ISO/IEC 27001 CERTIFICATION VS SOC 2 AUDIT

Understanding Two "Systems of Trust" and NUWAVE's Implementation

April 2023 | NUWAVE Data Protection Group

B2B ORGANIZATIONS TODAY ARE OFTEN ASKED by customers to produce an ISO/IEC 27001 certificate or a SOC 2 audit report. Two widely popular frameworks, both "systems of trust" demonstrate a level of commitment by service providers to assess risk, mitigate vulnerabilities, and safeguard customer data entrusted to it. But what are the similarities and differences between these frameworks? And what has NUWAVE chosen to implement?

ISO 27001 FOCUSES ON BUILDING A DATA PROTECTION PROGRAM called an Information Security Management System (ISMS). NUWAVE has chosen to implement an ISMS, which posits a method of managing security practices across three key areas: confidentiality[1], integrity[2] and availability[3]. In essence, ISO 27001 observes the following "1 / 2 / 3 cadence" of publishing policies, generating procedures and conducting audit to test evidence of practice.

1. Policies: Policies dictate practices the organization must follow; the policies are promises that customers can believe.
2. Procedures: Procedures demonstrate how the organization will achieve the promises.
3. Audit: Auditors examine policies to ensure they're complete, and that procedures are comprehensive. Auditors require "evidence of practice" to demonstrate the organization does what it promises and produce a report that clientele can review.

Organisations boasting an ISO 27001 certification can be trusted to safeguard customer data according to best practices, with an accompanying report that demonstrates strengths and weaknesses across practice areas. ISO 27001 is also the most common data protection program customers implement on an international basis, which is one of the reasons why it was chosen by NUWAVE as a form of attestation to present to its customers.

SOC 2 FOCUSES ON FIVE TRUST SERVICES CRITERIA (TSC): Security, Availability, Confidentiality, Processing Integrity, and Privacy. The SOC 2 system of audit was designed by the American Institute of Certified Public Accountants (AICPA), and as such, it's particularly favored in the United States. Many

[1] Confidentiality means keeping secret things secret.
[2] Integrity means data does not change unless acted upon by an authorized agent.
[3] Availability means services are accessible when needed.

large and well-known U.S.-based customers will request vendors to supply a SOC 2 audit report. More recently, the SOC 2 standard has been gaining tracking in Europe, especially as European companies look to do more business with U.S.-based entities.

Similarities and Differences Between ISO 27001 and SOC2

While SOC 2 refers to a set of audit reports to evidence the level of conformity of information security controls' design and operation against a set of defined criteria (TSC), ISO 27001 is a standard that establishes requirements for an Information Security Management System (ISMS), i.e., a set of practices to define, implement, operate, and improve information security. The table below shows a comparison between SOC 2 and ISO 27001 and their applicability.

System Criteria	SOC 2	ISO 27001
Structure	Attestation	International Standard
Geographic Applicability	Highly US-centric	International
Governance	American Institute of Certified Public Accountants (AICPA)[4]	International Organization for Standardization[5]
Average Implementation Timeframe	9 to 12 months	9 to 24 months
Definition	A set of audit reports to evidence the level of conformity to a set of defined criteria.	A standard that establishes requirements for an Information Security Management System (a type of data protection program).
Applicability by Industry	Can be applied to service organisations from any industry most commonly used by technology-based service organisations.	Designed to be used by organisations of any size or industry.
Compliance	Attestation by a licensed Certified Public Accountant (CPA) under the American	Certificate issued by an ISO certification body and auditor

[4] The American Institute of Certified Public Accountants (AICPA) is the U.S. national professional organization of Certified Public Accountants (CPAs) in the United States, which has a joint venture with the equivalency in the UK called the Chartered Institute of Management Accountants (CIMA), together producing the Chartered Global Management Accountant (CGMA) designation.

[5] As of 2022, there are 167 members representing ISO in their country, with each country having only one member. ISO has 804 technical committees and subcommittees concerned with standards development and has developed over 24,261 standards. (ISO, 2021)

System Criteria	SOC 2	ISO 27001
	Institute of Certified Public Accountants (AICPA).	by a Qualified Security Assessor (QSA).
What is it for?	To prove security level of systems against static principles and criteria.	To define, implement, operate, control, measure and improve overall security efficacy.
Requirements	80 to 100 controls to satisfy 35 criteria for security.	Up to 114 controls.
Review Period	Annually	Annually

It's important to understand that both ISO 27001 and SOC 2 are very similar standards. A mapping of each standard's criteria available on the AICPA website will demonstrate an average of approximately 80% overlap between these two systems of trust; in some cases, the overlap is as high as 90%. It is not unusual to see SaaS companies in the United States lean more toward SOC 2 for which the governing body is the American Institute of Certified Public Accountants, and where the assessors are Certified Public Accountants (CPAs). In the rest of the world, it is not unusual to see a preference toward ISO 27001, where the assessors are Qualified Security Assessors (QSAs). Both standards are intended to convey trust and assurance to customers that a system of governance and risk management is in place and operating, audited by independent auditors, producing an audit report of strengths and weaknesses.

SOC 2 is not a certification; it's an audit and results in an audit report, a critical customer-facing instrument that conveys assurance and trust from the perspective of an independent auditor. In contrast, ISO 27001 is a standard with prescriptive requirements; NUWAVE has implemented the ISO/IEC 27001 standard along with the ISO/IEC 27002 framework that covers 14 security control areas. The successful implementation ISO 27001 and ISO 27002 results in a certification that must undergo annual audit, which is also accompanied by an independent auditor's report.

Excerpts from International Companies Implementing ISO 27001

The follow commentary and quotes are provided from prominent international entities that have chosen to implement ISO 27001.

- **Deloitte:** "Achieving the ISO 27001 certification is an important milestone in our journey to achieve our organizational vision to be the Standard of Excellence, and the first choice of the most sought-after clients and talent," said Shree Parthasarathy, Partner, Deloitte. "The certification ensures that we have the perfect base set up, on which we need to capitalize and improve on a continual basis, so as to achieve operational excellence at the Cyber Intelligence Centre." (Parthasarathy, 2017)
- **Microsoft:** "The international acceptance and applicability of ISO/IEC 27001 is the key reason why certification to this standard is at the forefront of Microsoft's approach to implementing and managing information security." Maintaining ISO 27001 "demonstrates that Microsoft uses

internationally recognized processes and best practices to manage the infrastructure and organization that support and deliver its services. The certificate validates that Microsoft has implemented the guidelines and general principles for initiating, implementing, maintaining, and improving the management of information security." (Mazzoli, et al., 2022)

- **Google:** "ISO 27001 is one of the most widely recognized, internationally accepted independent security standards. Google has earned ISO 27001 certification for the systems, applications, people, technology, processes and data centers serving a number of Google produces." (Google)
- **Amazon:** SOC 2 "is often thought of as showing depth of security and controls because there's a thorough investigation and testing of each defined control. ISO 27001, on the other hand, shows a lot of breadth because it covers a comprehensive range of well recognized information security objectives." (Barr, 2010) The basis of ISO 27001 certification "is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System (ISMS) which defines how AWS perpetually manages security in a holistic, comprehensive manner." (Amazon, 2022)

NUWAVE's Decision Not to Undergo a SOC 2 Audit

As noted earlier, there's considerable overlap between a SOC 2 audit report and an ISO 27001 certification audit report, estimated at approximately 80% to 90%; both systems of trust convey confidence to customers that a risk management system is operative and that safeguards are in place to protect information and promote ongoing improvement. Both systems of trust require evidence of practice to be produced and challenged by the auditor. Whilst companies such as Google, Microsoft and AWS maintain both systems, the burden on SMB organizations to maintain both systems can be taxing, incumbered with the load of carrying high recurring costs, annual recertifications and audits. While having both reports may be convenient for customers that may preference one or the other, its impact to workforce productivity can be counterproductive to the SMB organisation.

Also, the ISO 27001 framework plays nicely with other standards that can be added to ISO's Annex L system, creating an integrated management system (IMS) as the company grows. For instance, a company can add a quality management system (QMS) by adding ISO 9001[6] that perfectly interconnects to the ISO 27001 standard, and later add an ISO 20000[7] service management system (SMS) for the same interplay. Furthermore, heightened cloud security controls can be supplemented by adding ISO 27017[8]

[6] ISO/IEC 9001:2015 deals with the fundamentals of a quality management system, including seven quality management principles. Over one million organisations worldwide are independently certified to ISO 9001. (ISO 9001, 2021)

[7] Developed by ISO/IEC JTC1/SC7, ISO/IEC 20000 was originally designed to reflect the best practice contained within the ITIL framework, including aspects from the Microsoft Operations Framework and ISACA's COBIT framework. ISO/IEC 20000:2018 specifies requirements to establishing, implementing, maintaining and continually improving a service management system (SMS). (ISO 20000, 2021)

[8] ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing: (1) additional implementation guidance for relevant controls specified in ISO/IEC 27002; (1) additional controls with implementation guidance that specifically relate to cloud services. (ISO 27017, 2021)

(cloud security) and ISO 27018[9] (PII in the cloud) to the ISO 27001 framework – all compatible with the forementioned standards. This is NUWAVE's direction.

Because of these reasons, and to foster future growth compatible with the roadmap of NUWAVE, the organisation has chosen the ISO-pathway for building trust with its customers and compliance with its statutory and contractual obligations.

Building the Future of Trust with ISO's Annex L Attestations

NUWAVE has a mature ISO 27001 implementation, and is adding several Annex L attestations as of this writing. The Information Security Management System is transforming into an Integrated Security Management System, and will be comprised of the following systems:

- ISO/IEC 27001 with most ISO/IEC 27002 control objectives;
- ISO/IEC 27017, the code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27018, the code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors; and
- ISO/IEC 27701, as an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management.

The certification stack, when fully implemented, will appear as follows.

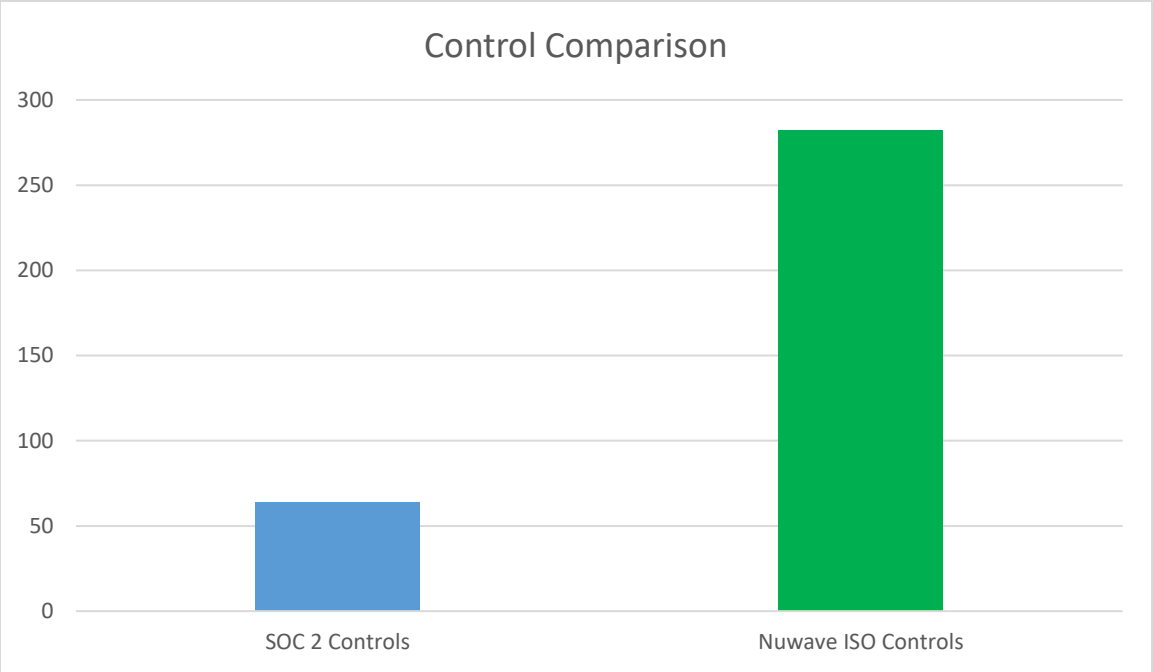
[9] This standard establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. (ISO 27018, 2019)

Conclusion and Control Objective Comparison

Taken together, the combined security and privacy system at NUWAVE results in a comprehensive audit report that examines the company's policies and procedures to verify alignment with the requirements of the standards, and tests evidence of practice, resulting in a significant audit report of strengths and weaknesses systemwide.

Control and Requirements Comparison Between SOC2 and ISO 27000 Stack	
SOC 2 TSCs	64 Requirements (Controls)
ISO 27001, 27017, 27018, 27701	282 Control Objectives

This is NUWAVE's pathway to convey assurance to customers that it can be trusted to safeguard customer data lawfully and properly according to modern best practices.



References

Amazon. (2022, July 31). ISO/IEC 27001:2013. *AWS Cloud Security*. Retrieved from https://aws.amazon.com/compliance/iso-27001-faqs/

Barr, J. (2010, November 16). AWS Receives ISO 27001 Certification. *AWS News Blog*. Retrieved from https://aws.amazon.com/blogs/aws/aws-receives-iso-27001-certification/

Google. (n.d.). ISO 27001 Certification. *Data Privacy and Security*. Retrieved September 17, 2022, from https://support.google.com/analytics/answer/3407084?hl=en

ISO 20000. (2021, July 6). *ISO/IEC 20000-1:2018: Information technology — Service management — Part 1: Service management system requirements*. Retrieved from International Organization for Standardization: https://www.iso.org/standard/70636.html

ISO. (2021, February 16). *About Us*. (G. Secretariat, Editor) Retrieved from International Organization for Standardization: https://www.iso.org/about-us.html

ISO 27017. (2021, April 19). *ISO/IEC 27017:2015: Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. Retrieved from International Organization for Standardization: https://www.iso.org/standard/43757.html

ISO 27018. (2019, January 15). *ISO/IEC 27018:2019: Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*. Retrieved from International Organization for Standardization: https://www.iso.org/standard/76559.html

ISO 9001. (2021, September 1). *ISO 9000 Family Quality Management*. Retrieved from International Organization for Standardization: https://www.iso.org/iso-9001-quality-management.html

Mazzoli, R., Jahiu, D., Cross, K., Vukos-Walker, C., Buck, A., Strome, D., & Woitasen, D. (2022, July 11). ISO/IEC 27001:2013 Information Security Management Standards. *Microsoft Compliance Offerings*. Retrieved September 17, 2022, from https://learn.microsoft.com/en-us/compliance/regulatory/offering-iso-27001

Parthasarathy, S. (2017, May 18). Deloitte's Cyber Intelligence Centre in India Achieves ISO 27001:2013 Certification from Intertek. *Intertek News*. Retrieved September 2022, 17, from https://www.intertek.com/news/2017/05-18-intertek-certifies-deloitte-cyber-centre-india-iso-27001/