Accedere

# ISMS Certification Services

# Table of Contents

# ISO Certification Services

Our ISO certification services, in the area of Security and Privacy, enable our customers to have SOC 2 and ISMS or PIMS audits under one roof thus saving considerable costs and efforts. The SOC 2 broadly covers the majority of the ISO 27001 certification requirements and as we conduct our SOC 2 Type 2 engagements that require continuous monitoring of the operative effectiveness of the controls, we are also able to evaluate most of the ISMS (ISO 27001) controls and PIMS (ISO 27701) controls for our customers. Thus, this is a win-win situation for our customers that they can get the ISO certifications along with the SOC 2 Compliance reports under one roof.

# ISO/IEC 27001, 27017,27018,27701- ISMS Related

Increasing Data breaches are a concern for most organizations. Technologies are constantly changing and thus we need to keep pace with the environment and adapt a process of change to enable the use of these new technologies in a safe manner. Implementing an Information Security Management System-ISMS standard such as ISO/IEC 27001:2013 is one way to ensure that those organizations follow a 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. ISMS add-ons-The ISO 27017 demonstrates Cloud Service Providers (CSP's) controls overs its cloud services. The ISO 27018 is used for Personal Data (PII) data in the cloud. The ISO27701 is the Privacy Information Management System (PIMS).

# Why ISMS

- Assures your customers about your organization's standards in managing the data.
- The organization follows an established ISO process that could reduce the likelihood of a potential security breach.
- Third-Parties or Vendors accept ISO 27001 (ISMS) Certificate as a vendor due diligence process.


Note: You may also check and download the ISO 27001 checklist, PDF Standard certification, costs for ISO 27001 Compliance, ISO 27001, 27002 Audit Certification Process, ISO 27001 vs SOC, ISO 27001 Cloud Security challenges and Cloud STAR Certification, C5 Cloud certification in our resources section

# Rising Cybersecurity Challenges

Cybercrime is a $6 Trillion Industry

63% incidents relate to negligence

$11.45 Million is total average cost of insider related incident

Less than 50% of organizations have an Internal Audit and Assurance program for Data Privacy

Source Ponemon Institute 2020 report and others

# Top Cloud Challenges

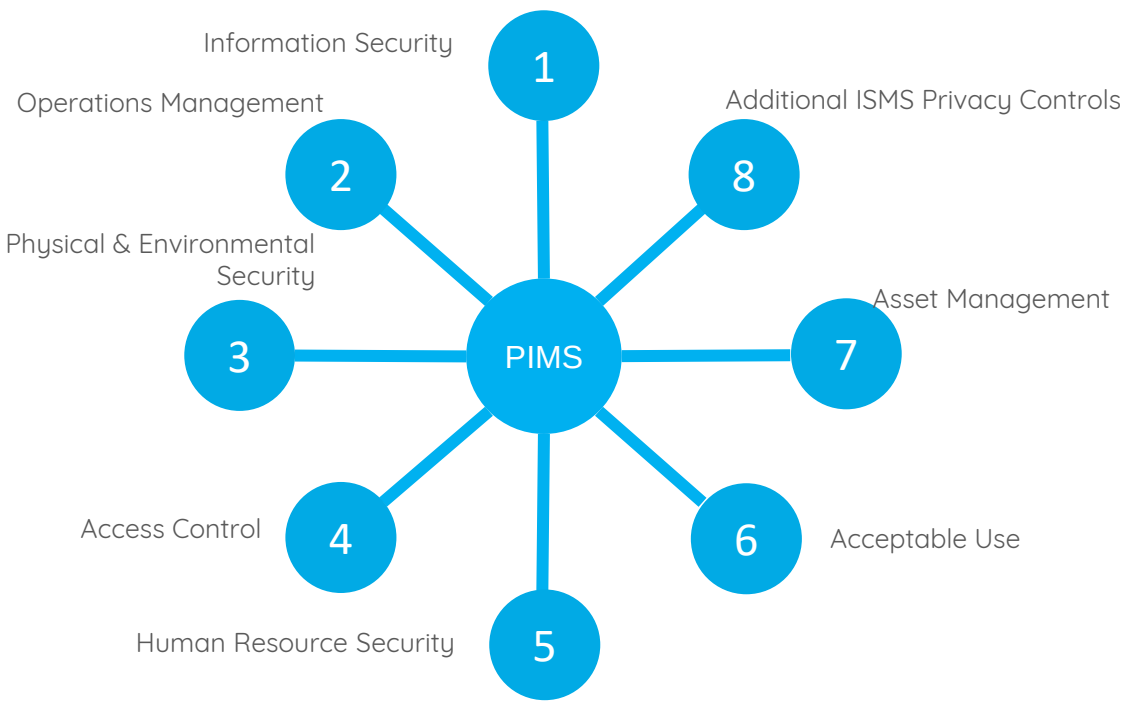
1. Misconfiguration and Inadequate Change Control
2. Lack of Cloud Security Architecture and Strategy
3. Insufficient Identity, Credential, Access And Key Management
4. Insider Threat
5. Weak Control Planes
6. Abuse and Nefarious Use of Cloud Services
7. Insecure Interfaces and APIs
8. Account Hijacking

# ISO 27701- Privacy Information Management System (PIMS)

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 27001 Information Security Management System (ISMS).
- Provide clear visibility of data management approaches with partners.
- It helps to identify, prioritize, and manage risks throughout the data lifecycle.
- Helps achieve compliance with data protection regulations such as GDPR.



# Privacy Compliance Challenges

Majority of organizations until recently have been using the mainly 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

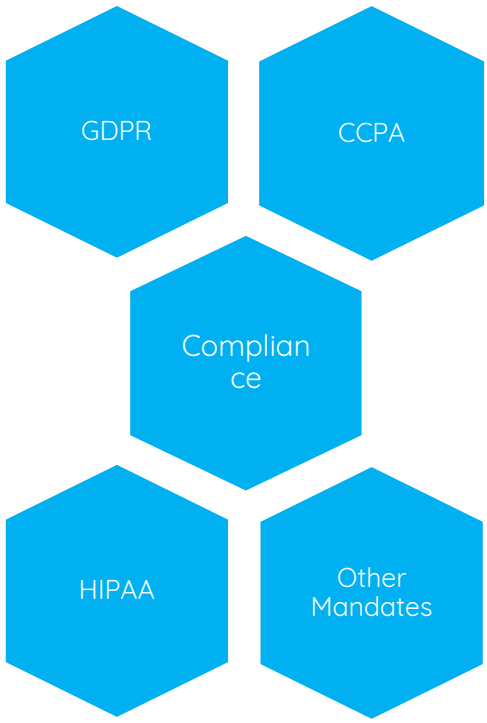
- Data is being bought and sold as a commodity on the dark web.
- Scanned Passports sell for about $ 15 each. US passports for $ 1000-2000.
- Social Security numbers with other information fetch about $ 8 each.
- Credit card data value can range from $ 5 to 45 depending on the volume and data with SSN, 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

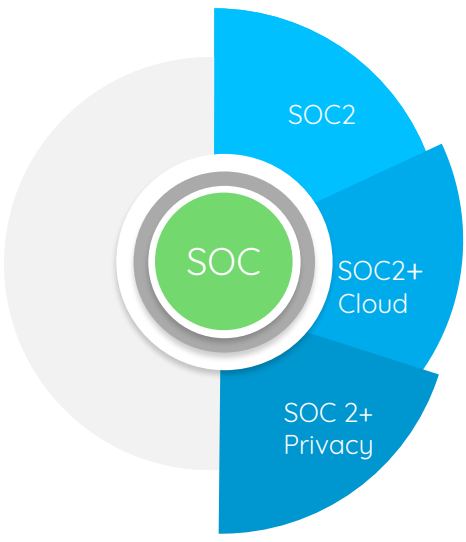
Organizations that fail to properly implement required controls or safeguards to protect PII may experience severe financial penalties, the imposition of corrective action plans, or ongoing oversight by regulators over a multi-year period. Other risks include the adverse publicity of breaches and damage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

# 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.

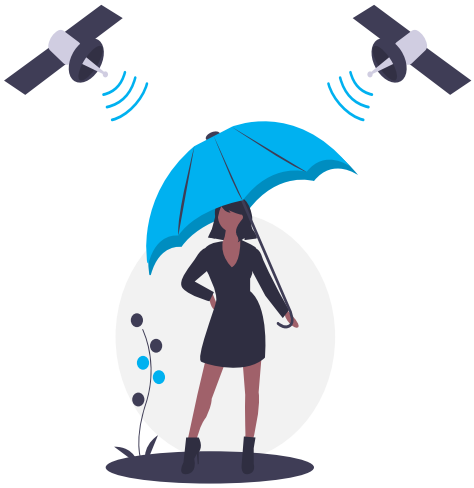


# ISMS vs SOC 2

| 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

We provide end to end ISMS, PIMS and SOC engagements for cybersecurity. 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 ISMS Certification Services can also cover ISO 27001 for Industrial Control Systems (ICS). Our unique delivery method improves timelines and thus reduces costs of your compliance. Our proven methodology saves times as well as costs thus giving you the benefit of timely assurance towards privacy compliance with reasonable costs.



## Our Value Delivery

1. Experienced team in the area of Cyber Security.
2. Licensed CPA, Firm registered with PCAOB and Cloud Security Alliance.
3. Project management methodology applied to each engagement. These engagements are executed by senior professionals.
4. Prompt services with engagements completed in record time.
5. Ongoing support. We are with you whenever you need us.
6. Our services are competitively priced to provide you a higher ROI.