Accedere

Privacy Compliance Services

Table of Contents

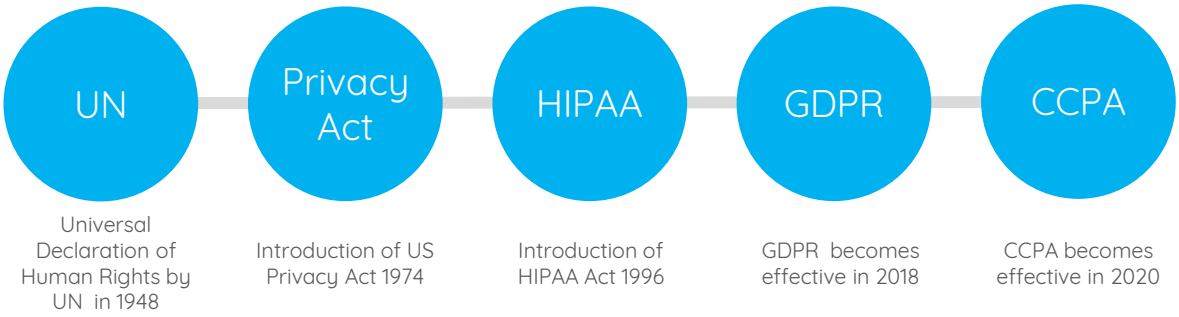
Privacy Compliance

Privacy has grabbed the attention of Boards of Directors (BoD's) across regions as organizations look to comply with new privacy regulations and compliance mandates such as GDPR, CCPA, and others. Privacy is the new buzzword, and the potential impact is very real. Personal data were processed for political and economic reasons without users' consent, as happened in the Cambridge Analytica event. In view of such recent incidents, the failure of the EU Safe Harbor and the Privacy Shield to provide real protection, privacy laws are now changing and have become more stringent. After GDPR, new privacy laws are enacted such as the US California Consumer Privacy Act (CCPA), and the Brazilian General Data Protection Law (LGPD), and many more are planned. HIPAA fines continue to rise too. It may be prudent for organizations to be more proactive and adapt measures for privacy governance to comply with such laws. Tools such as COBIT, ISO 27701, SOC 2 for Privacy can provide assurance to internal and external stakeholders as well as can help in the governance, risk management of the overall privacy program, and ensure compliance of HIPAA, GDPR, CCPA and other privacy mandates.

Some Top Privacy Fines

Organization	Amount in $	Penalizing Agency	Issue
Facebook	5 billion	FTC	Cambridge Analytica
Equifax	700 million	FTC	Data Breach
British Airways	230 million	ICO	Data Breach
Uber	148 million	FTC	Data Breach
Marriott	124 million	ICO	Data Breach
Yahoo	117.5 million	FTC	Data Breach
Google (YouTube)	200 million	FTC	Children's Privacy Violation (COPPA)

The Privacy Journey



The Privacy journey started in 1948 with UN, under Article 12, making a universal declaration of human rights . The US had its Privacy Act in 1974. and the HIPAA Act in 1996. Europe in the meantime had several Privacy mandates and then in 2018 the most famous GDPR took the world by storm. More recently the California State introduced the CCPA that was effective January 2020. Several other countries such as Australia, Canada, Brazil and others have stringent Privacy mandates too. In 2020 FTC levied a hefty 5 billion dollar fine on Facebook for their Cambridge Analytica issue. Privacy Compliance is now a top agenda of many organizations.

GDPR Effect

GDPR is a game changer in respect of privacy. It has addressed the privacy issue in a holistic manner and affects privacy of EU residents across the world. Irrespective of where the data about the EU residents is stored or processed, GDPR is applicable across the world. The penal provisions are stringent, with penalties up to 4% of the global turnover of the organization. Since GDPR became effective on May 25, 2018, several organizations have been penalized/fined for the data breaches.

About GDPR

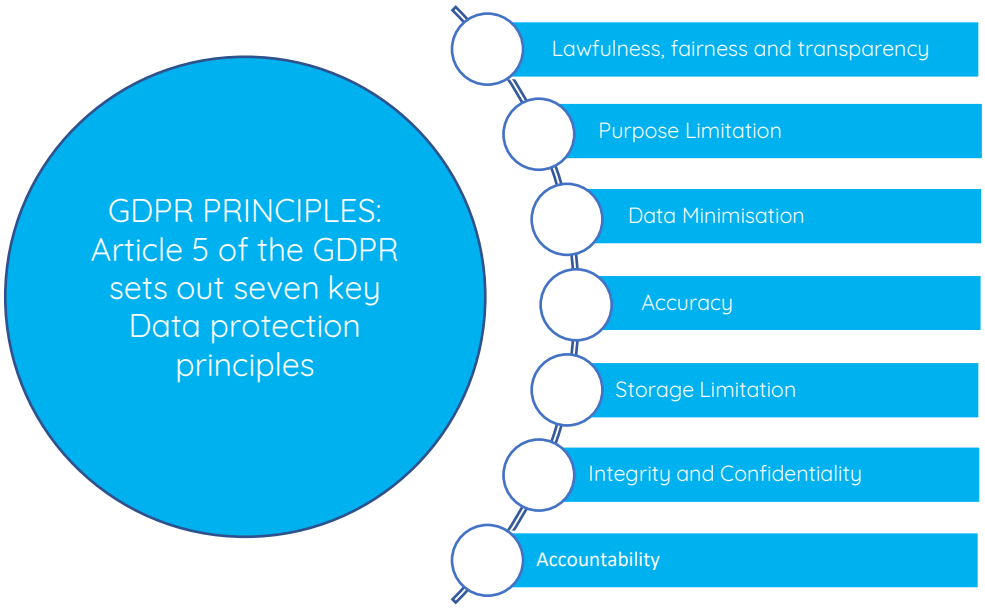
GDPR stands for the European Union General Data Protection Regulation. GDPR replaced the older EU Data Protection Directive and has been in effect since May 2018. GDPR applies to all EU organizations, whether commercial business or public authority, that collect, store or process the personal data of EU individuals.

It is also applicable to organizations established outside the EU that offers goods/services (paid or for free) or is monitoring the behavior of EU individuals.

The Regulation also requires many organizations, their controllers and processors, to appoint an EU representative based in one of the member states in which the relevant individuals are based. This is unless the processing is occasional and does not include large scale processing of special categories of data or processing of data relating to criminal convictions and offences.

The Brexit effect

GDPR is enforced in UK by the Information Commissioner's Office (ICO). So, UK organizations handling personal data still need to comply with the GDPR, regardless of Brexit.



Data Subject Rights under GDPR

The right to be informed

The right to rectification

The right to restrict processing

The right to object

The right to access

The right to erasure

The right to data portability

Rights in relation to automated decision making and Profiling

CCPA

On June 28, 2018, Governor Brown signed Assembly Bill 375, now known as the California Consumer Privacy Act of 2018 (CCPA), which grants consumers new rights with respect to the collection of their personal information. This regulation aims to establish procedures to facilitate consumers' rights under the CCPA and provide guidance to businesses for how to comply. The CCPA is effective from January 1, 2020.

Business compliance eligibility under CCPA

The CCPA controls the manner in which "businesses" treat the "personal information" of California residents. The CCPA defines "business" to mean any for-profit legal entity doing business in California that:

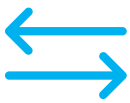
1. Has annual gross revenues in excess of $25 million.
2. Alone, or in combination, buys, receives, sells or shares the personal information of 50,000 or more California residents, households or devices.
3. Derives 50% or more of its annual revenues from selling California residents' personal information.

Data Subject Rights under CCPA

1. Right to Know About Personal Information Collected, Disclosed, or Sold (Notice)

2. Right to Request Deletion of Personal Information

3. Right to Opt-Out of the Sale of Personal Information.



4. Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights (Equality)

5. Right to access what information is collected by business.

HIPAA and Healthcare Privacy

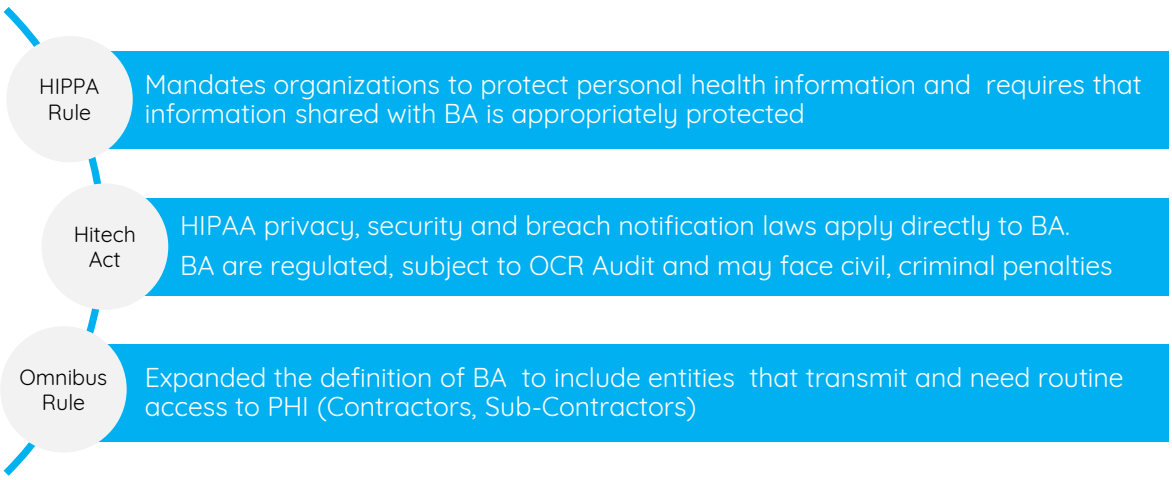
HITECH Act

The HITECH Act requires entities covered by the HIPAA to report data breaches, which affect 500 or more persons, to the United States Department of Health and Human Services (U.S.HHS), to the news media, and to the people affected by the data breaches. This subtitle extends the complete Privacy and Security Provisions of HIPAA to the business associates of covered entities. This includes the extension of updated civil and criminal penalties to the pertinent business associates. These changes are also required to be included in any business-associate agreements among the covered entities.

Omnibus Rule

covering Breach Notification and Enforcement Rules

In January 2013, HIPAA was updated via the Final Omnibus Rule. The updates included changes to the Security Rule, Breach Notification Rule and Enforcement Rule as required under the HITECH Act. The most significant changes were related to business associates directly responsible for compliance and prohibiting the sale of protected health information without individual authorization.



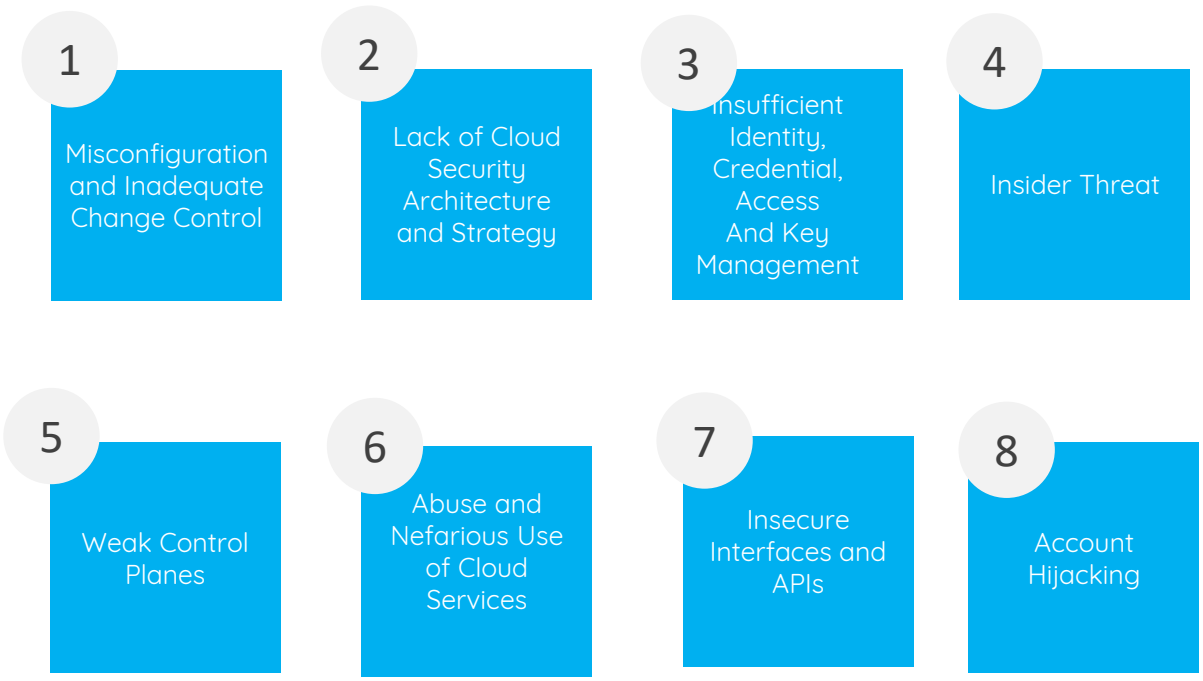
Privacy Compliance Challenges

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.

Top Cloud Challenges



Rising Privacy and Vendor Risks

90% organizations use third-parties to process data. And 70% transfer data outside of EU

Total number of breaches reported increased to 38% up from 16% in 2018

After 1 year of GDPR only 9% said they were fully compliant

Less than 50% of organizations had an Internal Audit and Assurance program

Source IAPP-EY 2019 Report

Why PII Data is Lucrative

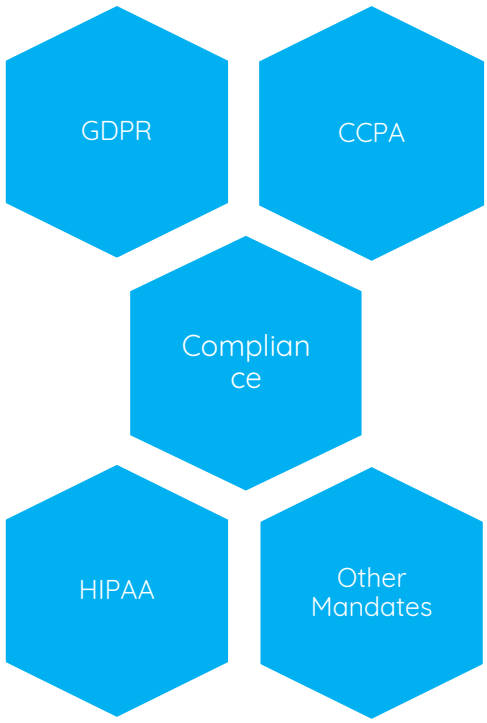
- Data is being bought and sold as a commodity on the dark web.
- Scanned Passports sell for about $ 15 each. US passports for $ 1000-2000.
- Social Security numbers with other information fetch about $ 8 each.
- Credit card data value can range from $ 5 to 45 depending on the volume and data with SSN,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

Privacy Risk Assessment

Privacy Assessments are important in order to understand the organization's privacy risks arising from new projects, initiatives, systems, processes, strategies, policies, business relationships etc.

The main goal of a privacy assessment include:

- The information collected should comply with all privacy-related legal and regulatory compliance requirements.
- Identifying the privacy risks, defining the same and monitoring incidents.
- Taking actions to mitigate the risks.

A Data Privacy Impact Assessment (DPIA) is a type of impact assessment which is typically designed to accomplish three main goals:

- Identify and evaluate the risks of data privacy and its impact on data breaches or other incidents and effects, should that happen.
- Identify appropriate privacy controls to mitigate unacceptable risks.
- To understand what aspects to monitor to ensure conformance with applicable legal, regulatory and policy requirements for privacy for e.g. GDPR, CCPA, HIPAA etc..

Data Flows and Data Life Cycle

To conduct an effective Privacy Impact Assessment, it is important to understand and take stock of the entire data life cycle management of the several data that the organization, collects, processes and stores. Many organizations do not define the end life cycle of the data and keep them endlessly thus increasing the risks of a data breach in case it is not encrypted. Managing encryption keys too can be a challenge. Hence it is important for organizations to have stock of the entire organization data to define the end life as well as data deletion, procedures at the end of the data life cycle. To understand the data life cycle, it is also important to understand the data flows for every specific data set.

Privacy Compliance Tools-COBIT

COBIT 2019 by ISACA s is the new updated version of the IT Governance framework.. COBIT offers a tailored flexible and open framework to define a privacy governance program that can be addressed by a collection of governance and management objectives and their components.

Based on the design factors and target process capability levels, an organization can adapt the framework and determine objectives, practices and activities. The excel toolkit helps in doing this. COBIT 2019 supports a CMMI-based process capability scheme.

COBIT 2019 now has 40 Governance and Management Objectives up from 37. the new ones include, Managed Data, Managed Projects and Managed Assurance. Organizations can adapt the COBIT framework for Privacy Assurance too for mandates such as HIPAA, GDPR, CCPA and others.

- EDM01—Ensured Governance Framework Setting and Maintenance
- EDM03—Ensured Risk Optimization
- APO12—Managed Risk
- APO14—Managed Data
- MEA04—Managed Assurance

Privacy Compliance Tools-NIST

In January 2020 NIST released its new Privacy Framework that can be used for Data Privacy Impact Assessments. The framework covers 3 aspects :

Core: Increasing granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk.

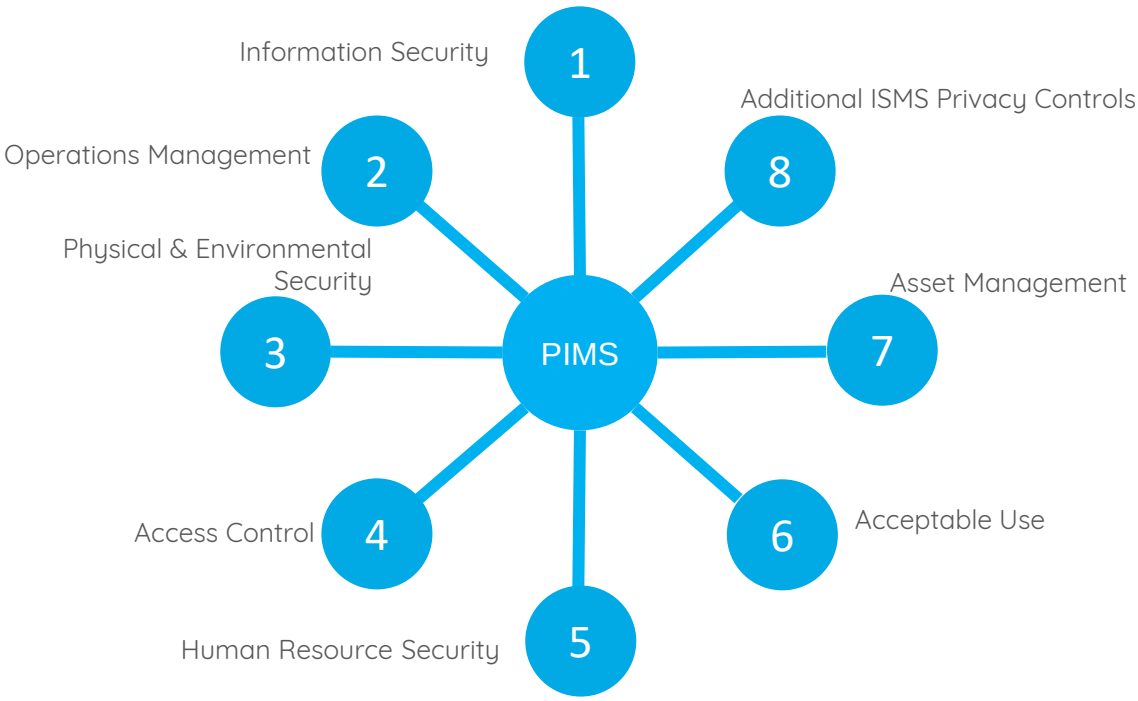
Profiles: Selection of specific Functions, Categories, and Sub-categories from the Core that an organization has prioritized to help it manage privacy risk.

Implementation Tiers: Communication about organization having sufficient processes & resources in place to manage privacy risk.

Privacy Compliance Tools-ISO 27701

In August 2019, the ISO announced a new certification ISO/IEC 27701 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. Some of the advantages of the PIMS are:

- Assures that the data subjects of customers are managed responsibly.
- .Integrate ISO 27001 Information Security Management System (ISMS).
- Provide clear visibility of data management approaches with partners.
- Helps to identify, prioritize and manage risks throughout the data lifecycle.
- Helps achieve compliance with data protection regulations.
- Indicates assurance that PII can be managed without infringing data subjects' privacy.



Privacy Compliance Tools-CSA's CCM

Cloud Security Alliance in its Cloud control Matrix (CCM) tool along with other cloud controls, also pprovides to evaluate the level of personal data protection offered by a CSP to cloud customers. The CCM is a guidance to achieve compliance with GDPR and to disclose the PII controls implemented by the CSP.

Assurance for Privacy Compliance

The SOC 2 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 privacy regulatory requirements. A single SOC 2 report can provide information about the organization's controls over PII data based on the AICPA's Privacy Trust Services Criteria and any specific privacy requirements. This SOC 2 can provide service organizations the ability to increase transparency and communicate through a single deliverable to customers, business partners, and stakeholders both in and outside the organization. Organizations should also demand a SOC 2 report from their business associates, CSP's and other third-parties or vendors. to understand and to have an assurance over the controls implemented and operating effectiveness of the relevant controls covering Privacy.

SOC 2 for Privacy

SOC 2 uses the AICPA Trust Services Criteria (TSC) for Privacy .With approximately 50 points of focus, the TSC organizes the privacy criteria as:

- Notice and communication of objectives—The entity provides notice to data subjects about its objectives related to privacy.
- Choice and consent—The entity communicates choices available regarding the collection, use, retention, disclosure and disposal of personal information to data subjects.
- Collection—The entity collects personal information to meet its objectives related to privacy.
- Use, retention and disposal—The entity limits the use, retention and disposal of personal information to meet its objectives related to privacy.

- Access—The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.

- Disclosure and notification—The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators and others to meet its objectives related to privacy.

- Quality—The entity collects and maintains accurate, up-to-date, complete and relevant personal information to meet its objectives related to privacy.

- Monitoring and enforcement—The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints and disputes.

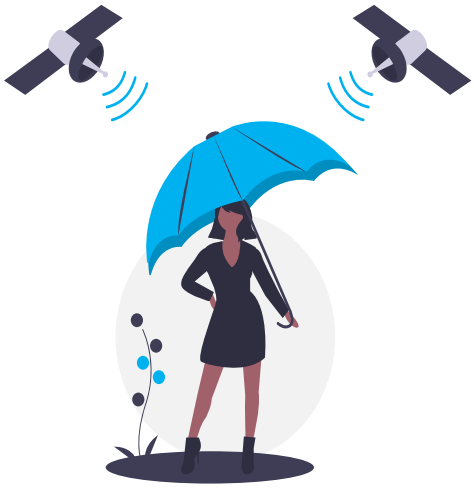
Aside from the Trust Services Criteria Privacy Controls, any specific privacy mandates can also be covered.

SOC 2 for Privacy Benefits

- SOC 2 Type 2 can cover the entire year and the effectiveness of the controls in place.
- It is a Third-Party Period- of-Time assessment and so has Accountability.
- Most other assurance programs or audits are only, at a point in time.
- Since it is a period assessment, it is more like a continuous compliance with low risk and high reliability.
- Comprehensive Framework for Privacy by AICPA.
- Provides a high reliability SOC 2 Seal by AICPA.

We Can Help With Your Privacy Compliance

We provide end to end SOC 2 examination report for privacy compliance. We can cover all key requirements to provide an assurance of your compliance with privacy mandates such as HIPAA, GDPR, CCPA and more such requirements. In a SOC 2 compliance engagement for privacy, we can additionally cover any specific privacy mandate to address your needs including ISO 27701 Certification. 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.