schellman
Quality. above all.

Your Guide to ISO 27701

ISO 27701 is valuable to organizations that have an existing ISO 27001 certification or are considering an ISO 27001 certification and want to include their privacy program into their Information Security Management System (ISMS). An accredited ISO 27001 certification that includes ISO 27701 demonstrates an organization's security and privacy practices through a validated third party assessment. This guide is intended to provide an overview of the ISO 27701 standard and the proper approach for including it into your ISMS.

WHITEPAPER

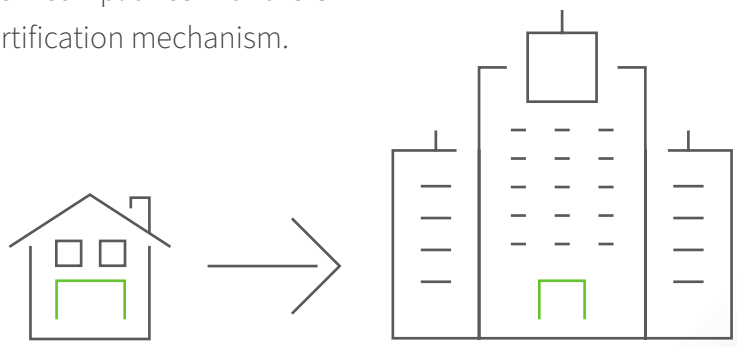
ISO 27701 allows for organizations to integrate their Privacy Information Management System, or PIMS, with their existing ISMS. This standard provides the implementation guidance for an organization to extend their ISMS to include a PIMS.

ISO 27701 can be used by controllers of Personally Identifiable Information (PII), including joint controllers, as well as processors and subprocessors of PII. A controller is defined as the organization that determines the purposes and means of processing PII. If another organization also determines the purposes and means of processing specific PII, that organization is considered a joint controller. A processor processes PII on behalf of a controller, as determined by the controller.

Who Should Consider ISO 27701

ISO 27701 applies to any organization, in any industry, of any type or size.

Put simply, if your organization collects, stores or processes PII, it has every reason to consider this certification. However, most organizations complete the certification due to a contractual obligation from a client or prospective client or use it as a competitive advantage. Additionally, organizations that are subject to the GDPR require a method to show compliance with the GDPR in absence of an approved certification mechanism.

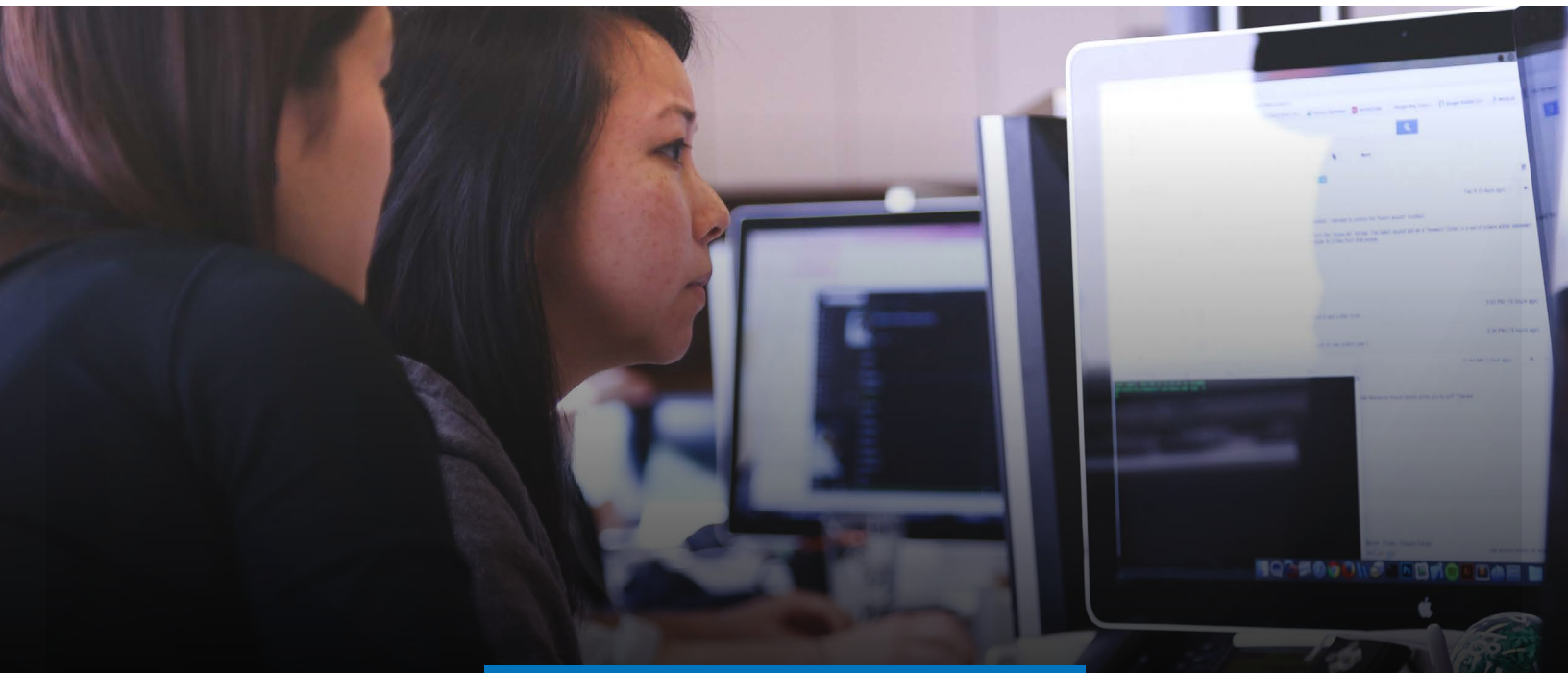


schellman
Quality. above all.

Benefits of Including ISO 27701 into an ISO 27001 Certification

Beyond a competitive advantage and protecting PII, including ISO 27701 into an ISO 27001 certification provides these additional benefits:

- Gives your company a functional, organization-wide plan to identify and mitigate not only information security but also privacy risks.
- Meeting the requirements of ISO 27001 and ISO 27701 means that you are required to perform specific activities at defined intervals (i.e. risk assessment, internal audit, etc.). The ISMS with an added PIMS is an active compliance framework, allowing your company to continually mature its security and privacy program while improving on current processes.



WHITEPAPER

schellman
Quality. above all.

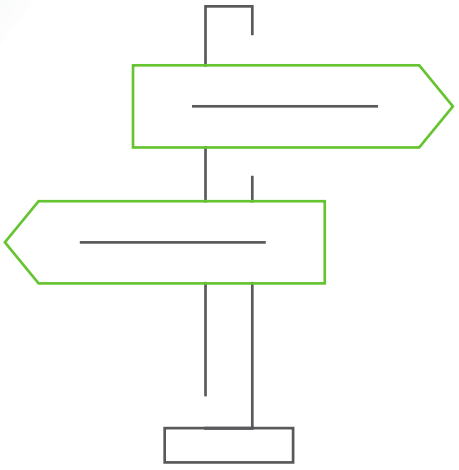
The Elements of the PIMS

While it may be tempting to look at each element of your company's PIMS individually, it is important to look at the big picture. The PIMS is intended to be a comprehensive, autonomous system that is continuous and interrelated with all of its different elements (clauses) and controls that include both ISO 27001 and ISO 27701. Just as a house is not a house without a foundation, a roof, walls, ducts, even nails; a PIMS is not effective unless all clauses are met and interrelated.

After the first year of including a PIMS into an existing management system, many organizations begin to mature and maximize their PIMS, allowing it to act as a comprehensive system. But, for now, it is completely acceptable to achieve conformance with the requirements (a success in its own right) during the first year.

Focus on meeting the PIMS requirement within ISO 27701 and then plan to work on continuous improvement as your company's overall ISMS, including its PIMS, becomes more integrated across your organization.

WHITEPAPER



It is important to understand that ISO 27701 is an add-on to an existing ISO 27001 ISMS. The standard should not be seen as independent but rather an integration of the PIMS requirements into the existing requirements of ISO 27001. Independent certifications can be performed against 27701; however, they would be unaccredited and lack in needed elements of a combined ISMS and PIMS.

The ISO 27701 standard includes several sections and clauses and also includes various mappings to ISO 29100, GDPR, and ISO 27018. Clauses 5-8 provide the necessary information an organization needs to ensure effective implementation of ISO 27701 into their ISMS. Those Clauses are further defined below, but at a high level, they include:

- ***Clause 5:***

  PIMS-specific requirements and other information regarding the information security requirements in ISO 27001 appropriate to an organization acting as either a PII controller or PII processor.

- ***Clause 6:***

  PIMS-specific guidance and other information regarding the information security controls in ISO 27002 and PIMS-specific guidance for an organization acting as either a PII controller or PII processor.

- ***Clause 7:***

  Additional ISO 27002 guidance for PII controllers.

- ***Clause 8:***

  Additional ISO 27002 guidance for PII processors.

There are also Annexes within ISO 27701 that are critical for an organization not to overlook. Specifically, Annex A provides PIMS-specific control objectives and controls for an organization acting as a PII controller (whether it employs a PII processor or not, and whether acting jointly with another PII controller or not). Annex B provides PIMS-specific control objectives and controls for an organization acting as a PII processor (whether it subcontracts the processing of PII to a separate PII processor or not, and including those processing PII as subcontractors to PII processors). Both Annexes in short are a summary of the control objectives and control requirements found in the applicable Clause 7 or Clause 8.

In short, to properly implement the requirements of ISO 27701 into an ISMS, they must ensure that the ISMS is updated to include privacy practices related to PII (per the requirements in Clause 5), implement relevant control implementation guidance for existing, applicable controls within 27002 (Clause 6), and, depending if the organization is a controller or processor, or both, implement the relevant and required controls to meet the control objectives (per the control objectives, controls, and implementation guidance in Clause 7 and Clause 8).

Clause 5:

PIMS Specific Requirements Related to ISO 27001

Clause 5 outlines the additional requirements that an organization must implement to ensure that their PIMS is effectively included into their ISMS. This Clause provides all requirements within ISO 27001, Clauses 4-10, and provides additional requirements, if applicable, to each of the elements within an ISMS.

The specifically noted additional requirements covered in this clause include modifications to the Context of the Organization and Planning.

- ***Clause 4 (Context of the Organization):***

  Requirements include understanding the organization and its context, understanding the needs and expectations of interested parties, and determining the scope of its ISMS. This would include the scope and role of the organization as a controller, processor, or both. An organization that acts as both a controller and processor will need to consider separate controls for each role as different data sets apply to the role of a controller than that of a processor.

- ***Clause 6 (Planning):***

  The risk assessment should identify risks related to the processing of PII, within the scope of the ISMS. The organization can either apply an integrated information security and privacy risk assessment process or two separate ones for information security and the risks related to the processing of PII. However, the same approach for the risk assessment based on the requirements of ISO 27001 would apply to the extended management system (i.e. risk program, risk assessment, risk owners, acceptable level of risk, risk treatment, statement of applicability, etc.).

Though ISO 27701 does not include any other implementation requirements for the management system other than those note above, the understanding is that all elements of the management system must be effective, with the inclusion of ISO 27701, to achieve an ISO 27001 certificate that includes ISO 27701, meaning the following, though not an exhaustive list:

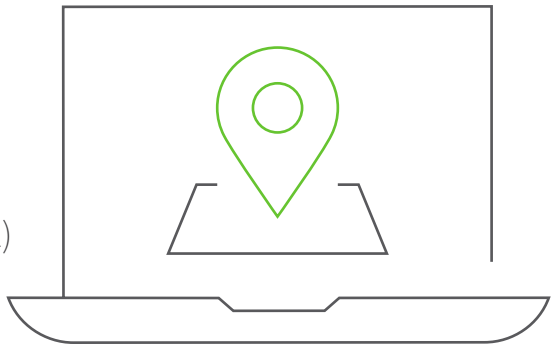
- Documentation relevant to both standards must follow the documentation management requirements
- Communication relevant to both standards must meet the communication requirements
- Necessary resources for both standards and processes must be available, competent, trained, and assigned
- The management system and supporting controls must continually operate effectively
- The internal audit program must encompass the entirety of the ISMS, including the PIMS
- Monitoring of controls and processes must be inclusive of both standards
- The management review must include the entirety of the ISMS, including the PIMS

Clause 6:

PIMS-specific guidance related to ISO 27002

Clause 6 contains the additional implementation guidance for existing controls within ISO 27002. All control domains, control objectives, and control requirements from ISO 27002 are included within Clause 6; however, only 32 of the overall 114 controls of ISO 27002 include additional implementation guidance from ISO 27701. The additional implementation guidance, however, applies to both controllers and processors. The additional implementation guidance covered in this Clause 6 include the following with the number of controls and additional implementation guidance included in parentheses:

5. Information Security Policies (1)
6. Organization of Information Security (2)
7. Human Resource Security (1)
8. Asset Management (5)
9. Access Control (3)
10. Cryptography (1)
11. Physical and Environmental Security (2)
12. Operations Security (3)
13. Communications Security (2)
14. System Acquisition, Development and Maintenance (5)
15. Supplier Relationships (1)
16. Security Incident Management (2)
17. Information Security Aspects of Business Continuity Management (0)
18. Compliance (4)



schellman
Quality. above all.

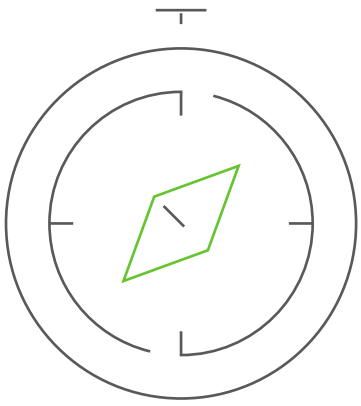
Clause 7 and Annex A:

Additional ISO 27002 Guidance for PII Controllers

Clause 7 provides the additional control objectives, controls and implementation guidance necessary for a PII controller to consider and implement based on requirements within ISO 27701. Some of these objectives and controls may not be applicable to controllers. Justification for those that are not applicable would need to be based on the risk assessment and documented within the statement of applicability. There are a total of 4 control objectives and 31 controls for PII controllers. Those 4 control objectives include the following areas (including the number of controls for each objective):

- Collection and processing (7.2 – 8 controls)
- Obligation to PII principals (7.3 – 10 controls)
- Privacy by design and default (7.4 – 9 controls)
- PII sharing, transferring or disclosing (7.5 – 4 controls)

Annex A of ISO 27701 includes the overview of the control objectives and controls applicable to controllers. Note that for controllers, implementing the requirements in Clause 5, Clause 6, and Clause 7 would complete the necessary inclusion of ISO 27701 into their ISMS/PIMS.



schellman
Quality. above all.

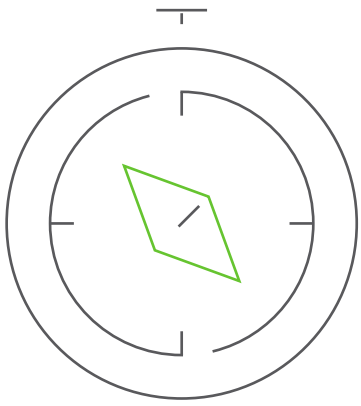
Clause 8 and Annex B:

Additional ISO 27002 Guidance for PII Processors

Clause 8 provides the additional control objectives, controls and implementation guidance necessary for a PII processor to consider and implement based on requirements within ISO 27701. Some of these objectives and controls may not be applicable to processors. Justification for those that are not applicable would need to be based on the risk assessment and documented within the statement of applicability. There are a total of 4 control objectives and 18 controls for PII processors. Those 4 control objectives include the following areas (including the number of controls for each objective):

- Collection and processing (8.2 – 6 controls)
- Obligation to PII principals (8.3 – 1 control)
- Privacy by design and default (8.4 – 3 controls)
- PII sharing, transferring or disclosing (8.5 – 8 controls)

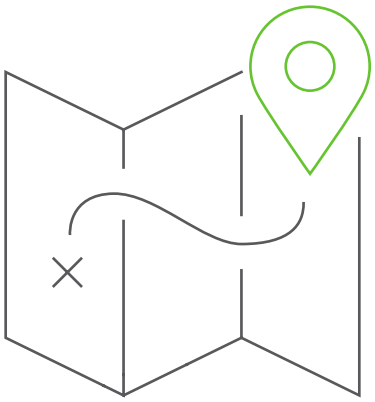
Annex B of ISO 27701 includes the overview of the control objectives and controls applicable to processors. Note that for processors, implementing the requirements in Clause 5, Clause 6, and Clause 8 would complete the necessary inclusion of ISO 27701 into their ISMS/PIMS.



So Where to Go from Here

Get the Standard

Most importantly, an organization needs to obtain a copy of the ISO 27701 standard. The beauty of any ISO assessment is that it is an open-book test. The certification body will assess you against the same requirements that you are aware of in the standard.



Understand Your Gaps

As mentioned above, the standard provides substantive implementation guidance and mappings, so it is beneficial for an organization to perform a cursory internal assessment to determine what the net-new requirements are and where there may be short comings. It is not uncommon, however, to have an external readiness assessment performed and it is quite beneficial to have the same certification body perform the readiness assessment that is also performing the certification. This allows for familiarity with the system and processes to better prepare for the certification effort.

Be Sure to Cover the Entire ISMS

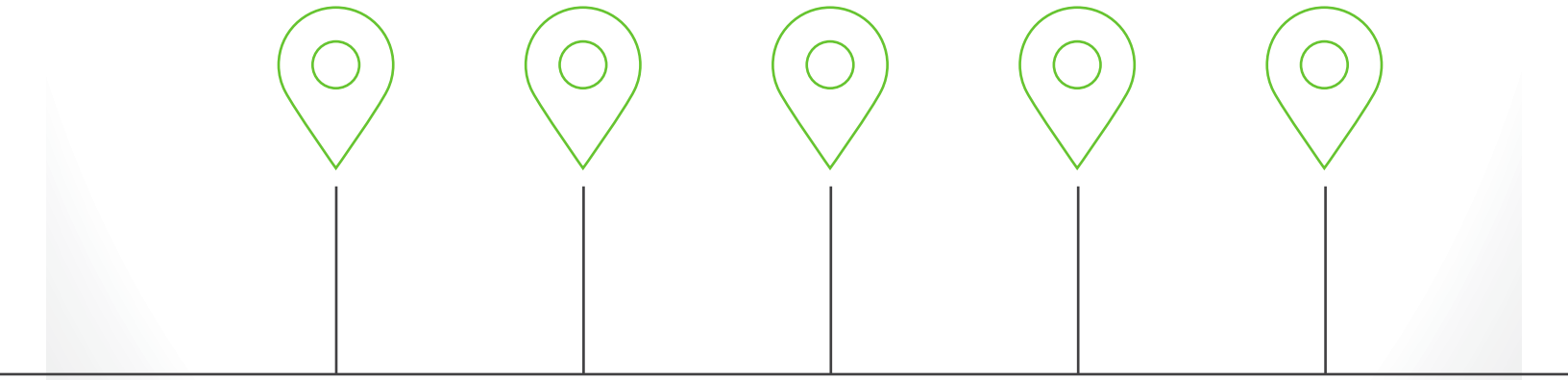
Unlike other ISO 27001 extensions (i.e. ISO 27017 or ISO 27018), ISO 27701 is more than just the control set. It includes necessary updates to the ISMS core clauses to ensure that the organization assesses and addresses the information security and privacy risk. Part of the implementation process to include ISO 27701 into your ISMS should include a holistic view of necessary updates and not to assume that the controls are what is most important.

Include All Responsible Parties

With ISO 27001, and a focus on information security risk, it is not uncommon to have those within the security organization managing and maintaining the ISMS. However, to effectively expand the ISMS to include the requirements of ISO 27701, the boundary of responsible parties should be reconsidered as it is likely that persons from the privacy team will need a seat at the table given the expanded role that privacy will have within the ISMS.

Plan for Your External Audit

With the timeline for implementation mostly based on looking forward to the external audit date and working backward, it is important to ensure that an organization allows itself the properly allotted time to design and implement the requirements of ISO 27701 into their ISMS. Should the timing not fit, there is always the option of performing a “special audit” which is outside of the regular cadence of the routine audit; the special audit would focus solely on the delta to the existing ISMS with the result, if the implementation was effective, being a revised certificate which would include ISO 27701 into the scope of your ISMS.



Why Schellman for ISO 27001?

We at Schellman believe our clients deserve the best. That's why we never use contractors and our audit staff is continually monitored to ensure that they are competent and provide effective assessments. This helps us provide for continuity of the audit team from year to year, allowing for the team members to know your company inside and out. Unlike other firms, we:

- Have over 70 lead auditors for ISO 27001
    - Privacy subject matter experts that have performed numerous GDPR and similar privacy assessments
    - A review of your privacy program that satisfies multiple privacy laws and regulations worldwide
- Provide you with a dedicated management team, which gives you an easily accessible point of contact without having to call a service line
- Have weekly status check-ins on the lead-up to audit, giving you time to ask questions or check on status updates
- Stick to our project timelines, which gives you your certificate in weeks rather than months
- Have cross-trained teams of auditors who can conduct multiple audits at once, saving you time and money

CLICK FOR MORE INFO

schellman
Quality, above all.

www.schellman.com
4010 W Boy Scout Blvd, Suite 600
Tampa, FL 33607
1.866.254.0000

Outside of the United States,
please dial: +1.973.854.4684