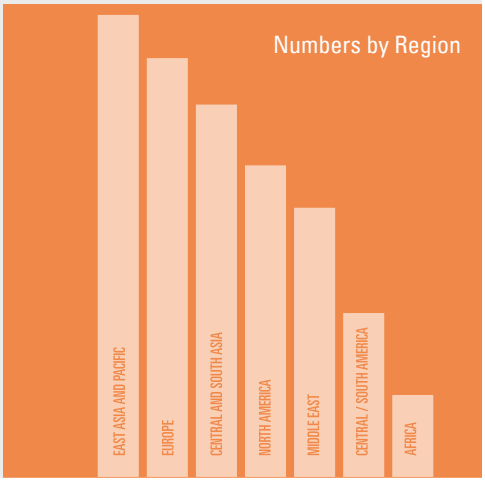
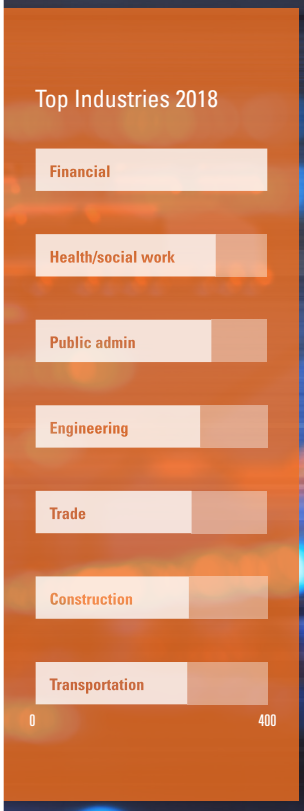
BE THE BENCHMARK

ADDRESSING PRIVACY MANAGEMENT WITH ISO/IEC 27701:2019

UNDERSTANDING REQUIREMENTS AND COMPLIANCE STRATEGIES





CONTENTS

OVERVIEW

A rapid increase in concerns over privacy relating to social media apps and IoT devices and the global proliferation of privacy laws and regulations mean organizations are now facing pressure from customers, end-users, investors, and regulators about how they manage the personal identifiable information (PII), or personal data, they collect when conducting their business. The enactment of many wide-influence privacy laws, such as the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the China Cybersecurity Law, has imposed significant pressure on organizations to look at the issue of privacy.

The concept of privacy is often misunderstood and/or incorrectly acted upon. Many organizations believe it is enough to not pass data on to third parties and ensure their databases are password protected. Concepts such as 'consent', 'purpose of collection', or 'cross-border transfer' are either ignored or not understood. The fierce penalties of GDPR and CCPA fines mean many organizations are now waking up to the risks and are finally beginning to pay proper attention to their privacy protection.

This white paper introduces the ISO/IEC 27701:2019 standard, discusses its structure and how it can be used to implement a Personal Information Management System (PIMS), and certification against the standard.

The intended audience of this white paper is:

- Organizations looking for general information about a PIMS; and
- Organizations planning to implement or to get certified for a PIMS against ISO/IEC 27701:2019

THE ISO/IEC 27701:2019 STANDARD

ISO/IEC 27701:2019 – Security Techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- requirements and guidelines – specifies the requirements and gives guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

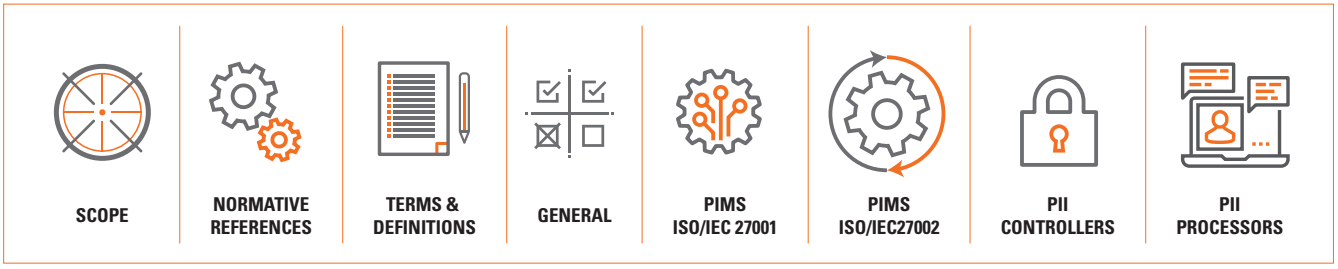
It is designed to work with ISO/IEC 27001 and is a combination of certifiable requirements and implementation guidelines. It is also an extension to ISO/IEC 27001, adding PIMS-related requirements such as clause 5, Annex A and Annex B. These requirements are *shall* statements – 67 in total in the standard. Additionally, the standard also adds guidance for PIMS in ISO/IEC 27002 – e.g. clauses 6, 7 and 8.

The structure of the standard is summarized in Table 1.

TABLE 1. STRUCTURE OF THE ISO/IEC 27701:2019 STANDARD AND ITS CONNECTION WITH ISO/IEC 27001 AND ISO/IEC 27002

CLAUSE	CLAUSE TITLE	REMARK
1	Scope	Applicability of the Standard
2	Normative references	Standard references
3	Terms, definitions and abbreviations	
4	General	Description of the structure of the Standard
5	PIMS-specific requirements related to ISO/IEC 27001	PIMS-specific requirements for requirements in ISO/IEC 27001
6	PIMS-specific guidance related to ISO/IEC 27002	PIMS-specific guidance for controls in ISO/IEC 27002
7	Additional ISO/IEC 27002 guidance for PII controllers	Additional ISO/IEC 27002 guidance for PII controllers
8	Additional ISO/IEC 27002 guidance for PII processors	Additional ISO/IEC 27002 guidance for PII processors
Annex A	Annex A (normative) PIMS-specific reference control objectives and controls (PII Controllers)	Applicable and mandatory controls for data controllers
Annex B	PIMS-specific reference control objectives and controls (PII Processors)	Applicable and mandatory controls for data processors
Annex C	Mapping to ISO/IEC 29100	Non certifiable, informative annexes
Annex D	Mapping to the General Data Protection Regulation	
Annex E	Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151	
Annex F	How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002	

SO 27701 REQUIREMENTS



Each clause outlines necessary requirements and steps that must be met before certification is granted.

CLAUSE 5

Clause 5 covers additional requirements to clauses 4 to 10 of ISO/IEC 27001:2013 and they are all certifiable. For example, clause 5.7.2 states:

> "The requirements stated in ISO/IEC 27001:2013, 9.2, along with the interpretation specified in 5.1 apply"

This standard does not add any new requirements for internal audits, as long as the organization understands that 'information security' in ISO/IEC 27001:2013 should be interpreted as extending to include the risks resulting from processing Personal Identifiable Information (PII).

ISO/IEC 27701:2019 has additional requirements for the following ISO/IEC 27001 clauses:

4.1	Understanding the organization and its context
4.2	Understanding the needs and expectations of interested parties
4.3	Determining the scope of the information security management system
6.1.2	Information security risk assessment
6.1.3	Information security risk treatment

CLAUSE 6

Clause 6 covers additional PIMS-related guidance for ISO/IEC 27002. For example, clause 6.9.4.4 (corresponding to 12.4.4 Clock Synchronization of ISO/IEC 27002:2013) does not contain any additional requirements because clock synchronization has little relevance to privacy risks. On the other hand, clause 6.9.3.1 (corresponding to 12.3.1 Information backup of ISO/IEC 27002:2013) has lengthy guidance because there can be privacy risks relating to information backup, such as data retention periods, cross-border data transfer, etc.

The following table summarizes the number of controls in each domain of ISO/IEC 27002. There is a total of 32 new controls amending ISO/IEC 27002. As with ISO/IEC 27002, guidance in clause 6 is non-certifiable.

CLAUSE IN ISO/IEC 27002	# OF CONTROLS AMENDED	CLAUSE IN ISO/IEC 27002	# OF CONTROLS AMENDED
5	1	12	3
6	2	13	2
7	1	14	5
8	5	15	1
9	3	16	2
10	1	17	0
11	2	18	4

CLAUSE 7

This clause provides guidance for PII controllers, with the controls being listed in Annex A of the standard. These controls are normative, meaning they are to be implemented if the organization is certified to be a controller (see PII Controller vs PII Processor under Certification below). The guidance provided in Clause 7 assists an organization in implementing these controls. This guidance is non-certifiable.

CLAUSES		# OF CONTROLS
A.7.2	Conditions for collection and processing	8 controls
A.7.3	Obligations to PII principals	10 controls
A.7.4	Privacy by design and by privacy default	9 controls
A.7.5	PII sharing, transfer and disclosure	4 controls

CLAUSE 8

Clause 8 provides guidance for PII processors. The controls for PII processors are listed in Annex B of the standard. Similar to Annex A, these controls are normative if the organization is certified to be a processor. The guidance in clause 8 is non-certifiable.

CLAUSES		# OF CONTROLS
B.8.2	Conditions for collection and processing	6 controls
B.8.3	Obligations to PII principals	1 control
B.8.4	Privacy by design and by privacy default	3 controls
B.8.5	PII sharing, transfer and disclosure	8 controls

PRIVACY INFORMATION MANAGEMENT SYSTEM VS INFORMATION SECURITY MANAGEMENT SYSTEM

While ISO/IEC 27001 – Information Security Management (ISMS) – provides useful insights into managing information security it does not have sufficient controls on data privacy. This means an organization can pass an ISMS audit without fully addressing applicable privacy regulatory obligations.

PIMS differs from a typical ISMS in several ways (see Table 2).

TABLE 2. DIFFERENCES BETWEEN A TYPICAL ISMS AND PIMS

	ISMS	PIMS
Organizational scope	Organizations may implement their ISMS to cover only their IT operations. The scope therefore only covers departments that directly impact IT operations, e.g. IT, facilities, security, human resources, etc.	Many departments not directly related to IT operations may collect and process PIIs (or personal data), especially from customers and end users, e.g. marketing, customer services, sales, etc.
Information/data covered in the scope	The ISMS typically protects the organization's own data, e.g. business plans, intellectual property, proprietary engineering data. It could just be established to ensure the integrity and availability of an organization's information systems, e.g. data center.	A PIMS covers all PIIs collected and processed by an organization, including employees, visitors, customers, and end users. It therefore covers data which might not be covered under the ISMS.
Protection focus	Focuses on confidentiality, integrity, and availability (CIA) of the information/data being protected. Even if PIIs are included in an ISMS, the focus is usually on their CIA, e.g. whether they are properly protected, stored, transferred, and retrieved.	Goes beyond CIA for PIIs. Many global privacy regulations include privacy principles, e.g. whether PIIs are collected lawfully, or used solely for their original purposes. They may also include data subject 'rights', e.g. the right to be informed, the right to rectify a PII, the right to object to direct marketing, etc. The PIMS contains provisions to handle these requirements which are often absent in an ISMS.

CERTIFICATION AND ACCREDITATION

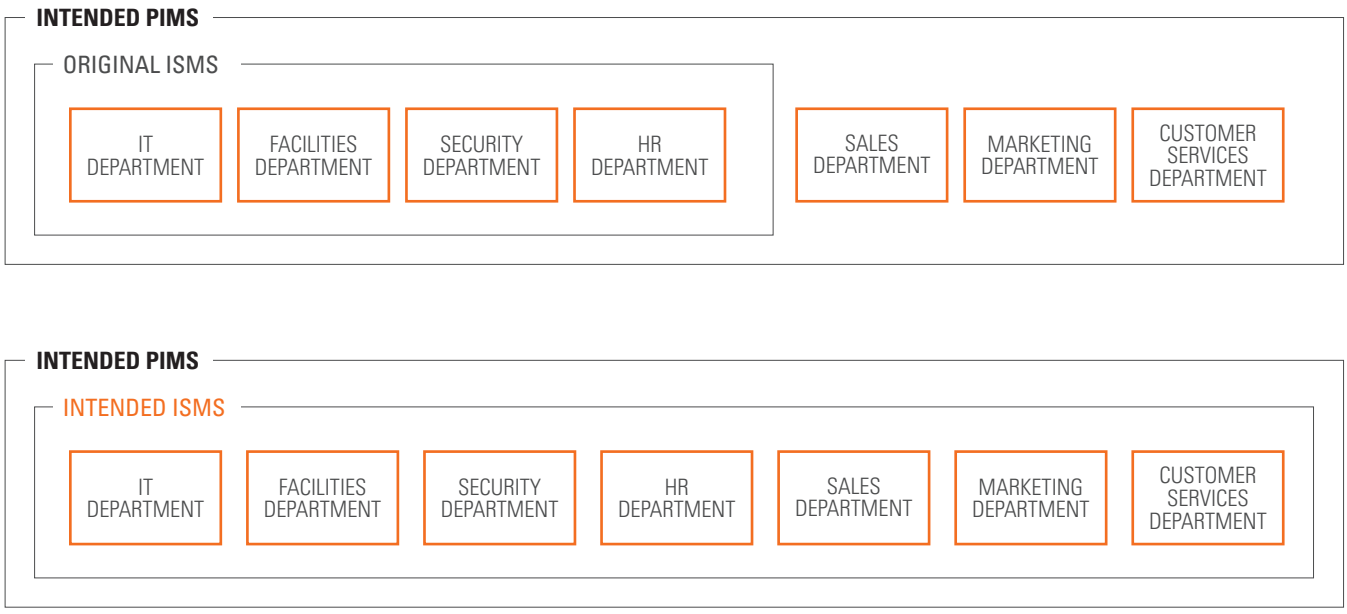
CERTIFICATION

SGS offers certification against ISO/IEC 27701:2019 for organizations which are already certified to ISO/IEC 27001:2013 or will be certified concurrently with ISO/IEC 27001:2013.

Organizations that are certified to ISO/IEC 27001:2013 need to review the scope of their ISMS and ensure it is either the same or larger than the planned scope of the PIMS. This review is important as the scope of many ISMS covers only the IT and/or associated departments while the PIMS covers all departments that collect and process PIIs (see Privacy Information Management System vs Information Security Management System for explanation).

If the scope of the ISMS is smaller than that of the PIMS, it will need to be extended to match the PIMS's scope (see Figure 1).

FIGURE 1. EXAMPLE OF A POSSIBLE EXTENSION OF THE ISMS TO SERVE AS THE FOUNDATION OF THE PIMS



PII CONTROLLER VS PII PROCESSOR

As described in earlier sections, the standard contains controls for both PII controllers and PII processors. In theory, any organization can act as controller and processor at the same time (see Table 3 for two examples).

When complying with regulations such as GDPR, an organization will need to fulfill the obligations of both roles. Under ISO/IEC 27701 certification, an organization can choose to be certified as controller, processor, or both. By selecting a particular role, however, the organization is not relieved of its full legal obligation. Therefore, the decision to certify as controller, processor, or both, should be based on the organization's business needs and management decision. The role to be certified will be stated on the certificate.

TABLE 3. EXAMPLES OF AN ORGANIZATION IS BOTH A PII CONTROLLER AND A PII PROCESSOR

SCENARIO	EXAMPLE	ORGANIZATION MAY ALSO PERFORM BOTH ROLES
An organization acting as PII processor for its customers	Data center serving as the IaaS platform for a SaaS customer.	The data center is also a PII controller when collecting the visitor's PII at the data center entrance – including CCTV footage of visitors. The data center also acts as PII controller for its employees.
An organization acting as PII controller	The website of a big data analytics firm that allows visitors to subscribe to their newsletter by providing an email address.	The firm analyses behavioral data passed to them from its customers it is hence a PII processor for its customers' PII.

OTHER PRIVACY STANDARDS

Prior to ISO/IEC 27701:2019, several ISO/IEC standards were available and many of them are still valid.

STANDARD	DESCRIPTION	REMARK
ISO/IEC 29151:2017	Code of practice for PII protection	+ 36 additional guidance in ISO/IEC 27002 + 13 additional controls on PII
ISO/IEC 27018:2019	Code of practice for protection of PII in public clouds acting as PII processors	+ 15 additional guidance in ISO/IEC 27002 related to PII in cloud + 11 additional cloud based PII controls

These two standards were released before the introduction of GDPR, CCPA, etc. but they do not contain all the provisions required for these regulations (e.g. automatic decision making and profiling). ISO/IEC 29151 + ISMS or ISO/IEC 27018 + ISMS were also not designed to be a PIMS. They add only the controls and do not contain the additional requirements to be added to the ISMS, such as a data privacy policy, data processing risk assessment, etc., that allow an organization to implement a PIMS. At the time of writing, these two standards are still valid.

Organizations are encouraged to evaluate their management needs before selecting the approach best suited to their strategy.

WHY SGS?

SGS is the world's leading inspection, verification, testing and certification company. SGS is recognised as the global benchmark for quality and integrity. With more than 89,000 employees, SGS operates a network of over 2,600 offices and laboratories around the world.

We provide competitive advantage, drive sustainability and deliver trust. At SGS, we are continually pushing ourselves to deliver innovative services and solutions that help our customers move their businesses forward.

Efficiency and cost-optimization are no longer the sole drivers in business development strategies. Successful businesses recognize the importance of offering their workforce continuous development and training. Motivated and effective teams create industry leaders.

CONTACT SGS


www.sgs.com


www.sgs.com/facebook


www.sgs.com/twitter


www.sgs.com/linkedin


certification@sgs.com