August 2019

ISO/IEC 27701 Privacy Information Management

Comparing ISO/IEC 27701 and BS 10012

Mapping guide

bsi.

...making excellence a habit.™

Mapping ISO/IEC 27701 to BS 10012:2017

BS ISO/IEC 27701:2019 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to information security standards BS EN ISO/IEC 27001 and BS EN ISO/IEC 27002.

It's the first international management system standard to help organizations manage personally identifiable information and respond to jurisdictional differences in privacy regulations globally. However, **BS 10012 Data protection - Specification for a personal information management system** is a British standard aligned to the GDPR and UK Data Protection Act 2018 that's used by organizations globally to put processes and controls in place to manage personal information.

This guide shows how the different clauses in ISO/IEC 27701 map to the clauses in BS 10012. It's designed for guidance purposes only and aims to help you understand the degree of correspondence between the two standards and the different ways they express privacy requirements.

ISO/IEC 27701 clause	ISO/IEC 27701 topic	BS 10012 topic	BS 10012 clause
5.2.1	Understanding the organization and its context	Understanding the organization and its context	4.1
5.2.2	Understanding the needs and expectations of interested parties	Understanding the needs and expectations of interested parties	4.2
5.2.3	Determining the scope of the information security management system	Determining the scope of the personal information management system	4.3
5.2.4	Information security management system	Personal information management system	4.4
5.3.1	Leadership and commitment	Leadership and commitment	5.1
5.3.2	Policy	Policy	5.2
5.3.3	Organizational roles, responsibilities and authorities	Organizational roles, responsibilities and authorities	5.3
5.4.1	Actions to address risks and opportunities	Actions to address risks and opportunities	6.1
5.4.2	Information security objectives and planning to achieve them	Embedding the PIMS in the organization's culture	5.4
		PIMS objectives and planning to achieve them	6.2
5.5.1	Resources	Resources	7.1
5.5.2	Competence	Competence	7.2
5.5.3	Awareness	Awareness	7.3

ISO/IEC 27701 clause	ISO/IEC 27701 topic	BS 10012 topic	BS 10012 clause
5.5.3	Awareness	Awareness	7.3
5.5.4	Communication	Communication	7.4
5.5.5	Documented information	Documented information	7.5
5.6.1	Operational planning and control	Operational planning and control	8.1
5.6.2	Information security risk assessment	Risk assessment and treatment	8.2.3
5.6.3	Information security risk treatment	Risk assessment and treatment	8.2.3
5.7.1	Monitoring, measurement, analysis and evaluation	Keeping PIMS up to date Maintenance Monitoring, measurement, analysis and evaluation	8.2.5 8.2.13 9.1
5.7.2	Internal audit	Internal audit	9.2
5.7.3	Management review	Management review	9.3
5.8.1	Nonconformity and corrective action	Nonconformity and corrective action Preventative actions	10.1 10.2
5.8.2	Continual improvement	Continual improvement	10.3

ISO/IEC 27701 clause	ISO/IEC 27701 topic	BS 10012 topic	BS 10012 clause
6.2.1	Management direction for information security	Policy	5.2
6.3.1	Internal organization	Embedding the PIMS in the organization's culture	5.4
		Key appointments	8.2.1
6.3.2	Mobile devices and teleworking	Security issues	8.2.11
6.4.1	Prior to employment	Training and awareness	8.2.4
6.4.2	During employment	Training and awareness	8.2.4
6.4.3	Termination and change of employment	Training and awareness	8.2.4
6.5.1	Responsibility for assets	Identifying and recording uses of personal information	8.2.2
6.5.2	Information classification	Identifying and recording uses of personal information	8.2.2
6.5.3	Media handling	Security issues	8.2.11
6.6.1	Business requirements of access control	Security issues	8.2.11
6.6.2	User access management	Security issues	8.2.11
6.6.3	User responsibilities	Security issues	8.2.11
6.6.4	System and application access control	Security issues	8.2.11
6.7.1	Cryptographic controls	Security issues	8.2.11
6.8.1	Secure areas	Security issues	8.2.11
6.8.2	Equipment	Security issues	8.2.11
6.9.1	Operational procedures and responsibilities	Operational planning and control	8.1
6.9.2	Protection from malware	Security issues	8.2.11
6.9.3	Backup	Security issues	8.2.11
6.9.4	Logging and monitoring	Security issues	8.2.11
6.9.5	Control of operational software	Security issues	8.2.11
6.9.6	Technical vulnerability management	Security issues	8.2.11
6.9.7	Information systems audit considerations	Internal audit	9.2
6.10.1	Network security management	Security issues	8.2.11

ISO/IEC 27701 clause	ISO/IEC 27701 topic	BS 10012 topic	BS 10012 clause
6.10.2	Information transfer	Security issues	8.2.11
6.11.1	Security requirements of information systems	Security issues	8.2.11
6.11.2	Security in development and support processes	Security issues	8.2.11
6.11.3	Test data	Security issues	8.2.11
6.12.1	Information security in supplier relationships	Security issues	8.2.11
6.12.2	Supplier service delivery management	Security issues	8.2.11
6.13.1	Management of information security incidents and improvements	Security issues	8.2.11
6.14.1	Information security continuity	Maintenance	8.2.13
6.14.2	Redundancies	Maintenance	8.2.13
6.15.1	Compliance with legal and contractual requirements	Fair, lawful and transparent processing	8.2.6
6.15.2	Information security reviews	Fair, lawful and transparent processing	8.2.6
7.2.1	Identify and document purpose	Identifying and recording uses of personal information Processing for specific legitimate purposes	8.2.2 8.2.7
7.2.2	Identify lawful basis	Fair, lawful and transparent processing	8.2.6
7.2.3	Determine when and how consent is to be obtained	Fair, lawful and transparent processing	8.2.6
7.2.4	Obtain and record consent	Fair, lawful and transparent processing	8.2.6
7.2.5	Privacy impact assessment	Actions to address risks and opportunities Risk assessment and treatment	6.1 8.2.3
7.2.6	Contracts with PII processors	Security issues	8.2.11
7.2.7	Joint PII controller	Risk assessment and treatment	8.2.3
7.2.8	Records related to processing PII	Identifying and recording uses of personal information	8.2.2
7.3.1	Determining and fulfilling obligations to PII principals	Fair, lawful and transparent processing Rights of natural persons	8.2.6 8.2.12
7.3.2	Determining information for PII principals	Fair, lawful and transparent processing	8.2.6

ISO/IEC 27701 clause	ISO/IEC 27701 topic	BS 10012 topic	
7.3.3	Providing information to PII principals	Fair, lawful and transparent processing	8.2.6
7.3.4	Providing mechanism to modify or withdraw consent	Fair, lawful and transparent processing	8.2.6
7.3.5	Providing mechanism to object to PII processing	Rights of natural persons	8.2.12
7.3.6	Access, correction and/or erasure	Accuracy	8.2.9
7.3.7	PII controllers' obligations to inform third parties	Rights of natural persons	8.2.12
7.3.8	Providing copy of PII processed	Rights of natural persons	8.2.12
7.3.9	Handling requests	Rights of natural persons	8.2.12
7.3.10	Automated decision making	Rights of natural persons	8.2.12
7.4.1	Limit collection	Actions to address risks and opportunities	6.1
		Adequate, relevant and in line with data minimization principals	8.2.8
7.4.2	Limit processing	Actions to address risks and opportunities	6.1
		Adequate, relevant and in line with data minimization principals	8.2.8
7.4.3	Accuracy and quality	Accuracy	8.2.9
7.4.4	PII minimization objectives	Adequate, relevant and in line with data minimization principals	8.2.8
7.4.5	PII de-identification and deletion at the end of processing	Retention and disposal	8.2.10
7.4.6	Temporary files	Security issues	8.2.11
7.4.7	Retention	Retention and disposal	8.2.10
7.4.8	Disposal	Retention and disposal	8.2.10
7.4.9	PII transmission controls	Security issues	8.2.11
7.5.1	Identify basis for PII transfer between jurisdictions	Security issues	8.2.11
7.5.2	Countries and international organizations to which PII can be transferred	Security issues	8.2.11
7.5.3	Records of transfer of PII	Security issues	8.2.11
7.5.4	Records of PII disclosure to third parties	Security issues	8.2.11

ISO/IEC 27701 clause	ISO/IEC 27701 topic	BS 10012 topic	BS 10012 clause
8.2.1	Customer agreement	Security issues	8.2.11
8.2.2	Organization's purposes	Security issues	8.2.11
8.2.3	Marketing and advertising use	Security issues	8.2.11
8.2.4	Infringing instruction	Security issues	8.2.11
8.2.5	Customer obligations	Security issues	8.2.11
8.2.6	Records related to processing PII	Security issues	8.2.11
8.3.1	Obligations to PII principals	Fair, lawful and transparent processing	8.2.6
8.4.1	Temporary files	Retention and disposal	8.2.10
8.4.2	Return, transfer or disposal of PII	Retention and disposal	8.2.10
8.4.3	PII transmission controls	Security issues	8.2.11
8.5.1	Basis for PII transfer between jurisdictions	Security issues	8.2.11
8.5.2	Countries and international organizations to which PII can be transferred	Security issues	8.2.11
8.5.3	Records of PII disclosure to third parties	Security issues	8.2.11
8.5.4	Notification of PII disclosure requests	Security issues	8.2.11
8.5.5	Legally binding PII disclosures	Security issues	8.2.11
8.5.6	Disclosures of subcontractors used to process PII	Security issues	8.2.11
8.5.7	Engagement of a subcontractor to process PII	Security issues	8.2.11
8.5.8	Change of subcontractor to process PII	Security issues	8.2.11

Mapping BS 10012:2017 to ISO/IEC 27701

BS 10012 clause	BS 10012 topic	ISO/IEC 27701 topic	ISO/IEC 27701 clause
4.1	Understanding the organization and its context	Understanding the organization and its context	5.2.1
4.2	Understanding the needs and expectations of interested parties	Understanding the needs and expectations of interested parties	5.2.2
4.3	Determining the scope of the personal information management system	Determining the scope of the information security management system	5.2.3
4.4	Personal information management system	Information security management system	5.2.4
5.1	Leadership and commitment	Leadership and commitment	5.3.1
5.2	Policy	Policy	5.3.2
		Management direction for information security	6.2.1
5.3	Organizational roles, responsibilities and authorities	Organizational roles, responsibilities and authorities	5.3.3
		Internal organization	6.3.1
5.4	Embedding the PIMS in the organization's culture	Information security objectives and planning to achieve them	5.4.2
		Internal organization	6.3.1
6.1	Actions to address risks and opportunities	Actions to address risks and opportunities	5.4.1
		Privacy impact assessment	7.2.5
		Limit collection	7.4.1
		Limit processing	7.4.2
6.2	PIMS objectives and planning to achieve them	Information security objectives and planning to achieve them	5.4.2
7.1	Resources	Resources	5.5.1
7.2	Competence	Competence	5.5.2
7.3	Awareness	Awareness	5.5.3
7.4	Communication	Communication	5.5.4

BS 10012 clause	BS 10012 topic	ISO/IEC 27701 topic	ISO/IEC 27701 clause
7.5	Documented information	Documented information	5.5.5
8.1	Operational planning and control	Operational planning and control	5.6.1
		Operational procedures and responsibilities	6.9.1
8.2.1	Key appointments	Organizational roles, responsibilities and authorities	5.3.3
		Internal organization	6.3.1
8.2.2	Identifying and recording uses of personal information	Responsibility for assets	6.5.1
		Information classification	6.5.2
		Identify and document purpose	7.2.1
		Records related to processing PII	7.2.8
8.2.3	Risk assessment and treatment	Information security risk assessment	5.6.2
		Information security risk treatment	5.6.3
		Privacy impact assessment	7.2.5
		Joint PII controller	7.2.7
8.2.4	Training and awareness	Prior to employment	6.4.1
		During employment	6.4.2
		Termination and change of employment	6.4.3
8.2.5	Keeping PIMS up to date	Monitoring, measurement, analysis and evaluation	5.7.1
8.2.6	Fair, lawful and transparent processing	Compliance with legal and contractual requirements	6.15.1
		Information security reviews	6.15.2
		Identify lawful basis	7.2.2
		Determine when and how consent is to be obtained	7.2.3
		Obtain and record consent	7.2.4
		Determining and fulfilling obligations to PII principals	7.3.1
		Determining information for PII principals	7.3.2
		Providing information to PII principals	7.3.3
		Providing mechanism to modify or withdraw consent	7.3.4
		Obligations to PII principals	8.3.1
8.2.7	Processing for specific legitimate purposes	Identify and document purpose	7.2.1

BS 10012 clause	BS 10012 topic	ISO/IEC 27701 topic	ISO/IEC 27701 clause
8.2.8	Adequate, relevant and in line with data minimization principals	Limit collection	7.4.1
		Limit processing	7.4.2
		PII minimization objectives	7.4.4
8.2.9	Accuracy	Access, correction and/or erasure	7.3.6
		Accuracy and quality	7.4.3
8.2.11	Security issues	Mobile devices and teleworking	6.3.2
		Media handling	6.5.3
		Business requirements of access control	6.6.1
		User access management	6.6.2
		User responsibilities	6.6.3
		System and application access control	6.6.4
		Cryptographic controls	6.7.1
		Secure areas	6.8.1
		Equipment	6.8.2
		Protection from malware	6.9.2
		Backup	6.9.3
		Logging and monitoring	6.9.4
		Control of operational software	6.9.5
		Technical vulnerability management	6.9.6
		Network security management	6.10.1
		Information transfer	6.10.2
		Security requirements of information systems	6.11.1
		Security in development and support processes	6.11.2
		Test data	6.11.3
		Information security in supplier relationships	6.12.1
		Supplier service delivery management	6.12.2
		Management of information security incidents and improvements	6.13.1
		Contracts with PII processors	7.2.6
		Temporary files	7.4.6
		PII transmission controls	7.4.9
		Identify basis for PII transfer between jurisdictions	7.5.1
		Countries and international organizations to which PII can be transferred	7.5.2
		Records of transfer of PII	7.5.3
		Records of PII disclosure to third parties	7.5.4
		Customer agreement	8.2.1
		Organization's purposes	8.2.2

BS 10012 clause	BS 10012 topic	ISO/IEC 27701 topic	ISO/IEC 27701 clause
8.2.11 (continued)	Security issues (continued)	Marketing and advertising use	8.2.3
		Infringing instruction	8.2.4
		Customer obligations	8.2.5
		Records related to processing PII	8.2.6
		PII transmission controls	8.4.3
		Basis for PII transfer between jurisdictions	8.5.1
		Countries and international organizations to which PII can be transferred	8.5.2
		Records of PII disclosure to third parties	8.5.3
		Notification of PII disclosure requests	8.5.4
		Legally binding PII disclosures	8.5.5
		Disclosures of subcontractors used to process PII	8.5.6
		Engagement of a subcontractor to process PII	8.5.7
		Change of subcontractor to process PII	8.5.8
8.2.12	Rights of natural persons	Determining and fulfilling obligations to PII principals	7.3.1
		Providing mechanism to object to PII processing	7.3.5
		PII controllers' obligations to inform third parties	7.3.7
		Providing copy of PII processed	7.3.8
		Handling requests	7.3.9
		Automated decision making	7.3.10
8.2.13	Maintenance	Monitoring, measurement, analysis and evaluation	5.7.1
		Information security continuity	6.14.1
		Redundancies	6.14.2
9.1	Monitoring, measurement, analysis and evaluation	Monitoring, measurement, analysis and evaluation	5.7.1
9.2	Internal audit	Internal audit	5.7.2
		Information systems audit considerations	6.9.7
9.3	Management review	Management review	5.7.3
10.1	Nonconformity and corrective action	Nonconformity and corrective action	5.8.1
10.2	Preventative actions	Nonconformity and corrective action	5.8.1
10.3	Continual improvement	Continual improvement	5.8.2

Why BSI?

BSI has been at the forefront of information security standards since 1995, having produced the world's first standard, BS 7799, now ISO/IEC 27001, the world's most popular information security standard. And we haven't stopped there, addressing the new emerging issues such as privacy, cyber and cloud security. That's why we're best placed to help you

Working with over 86,000 clients across 193 countries, BSI is a truly international business with skills and experience across a number of sectors including automotive, aerospace, built environment, food, and healthcare. Through its expertise in Standards Development and Knowledge Solutions, Assurance and Professional Services, BSI improves business performance to help clients grow sustainably, manage risk and ultimately be more resilient.

BSI/UK/1592/SC/0719/EN/GRP

Our products and services

Knowledge

The core of our business centres on the knowledge that we create and impart to our clients.
In the standards arena we continue to build our reputation as an expert body, bringing together experts from industry to shape standards at local, regional and international levels.
In fact, BSI originally created eight of the world's top 10 management system standards.

Assurance

Independent assessment of the conformity of a process or product to a particular standard ensures that our clients perform to a high level of excellence. We train our clients in world-class implementation and auditing techniques to ensure they maximize the benefits of standards.

Compliance

To experience real, long-term benefits, our clients need to ensure ongoing compliance to a regulation, market need or standard so that it becomes an embedded habit. We provide a range of services and differentiated management tools which help facilitate this process.

bsi.

BSI UK
389 Chiswick High Road
London W4 4AL
United Kingdom

T: +44 345 086 9001
E: cservices@bsigroup.com
bsigroup.com

Find out more about
ISO/IEC 27701 with BSI

Call +34 **91 400 86 20**
or visit **bsigroup.com/iso27701-ES**