SOC 2 PREPAREDNESS

Better Understand SOC 2 Compliance

By Leslie Ogu, Senior
Security Consultant, K logix

SOC 2 OVERVIEW

In a world where security is as much a hot topic for organizations as it is a concern, the impeding question has continued to linger on how they can truly protect themselves and their customers. Security is a constantly evolving landscape where threat actors find new methodologies each day to attempt to exploit organizations for the data they protect. For this reason, to safeguard customers and their data, as well as maintain their trust, organizations must show that they have effective and adequate security measures in place. To accomplish this, frameworks are a popular route companies have pursued as means of showing a customer that security is a priority, is kept in mind from the beginning, and is in place. One of the more prominent frameworks is American Institute of Certified Public Accountants' (AICPA) Systems and Organization Controls (SOC) 2.

SOC 2 CRITERIA

SOC 2 is a framework that focuses on controls for an organization to implement based on the Trust Services Categories (TSCs)of security, availability, privacy, confidentiality, and processing integrity. The criteria outlined in SOC 2 provide guidance on relevant areas of cybersecurity that pose the highest risk to organizations and provide insight into other areas of their security program that they should continue to improve. Below is a description of each criterion:

- Security: Measures taken to safeguard information and systems from unauthorized access, as well as potential damage or compromise that could affect the privacy, confidentiality, integrity and availability of the information or systems
- Privacy: Measures taken to manage how personal information is collected, utilized, maintained, disclosed, and disposed
- Confidentiality: Measures taken regarding information that is considered confidential to protect and manage it in an organization's systems
- Processing Integrity: Measures taken to ensure processing conducted by systems are accurate, monitored, timely, complete, and authorized in order to comply with an organization's standards to carry out normal business processes
- Availability: Measures taken to confirm information and systems are available to carry out business functions in compliance with an organization's standards and needs.

PREPARING FOR SOC 2 EVALUATION

To prepare for SOC 2, an organization must define their scope and gather relevant documentation. The American Institute of Certified Public Accountants' (AICPA) Assurance Services Executive Committee (ASEC) outlines the common criteria evaluated in a SOC 2 assessment to give organizations a clear understanding of what must be in place to pass.

These common criteria govern controls pertaining to:

- The control environment
- Information and communication
- Risk assessment

- Monitoring of controls
- Controls activities related to the design and implementation of controls

These criteria evaluate the operating effectiveness of an organization's controls using the Trust Services Categories (TSCs). The security category is included by default in a SOC 2 assessment. The remaining TSCs of confidentiality, processing integrity, availability, and privacy, are not required for SOC 2. However, organizations should consider incorporating principles from these criteria as they provide additional transparency to customers regarding their security program, and the areas where the organization provides protection. For example, by including availability in the scope, an organization showcases the strength of their business continuity and disaster recovery plans, and processes that will ensure business operate as usual following an incident.

In addition to the common criteria, AICPA provides supplemental criteria that provide increased security assurances deemed critical for service organizations.

These additional criteria govern controls pertaining to:

- Logical and physical access controls
- Systems operations
- Change management
- Risk mitigation

If an organization meets all these criteria, it has covered all security-relevant concerns for all principles within the TSCs.



One helpful measure for an organization would be to delegate a team to assist the different business units in helping the organization understand why SOC 2 is being pursued, executing the necessary preparation steps, coordinate document collection, ensure the business is in good position to proceed with the assessment, and overall, make certain the process runs smoothly.

DEFINING THE SCOPE

With SOC 2, an organization determines how in-depth the assessment will be by defining the scope. This allows an organization to focus on the areas it is strongest to pursue SOC 2.

The drawback of defining the scope is the organization runs the risk of specifying a scope not thorough enough for a customer to develop trust, such as:

- Defining a scope that is too broad:
  - Could consume time and resources needed to create controls for risks that don't exist in the organization
  - Cause an auditor to discover linked systems or controls that could expand the scope to less secure systems
- Defining a scope that is too narrow:
  - Could mean certain risks will not be identified and this would make the business more vulnerable
  - Result in a report being generated after the assessment that is less useful or beneficial for clients, vendors, etc.

For this reason, it is crucial to solidify a balanced scope that provides enough assurance to customers of the organization's security controls, as well as confirm the organization's resources are used wisely.

To help determine the scope, an organization should consider:

• Which TSCs apply to the organization and the services they offer?

- Which systems and documentation support the selected TSCs?
- Which type of report (Type 1 or 2) does the organization desire?

Once an organization confirms their responses, they can finalize their scope and begin collecting the necessary documents to get started.

GATHERING REQUIRED DOCUMENTS

The policies and supporting procedures needed for the SOC 2 evaluation are determined by the scope. All policies and procedures should be established within the organization (i.e., documented, formally reviewed, and approved). If there are processes not supported by documentation, the organization should address this by creating them; otherwise, it will be identified as an exception. For a Type 2 report, evidence must be presented to show the auditor that the organization is following their own policies.

Two additional required documents are the management assertion letter and system description. The management assertion letter will explain the systems used to execute the organization's services, how they are carried out, and how they meet the requirements of the selected TSCs. The system description provides an overview of the organization's infrastructure included in the SOC 2 evaluation. A control matrix is also something that can be provided, and it pinpoints the specific controls that are relevant to the selected TSCs.

SOC 2 EVALUATION

The assessment is carried out by an auditor from a licensed CPA firm that specializes in information security. The auditor will review all documentation provided by the organization, and depending on the type of report being requested, either assess the controls at a point in time (Type 1 report), or the operating effectiveness of the controls over a period (Type 2 report).



SOC II COMPLIANT

ADDITIONAL RESOURCES

Organizations have the option of conducting a SOC 2 readiness assessment that is conducted by an experienced auditor to determine whether their organization is SOC 2 compliant. The organization would receive a letter outlining the gaps that need to be addressed before pursuing SOC 2. Organizations can also take part in SOC 2 audit training to learn more about how to prepare for a SOC 2 evaluation. These resources can be extremely beneficial for an organization to attain SOC 2.

EVALUATION TIMELINE

The average timeframe1 for executing the SOC 2 process is as follows (dependent on the organization's size, selected TSCs, scope, and documentation requirements):

- Getting Organization Approval: ~1 month
- Defining Scope: ~1 month
- Generating Missing Documents: 1 – 3 months
- Collecting Documentation: 1 – 12 months
- Selecting CPA Firm: 2 weeks – 1 month
- Readiness Assessment: 5 weeks – 3 months
- Training: 1 month+
- SOC 2 Evaluation:
  - Type 1: 1 – 2 months
  - Type 2: 45 days – 3 months
- Reporting:

- Type 1: 2 – 3 weeks
- Type 2: 3 – 12 months

SOC 2 COSTS

The average costs for the SOC 2 process are as follows (dependent on the size and complexity of the organization, desired CPA firm, selected TSCs, defined scope, and scope requirements):

- Creating and Collecting Documentation: $3K – $80K
- Readiness Assessment: $10K – $15K
- Training: $2K+
- SOC 2 Evaluation
  - Type 1: $6K – $20K
  - Type 2: $25K – $60K
- Report
  - Type 1: $5K – $10K
  - Type 2: $12K – $20K
- Legal Fees: $5K – $12K

When pursuing SOC 2, preparation is paramount. If an organization is willing to take the necessary measures to prepare for the assessment, they should be in a good position to become SOC 2 compliant.

HOW K LOGIX HELPS

K logix assists customers in understanding security frameworks such as Systems and Organization Controls (SOC) 2, and how they are leveraged to bolster their security program, as well as mitigate successful attacks from threat actors. K logix provides services to prepare organizations to attain compliance for security frameworks, like SOC 2, and create a plan of action to achieve it. With the threat landscape constantly shifting, it is our top priority to ensure organizations are well equipped and well prepared to not only stop tomorrow's attack but protect customers and their data.

ABOUT THE AUTHOR



Leslie has over 13 years' experience in IT and cybersecurity. He is currently a Senior Information Security Consultant at K logix, focused on helping organizations navigate complex cyber risks. Lesie previously held positions at The Internal Revenue Service, George Washington University, The Department of Homeland Security, and Deloitte.

REFERENCE MATERIAL:

Image source: https://www.aicpa.org/
https://secureframe.com/hub/soc-2/audit-timeline
https://cloudsecurityalliance.org/blog/2022/09/15/how-long-does-it-take-to-complete-a-soc-2-audit/
https://www.assurancelab.com.au/resources/post/soc-2-timeline
https://blog.rsisecurity.com/how-long-does-soc-2-compliance-take/
https://www.riskcrew.com/2021/06/how-to-get-soc-2-compliance-and-how-long-does-it-take/
https://secureframe.com/hub/soc-2/audit-cost
https://sprinto.com/blog/soc-2-compliance-cost/
https://www.auditboard.com/blog/soc-2-audit-cost/
https://www.schellman.com/blog/what-does-a-soc-audit-cost
https://www.strongdm.com/blog/how-much-does-soc-2-cost