27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

ISO 27001 vs. ISO 27701 Matrix

WHITE PAPER

Advisera
Making certification simple.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
0	**Introduction**	**0**	**Introduction**	
0.1	General	0.1	General	Information about the high-level structure of the standards, the process approach adopted for managing the systems, and the possibility of integrating them with each other or with other ISO management systems. For more information on this topic, see this article: How to implement integrated management systems.
0.2	Compatibility with other management system standards	0.2	Compatibility with other management system standards	
1	**Scope**	**1**	**Scope**	**Statements about the generality of the standards (fit for all kinds of organizations, independent of size, type, and nature).** **ISO 27001 does not allow exclusions of clauses from sections 4 to 10 (it only allows exclusions of controls from Annex A) and clarifies ISO 27701 as an extension of ISO 27001 and ISO 27002 for specific protection of Personally Identifiable Information (PII).**
2	**Normative references**	**2**	**Normative references**	**ISO 27001 refers only to its documented vocabulary (ISO 27000).** **ISO 27701 refers to its documented vocabulary (ISO 27000 and ISO 29100) and to ISO 27001 and ISO 27002.**

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
3	**Terms and definitions**	**3**	**Terms and definitions**	**Both standards list their own "Fundamentals and vocabulary" (ISO 27000 for both ISO 27001 and ISO 27701, and ISO 29100 for ISO 27701), but ISO 27701 also includes its own definitions for "joint PII controller" and "Privacy Information Management System – PIMS."**
-	**-**	**4**	**General**	
-	-	4.1	Structure of this document	This section clarifies the organization of the standard, from clauses 5 to 8, and Annexes A to F, and their relationships with ISO 27001 and ISO 27002.
-	-	4.2	Application of ISO/IEC 27001:2013 requirements	This section shows the relationship between PIMS-specific requirements of the standard and ISO/IEC 27001 requirements.
-	-	4.3	Application of ISO/IEC 27002:2013 guidelines	This section shows the relationship between PIMS-specific guidance of the standard and ISO/IEC 27002 guidance.
-	-	4.4	Customer	This section shows how the term "customer" can be understood in the context of the standard according to the role of the organization in handling PII.
-	**-**	**5**	**PIMS-specific requirements related to ISO/IEC 27001**	

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
-	-	5.1	General	Brief explanation on how requirements of this standard are extended from ISO 27001 (basically, where ISO 27001 mentions “information security,” ISO 27701 mentions “information security and privacy”).
4	**Context of the organization**	**5.2**	**Context of the organization**	
4.1	Understanding the organization and its context	5.2.1	Understanding the organization and its context	These clauses require the organization to determine all internal and external issues that may be relevant to its business purposes and to the achievement of the objectives of their respective Information Security Management System (ISMS) / Privacy Information Management System (PIMS). In the case of ISO 27701, this also includes the definition of the organization’s role as PII controller (including in cases where it acts as a joint PII controller) and/or PII processor.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
4.2	Understanding the needs and expectations of interested parties	5.2.2	Understanding the needs and expectations of interested parties	The standards require the organization to assess who the interested parties are in terms of its respective ISMS / PIMS, what their needs and expectations may be, which legal and regulatory requirements, as well as contractual obligations, are applicable, and consequently, if any of these should become compliance obligations. Legal and regulatory requirements must be documented, kept updated, and communicated to all interested parties. ISO 27701 specifically requires the identification of parties interested in or responsible for the processing of PII, including the natural persons to whom the Personally Identifiable Information relates to. For both ISMS and PIMS, a single process can be defined for the identification of interested parties, as well as statutory, regulatory, contractual, and other requirements related to information security and privacy. See a sample document here: Procedure for Identification of Requirements. For both ISMS and PIMS, one document can be used to list requirements regarding information security and privacy. See a sample document here: List of Legal, Regulatory, Contractual and Other Requirements. For more information on this topic, see these articles: How to identify interested parties according to ISO 27001 and ISO 22301 and How to identify ISMS requirements of interested parties in ISO 27001.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
4.3	Determining the scope of the information security management system	5.2.3	Determining the scope of the information security management system	The scope, boundaries, and applicability of the ISMS / PIMS must be examined and defined considering the internal and external issues, interested parties and their needs and expectations, as well as legal and regulatory compliance obligations. Specifically for an ISMS, the existing interfaces and dependencies between the organization's activities and those performed by other organizations must be identified. Specifically for an PIMS, processing of PII must be included in the scope. The scope and justified exclusions must be kept as "documented information." One document can be used to define the scope for both standards. See a sample document here: ISMS Scope Document. For more information on this topic, see these articles: How to define the ISMS scope and Problems with defining the scope in ISO 27001.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
4.4	Information security management system	5.2.4	Information security management system	The ISMS / PIMS should be established and operated and, by using interacting processes, be controlled and continuously improved.
5	**Leadership**	**5.3**	**Leadership**	
5.1	Leadership and commitment	5.3.1	Leadership and commitment	Both clauses require top management and line managers with relevant roles in the organization to demonstrate genuine effort to engage people to support their respective management systems. These clauses provide many actions top management must commit to, in order to enhance the organization's levels of leadership, involvement, and cooperation in the operation of the ISMS / PIMS. For more information on this topic, please see the article: Roles and responsibilities of top management in ISO 27001 and ISO 22301.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
5.2	Policy	5.3.2	Policy	Top management has the responsibility to establish policies, which are aligned with the organization's purposes and provide a framework for setting "information security" / "information security and privacy" objectives, including a commitment to fulfill applicable requirements and the continual improvement of the ISMS / PIMS and their results. Both policies must be maintained as documented information, be communicated within the organization, be available to all interested parties, and be reviewed, periodically or when significant changes occur in the organizational context. The requirements are the same and could be met through a single document. See a sample document here: Information Security Policy. For more information on this topic, please see this article: What should you write in your Information Security Policy according to ISO 27001?
5.3	Organizational roles, responsibilities and authorities	5.3.3	Organizational roles, responsibilities and authorities	For both standards, top management must ensure that roles, responsibilities, and authorities are delegated and communicated effectively. The responsibility must also be assigned to ensure that the ISMS / PIMS meets the terms of its respective standard, and that the ISMS / PIMS performance can be accurately reported to top management. For example, a manager, or managers, must be indicated to oversee "information security" / "information security and privacy" activities; the same auditor can perform PIMS and ISMS audits, etc.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
				For more information on this topic, please see this article: What is the job of the Chief Information Security Officer (CISO) in ISO 27001?
6	**Planning**	**5.4**	**Planning**	
6.1	Actions to address risks and opportunities	5.4.1	Actions to address risks and opportunities	Basically, ISO 27701 adopts the same requirements of ISO 27001, adding the privacy protection issue, as you can see in the next lines of this section.
6.1.1	General	5.4.1.1	General	These clauses seek to cover the "preventive action" stated in the previous version of the ISO 27001 standard (ISO 27001:2005). The organization must plan actions to handle risks and opportunities relevant to the context of the organization (section 4.1) and the needs and expectations of interested parties (section 4.2), as a way to ensure that the ISMS / PIMS can achieve its intended outcomes and results, prevent or mitigate undesired consequences, and continually improve. These actions must consider their integration with ISMS / PIMS activities, as well as how effectiveness should be evaluated.
6.1.2	Information security risk assessment	5.4.1.2	Information security risk assessment	The ISO 27001 clauses about information security risk assessment and treatment planning are only refined in ISO 27701, considering the following requirements: • Risk assessment must be applied within the scope of PIMS;

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
6.1.3	Information security risk treatment	5.4.1.3	Information security risk treatment	• Risk assessment must be applied in the processing of PII within the scope of PIMS; • Risk assessment must ensure proper management of information security and privacy; • Assessment of potential consequences of realized risks must consider both the organization and the natural persons to whom the Personally Identifiable Information relates; • Applicable controls need to consider both ISO 27001 Annex A and ISO 27701 Annexes A and B; • Applicability of controls must consider both risks to information security and to processing of PII, as well as risks related to natural persons to whom the Personally Identifiable Information relates; • The Statement of Applicability needs to consider both ISO 27001 Annex A and ISO 27701 Annexes A and B. See a sample document here: Risk Assessment and Risk Treatment Methodology. For more information on this topic, please see this article: ISO 27001 risk assessment & treatment – 6 basic steps.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
6.2	Information security objectives and planning to achieve them	5.4.2	Information security objectives and planning to achieve them	"Information security" / "Information security and privacy" objectives should be established and communicated at appropriate levels, functions, and intervals, having considered their alignment with the "information security" / "information security and privacy" policy, the possibility of measurement, the applicable requirements, and results from risk assessment and risk treatment. The objectives must be updated when deemed necessary. They must be thought of in terms of what needs to be done, when it needs to be done by, what resources are required to achieve them, who is responsible for the objectives, and how results are to be evaluated, to ensure that objectives are being achieved and can be updated when circumstances require. These must be kept as documented information. For more information on this topic, please see this article: ISO 27001 control objectives –Why are they important?
7	**Support**	**5.5**	**Support**	
7.1	Resources	5.5.1	Resources	For both standards, the resources required by the ISMS / PIMS to achieve the stated objectives and show continual improvement must be defined and made available by the organization. For more information on this topic, please see this article: How to demonstrate resource provision in ISO 27001.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
7.2	Competence	5.5.2	Competence	The competence of people given responsibility for the ISMS / PIMS who work under the organization's control must meet the terms of the standards, to ensure that they are capable and confident and that their performance does not negatively affect the ISMS / PIMS. Competence can be demonstrated by experience, training, and/or education regarding the assumed tasks. When the competence is not enough, training must be identified and delivered, as well as measured to make sure the required level of competence was achieved. Evidence of competence in both standards must be kept as documented information. You can use one training plan for both standards to reduce records. See a sample document here: Training and Awareness Plan. For more help with information security and privacy training, please see the article How to perform training & awareness for ISO 27001 and ISO 22301.
7.3	Awareness	5.5.3	Awareness	Awareness is closely related to competence in the standards. People who work under the organization's control must be made aware of the Information Security / Privacy Policy and its contents, what their personal performance means to the ISMS / PIMS and its objectives, and what the implications of nonconformities may be to the management systems. See also: 8 Security Practices to Use in Your Employee Training and Awareness Program.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
7.4	Communication	5.5.4	Communication	Internal and external communication deemed relevant to the ISMS / PIMS must be determined, as well as the processes by which they must be effected, considering what needs to be communicated, by whom, when it should be done, and who needs to receive the communication. These requirements can be met by means of activities like writing announcements on a noticeboard, sending emails, conducting regular staff meetings, etc. For more help with this topic, see also: How to create a Communication Plan according to ISO 27001.
7.5	Documented information	5.5.5	Documented information	For both standards, documents and records (called "documented information") must be managed (i.e., created, updated, and controlled) – both documents and records required by the standards and those viewed as critical by the organization to the ISMS /PIMS and its daily operation. You can apply the same procedure to meet the requirements of both standards and establish the documentation system. See a sample document here: Procedure for Document and Record Control. For more help with this topic, see also: • List of mandatory documents required by ISO 27001 (2013 revision); • Document management in ISO 27001 & BS 25999 – 2; and • Records management in ISO 27001 and ISO 22301.
7.5.1	General	5.5.5.1	General	
7.5.2	Creating and updating	5.5.5.2	Creating and updating	
7.5.3	Control of documented information	5.5.5.3	Control of documented information	

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
8	**Operation**	**5.6**	**Operation**	
8.1	Operational planning and control	5.6.1	Operational planning and control	General statements here cover risks and opportunities for the management systems, and risks for information security and privacy: • processes, both internal and those outsourced deemed relevant, must be identified, planned, implemented, and controlled; • documented information deemed necessary to provide confidence that the processes are being performed and achieving their results as planned must be retained; • changes must be planned and controlled; and • impacts of unexpected changes must be evaluated, and proper actions considered.
8.2	Information security risk assessment	5.6.2.2	Information security risk assessment	These clauses about performing “information security” / “information security and privacy” risk assessment and treatment can help identify: • information security and privacy risks that can impact ISMS / PIMS defined objectives and desired outcomes; and

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
8.3	Information security risk treatment	5.6.2.3	Information security risk treatment	• actions, resources, responsibilities, and deadlines needed to prevent and handle events that are information and/or privacy related. See sample documents here: Risk Assessment Table, Risk Treatment Table, and Risk Treatment Plan. For more help with this topic, see also: • ISO 27001 risk assessment: How to match assets, threats and vulnerabilities • How to assess consequences and likelihood in ISO 27001 risk analysis
9	**Performance evaluation**	**5.7**	**Performance evaluation**	

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
9.1	Monitoring, measurement, analysis and evaluation	5.7.1	Monitoring, measurement, analysis and evaluation	Basically, the requirements here are: • establishment and evaluation of performance metrics regarding the effectiveness and efficiency of "information security" / "information security and privacy" processes, procedures, and functions; and • establishment and evaluation of performance metrics regarding ISMS / PIMS compliance with the standards, preventive actions in response to adverse trends, and the degree to which the "information security" / "information security and privacy" policies, objectives, and goals are being achieved. The methods established should take into consideration what needs to be monitored and measured, how to ensure the accuracy of results, and at what frequency to perform the monitoring, measurement, analysis, and evaluation of ISMS / PIMS data and results. Performance results must be properly retained as evidence of compliance and as a source to facilitate subsequent corrective actions.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
9.2	Internal audit	5.7.2	Internal audit	Briefly speaking, the requirements here are: Internal audits should be performed at planned intervals, considering the processes' relevance and the results of previous audits, to ensure effective implementation and maintenance, as well as compliance with the standard's requirements and any requirements defined by the organization itself. Criteria and scope for each audit must be defined. Auditors should be independent and have no conflict of interest over the audit subject. Auditors also must report the audit results to relevant management, and ensure that non-conformities are subject to the responsible managers, who in turn must ensure that any corrective measures needed are implemented in a timely manner. Finally, the auditor must also verify the effectiveness of corrective actions taken. The same procedure for internal audit can be applied for both standards. See a sample document here: Internal Audit Procedure. To learn more about this topic, please see these articles: How to make an Internal Audit checklist for ISO 27001 / ISO 22301 and How to prepare for an ISO 27001 internal audit.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
9.3	Management review	5.7.3	Management review	Management review must be performed at planned intervals, at a strategic and top management level, covering the required aspects all at once or by parts, in a way that is most suitable to business needs. The status of actions defined in previous reviews, significant internal and external factors that may impact the management system, “information security” / “information security and privacy” performance, and opportunities for improvement should be reviewed by top management so that relevant adjustments and improvement opportunities can be implemented. The same document can be used, but it has to contain separate input elements for both standards. See a sample document here: Management Review Minutes. For more details on this topic, please see the article: Why is management review important for ISO 27001 and ISO 22301?
10	**Improvement**	**5.8**	**Improvement**	
10.1	Nonconformity and corrective action	5.8.1	Nonconformity and corrective action	In short, the requirements here are:

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
10.2	Continual improvement	5.8.2	Continual improvement	• Outputs from management reviews, internal audits, and compliance and performance evaluation should all be used to form the basis for nonconformities and corrective actions. • Responses to mitigate a nonconformity and/or corrective action must be proportional to its impact and the need to eliminate the root cause. • The effectiveness of actions taken must be evaluated and documented. • Continual improvement must be used to achieve and maintain the suitability, adequacy, and effectiveness of the management system regarding fulfillment of the organizations' objectives. Continual improvement can make use, with a few adjustments, of the same procedure to handle non-conformity and corrective action. See a sample document here: Procedure for Corrective Action. For more details on this topic, please see these articles: • Practical use of corrective actions for ISO 27001 and ISO 22301 • Achieving continual improvement through the use of maturity models
-	**-**	**6**	**PIMS-specific guidance related to ISO/IEC 27002**	**Additional guidance is provided by ISO/IEC 27701 for some controls of ISO/IEC 27002**

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
-	-	6.2.1.1	Policies for information security (ISO/IEC 27002 control 5.1.1)	Organizations should include in their policies clear statements concerning support for and commitment to complying with PII applicable legal requirements (e.g., laws, regulations, and contracts), clarifying responsibilities between involved parties.
-	-	6.3.1.1	Information security roles and responsibilities (ISO/IEC 27002 control 6.1.1)	Points of contact for use of PII customer/principal should be defined. One or more persons should be appointed to manage a governance and privacy program.
-	-	6.3.2.1	Mobile device policy (ISO/IEC 27002 control 6.2.1)	Use of mobile devices should not lead to PII compromise.
-	-	6.4.2.2	Information security awareness and training (ISO/IEC 27002 control 7.2.2)	Relevant staff, especially those handling PII, should be aware of consequences to involved parties of breaching privacy or security rules and procedures.
-	-	6.5.2.1	Classification of information (ISO/IEC 27002 control 8.2.1)	PII should be explicitly considered in the organization's information classification system.
-	-	6.5.2.2	Labeling of information (ISO/IEC 27002 control 8.2.2)	People handling PII should be aware of how to recognize information that is PII.
-	-	6.5.3.1	Management of removable media (ISO/IEC 27002 control 8.3.1)	Use of removable media/devices used for PII should be documented.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
				Removable media/devices used for PII should use encryption whenever possible, or compensation controls when encryption is not available.
-	-	6.5.3.2	Disposal of media (ISO/IEC 27002 control 8.3.2)	It should be ensured that PII previously stored on disposed media will not be accessible, by means of documented disposal procedures.
-	-	6.5.3.3	Physical media transfer (ISO/IEC 27002 control 8.3.3)	Information about physical media used for incoming and outgoing PII should be recorded, and proper controls should be applied to protect PII in such media.
-	-	6.6.2.1	User registration and de-registration (ISO/IEC 27002 control 9.2.1)	Specific measures for managing users' accounts related to the administration or operation of systems processing PII should be implemented (e.g., handling of compromised password, checking of unused accounts, etc.).
-	-	6.6.2.2	User access provisioning (ISO/IEC 27002 control 9.2.2)	A record of user profiles created for accessing PII, as well as which users use them and which PII is accessed, should be maintained. User IDs should be unique for each user.
-	-	6.6.4.2	Secure log-on procedures (ISO/IEC 27002 control 9.4.2)	Secure log-on capabilities for users under customer control should be available when required by the customer.
-	-	6.7.1.1	Policy on the use of cryptographic controls (ISO/IEC 27002 control 10.1.1)	Information should be available about cryptographic solutions used for PII protection, and also about which capabilities can be provided to customers so they can apply their own cryptographic solutions.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
-	-	6.8.2.7	Secure disposal or re-use of equipment (ISO/IEC 27002 control 11.2.7)	It should be ensured that PII previously stored on disposed equipment, or designated for re-use, will not be accessible. Any equipment that can possibly contain PII should be treated as if it in fact contains PII.
-	-	6.8.2.9	Clear desk and clear screen policy (ISO/IEC 27002 control 11.2.9)	Hardcopies of material containing PII should be reduced to the minimum necessary to fulfill their identified purpose.
-	-	6.9.3.1	Information backup (ISO/IEC 27002 control 12.3.1)	Specific PII requirements should be included in the overall backup policy (e.g., erasure of PII contained in backup media, customer responsibilities, information to customers about backup capabilities, required procedures and logs for PII restoration, etc.).
-	-	6.9.4.1	Event logging (ISO/IEC 27002 control 12.4.1)	A process for log review should be implemented, with clearly define roles, responsibilities, and access rights. Criteria for defining when and how log information can be made available to customers should be defined, ensuring that the customer can only access data related to its own activities, and that data cannot be amended.
-	-	6.9.4.2	Protection of log information (ISO/IEC 27002 control 12.4.2)	Log information that can possibly contain PII should be protected to ensure it is used only as intended. A procedure to ensure logged information is properly disposed should be implemented by PI processors.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
-	-	6.10.2.1	Information transfer policies and procedures (ISO/IEC 27002 control 13.2.1)	Procedures for ensuring that the rules for processing PII are enforced should be defined.
-	-	6.10.2.4	Confidentiality and non-disclosure agreements (ISO/IEC 27002 control 13.2.4)	Confidentiality obligations should be enforced over personnel with access to PII, ensuring that they also comply with related policies and procedures for handling and protecting data.
-	-	6.11.1.2	Securing application services on public networks (ISO/IEC 27002 control 14.1.2)	PII should be encrypted when transmitted over networks not controlled by the organization.
-	-	6.11.2.1	Secure development policy (ISO/IEC 27002 control 14.2.1)	Policies for system development and design should include PII needs, contributing to privacy by design and privacy by default.
-	-	6.11.2.5	Secure systems engineering principles (ISO/IEC 27002 control 14.2.5)	PII processing elements should be designed following the privacy by design and privacy by default principles.
-	-	6.11.2.7	Outsourced development (ISO/IEC 27002 control 14.2.7)	Privacy by design and privacy by default principles, if applicable, should be applied to outsourced development.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
-	-	6.11.3.1	Protection of test data (ISO/IEC 27002 control 14.3.1)	Use of PII for testing should be avoided, and when this is not possible, controls similar to those applied in the production environment should be used.
-	-	6.12.1.2	Addressing security within supplier agreements (ISO/IEC 27002 control 15.1.2)	PII processing requirements and related security controls should be considered in agreements with suppliers, including allocation of responsibilities and assurance of compliance with applicable legal requirements by the suppliers and their partners. Organizations should include in agreements with PII processors that PII only will be processed according to its instructions.
-	-	6.13.1.1	Responsibilities and procedures (ISO/IEC 27002 control 16.1.1)	Procedures for handling breaches of PII should be established, including communication to required parties without unnecessary delay.
-	-	6.13.1.5	Response to information security incidents (ISO/IEC 27002 control 16.1.5)	PII-related incidents should be reviewed by the organization acting as the PII controller, to evaluate if a PII breach has occurred and proper measures need to be taken. Proper records about the handling of breached PII should be kept. Requirements for notification regarding a breach of PII should be included in agreements between a PII processor and its customer.
-	-	6.15.1.1	Identification of applicable legislation and contractual requirements (ISO/IEC 27002 control 18.1.1)	Potential legal sanctions, as well as significant fines, related to PII breaches should be identified by organizations.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
-	-	6.15.1.3	Protection of records (ISO/IEC 27002 control 18.1.3)	Current and old versions of privacy policies and procedures should be retained according to a defined retention schedule.
-	-	6.15.2.1	Independent review of information security (ISO/IEC 27002 control 18.2.1)	PII processors should provide their customers with independent evidence that information security and privacy are implemented and operated as planned.
-	-	6.15.2.3	Technical compliance review (ISO/IEC 27002 control 18.2.3)	Specific methods for reviewing tools and components involved in PII processing should be included in the overall technical review.
-	-	**7**	**Additional ISO/IEC 27002 guidance for PII controllers**	**This section provides details to be considered on the implementation of controls defined in ISO/IEC 27701 Annex A (for the benefit of better understanding, the most relevant guidance is summarized together with information presented in the section about ISO/IEC 27701 Annex A).**
-	-	**8**	**Additional ISO/IEC 27002 guidance for PII processors**	**This section provides details to be considered on the implementation of controls defined in ISO/IEC 27701 Annex B (for the benefit of better understanding, the most relevant guidance is summarized together with information presented in the section about ISO/IEC 27701 Annex B).**

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
Annex A	**Reference control objectives and controls**	**-**	**-**	**Even though ISO 27701 does not make changes to control objectives and controls described in ISO 27001 Annex A, based on the results of the information security and privacy risk assessment, practically all controls described in this ISO 27001 annex may be applicable to ISO 27701.** **For more detail on this subject, please take a look at these articles:** • **Overview of ISO 27001:2013 Annex A** • **How to structure the documents for ISO 27001 Annex A controls**
-	**-**	**Annex A**	**PIMS-specific reference control objectives and controls (PII Controllers)**	**This section provides control objectives and controls to be considered along with control objectives and controls from ISO/IEC 27001 Annex A.**
-	-	A.7.2	Conditions for collection and processing (8 controls)	Organizations should ensure that: • PII principals understand, in a documented manner, why their information is processed; • A relevant lawful basis for processing PII, according to identified purposes, is identified, documented, and is being fulfilled; • A process for obtaining consent from PII principals for processing their PII is defined and documented; • A record of the consent of PII principals is maintained; • A privacy impact assessment is considered, and implemented properly, whenever there is a change in processing PII context; • Proper written contracts with PII processors exist; • Clear roles and responsibilities are defined for processing PII with any joint PII controller;

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
				• Needed records to support PII processing obligations are maintained.
-	-	A.7.3	Obligations to PII principals (10 controls)	Organizations should ensure that: • Legal, regulatory, and contractual obligations to PII principals related to processing their PII are defined and documented, and that the means to fulfill them are provided; • Information about PII processing to be provided to the principals, and the timing to do so, are defined and documented; • Information about the PII controller and the processing of PII are easily accessible by PII principals; • Mechanisms for PII principals to modify or cancel their consent are available; • Mechanisms for PII principals to state their objection to the processing of their PII are available; • Policies, procedures, and/or mechanisms for PII principals to access, correct, and/or erase their information are available;

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
				• Changes in the context of PII shared with third parties are communicated, and supported by proper policies, procedures, and/or mechanisms; • Copies of required processed PII are provided when requested by PII principals; • Requests from PII principals are handled through documented policies and procedures; • Automated decisions about PII processing address identified legal obligations.
-	-	A.7.4	Privacy by design and privacy by default (9 controls)	Organizations should ensure that: • Collection of PII is limited to the minimum necessary for the identified purposes; • Processing of PII is limited to the minimum necessary for the identified purposes; • Accuracy, completeness, and updating of PII, according to identified purposes, are properly documented and ensured; • Objectives for data minimization, and mechanisms to achieve them, are defined and documented; • Any PII that is no longer needed is deleted or rendered unidentifiable as soon as it is not needed;

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
				• Temporary files related to processed PII are deleted according to documented procedures within defined times; • PII is not retained for periods longer than necessary for the identified purposes; • Documented policies, procedures, and/or mechanisms are available for PII disposal; • Transmitted PII is properly protected to ensure that it reaches its defined destination.
-	-	A.7.5	PII sharing, transfer and disclosure (4 controls)	Organizations should ensure that: • A relevant basis for PII transfer is identified and documented; • Countries and international organizations to which PII can be transferred are identified and documented; • Transfers of PII are recorded, and cooperation with parties to which PII was transferred is ensured; • Information about PII disclosure to third parties is recorded.

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
-	-	Annex B	PIMS-specific reference control objectives and controls (PII Processors)	This section provides control objectives and controls to be considered, along with control objectives and controls from ISO/IEC 27001 Annex A.
-	-	B.8.2	Conditions for collection and processing (6 controls)	Organizations should ensure that: • Provision of assistance to customers is included in contracts to process PII whenever relevant; • PII is processed only for the purposes agreed upon with the customer; • PII is not used for marketing purposes without the previous consent of the PII principal, and that this consent is not a condition for providing the service; • Potential infringement of regulation / legislation can happen in case a processing instruction is performed; • Proper information is provided to customers so they can demonstrate compliance with their obligations; • Records demonstrating the organization's compliance with its PII processing obligations are identified and maintained.
-	-	B.8.3	Obligations to PII principals (1 control)	The organization should ensure that: • It supports its customers in complying with PII principals related to obligations.
-	-	B.8.4	Privacy by design and privacy by default (3 controls)	The organization should ensure that:

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
				• Temporary files related to PII processing are disposed of according to documented procedures and defined periods; • PII can be returned, transferred, and/or disposed of in a secure manner, and a related policy covering this issue is available to the customer; • Transmitted PII is properly protected to ensure that it reaches its defined destination.
-	-	B.8.5	PII sharing, transfer and disclosure (8 controls)	The organization should ensure that: • Information about the basis for PII transfer is provided to customers in a timely manner; • Countries and international organizations to which PII can be transferred are identified and documented; • Information about PII disclosure to third parties is recorded; • Customers are notified about any legal requests for disclosure of their PII; • Any PII disclosure that is not legally binding is only made after the authorization of the PII customer; • The customer is informed about any subcontractors that will process PII before processing takes place; • Subcontractors are engaged in processing customer PII only according to defined contracts; • Customers are notified of intended changes by subcontractors.
-	-	**Annex C**	**Mapping to ISO/IEC 29100**	
-	-		ISO/IEC 29100 provides guidance for defining a privacy framework.	Relationship between ISO/IEC 29100 principles and controls in ISO/IEC 27701: • Principle 1 (Consent and choice): 8 controls for PII controllers and 1 control for PII processors;

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
				• Principle 2 (Purpose legitimacy and specification): 6 controls for PII controllers and 5 controls for PII processors; • Principle 3 (Collection limitation): 2 controls for PII controllers and 0 controls for PII processors; • Principle 4 (Data minimization): 3 controls for PII controllers and 1 control for PII processors; • Principle 5 (Use, retention and disclosure limitation): 7 controls for PII controllers and 3 controls for PII processors; • Principle 6 (Accuracy and quality): 1 control for PII controllers and 0 controls for PII processors; • Principle 7 (Openness, transparency and notice): 2 controls for PII controllers and 3 controls for PII processors; • Principle 8 (Individual participation and access): 5 controls for PII controllers and 1 control for PII processors; • Principle 9 (Accountability): 7 controls for PII controllers and 4 controls for PII processors; • Principle 10 (Information security): 2 controls for PII controllers and 1 control for PII processors; • Principle 11 (Privacy compliance): 1 control for PII controllers and 1 control for PII processors.
-	-	**Annex D**	**Mapping to General Data Protection Regulation**	

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
-	-		The GDPR defined rules for the handling of PII from EU citizens.	Articles from the GDPR related to ISO/IEC 27701: • 5 to 49, with exception for article 43 Subclauses from ISO/IEC 27701 related to the most articles from the GDPR are: • 5.2.1; • 6.3.1.1, 6.12.1.2, 6.13.1.1, 6.13.1.5, 6.15.1.1; • 7.2.2, 7.2.5, 7.2.8, 7.3.2, 7.3.6, 7.3.9, 7.5.1; • 8.5.1.
		Annex E	**Mapping to ISO/IEC 27018 and ISO/IEC 29151**	

ISO/IEC 27001:2013		ISO 27701:2019		Explanation
-	-		ISO/IEC 27018 provides guidance and controls for PII processors providing cloud services. ISO/IEC 29151 provides guidance and controls for PII controllers.	Clauses from ISO/IEC 27018 related to ISO/IEC 27701: • 5, 6, 7, 9, 11, 12, 13, 16, 18, A.2, A.3, A.5, A.6, A.8, A.10, A.11, and A.12 • Most clauses from ISO/IEC 27018 are related to clauses 6 and 8 of ISO/IEC 27701. Clauses from ISO/IEC 29151 related to ISO/IEC 27701: • 4, 5, 7, 8, 9, 11, 12, 13, 18, A.3, A.4, A.5, A.7, A.8, A.9, A.10, A.11, and A.13 • Most clauses from ISO/IEC 29151 are related to clauses 6 and 7 of ISO/IEC 27701.

		Annex F	**How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002**	**This annex provides guidance on:**
				• **how to extend the terms of an Information Security Management System (ISMS) so it can become a Privacy Information Management System (PIMS);**
				• **how to apply the standard.**
				  ○ **Use of the document as a whole;**
				  ○ **Use of specific requirements or guidance only;**
				  ○ **Use for refining the requirements of other standards.**

Check out ISO 27001 compliance software

To learn how to implement ISO 27001 through a step-by-step wizard and get all the necessary policies and procedures, sign up for a 30-day free trial of Conformio, the leading ISO 27001 compliance software.

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

Advisera Expert Solutions Ltd
for electronic business and business consulting

Our offices:
Zavizanska 12, 10000 Zagreb, Croatia
Via Maggio 1 C, Lugano, CH-6900, Switzerland
275 Seventh Ave, 7th Floor, New York, 10001, U.S.

Email: support@advisera.com
U.S. (international): +1 (646) 759 9933
United Kingdom (international): +44 1502 449001
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Australia: +61 3 4000 0020
Switzerland: +41 41 588 0722

EXPLORE **ADVISERA**

EUGDPR Academy · 27001 Academy · 9001 Academy · 14001 Academy · 45001 Academy · 13485 Academy · 9100 Academy

16949 Academy · 17025 Academy · 20000 Academy · Conformio · eTraining · AdviseraBooks

Advisera
Making certification simple.