SOC 2 vs. ISO 27001 Audit

As we talk about the two auditing standards, we should keep in mind that both are information security standards and involve an external audit performed with an intent of keeping your and client's data safe. Both are standards have different fundamental methodologies for providing an assurance. While, ISO 27001 is a certification of an ISMS (Information Security Management System) tested against an established framework, SSAE is an audit of the processes, policies and procedures an organization has in place.

ISO 27001 involves issuing a certificate of compliance by the auditor on completion which confirms that the organization meets the requirements set by the International Organization for Standardization (ISO) and International Electro technical Commission for protecting information and managing risk. A SOC 2 attestation involves a report prepared by the auditor to ascertain whether that a service organization's security controls meet the relevant Trust Services Criteria set by AICPA. While, both the standards cover most of the similar topics, they focus on differing audit criteria and the details of the two standards are completely different.

SOC 2 Assessment

SOC 2 audit involves evaluating a service organization's internal controls, policies, and procedures precisely based on the 5 trust services criteria i.e. security, availability, processing integrity, confidentiality, and privacy. The Trust Services Criteria are relevant to the services of organization as follows:

- **Security** – Protection of system against unauthorized access
- **Availability** – Availability of the system for operation and use
- **Processing Integrity** – The system is processing information completely, accurately and timely
- **Confidentiality** – Information classified as confidential is protected
- **Privacy** – Any personal information is collected, used, retained, disclosed, and destroyed in accordance with the entity's privacy notice.

ISO 27001 Audit

ISO 27001 is an internationally accepted standard for governing an organization's Information Security Management System (ISMS). The ISMS preserves the confidentiality, integrity, and availability of information by applying a risk management process and induces trust in external parties that information related risks are appropriately managed by the organization.

The ISO 27001 standard regulates how an organization creates and run an effective ISMS through policies and procedures and associated legal, physical, and technical controls supporting an organization's information risk management processes. An ISMS protects the confidentiality, integrity, and availability of information by applying a risk management

process. Following 7 sections of the ISO 27001:2013 standard (from section 4 to 10) provide the core guidelines for compliance with the standard:

- **Section 4:** Context of the Organization
- **Section 5:** Leadership
- **Section 6:** Planning
- **Section 7:** Support
- **Section 8:** Operation
- **Section 9:** Performance evaluation
- **Section 10:** Improvement.

Following are few other key differences between **SOC 2** and **ISO 27001** standards that further enhance your understanding:

The certifying and governing bodies

The SOC 2 report is attested by a licensed CPA (Certified Public Accountant) firm attests whereas an ISO 27001 certification is certified by a recognized ISO27001-accredited registrar. ISO 27001 is managed by the International Standards Organization (ISO) and SOC 2 attestation standards (SSAE 18) are regulated by the American Institute of Certified Public Accountants (AICPA).

Market Relevance

Both the standards are creditable security certifications accepted by clients widely. Precisely, if you are selling services to organizations in the United States, SOC 2 is better suited. However, if you are doing business internationally, ISO27001 is more extensively accepted by clients worldwide.

Certification Renewals

SOC 2 has two types namely Type 1 (*which gives a point in time design assessment*) and Type 2 (*which requires you to demonstrate effectiveness of your security controls for a period of time, typically twelve months*). Typically, a SOC 2 Type 2 needs to be renewed on an annual basis. On the other hand, an ISO27001 engagement includes a 3 year commitment where you have a point in time audit every year the certification and gets renewed annually after the successful completion of the audit.

Report Type obtained on completion

SOC 2 gives you a detailed report containing the auditor's opinion, management's assertion, description of controls, user control considerations, tests of controls, and the results. However, ISO certification is a single page certification issued to the company.

Applicability and use

A SOC 2 report laid out on the Trust service criteria is applicable to an organization's overall system while ISO 27001 based on the Information Security Framework is precisely applicable to organization's ISMS.

Further, SOC 2 attestation being a good industry practice is used measure a Service Organization against static security principles and criteria. The ISO 27001 is considered to be one of the best practices performed to establish, implement, maintain, and improve the ISMS of the organization.

Conclusion

Both SOC 2 and ISO 27001 are effective compliance methods for organizations to accept and can be utilized to get an edge over market competition, demonstrate the design and operating effectiveness of internal controls, and to achieve compliance with regulatory requirements.

One can decide to go through either a SOC 2 or ISO 27001 engagement based on their understanding of markets, customer's and the regulatory requirements that they need qualify. Hope, you have a clearer picture about the two standards now. Please feel free to reach out to us in case you have any queries or to seek more information.