
- Hotline
- Home

**DEPARTMENT OF INNOVATION & TECHNOLOGY**

| Audits | Release Date | |
|---|---|---|
| **Enterprise Resource Planning System -- System and Organization Control Report and Report Required Under *Government Auditing Standards* 2021**<br>Summary Report Digest - PDF<br>Summary Report Digest*<br>Full S.O.C. Report<br>G.A.S. Report | 08/12/2021 | FY21 ERP SOC 1 Type 2 Report |
| **Information Technology Shared Services -- System and Organization Control Report and Report Required Under *Government Auditing Standards* 2021**<br>Summary Report Digest - PDF<br>Summary Report Digest*<br>Full S.O.C. Report<br>G.A.S. Report | 08/12/2021 | FY21 DoIT SOC 1 Type 2 Report |
| **Information Technology and Hosting Systems -- System and Organization Control Report and Report Required Under *Government Auditing Standards* 2021**<br>Summary Report Digest - PDF<br>Summary Report Digest*<br>Full S.O.C. Report<br>G.A.S. Report | 08/12/2021 | FY21 DoIT SOC 2 Type 2 Report |
| **Compliance Examination for the Period Ending June 30, 2020**<br>Summary Report Digest - PDF<br>Summary Report Digest*<br>Full Report | 06/02/2021 | FY21 DoIT Compliance Report |
| **State of Illinois, Enterprise Resource Planning System -- System and Organization Control Report and Report Required Under *Government Auditing Standards* 2020**<br>Summary Report Digest<br>Summary Report Digest *<br>Full SOC Report<br>G.A.S. Report | 08/12/2020 | FY20 ERP SOC 1 Type 2 Report |
| **Information Technology Shared Services -- System and Organization Control Report and Report Required Under *Government Auditing Standards* 2020**<br>Summary Report Digest<br>Summary Report Digest *<br>Full SOC Report<br>G.A.S. Report | 08/12/2020 | FY20 DoIT SOC 1 Type 2 Report |

# DoIT SOC Type Report Content

**STATE OF ILLINOIS**

**DEPARTMENT OF INNOVATION AND TECHNOLOGY**

**TABLE OF CONTENTS**



Section I: OAG report & Auditor's opinion

Section II: Assertion

Section III: Description of Systems, Complementary Subservice Organization Controls. User Entity Responsibilities

Section IV: applicable controls, testing, result

Section V: Corrective Action Plan

# Major Controls covered in Report

- Subservice organizations
- Human Resources (Hiring, Training)
- Risk Assessment Process
- Internal/External Communication
- Monitoring activities
- Logical Access
- Network Services
- Change Management
- Security Operations Center
- EndPoint Protection
- Backups
- Physical Security
- SOC1: Application controls related to AIS, CPS, CTAS, eTime
- SOC2: Software, Network Firewalls,  Recovery

# DoIT SOC Report

**Key Elements**

- Testing Results & Exceptions
- Complementary Subservice Organization Controls
- User Entity Responsibilities

# Complementary Subservice Organization Controls

**Definition:** Controls that management of the service organization (vendor) assumes will be implemented by the subservice organizations and are necessary to achieve the control objectives stated in management's description of the service organization's system.

**Examples:**

1. Controls are implemented to provide IT managed services which are performed in accordance with contracts.

2. Controls are implemented to provide assurance that access to networks and applications is approved, reviewed periodically, and access is terminated timely.

3. Controls are implemented to provide reasonable assurance that only authorized personnel are able to make changes to network and Applications.

# Complementary User Entity Controls

**Complementary User Entity Controls (CUECs)- User Entity Responsibilities**

**Definition:** The controls that service provider wants the customer to have in place in order to achieve the service provider's control objectives.

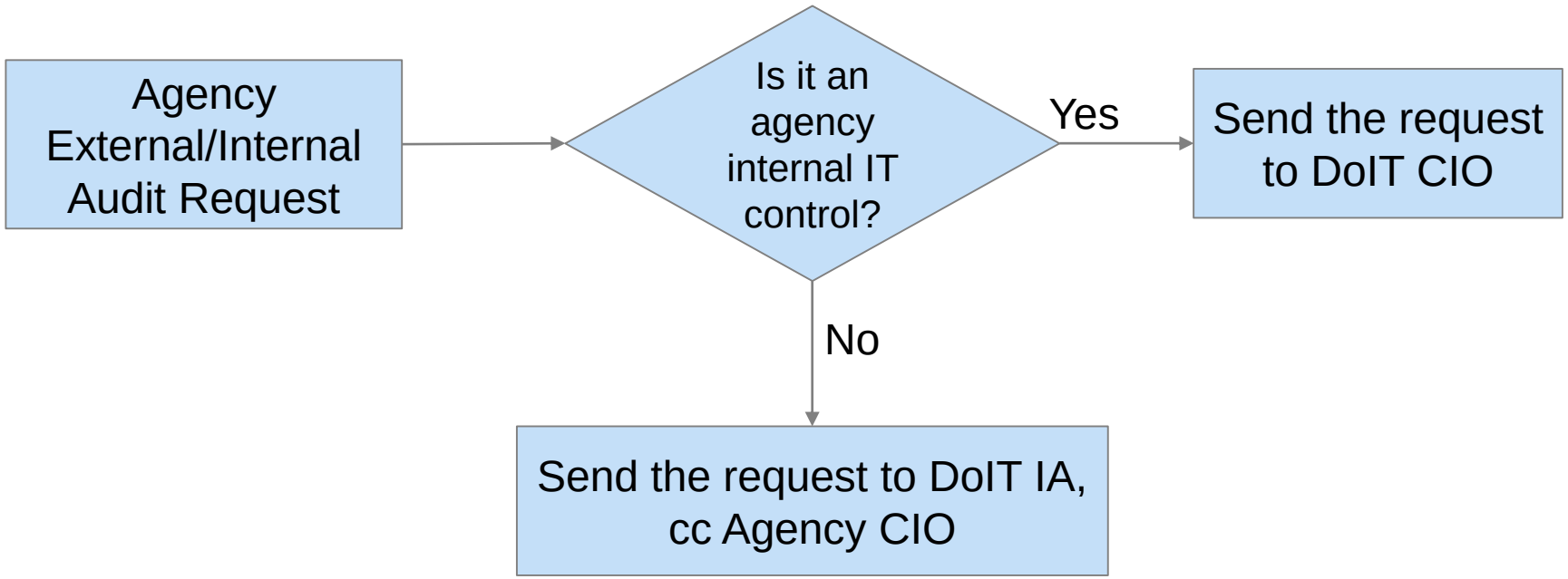
**Examples:**

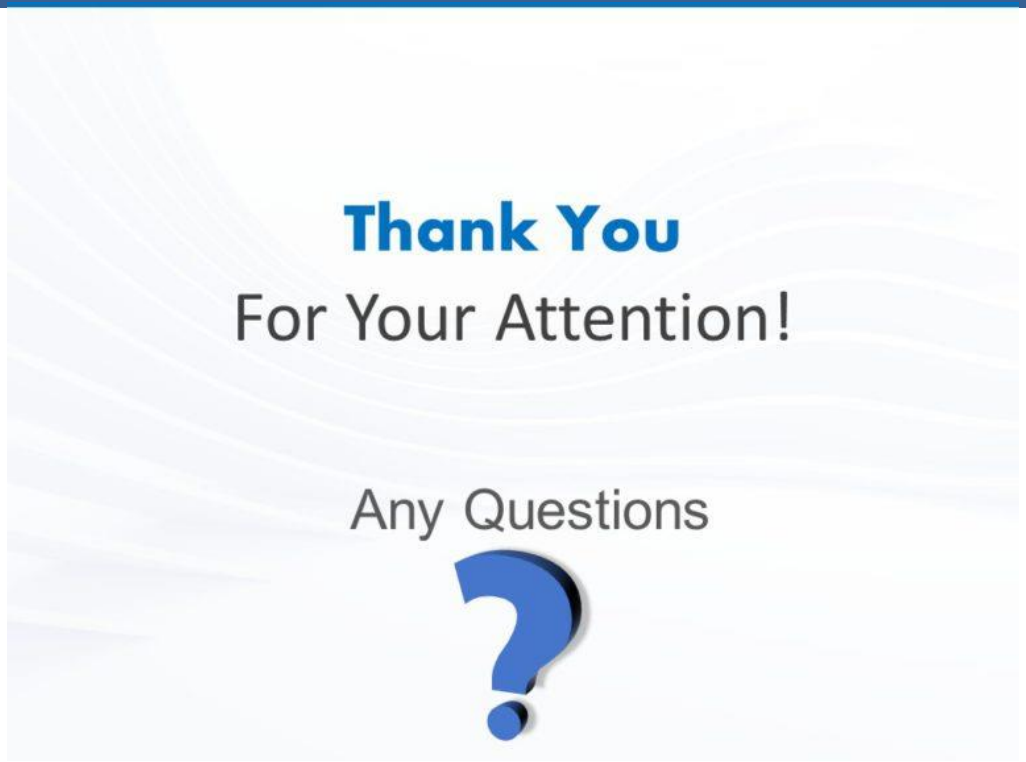
1. Agency is responsible for the complete and accurate entry and maintenance of data into the application.

2. Agency is responsible for submission of a service request documenting issues and needs of the environment and applications.

3. Agency is responsible for reviewing the user access rights to their data.

# Assistance from DoIT




John Valtierra, John.Valtierra@illinois.gov
Judy Zhu, Judy.Zhu@illinois.gov


# Thank you