

A woman with her hair in a ponytail, wearing a dark blazer over a white shirt, stands in a server room. She is holding a laptop and looking at the screen. The room is dimly lit with blue ambient light, and server racks with glowing lights are visible in the background. An orange triangle is in the top-left corner.

The key changes in ISO/IEC FDIS 27701

SGS



INTRODUCTION

ISO/IEC 27701 is an international standard for privacy information management systems (PIMS) published by ISO.

The first edition was released in 2019 (i.e., ISO/IEC 27701:2019) as an extension to ISO/IEC 27001 and ISO/IEC 27002. As a result of this approach, an organization must obtain the ISO/IEC 27001 certification before being ISO/IEC 27701 certified. In addition, the PIMS scope must be the same as or within the ISMS scope. Another reason for having to certify to ISO/IEC 27001 first is to ensure that, personal identifiable information (PII), being an important information asset of an organization,

must also have some information security governance and controls to protect its confidentiality, integrity and availability.

ISO/IEC 27701:2019 was written based on ISO/IEC 27001:2013 and ISO/IEC 27002:2013. In 2022, the latter two standards were replaced by ISO/IEC 27001:2022 and ISO/IEC 27002:2022, respectively, with significant changes in Annex A controls (read our [ISO/IEC 27001](#) and [ISO/IEC 27002](#) whitepapers for the key changes).

Following the release of ISO/IEC 27001:2022 in October 2022, ISO/IEC initiated the revision of ISO/IEC 27701:2019 in the same month.

After considering the comments from the usage community regarding the use of the first edition, ISO redrafted the standard as a stand-alone document. It is at the Final Draft International Standard (FDIS) stage as of the writing of this white paper. Ultimately, the approved FDIS will be registered as ISO/IEC 27701:2025 to supersede ISO/IEC 27701:2019.

This article compares the changes in ISO/IEC FDIS 27701 with ISO/IEC 27701:2019.

TITLE

ISO/IEC FDIS 27701 is retitled to Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance.

The title change reflects that ISO/IEC FDIS 27701 has no extension relationship with ISO/IEC 27001 and ISO/IEC 27002.

ISO/IEC FDIS 27701	ISO/IEC 27701:2019
Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

STRUCTURE & REQUIREMENTS

As aforementioned, ISO/IEC FDIS 27701 is redrafted as a stand-alone document. It applies the high-level structure developed by ISO to improve the alignment with other ISO management system standards, e.g., ISO 9001, ISO/IEC 20000-1, ISO/IEC 27001, ISO/IEC 42001 etc.

Consequently, an organization does not need to be ISO/IEC 27001 certified as a condition of attaining the ISO/IEC 27701 certification.

ISO/IEC FDIS 27701 Clauses 4 to 10 set out the requirements of the Privacy Information Management System (PIMS). An organization must demonstrate that it conforms to the requirements with no exclusion allowed when it claims conformity to the document.

In ISO/IEC 27701:2019, only clause 5 consists of PIMS requirements; clauses 6 to 8 are implementation guidance that an organization can choose to implement as appropriate.

TABLE 1 at the end of this whitepaper consists of the clause mapping of ISO/IEC FDIS 27701 and ISO/IEC 27701:2019.

SECURITY OF PII

Although ISO/IEC FDIS 27701 is no longer an extension of ISO/IEC 27001, security of PII is not abandoned in the new edition.

According to Clauses 6.1.2 (Privacy risk assessment) and 6.1.3 (Privacy risk treatment), an organization needs to identify “the privacy risk associated with the protection of privacy and information security risks within the scope of the Privacy information management system” and subsequently treat the risks by identifying and documenting the information security programme implemented with the appropriate security controls.

In Clause 6.1.3, 15 security elements are suggested to be addressed in the information security programme, including information security

risk management and 14 security domains. ISO/IEC 27001 and ISO/IEC 27002 are referenced in Clause 6.1.3, note 2.

In ISO/IEC FDIS 27701 Annex A, 29 possible information security controls are listed for PII controllers and PII processors.

ANNEXES A AND B

Like ISO/IEC 27001, ISO/IEC FDIS 27701 Annex A contains a list of possible privacy controls.

Generally, the controls and control objectives remain unchanged by comparing to ISO/IEC 27701:2019. The information security controls with additional implementation guidance in ISO/IEC 27701:2019 Clause 6 are moved to ISO/IEC FDIS 27701 Annex A.

The Annex A is comprised of 3 tables. Table A.1 contains controls applicable to PII controllers. Table A.2 contains controls applicable to PII processors and Table A.3 contains information security controls applicable to both PII controllers and PII processors. In summary, there are 31 controls for PII controllers, 18 controls for PII processors, and 29 controls for PII controllers and PII processors.

Some ISO/IEC 27001 practitioners believe that the ISO/IEC 27001 Annex A controls are exhaustive and no additional information security controls can be included in the ISMS. To avoid the ISO/IEC FDIS 27701 implementors having similar comprehension, ISO/IEC FDIS 27701 Clause 6.1.3 states: “The privacy controls listed in Annex A are not exhaustive and additional privacy controls can be included if needed.”

As the title suggests, ISO/IEC FDIS 27701 consists of implementation guidance for privacy and information security controls. The guidance is in Annex B (normative) - Implementation guidance for PII controllers and PII processors. The word “normative” seems to imply that the selected controls must be implemented according to the guidance in Annex B.

Nevertheless, ISO/IEC FDIS 27701 Clause 6.1.3 h) clarifies that an organization needs to consider the guidance in Annex B only for the implementation of controls.

In view of the content, there are no significant changes to the implementation guidance in ISO/IEC FDIS 27701 Annex B by comparing to that in ISO/IEC 27701:2019 Clauses 6 to 8, except for some minor editorial updates.

The TABLE 2 consists of control and implementation guidance mapping of ISO/IEC FDIS 27701 and ISO/IEC 27701:2019.

NOTE ON CERTIFICATION AND TRANSITION TO THE 2ND EDITION

Organizations who are seeking new certification or certified organizations seeking upgrade to the 2nd edition should consult their certification body regarding the latest certification arrangement and deadlines. As of the writing of this whitepaper, the certification and transition rules for the 2nd edition are not released yet. Historically, the certification and transition rules are released within 1-2 months after the release of the standard. The accreditation bodies will then adopt these rules, with or without additional requirements imposed by respective accreditation body.

SUMMARY

On 19 Dec 2024, ISO/IEC FDIS 27701 was registered for formal approval. Next, an 8-week FDIS ballot will be initiated before the new edition is officially launched to supersede ISO/IEC 27701:2019.

SGS will keep on top of the development of the standard and that of the certification and transition rules and will keep our clients and the certification community abreast of the transition plan to the new edition of ISO/IEC 27701 as soon as they come out.

TABLE 1

The table below maps the ISO/IEC FDIS 27701 clauses with that of the ISO/IEC 27701:2019 to illustrate the structural change of the new edition.

ISO/IEC FDIS 27701		ISO/IEC 27701:2019		REMARK
Clause 1	Scope	Clause 1	Scope	<ul style="list-style-type: none">Removed "...in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization." in the FDISRemoved the condition of requiring an organization to be a PII controller and / or PII processor processing PII within an ISMS
Clause 2	Normative references	Clause 2	Normative references	<ul style="list-style-type: none">Removed ISO/IEC 27000, ISO/IEC 27001 and ISO/IEC 27002 in the FDIS
Clause 3	Terms, definitions and abbreviations	Clause 3	Terms, definitions and abbreviations	<ul style="list-style-type: none">Removed the application of the terms and definitions in ISO/IEC 27000Added management system terms and definitions, e.g., organization, top management, policy, etc.Added standard-specific terms and definitions, e.g., customer, information security programme, statement of applicability
/	/	Clause 4	General	/
		Clause 4.1	Structure of this document	Removed in the FDIS
		Clause 4.2	Application of ISO/IEC 27001:2013 requirements	Removed in the FDIS
		Clause 4.3	Application of ISO/IEC 27002:2013 guidelines	Removed in the FDIS
		Clause 4.4	Customer	The definition of "customer" is retained in ISO/IEC FDIS 27701 Clause 4.2.
Clause 4	Context of the organization	Clause 5.2	Context of the organization	/
Clause 4.1	Understanding the organization and its context	Clause 5.2.1	Understanding the organization and its context	<ul style="list-style-type: none">Included the climate change requirement- "The organization shall determine whether climate change is a relevant issue."
Clause 4.2	Understanding the needs and expectations of interested parties	Clause 5.2.2	Understanding the needs and expectations of interested parties	<ul style="list-style-type: none">Include the climate change note- "Relevant interested parties can have requirements related to climate change."Added standard-specific requirements:<ul style="list-style-type: none">Parties that having interests or responsibilities associated with the processing of PII shall be determined as interested parties, including the PII principalsThe definition of "customer" in PIMS
Clause 4.3	Determining the scope of the privacy information management system	Clause 5.2.3	Determining the scope of the information security management system	<ul style="list-style-type: none">Removed the note "The determination of the scope of the PIMS can require revising the scope of the information security management system, because of the extended interpretation of "information security" according to 5.1."
Clause 4.4	Privacy information management system	Clause 5.2.4	Information security management system	<ul style="list-style-type: none">Removed the requirement that PIMS shall be developed in accordance with ISO/IEC 27001:2013 Clauses 4 to 10
Clause 5	Leadership	Clause 5.3	Leadership	/
Clause 5.1	Leadership & commitment	Clause 5.3.1	Leadership & commitment	/
Clause 5.2	Privacy Policy	Clause 5.3.2	Policy	/
Clause 5.3	Roles, responsibilities and authorities	Clause 5.3.3	Organizational roles, responsibilities & authorities	/
Clause 6	Planning	Clause 5.4	Planning	/
Clause 6.1	Actions to address risks and opportunities	Clause 5.4.1	Actions to address risks and opportunities	/
Clause 6.1.1	General	Clause 5.4.1.1	General	/
Clause 6.1.2	Privacy risk assessment	Clause 5.4.1.2	Information security risk assessment	/
Clause 6.1.3	Privacy risk treatment	Clause 5.4.1.3	Information security risk treatment	/
Clause 6.2	Privacy objectives and planning to achieve them	Clause 5.4.2	Information security objectives and planning to achieve them	/
Clause 6.3	Planning of changes	/	/	/

ISO/IEC FDIS 27701		ISO/IEC 27701:2019		REMARK
Clause 7	Support	Clause 5.5	Support	/
Clause 7.1	Resources	Clause 5.5.1	Resources	/
Clause 7.2	Competence	Clause 5.5.2	Competence	/
Clause 7.3	Awareness	Clause 5.5.3	Awareness	/
Clause 7.4	Communication	Clause 5.5.4	Communication	/
Clause 7.5	Documented information	Clause 5.5.5	Documented information	/
Clause 7.5.1	General	Clause 5.5.5.1	General	/
Clause 7.5.2	Creating and updating documented information	Clause 5.5.5.2	Creating and updating	/
Clause 7.5.3	Control of documented information	Clause 5.5.5.3	Control of documented information	/
Clause 8	Operation	Clause 5.6	Operation	/
Clause 8.1	Operational planning and control	Clause 5.6.1	Operational planning and control	/
Clause 8.2	Privacy risk assessment	Clause 5.6.2	Information security risk assessment	/
Clause 8.3	Privacy risk treatment	Clause 5.6.3	Information security risk treatment	/
Clause 9	Performance	Clause 5.7	Performance evaluation	/
Clause 9.1	Monitoring, measurement, analysis and evaluation	Clause 5.7.1	Monitoring, measurement, analysis and evaluation	<ul style="list-style-type: none">Excluded two points that are commonly seen in other management system standards:<ul style="list-style-type: none">Who shall monitor and measureWho shall analyse and evaluate these results
Clause 9.2	Internal audit	Clause 5.7.2	Internal audit	/
Clause 9.2.1	General			/
Clause 9.2.2	Internal audit programme			/
Clause 9.3	Management review	Clause 5.7.3	Management review	/
Clause 9.3.1	General			/
Clause 9.3.2	Management review inputs			<ul style="list-style-type: none">Excluded three points that are commonly seen in other management system standards:<ul style="list-style-type: none">Fulfilment of objectivesFeedback from interested partiesResults of risk assessment and status of risk treatment plan
Clause 9.3.3	Management review results			/
Clause 10	Improvement	Clause 5.8	Improvement	/
Clause 10.1	Continual improvement	Clause 5.8.2	Continual improvement	/
Clause 10.2	Nonconformity and corrective action	Clause 5.8.1	Nonconformity and corrective action	/
Annex A (normative)	PIMS reference control objectives and controls for PII Controllers and PII Processors	/	/	/
Table A.1	Control objectives and controls for PII controllers	Annex A (normative)	PIMS-specific reference control objectives and controls (PII Controllers)	<ul style="list-style-type: none">The controls and control objectives remain unchanged with minor editorial changes to two controlsTotal 31 controls for PII controllers
Table A.2	Control objectives and controls for PII processors	Annex B (normative)	PIMS-specific reference control objectives and controls (PII Processors)	<ul style="list-style-type: none">The controls and control objectives remain unchanged with:<ul style="list-style-type: none">Minor editorial changes to several controlsRenamed control "Obligations to PII principals" to "Comply with obligations to PII principals"Total 18 controls for PII processors
Table A.3	Control objectives and controls for PII controllers and PII processors	Clause 6	PIMS-specific guidance related to ISO/IEC 27002	<ul style="list-style-type: none">Table A.3 is a list of non-exclusive information security controls for PII controllers and PII processorsTotal 29 information security controlsThe information security controls with additional implementation guidance in ISO/IEC 27701:2019 Clause 6 are extracted to the tableMinor editorial changes to two controls

ISO/IEC FDIS 27701		ISO/IEC 27701:2019		REMARK
Annex B (normative)	Implementation guidance for PII Controllers and PII processors	/	/	/
B.1	Implementation guidance for PII controllers	Clause 7	Additional ISO/IEC 27002 guidance for PII controllers	• The implementation guidance remains unchanged with minor editorial changes to some controls
B.2	Implementation guidance for PII processors	Clause 8	Additional ISO/IEC 27002 guidance for PII processors	
B.3	Implementation guidance for PII controllers and PII processors	Clause 6	PIMS-specific guidance related to ISO/IEC 27002	
Annex C (informative)	Mapping to ISO/IEC 29100	Annex C (informative)	Mapping to ISO/IEC 29100	/
Annex D (informative)	Mapping to the General Data Protection Regulation	Annex D (informative)	Mapping to the General Data Protection Regulation	/
Annex E (informative)	Mapping to ISO/IEC 27018 and ISO/IEC 29151	Annex E (informative)	Mapping to ISO/IEC 27018 and ISO/IEC 29151	/
Annex F (informative)	Correspondence with ISO/IEC 27701:2019	/	/	New Annex
/	/	Annex F (informative)	How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002	Removed

TABLE 2

Mapping the controls and implementation guidance for PII controllers to ISO/IEC 27701:2019.

ISO/IEC FDIS 27701		ISO/IEC 27701:2019			
CONTROL		IMPLEMENTATION GUIDANCE	CONTROL		IMPLEMENTATION GUIDANCE
	Conditions for collection and processing	B.1.2	A.7.2	Conditions for collection and processing	Clause 7.2
A.1.2.2	Identify and document purpose	B.1.2.2	A.7.2.1	Identify and document purpose	Clause 7.2.1
A.1.2.3	Identify lawful basis	B.1.2.3	A.7.2.2	Identify lawful basis	Clause 7.2.2
A.1.2.4	Determine when and how consent is to be obtained	B.1.2.4	A.7.2.3	Determine when and how consent is to be obtained	Clause 7.2.3
A.1.2.5	Obtain and record consent	B.1.2.5	A.7.2.4	Obtain and record consent	Clause 7.2.4
A.1.2.6	Privacy impact assessment	B.1.2.6	A.7.2.5	Privacy impact assessment	Clause 7.2.5
A.1.2.7	Contracts with PII processors	B.1.2.7	A.7.2.6	Contracts with PII processors	Clause 7.2.6
A.1.2.8	Joint PII controller	B.1.2.8	A.7.2.7	Joint PII controller	Clause 7.2.7
A.1.2.9	Records related to processing PII	B.1.2.9	A.7.2.8	Records related to processing PII	Clause 7.2.8
	Obligations to PII principals	B.1.3	A.7.3	Obligations to PII principals	Clause 7.3
A.1.3.2	Determining and fulfilling obligations to PII principals	B.1.3.2	A.7.3.1	Determining and fulfilling obligations to PII Principals	Clause 7.3.1
A.1.3.3	Determining information for PII principals	B.1.3.3	A.7.3.2	Determining information for PII principals	Clause 7.3.2
A.1.3.4	Providing information to PII principals	B.1.3.4	A.7.3.3	Providing information to PII principals	Clause 7.3.3
A.1.3.5	Providing mechanism to modify or withdraw consent	B.1.3.5	A.7.3.4	Providing mechanism to modify or withdraw consent	Clause 7.3.4
A.1.3.6	Providing mechanism to object to PII processing	B.1.3.6	A.7.3.5	Providing mechanism to object to PII processing	Clause 7.3.5
A.1.3.7	Access, correction or erasure	B.1.3.7	A.7.3.6	Access, correction and/or erasure	Clause 7.3.6
A.1.3.8	PII controllers' obligations to inform third parties	B.1.3.8	A.7.3.7	PII controllers' obligations to inform third parties	Clause 7.3.7
A.1.3.9	Providing copy of PII processed	B.1.3.9	A.7.3.8	Providing copy of PII processed	Clause 7.3.8
A.1.3.10	Handling requests	B.1.3.10	A.7.3.9	Handling requests	Clause 7.3.9
A.1.3.11	Automated decision making	B.1.3.11	A.7.3.10	Automated decision making	Clause 7.3.10
	Privacy by design and by privacy default	B.1.4	A.7.4	Privacy by design and privacy by default	Clause 7.4
A.1.4.2	Limit collection	B.1.4.2	A.7.4.1	Limit collection	Clause 7.4.1
A.1.4.3	Limit processing	B.1.4.3	A.7.4.2	Limit processing	Clause 7.4.2
A.1.4.4	Accuracy and quality	B.1.4.4	A.7.4.3	Accuracy and quality	Clause 7.4.3
A.1.4.5	PII minimization objectives	B.1.4.5	A.7.4.4	PII minimization objectives	Clause 7.4.4

ISO/IEC FDIS 27701		ISO/IEC 27701:2019			
CONTROL		IMPLEMENTATION GUIDANCE	CONTROL		IMPLEMENTATION GUIDANCE
A.1.4.6	PII de-identification and deletion at the end of processing	B.1.4.6	A.7.4.5	PII de-identification and deletion at the end of processing	Clause 7.4.5
A.1.4.7	Temporary files	B.1.4.7	A.7.4.6	Temporary files	Clause 7.4.6
A.1.4.8	Retention	B.1.4.8	A.7.4.7	Retention	Clause 7.4.7
A.1.4.9	Disposal	B.1.4.9	A.7.4.8	Disposal	Clause 7.4.8
A.1.4.10	PII transmission controls	B.1.4.10	A.7.4.9	PII transmission controls	Clause 7.4.9
	PII sharing, transfer and disclosure	B.1.5	A.7.5	PII sharing, transfer and disclosure	Clause 7.5
A.1.5.2	Identify basis for PII transfer between jurisdictions	B.1.5.2	A.7.5.1	Identify basis for PII transfer between jurisdictions	Clause 7.5.1
A.1.5.3	Countries and international organizations to which PII can be transferred	B.1.5.3	A.7.5.2	Countries and international organizations to which PII can be transferred	Clause 7.5.2
A.1.5.4	Records of transfer of PII	B.1.5.4	A.7.5.3	Records of transfer of PII	Clause 7.5.3
A.1.5.5	Records of PII disclosures to third parties	B.1.5.5	A.7.5.4	Records of PII disclosures to third parties	Clause 7.5.4

Mapping the controls and implementation guidance for PII processors to ISO/IEC 27701:2019.

ISO/IEC FDIS 27701		ISO/IEC 27701:2019			
CONTROL		IMPLEMENTATION GUIDANCE	CONTROL		IMPLEMENTATION GUIDANCE
	Conditions for collection and processing	B.2.2	B.8.2	Conditions for collection and processing	Clause 8.2
A.2.2.2	Customer agreement	B.2.2.2	B.8.2.1	Customer agreement	Clause 8.2.1
A.2.2.3	Organization's purposes	B.2.2.3	B.8.2.2	Organization's purposes	Clause 8.2.2
A.2.2.4	Marketing and advertising use	B.2.2.4	B.8.2.3	Marketing and advertising use	Clause 8.2.3
A.2.2.5	Infringing instruction	B.2.2.5	B.8.2.4	Infringing instruction	Clause 8.2.4
A.2.2.6	Customer obligations	B.2.2.6	B.8.2.5	Customer obligations	Clause 8.2.5
A.2.2.7	Records related to processing PII	B.2.2.7	B.8.2.6	Records related to processing PII	Clause 8.2.6
	Obligations to PII principals	B.2.3	B.8.3	Obligations to PII principals	Clause 8.3
A.2.3.2	Comply with obligations to PII principals	B.2.3.2	B.8.3.1	Comply with obligations to PII principals	Clause 8.3.1
	Privacy by design and privacy by default	B.2.4	B.8.4	Privacy by design and privacy by default	Clause 8.4
A.2.4.2	Temporary files	B.2.4.2	B.8.4.1	Temporary files	Clause 8.4.1
A.2.4.3	Return, transfer or disposal of PII	B.2.4.3	B.8.4.2	Return, transfer or disposal of PII	Clause 8.4.2
A.2.4.4	PII transmission controls	B.2.4.4	B.8.4.3	PII transmission controls	Clause 8.4.3
	PII sharing, transfer and disclosure	B.2.5	B.8.5	PII sharing, transfer and disclosure	Clause 8.5
A.2.5.2	Basis for PII transfer between jurisdictions	B.2.5.2	B.8.5.1	Basis for PII transfer between jurisdictions	Clause 8.5.1
A.2.5.3	Countries and international organizations to which PII can be transferred	B.2.5.3	B.8.5.2	Countries and international organizations to which PII can be transferred	Clause 8.5.2
A.2.5.4	Records of PII disclosures to third parties	B.2.5.4	B.8.5.3	Records of PII disclosures to third parties	Clause 8.5.3
A.2.5.5	Notification of PII disclosure requests	B.2.5.5	B.8.5.4	Notification of PII disclosure requests	Clause 8.5.4
A.2.5.6	Legally binding PII disclosures	B.2.5.6	B.8.5.5	Legally binding PII disclosures	Clause 8.5.5
A.2.5.7	Disclosure of subcontractors used to process PII	B.2.5.7	B.8.5.6	Disclosure of subcontractors used to process PII	Clause 8.5.6
A.2.5.8	Engagement of a subcontractor to process PII	B.2.5.8	B.8.5.7	Engagement of a subcontractor to process PII	Clause 8.5.7
A.2.5.9	Change of subcontractor to process PII	B.2.5.9	B.8.5.8	Change of subcontractor to process PII	Clause 8.5.8

Mapping the controls and implementation guidance for PII controllers and PII processors to ISO/IEC 27701:2019 and ISO/IEC 27002:2022.

ISO/IEC FDIS 27701		ISO/IEC 27701:2019		ISO/IEC 27002:2022	
A.3.3	Policies for information security	Clause 6.2.1.1	Conditions for collection & processing	Clause 5.1	Policies for information security
		Clause 6.2.1.2	Identify and document purpose		
A.3.4	Information security roles and responsibilities	Clause 6.3.1.1	Information security roles and responsibilities	Clause 5.2	Information security roles and responsibilities
A.3.5	Classification of information	Clause 6.5.2.1	Classification of information	Clause 5.12	Classification of information
A.3.6	Labelling of information	Clause 6.5.2.1	Labelling of information	Clause 5.13	Labelling of information
A.3.7	Information transfer	Clause 6.10.2.1	Information transfer policies and procedures	Clause 5.14	Information transfer
		Clause 6.10.2.2	Agreements for information transfer		
		Clause 6.10.2.3	Electronic messaging		
A.3.8	Identity management	Clause 6.6.2.1	User registration and de-registration	Clause 5.16	Identity management
A.3.9	Access rights	Clause 6.6.2.2	User access provisioning	Clause 5.18	Access rights
		Clause 6.6.2.5	Review of user access rights		
		Clause 6.6.2.6	Removal or adjustment of access rights		
A.3.10	Addressing information security within supplier agreements	Clause 6.12.1.1	Information security policy for supplier relationships	Clause 5.20	Addressing information security within supplier agreements
		Clause 6.12.1.2	Addressing security within supplier agreements		
A.3.11	Information security incident management planning and preparation	Clause 6.13.1.4	Assessment of and decisions on information security events	Clause 5.24	Information security incident management planning and preparation
A.3.12	Response to information security incidents	Clause 6.13.1.5	Response to information security incidents	Clause 5.26	Response to information security incidents
A.3.13	Legal, statutory, regulatory and contractual requirements	Clause 6.15.1.1	Identification of applicable legislation and contractual requirements	Clause 5.31	Legal, statutory, regulatory and contractual requirements
		Clause 6.15.1.5	Regulation of cryptographic controls		
A.3.14	Protection of records	Clause 6.15.1.3	Protection of records	Clause 5.33	Protection of records
A.3.15	Independent review of information security	Clause 6.15.2.1	Independent review of information security	Clause 5.35	Independent review of information security
A.3.16	Compliance with policies, rules and standards for information security	Clause 6.15.2.2	Compliance with security policies and standards	Clause 5.36	Compliance with policies, rules and standards for information security
		Clause 6.15.2.3	Technical compliance review		
A.3.17	Information security awareness, education and training	Clause 6.4.2.2	Information security awareness, education and training	Clause 6.3	Information security awareness, education and training
A.3.18	Confidentiality or non-disclosure agreements	Clause 6.10.2.4	Confidentiality or non-disclosure agreements	Clause 6.6	Confidentiality or non-disclosure agreements
A.3.19	Clear desk and clear screen	Clause 6.8.2.9	Clear desk and clear screen policy	Clause 7.7	Clear desk and clear screen
A.3.20	Storage media	Clause 6.5.3.1	Management of removable media	Clause 7.10	Storage media
		Clause 6.5.3.2	Disposal of media		
		Clause 6.5.3.3	Physical media transfer		
		Clause 6.8.2.5	Removal of assets		
A.3.21	Secure disposal or re-use of equipment	Clause 6.8.2.7	Secure disposal or re-use of equipment	Clause 7.14	Secure disposal or re-use of equipment
A.3.22	User endpoint devices	Clause 6.3.2.1	Mobile device policy	Clause 8.1	User endpoint devices
		Clause 6.8.2.8	Unattended user equipment		
A.3.23	Secure authentication	Clause 6.6.4.2	Secure log-on procedures	Clause 8.5	Secure authentication
A.3.24	Information backup	Clause 6.9.3.1	Information backup	Clause 8.13	Information backup
A.3.25	Logging	Clause 6.9.4.1	Event logging	Clause 8.15	Logging
		Clause 6.9.4.2	Protection of log information		
		Clause 6.9.4.3	Administrator and operator logs		

ISO/IEC FDIS 27701		ISO/IEC 27701:2019		ISO/IEC 27002:2022	
A.3.26	Use of cryptography	Clause 6.7.1.1	Policy on the use of cryptographic controls	Clause 8.24	Use of cryptography
		Clause 6.7.1.2	Key management		
A.3.27	Secure development life cycle	Clause 6.11.2.1	Secure development policy	Clause 8.25	Secure development life cycle
A.3.28	Application security requirements	Clause 6.11.1.2	Securing application services on public networks	Clause 8.26	Application security requirements
		Clause 6.11.1.3	Protecting application services transactions		
A.3.29	Secure system architecture and engineering principles	Clause 6.11.2.5	Secure systems engineering principles	Clause 8.27	Secure system architecture and engineering principles
A.3.30	Outsourced development	Clause 6.11.2.7	Outsourced development	Clause 8.30	Outsourced development
A.3.31	Test information	Clause 6.11.3.1	Protection of test data	Clause 8.33	Test information



When you need to be sure