As a member of the RSM US Alliance, we would like to share the following with you.

Effective SOC reporting: Understanding the right options for your organization
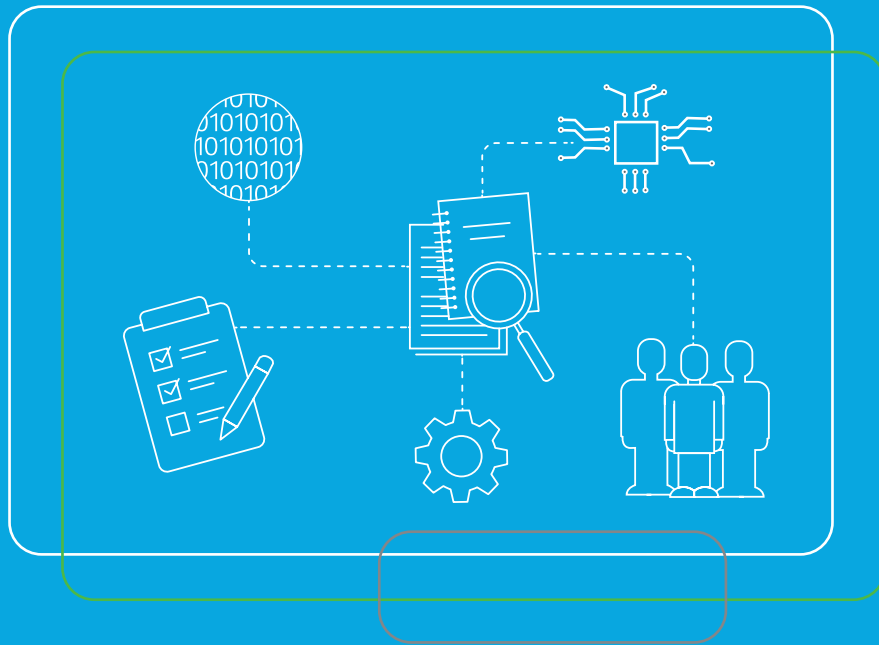
LOCALLY OWNED. NATIONALLY AFFILIATED. GLOBALLY CONNECTED.

An independently owned member
RSM US Alliance

RSM

Vasquez & Company is a proud member of the RSM US Alliance, a premier affiliation of independent accounting and consulting firms in the United States. RSM US Alliance provides our firm with access to resources of RSM US LLP, the leading provider of audit, tax and consulting services focused on the middle market. RSM US LLP is a licensed CPA firm and the U.S. member of RSM International, a global network of independent audit, tax and consulting firms with more than 43,000 people in over 120 countries.

Our membership in RSM US Alliance has elevated our capabilities in the marketplace, helping to differentiate our firm from the competition while allowing us to maintain our independence and entrepreneurial culture. We have access to a valuable peer network of like-sized firms as well as a broad range of tools, expertise and technical resources.

Los Angeles
+1 213.873.1700

Sacramento
+1 916.503.3269

San Diego
+1 619-254-6605

Manila
+1 213.873.1720

For more information:
solutions@vasquezcpa.com

Effective SOC reporting: Understanding the right options for your organization

Prepared by:

David Wood, Partner, RSM US LLP
david.wood@rsmus.com, +1 847 413 2066

Matt Gill, Partner, RSM US LLP
matt.gill@rsmus.com, +1 312 634 3979

Organizations have a variety of third–party reporting options, raising key questions about the most effective means to convey the control environment in place to users. System and organization control (SOC) reports are designed by the American Institute of CPAs (AICPA) to communicate those controls, but organizations must understand which report to choose to help users assess the risks of outsourcing providers.

For example, a SOC 1 report focuses on internal controls over financial reporting, with a Type 1 report assessing the design and implementation of controls as of a point in time and a Type 2 report assessing the design and implementation as well as the operating effectiveness of controls over a period of time. However, users are often more interested in security, availability, processing integrity, confidentiality or privacy. In these cases, a SOC 2 or SOC 3 report may be more appropriate.

In addition, with cyberthreats emerging and evolving each day, organizations are under pressure to document and detail their controls and capabilities to detect, deter and recover from cybersecurity events. In response, the AICPA has developed a SOC for cybersecurity reporting framework to help users gain a better understanding of an organization's cybersecurity risk management efforts.
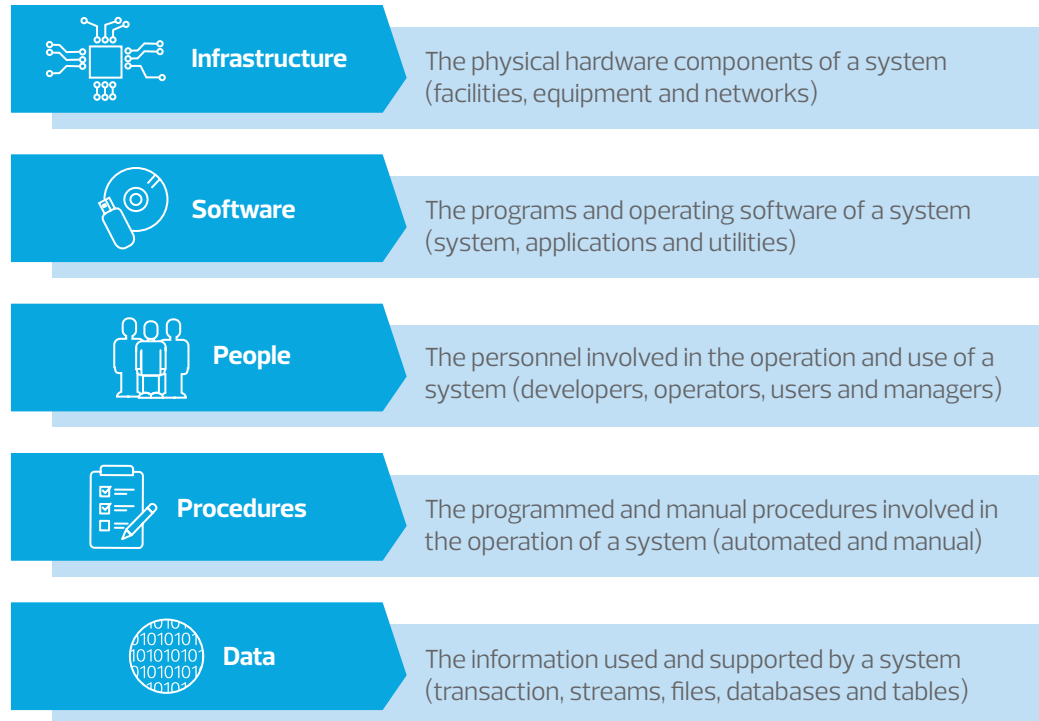
THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

The following chart provides details on the objectives of and differences between each SOC reporting option:

Reporting option	SOC 1	SOC 2	SOC 3	SOC Cyber
Purpose	Controls over financial reporting	Controls over security, availability, processing integrity, confidentiality and/or privacy to meet the organization's service commitments and system requirements		Provide useful information about an entity's cybersecurity risk management program
Intended audience and report distributions	Restricted use—knowledgeable parties at the service organization and user entity User entity auditors	Restricted use—knowledgeable parties at the service organization and user entity Users could include but are not limited to: ■ Management of the service organization ■ Existing customers ■ Prospective customers ■ Regulators	General use—individuals whose decisions might be affected by the effectiveness of controls over security, availability, processing integrity, confidentiality and/or privacy	General use—individuals whose decisions might be affected by the effectiveness of the entity's cybersecurity risk management program Users could include but are not limited to: ■ Board of directors of the service organization ■ Existing and prospective customers ■ Business partners ■ Investors and analysts ■ Regulators
Report sections	■ Report of independent service auditor ■ Management's assertion ■ Description of the service organization's system ■ For Type 2 reports, description of tests and related results		■ Report of independent service auditor ■ Management's assertion ■ Description of scope, or boundaries of system	■ Management's assertion ■ Report of independent accountant ■ Description of the cybersecurity risk management program
Control objectives or criteria	Service organization determines based on financial reporting needs of a broad range of users	Trust Services Criteria (TSC) and the description criteria for a description of a service organization's system	TSC, the boundaries of the system, and the principal service commitments and system requirements	Description criteria and TSC for control criteria or other suitable criteria as defined by the AICPA
Opinion	An opinion of the fairness of the presentation of the description of the service organization's system, the suitability of the design of the controls, and in a Type 2 report, the operating effectiveness of the controls In a Type 2 report, a description of the service auditor's tests of controls and the results thereof	An opinion that the presentation of the description is based on the description criteria, the suitability of the design of controls, and in a Type 2 report, the operating effectiveness of controls to meet the service commitments and system requirements based on the applicable TSC	An opinion on management's assertion that the controls are effective to meet the service commitments and system requirements based on the applicable TSC	An opinion on whether the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether the controls within that program are effective to achieve the entity's cybersecurity objectives based on the control criteria

With the importance of obtaining assurance beyond financial reporting risk, many service providers are being required to have a SOC 2 report in order to be considered as a business partner. Both SOC 2 and 3 reports require a detailed description of the system.

Components of the service organization system

The AICPA requires a service organization to describe all system components within its report. This description must be detailed enough to provide users with insight into all layers of technology within the organization, including:

Infrastructure — The physical hardware components of a system (facilities, equipment and networks)

Software — The programs and operating software of a system (system, applications and utilities)

People — The personnel involved in the operation and use of a system (developers, operators, users and managers)

Procedures — The programmed and manual procedures involved in the operation of a system (automated and manual)

Data — The information used and supported by a system (transaction, streams, files, databases and tables)

Understanding SOC 2 and 3 options

When issuing a SOC 2 and 3 report, service organizations have the ability to perform one or many of the trust service categories based on the service they provide to user entities and the contractual obligations and commitments they have with customers.

> **Security: The required category**
> Also known as common criteria, it's the foundation of an organization's systems controls environment, and is therefore a required category. Beyond that, service organizations can pick any or none of the remaining four categories depending on their specific needs (see page four for detailed description of categories).

The AICPA has developed a variety of different criteria that make up each category. While selecting a category beyond security is optional, once a service organization picks a category, every criteria must be achieved. Those criteria are predefined, so organizations know what compliance needs are required through their control activities.

The categories and criteria underwent several changes for 2017, reflecting a new focus on cybersecurity and an enhanced perspective on the data transaction life cycle. These changes were made to include COSO 2013 guidelines and emerging cybersecurity risks.

Trust services categories

Category	Category	Criteria
Security (common criteria)	Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives	Focuses on many criteria that are shared amongst all the categories as well as those specific to security including the implementation and dissemination of a security policy and accompanying procedures that include but are not limited to: • Control environment • Communication and information • Risk assessment • Monitoring activities • Control activities • Handling of security breaches and other incidents • Logical and physical security • System operations • Change management • Risk mitigation
Availability	Information and systems are available for operation and use to meet the entity's objectives	Focuses on the definition of availability requirements for systems, and in its policies and procedures, requires but is not limited to: • Implementation of measures that prevent or mitigate threats • Exception-handling procedures regarding system availability • Procedures that provide for the integrity of backup data and systems maintained to support related security policies
Confidentiality	Information designated as confidential is protected to meet the entity's objectives	Focuses on the definition of confidentiality requirements for systems, and in its policies and procedures, requires but is not limited to: • Procedures related to confidentiality of inputs, data processing and outputs that are consistent with policies • Understanding how data is protected while in transit • Understanding of ways that confidential information gets accessed, used and disclosed • Data loss prevention policies and programs • Protection of confidential information during change management activities
Processing integrity	System processing is complete, valid, accurate, timely and authorized to meet the entity's objectives	Focuses on the documentation and implementation of controls to confirm that system processing takes place as appropriate, and in its policies and procedures, requires but is not limited to: • Procedures related to completeness, accuracy, timeliness and authorization of inputs consistent with policies • Procedures for handling exceptions that are consistent with policies Note: additional requirements apply to e-commerce systems
Privacy	Personal information is collected, used, retained, disclosed and disposed to meet the entity's objectives	The privacy trust services principle is the largest of the principles and requires the definition, documentation and communication of, as well as accountability for, privacy-related policies and procedures. As part of the privacy policies and procedures, the service organization must consider and have in place such procedures and accompanying disclosures as: • Management of privacy policies and procedures • Collection, use, retention and disposal of personal information • Disclosure of personal information to third parties • Privacy incident and breach management • Monitoring and enforcement of the program

Trust service categories: What do we see in the marketplace?

While the security category is required, availability is the most popular of the other four, followed by confidentiality. In the last few years, confidentiality has gained significant momentum, as various regulations from different governing bodies and even large corporations have implemented new requirements for how service organizations must handle personally identifiable information (PII), protected health information (PHI) or other information that is deemed confidential.

Processing integrity is an applicable category if an organization processes a high-volume of information (e.g., a claims processor). However, these reports typically are similar in scope to a SOC 1 report, so many organizations that require processing integrity can likely rely on the SOC 1 information that has already been issued.

Privacy: Often the most challenging category
The AICPA frequently changes the criteria, and it is typically challenging to achieve. The volume of privacy criteria is large in comparison to the other optional criteria with very specific requirements rather than some of the more generic demands in the other criteria.

Privacy also requires a larger cost to a service organization both to prepare and be ready for an eventual attestation. A more significant amount of remediation is often involved with privacy and the cost to issue the report is substantial in comparison to the other criteria. In many cases, many aspects of the confidentiality principle overlap with privacy, and confidentiality may be the better fit for the organization.

Choosing and executing the right SOC report

Selecting the appropriate reporting options(s)

The first step in determining which SOC reporting option an organization should choose is to discuss the services offered. Do those services affect financial statements, or are they only managing applications, systems or data? Another key driver for SOC report selection is reviewing contractual obligations and requirements and determining the commitment to customers.

Service organizations also must understand the level of detail that is needed from a SOC report. The amount of detail is a key differentiator between SOC 2 and SOC 3 reports. Much of the work that goes behind SOC 2 and 3 reports are the same with the same set of categories, criteria and testing. However, a SOC 3 report is a very brief report, with very limited results, tests and controls shown.

Regarding presentation, the SOC 2, which is more common, is more in line with an SOC 1 report, providing a full description of an organization's system. It has all of the controls in the organization and the testing and results for each individual control test.

Getting prepared for an SOC attestation

In addition to choosing a report, an organization must understand how to prepare for an attestation. An SOC readiness assessment can help in these efforts in several ways, including:

- Assisting in documenting management's control activities
- Mapping those controls to either control objectives or criteria
- Assisting management in drafting the systems description
- Identifying potential gaps or observations in the control environment
- Providing detailed recommendations for remediation

The ultimate goal of a readiness assessment is for the service organization to determine if they are prepared for a future SOC attestation.
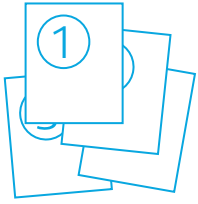
Types of SOC attestations

Many service organizations have difficulty differentiating the types of SOC attestations, their purpose and which is necessary. As mentioned earlier, SOC 1 and SOC 2 reports each have Type 1 and Type 2 reports, depending on specific needs. A Type 1 assessment is an attestation over the design and implementation of an organization's controls as of a specific point in time. Alternatively, a Type 2 report is an attestation of the design, implementation and operating effectiveness of controls over a period of time.

The SOC reporting timeline

Readiness	Remediation	Report (issued 45 days after report period end)
8 weeks	1–3 months	12 months*

*The most common reports cover a 12–month period. However, reports can cover a period of 6–12 months.

In our experience, SOC readiness engagements typically take between six and eight weeks and attestations are normally issued from 45–60 days after the report end date. We provide observations in real time, so the organization can begin remediation immediately. Once the readiness assessment is completed, it is management's responsibility to remediate the issues that are identified. However, that time can vary depending on management's availability and the necessary scope of changes. That should take place before a SOC 1 Type 2 or SOC 2 Type 2 report period begins.

Conclusion

On the surface, SOC reporting can seem like a complex initiative for service organizations. However, understanding the differences between reports and implementing the necessary steps to prepare for an attestation can greatly streamline the process. Ultimately, SOC reporting is a necessary initiative for businesses to understand and assess the control environments of business partners, and service organizations must implement steps to ensure the process is efficient and accurate, and the right reports are chosen and delivered.

+1 800 274 3978
rsmus.com

RSM