Accedere

ISO/IEC Certification for Data Security & Privacy

Table of Contents

About Us

Accedere is a Cybersecurity firm with a major focus on AICPA SSAE 18 Attestation (formerly SSAE 16), SOC 1, SOC 2 Type 2 and SOC 3 Compliance Reports, ISO/IEC 27xxx Audits, Cloud Security, Privacy Compliance (HIPAA, GDPR, CCPA, etc.) and Data Security Audit Services. We are an ISO/IEC Certification Body, SOX, Privacy, SSAE 18, SOC Auditors (Service Auditors) registered with PCAOB, and Cloud Security Alliance as Auditors for their STAR program.

The company has managed many cybersecurity projects covering SOC reporting, Privacy, IoT, SCADA and Industrial Control System (ICS), Governance Risk, and Compliance. We have expertise in implementing frameworks and compliance mandates such as ISO/IEC 27xxx series, IEC 62443/ISA99, NERC-CIP, NIST 800-82, COBIT, etc.

"We are Accredited by IAS as an ISO/IEC Certification Body"

Ashwin Chaudhary is the CEO of Accedere. He is a CPA from Colorado, MBA, CITP, CISA, CISM, CGEIT, CRISC, CISSP, CDPSE, CCSK, PMP, ISO27001 LA, ITILv3 certified cybersecurity professional with over 19 years of cybersecurity/privacy and 34 years of industry experience. He has managed many cybersecurity projects covering SOC reporting, Privacy, IoT, SCADA and Industrial Control System (ICS), Governance Risk, and Compliance. He has expertise in implementing frameworks and compliance mandates such as ISO/IEC 27xxx series, IEC 62443/ISA99, NERC-CIP, NIST 800-82, COBIT, etc. He also has hands-on deployment experience with projects covering implementation of the Security Operations Centre (SOC), Security Tools, etc.

Rising Cybersecurity & Third-Party Challenges

Cybercrime to cost the world $10.5 Trillion Annually by 2025.

63% of all Data Breaches are directly linked to third-parties

Data breaches exposed 36 billion records in the first half of 2020.

80% of all Data Breaches have Personal/PII data

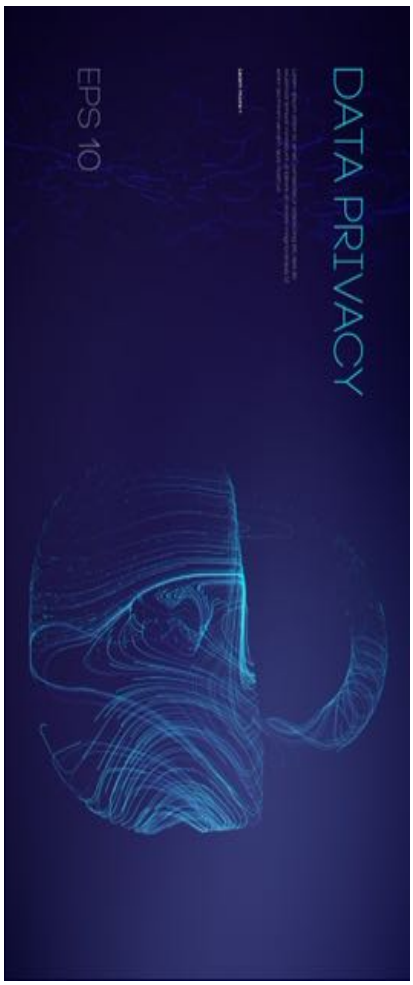
Source cybercrime magazine, gartner report and others

Top Cloud Challenges

1. Misconfiguration and Inadequate Change Control
2. Lack of Cloud Security Architecture and Strategy
3. Insufficient Identity, Credential, Access and Key Management
4. Insider Threat
5. Weak Control Planes
6. Abuse and Nefarious Use of Cloud Services
7. Insecure Interfaces and APIs
8. Account Hijacking

Privacy Compliance Challenges

Majority of organizations until recently have been mainly using the legal team to manage privacy compliance. Since GDPR the situation has evolved, as privacy now is not just managing cookies or opt-ins or opt-outs. Privacy compliance requires a holistic and collaborative approach with team members from Business, IT, Security, Legal, and others. A siloed approach does not work.



Organizations need a Privacy Governance Program with a top-down approach to manage privacy risks and compliance challenges. The IAPP-EY 2019 report indicated that less than 50% of the organizations have an internal or external assurance for privacy. When there are no internal or external privacy audits, organizations may not have knowledge of their privacy maturity and they may only understand the hard way when they have a data breach. The same report also suggested that 90% of organizations use third-parties (vendors) to store or process data. Some of these vendors may also be Cloud Service Providers (CSPs).

The cloud environment is not safe either. One of the top cloud risks is the misconfigured servers that lead to data breaches too. Another major risk is insecure APIs. Organizations use API's to transfer data to the business partners without a secure architecture in place, and without conducting a proper vendor due diligence or evaluating the data flow lifecycle risks.

Why PII Data is Lucrative

- Data is being bought and sold as a commodity on the dark web.
- Scanned Passports sell for about $ 15 each. US passports for $ 1000-2000.
- Social Security numbers with other information fetch about $ 8 each.
- Credit card data value can range from $ 5 to 45 depending on the volume and data with SSN, Date of Birth, CVV.
- Educational Diplomas may be between $ 100-400.
- Medical records can get about $ 2000.
- PII Data combined analytics can be misused for political, financial gains as in the case of Cambridge Analytica.
- According to the U.S. General Accounting Office, 87% of the U.S. population can be uniquely identified using only gender, date of birth and ZIP code.

Privacy Compliance Requirements

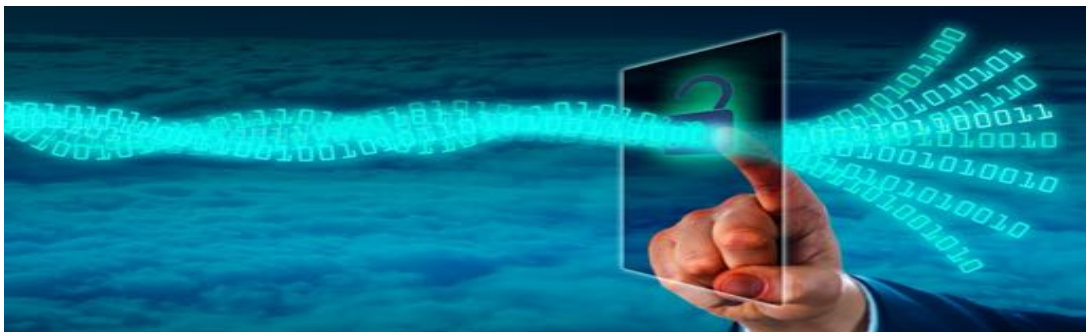
With increasing privacy mandates and stringent compliance requirements, organizations are feeling more challenging times ahead. The sheer amount of privacy fines being levied has created enough scare amongst the Board of Directors of large organizations.

Concepts such as Privacy by Design, Data Minimization, Data De-identification using Anonymization, or Pseudonymization encryption methods are causing several implementation challenges.

As seen in the privacy challenges, organizations now need to establish a Privacy Governance Program with a Senior person taking responsibility for the Program by involving all organization stakeholders. Tools discussed later can be very helpful in Privacy Governance. A periodic internal and external independent audit should be made mandatory by organizations to understand the level of maturity and of compliance towards the applicable privacy mandates.

Non-Compliance Implications

Organizations that fail to properly implement required controls or safeguards to protect PII may experience severe financial penalties, the imposition of corrective action plans, or ongoing oversight by regulators over a multi-year period. Other risks include the adverse publicity of breaches and damage to their brand.



ISO/IEC 27000 Family

ISO/IEC 27000 family is a culmination of Information Security Management Standards. This series is developed by the ISO (International Organization for Standardization) in partnership with IEC (International Electrotechnical Commission).

Increasing Data breaches are a concern for most organizations. Technology is constantly evolving, and it is imperative to adapt/keep up with these new developments and adopt a process of change that enables the use of these new technological developments in a safe & secure manner.

These standards are curated to assist organizations in managing cyber attacks & internal data security threats. Any organization has technological vulnerabilities which aren't immediately obvious. There are different standards, guidelines and industry specific standard guidelines which form the family of ISO/IEC 27000; some of the widely implemented are as below:

ISO/IEC 27001

Information Security Management System (ISMS)

ISO/IEC 27001 has global acceptance and recognition for its benchmark in effective management of information assets. Hence, implementing ISMS paves a way for organizations to ensure that they follow a systematic process for its information systems to provide an assurance to its vendors and third-parties that the systems and data are appropriately protected. The ISMS provides an audit certificate of Confidentiality, Integrity and Availability (CIA) of cybersecurity of the organization that follows an Internationally recognized process to manage their customer's information.

Why get ISMS?

- Reduces the chances of security breaches within your IT environment
- Minimizes / controls IT related risks & provides a systematic detection of vulnerabilities
- Confidentiality of organizational / client information & data
- Fulfills internationally recognized requirements
- Competitive edge due to globally recognized standard and increased trust with partners, customers & the public

ISO/IEC 27701

Privacy Information Management System (PIMS)

The ISO/IEC 27701 is an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management system (PIMS). It provides guidelines for implementing, maintaining and continually improving organizations PIMS. Today almost every organization holds PII. This standard is ideal for organizations wishing to implement a PIMS that supports their ISMS objectives and helps meet their data privacy compliance requirements.

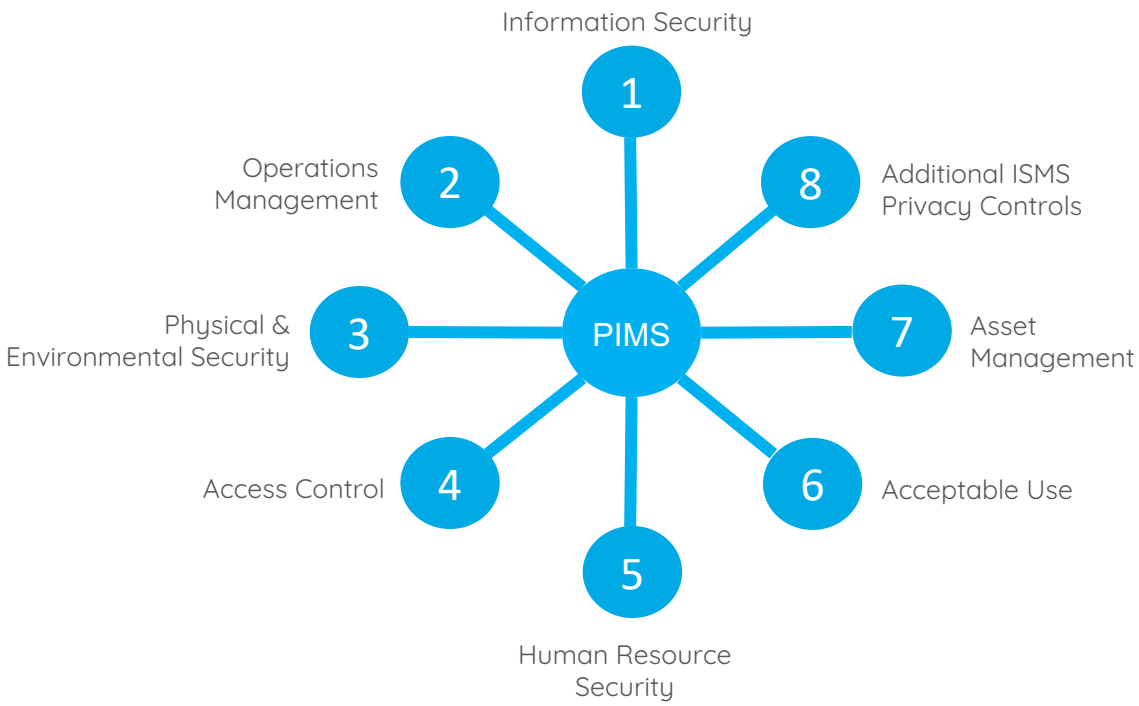
ISO/IEC 27701

Certified by Accedere

In August 2019, the ISO announced a new certification ISO/IEC 27701:2019 also known as the Privacy Information Management System or PIMS. It is an add on certification on top of the ISMS or the ISO/IEC 27001.

Why PIMS

- Assures that the data subjects of customers are managed responsibly
- Integrates with ISO/IEC 27001 Information Security Management System (ISMS)
- Provide clear visibility of data management approaches with partners
- It helps to identify, prioritize, & manage risks throughout the data lifecycle
- Helps achieve compliance with data protection regulations such as GDPR



ISO/IEC 27010

Indicates how information should be treated when it is shared among multiple organizations, what risks may appear, and the controls that should be used to mitigate them, especially when they are related to security management in critical infrastructures. It provides controls & guidance specifically relating to initiating, implementing, maintaining, and improving information security in inter-organizational & inter-sector communications.

ISO/IEC 27011

Establishes the principles for implementing, maintaining and managing an information security management system in telecommunications organizations, indicating how to implement controls efficiently. The adoption of this Recommendation | ISO/IEC 27011:2016 will allow telecommunications organizations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security property.

ISO/IEC 27017

Provides a guide to 37 specific controls for cloud services, these controls are based on the 27002 standard. It is a code of practice for Information Security Controls based on ISO/IEC 27002 for Cloud Services Standard. Its implementation gives the organization guidelines for information security controls applicable to the provision and use of Cloud services. This is also useful for organizations evaluating security position of protentional Cloud service providers.

ISO/IEC 27018

Certified by Accedere

ISO/IEC 27018

Provides a code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors in line with the privacy principles in ISO/IEC 29100 for the public Cloud computing environment.

ISO/IEC 27019

Provides a guide based on standard 27002 to apply to energy-related industries so that they can implement an information security management system.

ISO/IEC 27799

It defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that International Standard.

ISO/IEC 27031

Describes the concepts and principles of information and communication technology (ICT) readiness for business continuity and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity.

ISO/IEC 27031
Certified by Accedere

ISO/IEC 27555

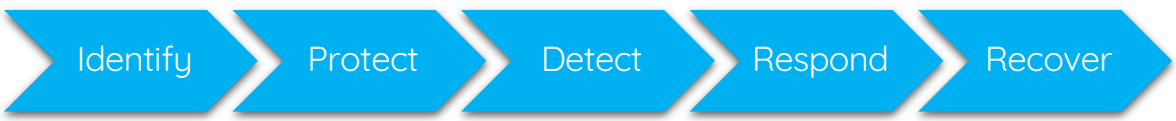
This standard will guide the deletion of Personally Identifiable Information using a systematic approach supporting ISO/IEC 29100 “Privacy framework”. The standard is intended for organizations that store and process PII “and other personal data”. PII Controllers who are primarily accountable for compliance with privacy laws.

ISO/IEC TS 27022

This standard provides a process reference model (PRM) for information security management, which differentiates between ISMS processes and measures/controls initiated by them and describes the ISMS processes implied by ISO/IEC 27001.

ISO/IEC TS 27110

This standard specifies guidelines for developing a cybersecurity framework. Given that there are multiple cybersecurity framework creators, there are a multitude of cybersecurity frameworks. Organizations using cybersecurity frameworks are challenged with harmonizing different lexicons and conceptual structures to meet their requirements. The additional effort could be better spent implementing cybersecurity and combating threats. The goal of this standard is to ensure a minimum set of concepts are used to define cybersecurity frameworks to help ease the burden of cybersecurity creators and cybersecurity framework users.

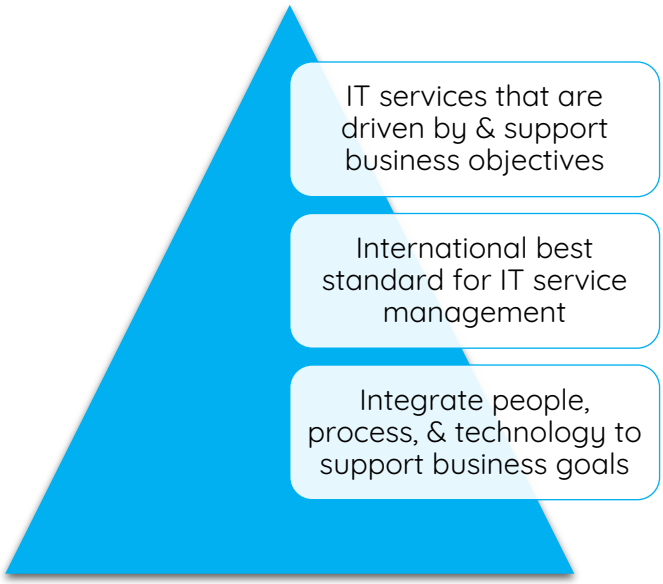


Other Related Standards

ISO/IEC 20000

ISO/IEC 20000 is the international ITSM (IT service management) standard. It enables IT departments to ensure that their ITSM processes are aligned with the business's needs and international best practices. It helps organizations to benchmark how they deliver managed services, measure service levels and assess their performance.

The standard specifies requirements for an organization to establish, implement, maintain & continually improve a service management system (SMS). Requirements specified in this document include the planning, design, transition, delivery and improvement of services to meet the service requirements and deliver value.



ISO/IEC 22301

ISO/IEC 22301 standard helps organizations identify and prioritize threats. Today globally companies suffer due to cyberattacks, data breaches or natural disasters which can interrupt business continuity and quickly damage company's reputation. In such situations, organizations and businesses need to implement, maintain and keep refining their business continuity management system (BCMS).

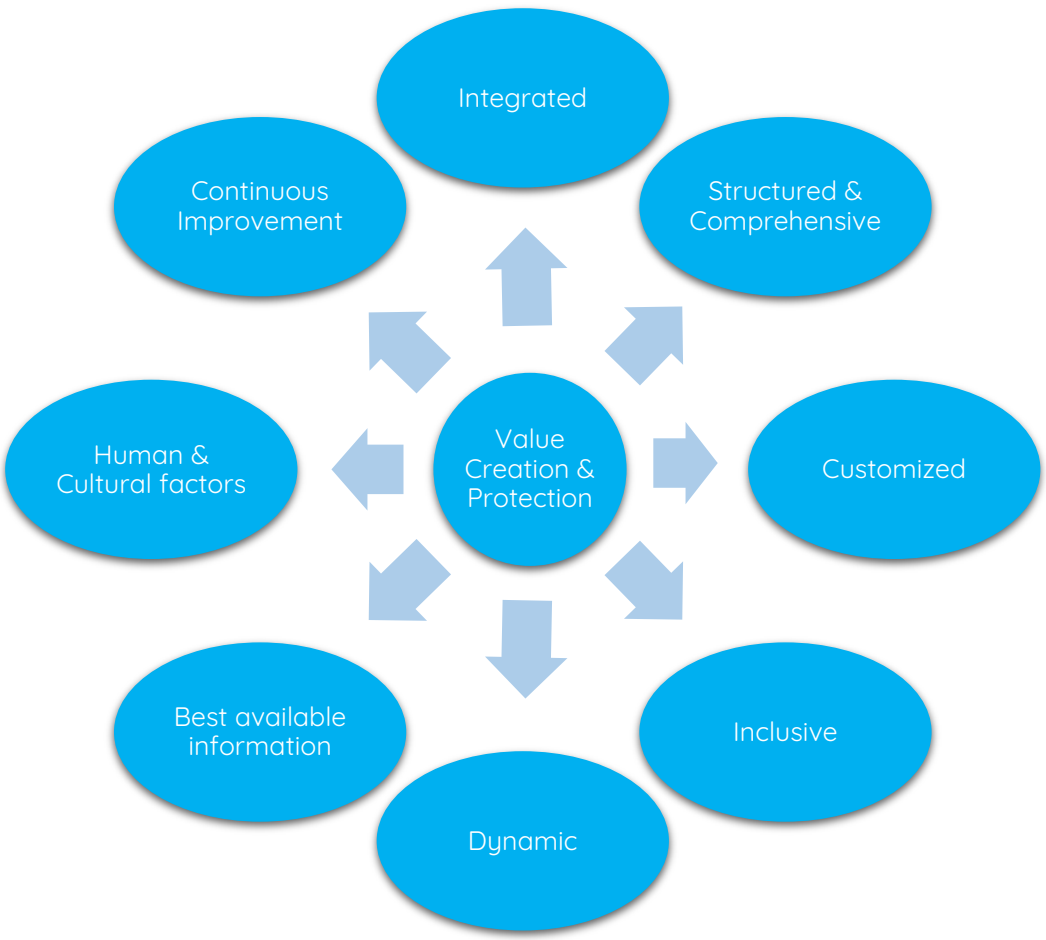
BCMS helps organizations reduce the likelihood & impact of disruption and downtime, protect assets if something does go wrong, continue operating through the disruption, and recover quickly from any incidents.

ISO 31000

The long-term success of an organization relies on many things, from continually assessing and updating their offering to optimizing their processes. As if this weren't enough of a challenge, they also need to account for the unexpected in managing risk.

ISO 31000 - Risk management, provides principles, a framework and a process for managing risk. In addition to addressing operational continuity, ISO 31000 provides a level of reassurance in terms of economic resilience, professional reputation and environmental and safety outcomes. In a world of uncertainty, ISO 31000 is tailor-made for any organization seeking clear guidance on risk management.

Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.



ISO 23195

This standard defines a common terminology to be used in the context of third-party payment (TPP). It establishes two logical structural models in which the assets to be protected are clarified and specifies security objectives based on the analysis of the logical structural models and the interaction of the assets affected by threats, organizational security policies & assumptions. These security objectives are set out in order to counter the threats resulting from the intermediary nature of TPPSPs offering payment services compared with simpler payment models where the payer and the payee directly interact with their respective account servicing payment service provider (ASPSP).

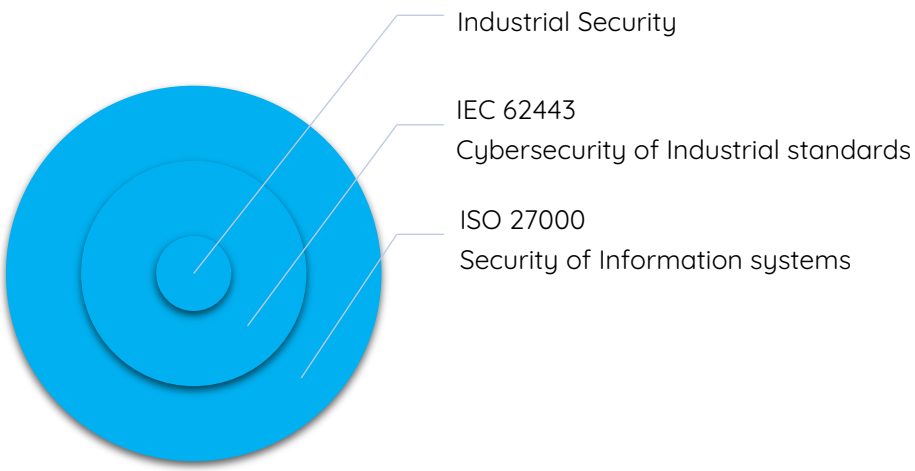
ISO 23195
Certified by Accedere

ISO 8000

ISO 8000 is the international standard for the exchange of quality data and information. It defines quality data as “portable data that meets stated requirements”. The standard is concerned with how data is encoded and formatted so that it is explicit & can be used to reliably deliver quality information. The purpose of ISO 8000 is to make it easier to contract for quality data and to identify companies and software applications that can deliver quality data.

IEC 62443

The Industrial Automation & Control Systems industry faces exciting opportunities, however, along with these opportunities come security threats: industrial environments must be prepared for rising cyberattacks to prevent equipment damage, downtime, and safety issues. Therefore, international industrial security experts have developed authoritative guidance on industrial security: The new IEC 62443 international industrial security standard. IEC-62443 is a series of standards including technical reports to secure Industrial Automation and Control Systems (IACS). It provides a systematic and practical approach to cybersecurity for industrial systems. Every stage and aspect of industrial cybersecurity is covered, from risk assessment through operations.



SOC 2 & ISO/IEC 27xxx Integrated Audit

Our ISO certification services cover Data Security and Privacy Breach that enable our customers to have SOC 2 and ISMS or PIMS audits under one roof, thus saving considerable costs and efforts.

As the SOC 2 broadly covers many of the ISO 27001 certification requirements, it makes sense for organizations to combine the audits managed by us. The AICPA SOC 2 Type 2 engagements require continuous monitoring for evaluating the operative effectiveness of the controls. Parallelly we can also evaluate most of the controls as per ISO/IEC 27000 including ISMS (ISO 27001) controls or PIMS (ISO 27701) controls pertaining to our customers' environment.

Thus, this is a win-win situation for our customers as they can get the ISO certifications along with the SOC 2 Type 2 Compliance reports under one roof and perhaps both conducted together can save your time, effort, and cost.

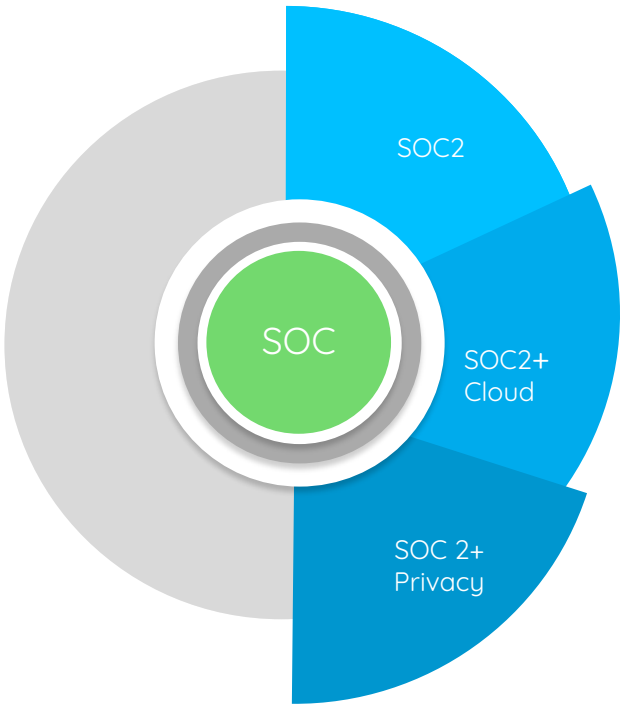
Vendor Assurance with SOC Reports

The SOC compliance report provides an assurance to the internal and external stakeholders of the organization, the specific controls implemented and/or operating effectively for complying with the applicable criteria of the Trust Services Criteria (TSC) 2017 by a Third-Party or Vendor. A single SOC report can provide information about the organization's controls over cybersecurity based on the AICPA's TSC Criteria along with any specific other framework chosen.

This SOC report can provide service organizations the ability to increase transparency and communicate through a single deliverable to their customers, business partners, and stakeholders both in and outside the organization. Organizations should also demand a SOC report from their business associates, CSP's and other third-parties or vendors. to understand and to have an assurance over the specific controls implemented and operating effectiveness of the relevant controls covering cybersecurity including privacy, as applicable to the risks of the organization.

Combined SOC and ISMS Audits

- A SOC 2 Type 2 can cover the entire year and the effectiveness of the controls in place. The ISMS Surveillance Audits can be completed as a part of the ongoing yearly monitoring.
- A SOC 2 examination covers more Points of Focus (Control Objectives in terms of ISMS) and hence is broader and covers all ISMS requirements and more, based on the applicable Trust Services Criteria.
- A SOC 2 report is a Third-Party Period-of-Time assessment and will provide accountability and ISMS shall be covered as part of it automatically.
- Only one set of artifacts are required for both SOC and ISMS.
- Saves considerable time and effort.
- Comprehensive Framework and Seal by AICPA and ISO both together.



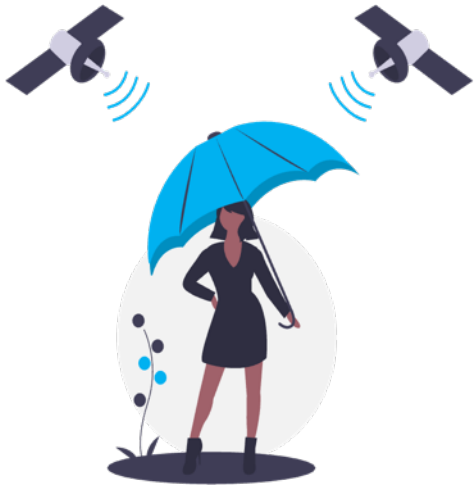
ISO 27001 vs SOC 2 Comparison

Sr. No	Area	ISO 27001/27017	SOC 2 Type 2
1	Standard	International Standard ISO/IEC 27001, Second Edition 2013-10-01, ISMS- Information Security Management Systems Plus Add-Ons	Trust Services Principles and Criteria for Security, Availability, Process Integrity, Confidentiality and Privacy
2	Governance	IAF Accredited Boards e.g. ANAB, UKAS, NABCB	AICPA
3	Purpose	Demonstrate organization's establishment and certification of ISMS that meets specified requirements	Assurance of service organization to its customers that it has met applicable Trust Services Criteria
4	Applicability	Statement of Applicability (SoA) of controls	System Description by Management
5	Period Covered	Point in Time. i.e. as on a date	Period of Time i.e. for the period from xxxx (date) to yyyy (date)
6	Objective	Establish, implement, maintain, and improve the ISMS	Provide Assurance of Risks for a service Organization against specific criteria
7	Period Covered	Re-Certified for every 3 years	Attestation provided every 1 year (or 6 months)
8	Audit Frequency	Surveillance audit conducted Annually	Continuous monitoring during the period
9	Certified/ Attested by	Accredited Certification Body	Attestation by a Licensed CPA Firm
10	Nature of Testing	Design effectiveness	Design effectiveness and operating effectiveness
11	Controls in report	Details of controls not provided	Details of controls provided
12	Focus	Organization's ability to maintain an ISMS. Used for Third-Party or Vendor Compliance	Mitigating Risks of technology and the processes of the specific Third-Party or Vendor Compliance
13	Report	Single page Certification	Report containing the auditor's opinion, management's assertion, description of controls, user control considerations, tests of controls, and results
14	Difficulty to Achieve	Moderate	Higher
15	Structure	ISMS and applicable add on framework	Trust Services Criteria

We Can Help With Your Cybersecurity, Data Breaches and Privacy Requirements

Since we are an IAS accredited certification body, we can provide you with any 27xxx certification as per your requirements. Our ISO/IEC 27001 Certification stand-alone or combined with any other 27xxx standard can give you complete cybersecurity coverage.

We can cover all key requirements to provide an assurance of your ISMS, PIMS and Trust Service Criteria compliance. We can offer combined ISMS, PIMS and SOC examinations to save you time and effort. Our unique delivery method improves timelines and thus reduces costs of your compliance.



Our Value Delivery

1. Experienced team in the area of Cyber Security, Data Breach & Privacy
2. Licensed CPA, Firm registered with PCAOB and Cloud Security Alliance.
3. IAS Certified Certification Body for ISO/IEC 27xxx
4. Prompt services with engagements completed in record time. These engagements are executed by senior professionals.
5. Ongoing support. We are with you whenever you need us.
6. Our services are competitively priced to provide you a higher ROI.