Understanding How Users Would Make Use of a SOC2 Report

By Audrey Katcher, RubinBrown LLP for the Trust/Data Integrity Task Force

This document provides guidance to users of a SOC 2 report on the factors they should consider when evaluating the relationship of the controls being reported on in the SOC 2 report to their environment.

Definitions

Service organization. An organization or segment of an organization that provides services to User Entities, which are likely to be relevant to those User Entities' controls over its system relevant to security, availability, processing integrity, confidentiality, or privacy.

Service auditor. A practitioner who reports on controls over its system relevant to security, availability, processing integrity, confidentiality, and/or privacy at a service organization.

SOC 2 report**.** A report on a service organization's controls over its system relevant to security, availability, processing integrity, confidentiality, and/or privacy.

User entity**.** An entity that uses the services provided by the service organization. Constituents in the User Entity include management such as those with finance, internal audit, compliance, IT or other security and privacy responsibilities. For example, an IT department within a user organization may rely on the service organization for system availability.

Introduction

A User Entity who relies on a service organization that processes, maintains, or stores information for the User Entity needs to understand and monitor the systems being relied upon for such services in order to:

- assess stewardship or accountability
- assess the entity's ability to comply with certain aspects of laws and regulations, for example, the Health Insurance Portability and Accountability Act (HIPAA), contractual responsibilities, and commitments to stakeholders
- assess the integrity of the information provided
- assess regulatory the activities of the entity

User Entity Responsibility

Introduction

Management of a User Entity is responsible for assessing and addressing the risks faced by the User Entity.

When a User Entity engages a service organization to perform key processes or functions for it, the entity exposes itself to additional risks related to the service organization's system. Although management of a User Entity can delegate tasks or functions to a service organization, the responsibility for those tasks and the service organization provides cannot be delegated.

Management of the User Entity is held responsible by those charged with governance (for example, the board of directors), customers, shareholders, regulators and other affected parties for establishing effective internal control over outsourced functions.

To assess and address the risks associated with an outsourced service, management of the User Entity needs information about the service organization's controls over the system through which the services are delivered.

Understanding How Users Would Make Use of a SOC2 Report

By Audrey Katcher, RubinBrown LLP for the Trust/Data Integrity Task Force

Processing (performance of tasks or functions) at the service organization should enable operational integrity which is consistent with the User Entity's control environment.

When assessing controls at a service organization that may be relevant to and affect the services provided to User Entities, management of a User Entity may ask the service organization for a SOC 2 report on the design and operating effectiveness of controls over the service organization's system that may be relevant to the security, availability, or processing integrity of the system, or the confidentiality/ privacy of the information processed for User Entities. This report addresses risks and opportunities of IT-enabled systems and privacy programs beyond the controls necessary for financial reporting.

The User Entity Approach

A User Entity approach for evaluating the service organization's operational integrity and compliance and the use of a SOC 2 report typically should be as follows:

1. Assess the Risk
2. Understand the Service Organization
3. Understand the SOC 2 Report
4. Understand Complementary User Entity Controls

This approach is achieved through User Entity internal procedures and interaction with the service organization. After evaluating the service organization, the User Entity may decide to implement and monitor service level agreements, perform tests at the service organization or rely on the testing performed by an independent party.

Assess Risk

The significance and relevance of the operational and compliance reliance the User Entity places on the performance of tasks and functions at the service organization should be assessed. This assessment includes consideration of the types of services performed by the service organization, nature of the service organization relationship, and the degree of interaction with the service organization. Other considerations relate to understanding what processing is happening at the application, data, management, networking, storage and physical levels.

Since the nature of relationships will vary (between service organization and User Entity) there is no uniform or one-size-fits-all approach to managing this risk – or "certifying" the service organization.

Taking a risk based approach to User Entity reliance is necessary. The types of services provided may vary widely, and the need to assess which gaps are applicable to the User Entity environment is a key first step. This should consider the core aspects of the service organization's processing that the User Entity needs controlled: security, availability, processing integrity, confidentiality, and/or privacy of the User Entity's information.

Once the significance and relevance of the services are determined, the User Entity should understand the Policies, Communications, Procedures and Monitoring performed at the service organization to support the security, availability, processing integrity, confidentiality, and/or privacy of User Entity information.

Understanding How Users Would Make Use of a SOC2 Report

By Audrey Katcher, RubinBrown LLP for the Trust/Data Integrity Task Force

Use of a third party (a service organization) not only expands the risk beyond the boundaries of the User Entity organization, it also requires a User Entity to consider how risks have changed due to outsourcing. Changing how the service is delivered (through a third party service organization rather than through an internal department) changes the characteristics of risk. Examples of such risks are:

- increased portability of information
- virtualization of the information storage
- architecture that is more flexible (storage, processing, virtual networks)
- dynamic allocation of resources
- increased sharing of IT resource
- dependency on others for availability of information (for example, to support investigations).

An expansion of risk leads to an increased need for trust in the service organization's processing. When evaluating the risks which affect the trust, the following criteria are important: Security, Availability, Processing Integrity, Confidentiality, or Privacy.

The following example questions (not an all inclusive list) may help assess the operational and compliance risks a User Entity should consider:

- What risk is of concern as it relates to the service organization services?
- Is there concern related to processing being adequately designed/operating effectively to achieve operational and compliance objectives?
- Is assurance needed regarding other internal controls and/or security of the outsourced operations?
- What data, application, transaction processing is being performed by a service organization?
- What is the risk related to adherence to other performance/contractual/regulatory expectations?
- How is information protected? What policies, procedures, communications and monitoring support the security, confidentiality and privacy of information being processed?
- How is information available? What policies, procedures, communications and monitoring support the availability and processing integrity of information being processed?
- How do the operational and compliance controls at the service organization compare to existing User Entity controls?
- What documentation on how the environment and services are assessed for risk and controls is available to the User Entity?
- What is the separation of compliance responsibilities between the service organization and the User Entity?

Understand the Service Organization

The Service Organization may perform control processes relevant to the User Entity controls which are intended to mitigate risks related to security, availability, processing integrity, confidentiality, and/or privacy and are intended to assist management of a User Entity in carrying out its responsibility for monitoring the services it receives, including the operating effectiveness of a service organization's controls over those services.

The User Entity should understand the nature and extent of their reliance on services provided (including the nature of the relationships and degree of interaction).

Examples of services provided by service organizations.

- Cloud computing. Providing on-demand network access to a shared pool of configurable computing resources, for example, networks, servers, data/systems storage, applications, and services.
- Logical security management. Managing access to networks and computing systems for User Entities, for example, granting access to a system and preventing, or detecting and mitigating system intrusion.
- Financial services customer accounting. Processing financial transactions on behalf of customers of a financial institution or investment company. Examples are processing customer securities transactions, maintaining customer account records, providing customer transaction confirmations and statements, and providing related customer services through the web.
- Contact center for customer service. Providing customers of User Entities with on-line or telephonic post sales support and service management. Examples of these services are warranty inquiries and processing, trouble shooting, and responding to customer complaints.
- Sales force automation. Providing and maintaining software to automate business tasks for User Entities that have a sales force. Examples of such tasks are order processing, information sharing, order tracking, contact management, customer management, sales forecast analysis, and employee performance evaluation.
- Health care claims management and processing. Providing medical providers, employers, and insured parties of employers with systems that securely and confidentially support the processing of medical records and related health insurance claims.

Understand the report

The User Entity should understand the SOC 2 report coverage of the environment in support of User Entity processing. The User Entity should understand whether:

- the services relevant to the User Entity are included.
- there is a clear system description.
- the controls are relevant, with consideration of planned reliance on the operational and compliance controls, and the relationship to complementary User Entity activities.
- the report covers a period of time or a point in time and whether that time period is relevant to the User Entity's coverage needs.
- There is contiguous coverage between reports.

There should also be consideration of the level of change and the cyclical nature of processing within the system as well as historical information about the system.

It is important to understand the delineated boundaries of the system under examinations for trust services principles and criteria of security, availability, processing integrity, confidentiality and/or privacy. Knowing these boundaries help the user organization understand the control coverage over the processing relevant to their environment.

A reliable system is one that is capable of operating without material error, fault, or failure during a specified period in a specified environment. The SOC 2 report may provide a report on systems reliability that addresses the trust services principles and criteria of security, availability, processing integrity and/or privacy. Theses criteria are used to evaluate whether a system is reliable. If the weaknesses result in procedures the user cannot rely upon, the User Entity should determine the response to weaknesses identified in the SOC 2 report. The User Entity response may include performing tests of controls at the service organization or further identifying mitigating or complementary controls at the User Entity which are relevant.

Understand Complementary User Entity Controls

Understanding How Users Would Make Use of a SOC2 Report

By Audrey Katcher, RubinBrown LLP for the Trust/Data Integrity Task Force

In many cases, the control objectives stated in the service organizations' description of controls cannot be achieved by the service organization alone because their achievement requires that User Entities implement certain controls (complementary User Entity controls). The User Entity should evaluate the performance of their User Entity controls.

Report use restriction

The need for restriction on the use of a SOC 2 report may result from a number of circumstances, including the purpose of the report, the criteria used in preparation of the subject matter, the extent to which the procedures performed are known or understood, and the potential for the report to be misunderstood when taken out of the context in which it was intended to be used. (per paragraph .79 of AT section101).

Because of the potential for misunderstanding, the following paragraphs describe the knowledge a potential user of the report should have and identifies the report users who are most likely to have such knowledge

A report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy is intended to provide User Entities with information about the fairness of the presentation of management's description of the service organization's system, the suitability of the design and in a Type 2 report, and the operating effectiveness of the controls included in the description. Because the report may be misunderstood when taken out of the context in which it was intended to be used, the service auditor should restrict the use of the report to parties that are knowledgeable about:

- the nature of the service provided by the service organization
- how the service organization's system interacts with User Entities, subservice organizations, and other parties
- internal control and its limitations
- control objectives, the risks that may threaten the achievement of control objectives, and how controls address those risks

Report users who are most likely to have such knowledge include:

- management of the User Entities,
- practitioners evaluating or reporting on controls at a User Entity,
- independent auditors of the User Entities,
- regulators, and
- others performing services related to controls at the service organization, such as a service auditor reporting on controls at a User Entity that is also a service provider to other User Entities.

Other

This document is not intended to provide guidance to:

- management of a User Entity in assessing a service organization's controls that are likely to be relevant to a User Entity's internal control over financial reporting
- auditors of User Entities (user auditors) in planning and performing an audit of a User Entity's financial statements.