# Privacy Information Management System ISO/IEC 27701

*An international standard to support privacy accountability and regulatory compliance among controllers and processors within the global data processing supply chain*

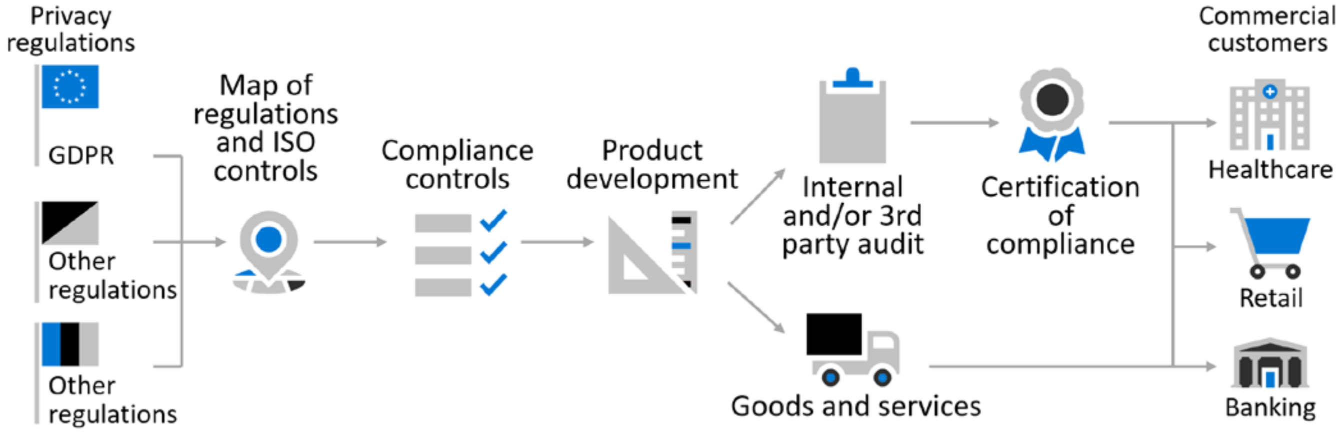
The European Union's General Data Protection Regulation (GDPR), has ushered in a new era of privacy regulatory and compliance globally. More and more privacy regulations, many modeled after the GDPR, have been enacted in different jurisdictions (be that market/industry, or physical location). As a result, organizations must implement policies and procedures to assure compliance with the growing list of privacy regulations. In addition, we are collectively in the midst of rapid digital transformation where data collection and processing are increasing dramatically. The simultaneous growth in data volume and regulatory requirements pertaining to that data makes compliance increasingly complex for organizations of all types.

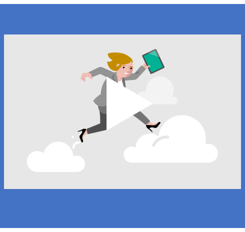
The new international standard Privacy Information Management System (PIMS) ISO/IEC 27701 (formerly known as ISO/IEC 27552 during drafting period), was designed to help organizations reconcile privacy regulatory requirements. The standard outlines a comprehensive set of operational controls that can be mapped to various regulations, including the GDPR. Once mapped, the PIMS operational controls can be implemented by privacy professionals and audited by internal or third-party auditors resulting in a certification and comprehensive evidence of conformity.

## Compliance challenges

ISO/IEC 27701 addresses three key compliance challenges

| **Too many regulatory requirements to juggle** | **Too costly to audit regulation-by-regulation** | **Promises of compliance without proof is potentially risky** |
|---|---|---|
| Reconciling multiple regulatory requirements through the use a universal set of operational controls enables consistent and efficient implementation. | Auditors, both internal and third party, can assess regulatory compliance using a universal operational control set within a single audit cycle. | Commercial agreements involving movement of personal information may warrant certification of compliance. |





Watch the PIMS introductory video

## Too many regulatory requirements to juggle

ISO/IEC 27701 includes an annex containing the operational controls of the standard that are mapped against relevant requirements in GDPR for controllers and processors. This mapping is just an example of how privacy regulations can be operationalized with the ISO framework. As additional mappings with other regulations become available and are validated[1], the operational controls from the standard can be transferred directly from regulatory review to implementation. This universal framework allows organizations to reliably operationalize the relevant regulatory requirements without "reinventing the wheel".

## Too costly to audit regulation-by-regulation

Let's go back to our opening statement on the current landscape. As more and more privacy regulations come into force in various jurisdictions, the pressure to provide evidence of compliance will also increase. But the costs of disparate regulatory certifications will become prohibitive if every regulation calls for its own unique audit. By outlining a set of universal operational controls, PIMS also outlines a universal compliance framework to audit against, and potentially certify, for multiple regulatory requirements.

It is important to recognize that an official GDPR certification requires pending approval decisions to be made by the European regulators. *While the alignment between PIMS and GDPR is evident, a PIMS certification should be taken as evidence of GDPR compliance, not as an official GDPR certification until regulatory decisions are finalized.*

Expecting vendors to certify against PIMS will be effective for establishing responsible privacy practices by suppliers and partners no matter the size of your organization.

## Promises of compliance without proof is potentially risky

Modern organizations engage in complex data transfers with a deep network of business partners including partner organizations or co-controllers, processors such as cloud providers, and sub-processors such as vendors who support those same processors. Failure to comply with regulations in any part of this network may lead to cascading compliance issues across the supply chain. This is where a verification of compliance can be valuable beyond the assurance provided by contractual terms between these organizations. Since the global economy dictates that most of these organizations are spread out around the world, it is practical to use an international standard from ISO to manage compliance across the network.

This reliance on compliance increases the importance of certification to the standard. While not all companies and organizations need to earn such certification, most will benefit from partners and vendors who do, especially when sensitive or high volumes of data processing is involved.

[1] A pending open-source project is underway to enable the privacy community to map additional regulations and validate existing mappings. Please stay tune for announcement.

## Building blocks of the standard

PIMS is built on top of one of the most widely adopted international standards for information security management, ISO/IEC 27001. If your organization is already familiar with ISO/IEC 27001, it will be logical and more efficient to integrate the new privacy controls of PIMS. This means the implementation and audit of both will be less expensive and easier to achieve.

**Key points on ISO/IEC 27001 and PIMS:**

- ISO/IEC 27001 is one of the most used ISO standards in the world, with many companies already certified to it.
- PIMS includes new controller- and processor-specific controls that help bridge the gap between privacy and security and provides a point of integration between what may be two separate functions in organizations.
- Privacy depends on security. Likewise, PIMS depends on ISO/IEC 27001 for security management. Certification for PIMS must be obtained as an extension of an ISO/IEC 27001 certification and cannot be obtained independently.

## What should your organization do with PIMS?

No matter the size of your organization and whether it is a controller or a processor, your organization should consider pursuing certification, either for your own organization, or requesting it from vendors or suppliers based on your business requirements. This applies especially for processors, sub-processors, and co-controllers that are processing sensitive or high volumes of personal data. In any case, your organization should assess its business needs to determine if certification for its own products and services are suitable.

**Visit the Microsoft Trust Center for more information on PIMS, ISO 27001, GDPR, and other privacy regulations.**

## Feature Resources

ISO/IEC 27701 (PIMS) for purchase

BSI whitepaper and content about PIMS

PIMS Introductory video