EDB
Postgres for the AI Generation

An Overview and Comparison of ISO 27001 and SOC 2 Standards

www.enterprisedb.com

TABLE OF CONTENTS

Introduction

In today's ever-changing digital landscape, organizations face increasing challenges in managing and securing sensitive information. Two widely recognized standards that address these concerns are ISO 27001 and SOC 2. While both primarily focus on information security, they have distinct scopes, objectives, and applicabilities. This white paper aims to provide a comprehensive comparison of ISO 27001 and SOC 2 standards, highlighting their differences, similarities, and the business justifications for their adoption.

Overview

Section 1: Overview of ISO 27001

ISO 27001 is an international standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO 27001:2022 is the latest version of the international standard for information security management systems (ISMS), replacing ISO 27001:2013, and provides a robust framework for organizations to establish, implement, maintain, and continually improve their systems. By adopting ISO 27001, organizations can effectively manage risks, protect valuable information assets, and demonstrate their commitment to information security excellence in today's increasingly interconnected and digital business environment. Key features and considerations of ISO 27001 include:

- **Scope:** The standard covers all types of organizations, regardless of size, industry, or sector. It is designed to be flexible and scalable, accommodating the diverse needs and risk profiles of different organizations.
    - It addresses the requirements for establishing, implementing, maintaining, and continually improving an ISMS within the context of the organization's overall business risks.
- **Objectives:** The standard focuses on establishing a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability.
- **ISMS:** The core of ISO 27001 is the ISMS, which is a framework of policies and procedures that includes legal, physical, and technical controls involved in an organization's information risk management processes.
    - Its intent is to outline a systematic approach to managing sensitive information, covering risk assessment, risk treatment, monitoring, and continual improvement.
- **Risk-based approach:** ISO 27001 emphasizes a risk-based approach in which organizations are required to identify information security risks and implement controls to manage and mitigate these risks effectively.
    - Risk assessments and risk treatments are fundamental processes within the ISMS, ensuring that security measures are aligned with identified risks and organizational objectives.
- **ISO 27001:2022 domain structure:** Annex A controls (as defined within ISO 27002) are divided into four domains and 93 controls:
    - Organizational: 37 controls
    - People: 8 controls
    - Physical: 14 controls
    - Technological: 34 controls
- **Benefits:** The standard enhances trust with stakeholders, ensures compliance with legal and regulatory requirements, and improves overall organizational resilience against security threats.

Section 2: Overview of SOC 2

Service Organization Control (SOC) 2, developed by the American Institute of CPAs (AICPA), is specifically designed for service providers responsible for handling customer data and providing services such as software as a service (SaaS), data hosting, and managed IT services. It is based on five Trust Service Criteria (TSCs) related to security, availability, processing integrity, confidentiality, and privacy. Each criterion outlines requirements for which service organizations must implement controls to demonstrate compliance and provide assurance to stakeholders. Key features and considerations of SOC 2 include:

- **Scope:** This primarily applies to service organizations that handle customer data in the cloud, such as SaaS providers, data centers, and managed service providers.
- **Objectives:** These are used to assess the controls relevant to the security, availability, and processing integrity of the systems used to process data and the confidentiality and privacy of the information processed by these systems. The TSCs included within the scope of a SOC audit are determined by the service organization and agreed upon by the independent audit firm during audit planning.
    - The security TSC is required in any SOC audit. It not only sets overarching security standards for the service organization but also overlaps with the others, setting security controls for availability, confidentiality, privacy, and processing integrity.
    - SOC 2 audits must be conducted by an external auditor from a licensed certified public accounting firm and result in the delivery of an attestation report that includes the auditor's independent opinion of compliance with in-scope SOC 2 criteria.
- **Report types:** There are three types of SOC 2 reports:
    - SOC 2 Type 1: Reports on the suitability of the design of controls at a specific point in time
    - SOC 2 Type 2: Reports on the operational effectiveness of controls over a period of time
    - SOC 3 Type 2: Reports that provide a high-level overview of an organization's controls and security risks designed for a general audience and that can be distributed freely or posted to the public on an organization's website
- **Review date vs. review period:** A SOC 2 audit entails an evaluation of either the design (Type 1) and/or operating effectiveness (Type 2) of a service organization's controls by an independent auditor.
    - Type 1 reports define a review date (e.g., December 31) for which control design is evaluated as of that point in time.
    - Type 2 reports define a review period (e.g., January 1–December 31) for which operating effectiveness of controls is evaluated over that period of time.
- **Principal service commitments:** These are the assurances and commitments that service organizations make to their customers regarding the handling of customer data and the effectiveness of their control environment. These commitments are foundational to the SOC 2 and must be identified in alignment with the in-scope TSCs and have supporting controls in place to satisfy the commitments that are evaluated as part of the audit.
- **Control objectives and activities:** Service organizations define control objectives and activities to address each TSC based on their specific services and the nature of the customer data they handle.
    - Controls typically include policies, procedures, and technical measures aimed at safeguarding customer data, ensuring system availability, maintaining data integrity, and protecting confidentiality and privacy.
- **Benefits:** The SOC 2 system provides assurance to customers regarding the security and privacy of their data, helps service providers meet regulatory requirements, and improves risk posture along with internal processes and controls.

Section 3: Differences between ISO 27001 and SOC 2

While both standards aim to enhance information security, there are notable differences:

- **Applicability:** ISO 27001 is applicable to all organizations, whereas SOC 2 is specifically designed for service providers and scoped to evaluate specific systems, products, or services.
- **Focus:** ISO 27001 focuses on establishing and maintaining an ISMS, whereas SOC 2 focuses on controls relevant to service providers handling customer data.
- **Certification vs. attestation:** ISO 27001 allows for certification of compliance with the standard issued by an accredited certification body that can be posted to an externally facing directory. SOC 2 compliance does not result in the issuance of a certificate but rather an attestation report issued by a licensed external auditor, including that auditor's independent opinion regarding whether controls were suitably designed to meet the specified criteria and/or were operating effectively during the audit review period.
- **Audience:** ISO 27001 generally holds broader international recognition and acceptance across diverse industries and regulatory environments worldwide, whereas SOC 2 is viewed as more predominant in the US and is designed to focus on service organizations that handle customer data.
- **SOC 2 controls vs. ISO requirements:** SOC 2 controls are implemented by the service organization and are typically tailored in nature, must satisfy principal service commitments, and allow for more flexibility to meet criteria requirements. ISO 27001 requirements map directly to the Annex A controls that are defined within the ISO 27002 standard. These controls are not meant to be tailored or modified by certification bodies or the auditee, although the supporting processes in place to meet requirements are unique to the organization.

Section 4: Similarities between ISO 27001 and SOC 2

Despite their differences, ISO 27001 and SOC 2 share common objectives and principles:

- **Information security management:** Both standards emphasize the importance of managing and protecting sensitive information.
- **Risk management:** Both frameworks require risk assessments and management processes to identify and mitigate information security risks.
- **Overlap:** While not identical, there is overlap in the types of controls and requirements addressed within each standard, including:
    - **Access control:** Implementing controls to prevent unauthorized access to systems and data
    - **Risk assessment and management:** Emphasizing a risk-based approach to information security and implementation of controls to manage and mitigate risks effectively.
    - **Monitoring and logging:** Implementing controls to monitor information systems, networks, and applications to detect security events and vulnerabilities and mitigate potential data breaches and other security incidents
    - **Incident management:** Establishing procedures for detecting, responding to, and mitigating security incidents
    - **Physical and environmental security:** Protecting physical premises and information systems from unauthorized access, damage, and interference
    - **Human resource security:** Addressing security aspects related to employees, contractors, and third-party users
    - **Compliance:** Ensuring compliance with legal, regulatory, and contractual requirements related to information security
- **Continuous improvement:** Both encourage ongoing monitoring, review, and improvement of information security practices.
- **Assurance to stakeholders:**
    - **SOC 2:** Provides assurance to customers and stakeholders about the security and privacy of their data through independent audit reports (Type 1 and Type 2)
    - **ISO 27001:** Provides assurance to stakeholders, including customers, regulators, and business partners, through formal certification audits conducted by accredited certification bodies

Section 5: Business justification for ISO 27001 adoption

Organizations may choose ISO 27001 for various reasons:

- **Comprehensive approach:** ISO 27001 certification provides a holistic framework for managing information security across all aspects of an organization.
- **Global recognition:** ISO 27001 certification is globally recognized, enhancing credibility and competitiveness in the international market.
- **Regulatory compliance:** The standard helps organizations comply with legal and regulatory requirements related to information security.

Section 6: Business justification for SOC 2 adoption

Service providers may opt for SOC 2 for:

- **Customer assurance:** SOC 2 assures customers that their data is handled securely and meets industry standards for privacy and confidentiality.
- **Competitive advantage:** SOC 2 differentiates service providers by demonstrating a commitment to security and compliance.
- **Operational efficiency:** SOC 2 improves internal processes and controls related to data security and availability.

Conclusion

In conclusion, while ISO 27001 and SOC 2 each have a distinct scope and focus, both standards play crucial roles in enhancing information security and organizational resilience. The choice between ISO 27001 and SOC 2 should align with the specific needs, objectives, and operational context of the organization or service provider. By understanding their differences, similarities, and respective business justifications, organizations can make informed decisions to strengthen their information security posture and meet stakeholder expectations effectively.

EDB provides a data and AI platform that enables organizations to harness the full power of Postgres for transactional, analytical, and AI workloads across any cloud, any time.

For more information, visit www.enterprisedb.com.