ISO/IEC JTC 1/SC 27/WG 1 "Information security management systems"
Convenorship: **BSI**
Convenor: **Humphreys Edward J. Prof.**

WG 1 SD 7 - Use of ISO/IEC 27001 family of standards in Governmental / Regulatory requirements (March 2021 edition)

Document type	Related content	Document date	Expected action
Project / Other		2021-03-29	**INFO**

Description

This edition replaces the version in WG 1 N2710.

SC 27/WG 1
Information Security Management Systems

Date: 2021/03/29

WG1 Standing Document 7 -- ISO/IEC 27001 family of standards references list

Use of ISO/IEC 27001 family of standards in Governmental / Regulatory requirements

WG1 Standing Document 7 (SD 7)

CONTENTS

WG1 Standing Document 7 (SD 7)

Foreword

This Standing Document 7 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology, Subcommittee 27, Security techniques, WG 1 ISMS Standards*.

WG1 Standing Document 7 (SD 7)

Introduction

The WG1 Standing Document 7 “ISO/IEC 27001 family of standards references list” provides references to laws, regulations, and guidelines relying on this family of standards to assist organisations from both public and private sectors, as well as individuals, to perform their activities, which require knowledge and understanding within the information security domain.

It has to be noted that the listed references require and/or recommend the use of standards of this family by certain organisations and/or sectors while delivering business services, or establishing for example their information security or privacy and data protection frameworks.

Please note that the content provided within the WG1 Standing Document 7 shall not be considered as:

- Legal interpretations; and
- Having been legally validated by a global law firm or relevant lawyers.

WG1 Standing Document 7 -- ISO/IEC 27001 family of standards references list

1 Scope

This WG1 Standing Document 7 contains references to laws, regulations and guidelines relying on International Standards of the ISO/IEC 27001 family to require or assist organisations, in particular of the following sectors, as well as individuals, in performing their activities:

a) Public;

b) Finance;

c) Energy;

d) Communications and Media/Multimedia; and

e) Health.

This WG1 Standing Document 7 could also support organisations in:

a) Identifying the International Standards of the ISO/IEC 27001 family that are recommended and/or required within the scope of their activities; and

b) Developing appropriate information security documentation by benchmarking it with similar practices around the word.

This WG1 Standing Document 7 shall not be considered as:

- Legal interpretations; and
- Having been legally validated by a global law firm or relevant lawyers.

2 Terms and definitions

For the purposes of this document, the following term applies:

2.1

Personal Data

All kinds of information that is directly or indirectly referable to a natural person who is alive constitute personal data[1]

[1] from the regulation on data protection of Sweden
http://www.datainspektionen.se/in-english/legislation/the-personal-data-act/

3 Symbols and abbreviated terms

For the purposes of this document, following abbreviated terms apply:

ANSSI	Agence nationale de la sécurité des systèmes d'Information
BSI	Bundesamt für Sicherheit in der Informationstechnik
CCDP	Commissioner for Privacy and Data Protection
CNII	Critical National Information Infrastructure
DIA	Department of Internal Affairs
EU	European Union
GCIO	Government CIO
IaaS	Infrastructure as a Service
ISMS	Information Security Management System
NTP	Normas Técnicas Peruanas
PaaS	Platform as a Service
PCM	Presidencia del Consejo de Ministros
RM	Resolución Ministerial
SaaS	Software as a Service
VPS	Victorian Public Sector
VPDSF	Victorian Protective Data Security Framework
VPDSS	Victorian Protective Data Security Standards

4 ISO/IEC 27001 family of standards references list

4.1 Argentina

<table>
<tr><th colspan="2">“Information security” domain – Public sector</th></tr>
<tr><td>Reference(s)</td><td>Information security policy (ANNEX - RESOLUTION ENARGAS W I / 4559) 2017
https://www.argentina.gob.ar/sites/default/files/infoleg/res4559.pdf

In response to the Administrative Decision of the National Office of Information Technologies that established the obligation for the organisms of the National Public Sector to create an Information Security Committee and appoint a coordinator for this committee. (DA 669/2004).</td></tr>
<tr><td>Organisation(s)</td><td>National Gas Regulation Body (ENARGAS)
https://www.enargas.gob.ar/home.php</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards
Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002:2013</th></tr>
<tr><td>Recommended</td><td></td><td>X</td></tr>
</table>
</td></tr>
<tr><td>Comments</td><td>All definitions in this Information Security Policy estimated to be aligned with internationally accepted standards for the practice of information security, particularly regarding: IRAM/ISO/IEC 27002:2013.</td></tr>
</table>

4.2 Australia

<table>
<tr><th colspan="2">“Privacy and data protection” domain – Public sector</th></tr>
<tr><td>Reference(s)</td><td>Victorian Protective Data Security Standards (VPDSS) v2.0
https://ovic.vic.gov.au/data-protection/standards/

The standards published by the Commissioner for Privacy and Data Protection and forming part of the Victorian Protective Data Security Framework (VPDSF), and establish 18 mandatory requirements to protect data security across the Victorian public sector.</td></tr>
<tr><td>Organisation(s)</td><td>Commissioner for Privacy and Data Protection (CPDP)
https://www.cpdp.vic.gov.au/</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards
Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th></tr>
<tr><td>Recommended</td><td>X</td><td>X</td></tr>
</table>

*Applicable to Victorian Public Sector (VPS) agencies and contracted service providers and external agencies with either direct or indirect access to public sector data.
</td></tr>
<tr><td>Comments</td><td>Mandatory security risk profile assessment (SRPA), protective data security plan (PDSP) and compliance/maturity report are submitted to CPDP every two years.</td></tr>
</table>

4.3 Denmark

"Privacy and data protection" domain – Public sector	
Reference(s)	**Act on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act)** https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf
Organisation(s)	The Danish Data Protection Agency https://www.datatilsynet.dk/english
Referenced standards associated to ISO/IEC 27001 family	N/A.
Assurance/Control mechanism	The Danish Data Protection Agency is the independent authority that supervises compliance with the rules on protection of personal data. The Agency provide guidance and advice as well as deal with complaints and make inspections.

"Information security" domain – Public sector	
Reference(s)	**Danish Cyber and Information Security Strategy 2018-2021** https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf
Organisation(s)	Agency for Digitisation https://en.digst.dk/
Referenced standards associated to ISO/IEC 27001 family	

Standards / Degree of use	ISO/IEC 27001	ISO/IEC 27002	ISO/IEC 27005
Mandatory	**X**		
Recommended		**X**	**X**

Assurance/Control mechanism	In order to ensure comprehensive implementation of ISO 27001 within central government organisations, the Danish Agency for Digitisation follow up on the organisations' implementation efforts every six months by means of an extensive questionnaire. Authorities who have yet to implement the standard are required to submit an action plan describing what measures they plan to implement in order to ensure comprehensive implementation of the standard.

4.4 European Union

<table>
<tr><th colspan="2">“Information security” domain – Financial sector</th></tr>
<tr><td>Reference(s)</td><td>Commission Delegated Regulation (EU) No 907/2014
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0907

Commission Delegated Regulation (EU) No 907/2014 of 11 March 2014 supplementing Regulation (EU) No 1306/2013 of the European Parliament and of the Council, with regard to paying agencies and other bodies, financial management, clearance of accounts, securities and use of euro.</td></tr>
<tr><td>Organisation(s)</td><td>European Commission
https://ec.europa.eu/</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th></tr>
<tr><td>Mandatory</td><td>X</td><td>X</td></tr>
</table>
*Applicable to paying agencies and other bodies, financial management, clearance of accounts, securities and use of euro.
</td></tr>
<tr><td>Comments</td><td>-</td></tr>
</table>

4.5 Germany

<table>
<tr><th colspan="2">“Information security” domain – Energy sector</th></tr>
<tr><td colspan="2">“IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz”, August 2015</td></tr>
<tr><td>Reference(s)</td><td>“IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz”, August 2015
https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf?__blob=publicationFile&v=2

The document is a catalogue of security requirements designed to protect against threats to the telecommunications and electronic data processing systems necessary for secure network operation and it is drawn up and published by the Federal Network Agency, in consultation with the Federal Office for Information Security (BSI).</td></tr>
<tr><td>Organisation(s)</td><td>Bundesnetzagentur (The Federal Network Agency)
https://www.bundesnetzagentur.de/EN/Home/home_node.html</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th><th>ISO/IEC TR 27019</th></tr>
<tr><td>Mandatory</td><td>X</td><td>X</td><td>X</td></tr>
</table>
</td></tr>
<tr><td>Assurance/Control mechanism</td><td>The IT security catalogue obliges electricity and gas network operators to implement IT security standards. The core requirement is the certification of an information security management system (ISMS) according to DIN ISO/IEC 27001 and ISO/IEC 27019 until the 31. January 2018.

The certification bodies have to fulfil a conformity assessment Program for accreditation of certification bodies for the IT safety catalogue according to EnWG§11,1a on the basis of ISO/IEC 27006.

The first step towards achieving a certification is the Stage 1 (readiness Audit) – followed by a full Stage 2 Audit for the whole Scope to verify the conformity to the IT-Sicherheitskatalog. After the initial certification a (at least) yearly surveillance audit takes place. After the third surveillance year a full Re-certification Audit is performed.</td></tr>
<tr><td colspan="2">“IT-Sicherheitskatalog für Betreiber von Energieanlagen“</td></tr>
<tr><td>Reference(s)</td><td>“IT-Sicherheitskatalog für Betreiber von Energieanlagen“, Dezember 2018
https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_2018.pdf?__blob=publicationFile&v=4

The document is a catalogue of security requirements designed to protect against threats to the ICT systems of energy producing facilities and it is drawn up and published by the Federal Network Agency, in consultation with the Federal Office for Information Security.</td></tr>
<tr><td>Organisation(s)</td><td>Bundesnetzagentur (The Federal Network Agency)</td></tr>
</table>

<table>
<tr><td></td><td>https://www.bundesnetzagentur.de/EN/Home/home_node.html</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th><th>ISO/IEC TR 27019</th></tr>
<tr><td>Mandatory</td><td>X</td><td>X</td><td>X</td></tr>
</table>
</td></tr>
<tr><td>Assurance/Control mechanism</td><td>The IT security catalogue obliges energy producing facilities to implement IT security standards. The core requirement is the certification of an information security management system (ISMS) according to the German translation of ISO/IEC 27001 and considering ISO/IEC 27019 until March 31st 2021.

A special conformity assessment program is developed by the Federal Network Agency certification bodies have to adhere to.</td></tr>
<tr><td colspan="2">"Technische Richtlinie TR-03109-6 Smart-Meter-Gateway-Administration"</td></tr>
<tr><td>Reference(s)</td><td>"Technische Richtlinie TR-03109-6 Smart-Meter-Gateway-Administration", August 2016
https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/AdministrationBetrieb/TechnRichtlinie/TR_03109-6_node.html

The document is a catalogue of security requirements designed to protect against threats to the telecommunications and electronic data processing systems necessary for smart meter gateway administration and it is drawn up and published by the Federal Office for Information Security (BSI)telecommunications and electronic data processing systems necessary for smart meter gateway administration and it is drawn up and published by the Federal Office for Information Security (BSI).</td></tr>
<tr><td>Organisation(s)</td><td>Bundesnetzagentur (The Federal Network Agency)
https://www.bundesnetzagentur.de/EN/Home/home_node.html</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC TR 27019</th></tr>
<tr><td>Mandatory</td><td>X</td><td></td></tr>
<tr><td>Recommended</td><td></td><td>X</td></tr>
</table>
</td></tr>
<tr><td>Assurance/Control mechanism</td><td>The technical guideline obliges the smart meter gateway administrator to implement IT security standards.

The core requirement is the certification of an information security management system (ISMS) according to ISO/IEC 27001 or the German IT Grundschutz before being allowed to assume the operative role as gateway administrator.

The utilization of the ISO/IEC 27019 is recommended. The certification bodies have to be accredited on the basis of ISO/IEC 27006. Additionally, auditors have to be certified by BSI.</td></tr>
</table>

<table>
<tr><th colspan="2">“Information security” domain – Communications & media/multimedia</th></tr>
<tr><td>Reference(s)</td><td>"Technische Richtlinie De-Mail BSI-TR 01201 Teil 6.2 "
https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/DeMail/TechnischeRichtlinien/TechnRichtlinien_node.html

Technical Guideline BSI-TR 01201 for De-Mail Service Provider (De-Mail-Diensteanbieter, DMDA) according to Art. 18 section 2 of German De-Mail law (§ 18 Abs.2 De-Mail-G).

BSI-TR 01201 part 6.2 provides additional requirements and guidance sector-specific for DMDA by complementing or amending ISO/IEC 27001 resp. ISO/IEC 27002 following ISO/IEC 27009. It is drawn up and published by the Federal Office for Information Security (BSI).</td></tr>
<tr><td>Organisation(s)</td><td>Bundesnetzagentur (The Federal Network Agency)
https://www.bundesnetzagentur.de/EN/Home/home_node.html</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td><table><tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th></tr><tr><td>Recommended</td><td>X</td></tr></table></td></tr>
<tr><td>Assurance/Control mechanism</td><td>The technical guideline obliges the De-Mail service provider to implement an information security management system (ISMS) and requires the certification according to ISO/IEC 27001 (or based on the German IT-Grundschutz) and sector-specific to “BSI-TR 01201 Teil 6.2“ before being accredited as De-Mail service provider. Additionally, auditors have to be certified by BSI.</td></tr>
</table>

4.6 India

<table>
<tr><th colspan="2">“Information security” domain – Public and private sectors</th></tr>
<tr><td>Reference(s)</td><td>Information Technology Act (Intermediaries guidelines) Rules, 2011
http://meity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf</td></tr>
<tr><td>Organisation(s)</td><td>Ministry of communication and information technology
http://meity.gov.in/</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td><table><tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th></tr><tr><td>Recommended</td><td>X</td></tr></table></td></tr>
<tr><td>Comments</td><td>-</td></tr>
</table>

<table>
<tr><th colspan="2">“Information security” domain – Financial sector</th></tr>
<tr><td>Reference(s)</td><td>RBI Working Group Recommendations on InfoSec
https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111.pdf

Report of the Working Group on information security, electronic banking, technology risk management, and tackling cyber frauds which provides detailed suggestions in areas relating to IT Governance, Information security, IT operations, Information system audit, Cyber frauds, Business Continuity Planning, customer education and legal issues arising out of use of IT.</td></tr>
<tr><td>Organisation(s)</td><td>Reserve Bank of India
https://www.rbi.org.in/</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td><table><tr><th>Standards
Degree of use</th><th>ISO/IEC 27001</th></tr><tr><td>Recommended</td><td>X</td></tr></table>
*Applicable to all commercial banks in India.</td></tr>
<tr><td>Comments</td><td>-</td></tr>
</table>

4.7 Italy

<table>
<tr><th colspan="2">“Privacy and data protection” domain – Public sector</th></tr>
<tr><td>Reference(s)</td><td>General Application Order Concerning Biometrics - November 12th, 2014
http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3590114

This order issued by the Italian Data Protection Authority regulates the use of biometric technology and the data protection measures required to be adopted.</td></tr>
<tr><td>Organisation(s)</td><td>Italian Data Protection Authority
http://www.garanteprivacy.it/</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td><table><tr><th>Standards
Degree of use</th><th>ISO/IEC 27001</th></tr><tr><td>Recommended</td><td>X</td></tr></table>
*An ISO/IEC 27001 certification including biometric technologies in its scope can be leveraged to avoid the redaction of a report describing the technical and organizational features of the measures implemented to protect biometric data.</td></tr>
<tr><td>Comments</td><td>-</td></tr>
</table>

4.8 Lithuania

"Privacy and data protection" domain – Public sector	
Reference(s)	**Guidelines on security measures and risk assessment of processed personal data for controllers and processors** https://vdai.lrv.lt/uploads/vdai/documents/files/VDAI_saugumo_priemoniu_gaires-2020-06-18.pdf These guidelines have been published by the Lithuanian State Data Protection Inspectorate on June 2020.
Organisation(s)	State Data Protection Inspectorate https://vdai.lrv.lt/lt/
Referenced standards associated to ISO/IEC 27001 family	

Standards / Degree of use	ISO/IEC 27001:2017	ISO/IEC 27701:2019
Recommended	**X**	**X**

Comments	-

4.9 Luxembourg

"Information security" domain – Public sector	
Reference(s)	➢ **ANSSI, Information Security Policy, General policy (ISP-LU), POL_0-0** ➢ **ANSSI Information Security Policy, Information Security Management System (ISP-ISMS), POL_1.0** These policies apply to public services and critical infrastructures.
Organisation(s)	Agence nationale de la sécurité des systèmes d'Information (ANSSI) https://cybersecurite.public.lu/fr/securite-information/mission.html
Referenced standards associated to ISO/IEC 27001 family	

Standards / Degree of use	ISO/IEC 27001	ISO/IEC 27002
Recommended	**X**	**X**

Comments	-

<table>
<tr><th colspan="2">“Digitalization and electronic archiving” domain – Public and private sectors</th></tr>
<tr><td>Reference(s)</td><td>➢ Law of July 25th, 2015 on digitalization and electronic archiving
http://legilux.public.lu/eli/etat/leg/loi/2015/07/25/n1/jo

➢ Grand-Ducal Regulation of September 21st 2017 related to digitalization and electronic archiving (“Règlement grand-ducal du 21 septembre 2017 modifiant le règlement grand-ducal modifié du 25 juillet 2015 portant exécution de l’article 4, paragraphe 1er, de la loi du 25 juillet 2015 relative à l’archivage électronique“
http://legilux.public.lu/eli/etat/leg/rgd/2017/09/21/a865/jo</td></tr>
<tr><td>Organisation(s)</td><td>ILNAS
https://portail-qualite.public.lu/fr.html</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards
Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th></tr>
<tr><td>Mandatory</td><td>X</td><td>X</td></tr>
</table>

The law of July 25th, 2015 on digitalization and electronic archiving defines the legal framework relating to digitization and e-archiving services in the Grand-Duchy of Luxembourg. In particular, it introduces the legal status of “Prestataire de Services de Dématérialisation ou de Conservation (PSDC), or “Digitization or e-Archiving Service Provider" (DASP) in English.

According to this law, a digital copy will be presumed to be true to the original analogue document if it was produced by the digitization process of an organization that has obtained the DASP status. Similarly, digital archives are considered to be equivalent to their digital originals if they were archived by the electronic archiving processes of an organization that has obtained the DASP status.

The DASP status can only be granted by the national supervisory authority, ILNAS. One prerequisite for an organization to be granted the DASP status is that the organization has obtained a certification that demonstrates its compliance with the requirements and controls defined in the “Technical regulation for a management system and security controls for digitization or archiving service providers”, which is introduced in the Grand-Ducal Regulation of September 21st 2017 relating to electronic archiving. The Technical regulation can be seen as an addition to ISO/IEC 27001:2013 and ISO/IEC 27002:2013, written according to ISO/IEC 27009:2016, amending and completing the content thereof specifically for digitization or e-archiving processes.

If ILNAS determines that an organization fulfills, in particular, the criteria established by the law on digitalization and electronic archiving, the technical regulation for a management system and security controls for digitization or archiving service providers, ILNAS will add the certified organization to the list of PSDCs, indicating the processes in scope of the certification, and thereby granting it the DASP status.</td></tr>
<tr><td>Assurance/Control mechanism</td><td>Certification according to ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015, based on criteria given in ISO/IEC 27001 and the technical regulation for a management system and security controls for digitization or archiving service providers, considered as sector specific extension of ISO/IEC 27001.

Supervision by the national supervisory authority ILNAS.</td></tr>
</table>

4.10 Malaysia

<table>
<tr><th colspan="2">“Information security” domain – Communications & media/multimedia</th></tr>
<tr><td>Reference(s)</td><td>MS ISO/IEC 27001:2007 Information Security Management System (ISMS) Implementation and Certification for Critical National Information Infrastructure (CNII) under Communication and Multimedia Industry
http://www.skmm.gov.my/Resources/Industry/Industry-ISMS-Implementation.aspx

The document provides detailed information on the MS ISO/IEC 27001:2007 Information Security Management System (ISMS) implementation and certification for communication and multimedia industry in Malaysia.</td></tr>
<tr><td>Organisation(s)</td><td>Malaysian Communications and Multimedia Commission
http://www.skmm.gov.my/</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th><th>ISO/IEC 27004</th><th>ISO/IEC 27005</th><th>ISO/IEC 27011</th><th>ISO/IEC 27035-1</th></tr>
<tr><td>Mandatory</td><td>X</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Recommended</td><td></td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
</table>

*ISO/IEC 20000 ITMS is also recommended for use to organisation that has multiple management system(s) within the organization.

*ISO/IEC 27001:2013 and ISO/IEC 27002:2013 are applicable to all Communications and Multimedia licensee that has been identified as Critical National Information Infrastructure (CNII). The rest are applicable to all Communications and Multimedia licensee in Malaysia.</td></tr>
<tr><td>Assurance/Control mechanism</td><td>➢ Industry Assessment; and
➢ Submission of Response to Questionnaire on ISMS implementation status / readiness.</td></tr>
<tr><td>Comments</td><td>ISO/IEC 27001:2013 implementation is monitored by the regulator through:
➢ Periodic Audit; and
➢ Submission of Response to Questionnaire on ISMS implementation status / readiness.</td></tr>
</table>

4.11 Mexico

<table>
<tr><th colspan="2">“Privacy and data protection” domain – Public sector</th></tr>
<tr><td>Reference(s)</td><td>
➢ Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

The General data Protection Law applicable to the public administration sector in Mexico was published in January 2017 and established the requirement for a Personal Data and Security Management System, including a security document that shall include:
• Personal data and treatment systems inventory
• Functions and responsibilities for people treating personal data
• Risk Analysis
• Gap Analysis
• Work plan
• Security measures monitoring and revision mechanisms
• Training program

➢ Recomendaciones para el manejo de incidentes de seguridad de datos personales
http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

Recommendations for personal data security incidents.

➢ Guía para el tratamiento de datos biométricos
http://inicio.inai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf

Guidance for the treatment for biometric data.

➢ Recomendaciones sobre protección de datos personales contenidos en la Credencial para Votar
http://inicio.inai.org.mx/DocumentosdeInteres/RecomendacionesCredencialV.pdf

Recommendations for the protection of personal data contained in voting cards.

➢ Programa de Protección de Datos Personales
http://inicio.inai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

Guidance to produce the personal data protection program
</td></tr>
<tr><td>Organisation(s)</td><td>Instituto Nacional de Accesos a la Información y Protección de Datos Personales (INAI), Data protection authority
http://inicio.inai.org.mx</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th></tr>
<tr><td>Recommended</td><td>X</td><td>X</td></tr>
</table>
</td></tr>
</table>

Assurance/Control mechanism	Every instance of the Federal Public Administration has an Internal Control Body, which is in charge to review and assess compliance with the law. The Public Function Minister (Secretaría de la Función Pública) is in charge of the role of every Internal Control Body.

"Privacy and data protection" domain – Private sector	
Reference(s)	➢ **Ley Federal de Protección de Datos Personales en Posesión de los Particulares** http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf ➢ **Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares** www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf Federal Data Protection law applicable to the private sector was published in 2010 and 2011 respectively. ➢ **Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales** http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf Guidance for the implementation of a data protection security management system. ➢ **Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas** http://inicio.inai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf Manual for personal data security for Small and medium organisations. ➢ **Tabla de equivalencia funcional entre estándares de seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en materia de seguridad de datos personales** http://inicio.inai.org.mx/DocumentosdeInteres/Tabla_de_Equivalencia_Funcional(Junio2015).pdf Equivalency table with security standards and the Mexican data protection law, its regulation and the personal data security recommendations; referring ISO/IEC 27001 and the standard that better complies with the data protection law.
Organisation(s)	Instituto Nacional de Accesos a la Información y Protección de Datos Personales (INAI), Data protection authority http://inicio.inai.org.mx
Referenced standards associated to ISO/IEC 27001 family	

Standards / Degree of use	ISO/IEC 27001	ISO/IEC 27002
Recommended	**X**	**X**

Assurance/Control mechanism	Verification procedures applied by the data protection authority The law and regulation include a certification mechanism provided by third parties accredited through ISO standards to demonstrate compliance to the authority, ISO/IEC 27001 is one of the self-regulation models that can be followed to obtain the certification. The data protection authority maintains a register of the certified organizations in: http://rea.inai.org.mx/_catalogs/masterpage/Sec6_1.aspx

4.12 New Zealand

<table>
<tr><th colspan="2">“Information security” domain – Public sector</th></tr>
<tr><td>Reference(s)</td><td>Information Security and Privacy Considerations
https://www.ict.govt.nz/assets/ICT-System-Assurance/Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf

[EDITORS NOTE: provided URL does not work anymore. Editors kindly request to NZ experts to update the present section.]

This document presents information security and privacy implications that need to be carefully considered and managed by agencies seeking to take advantage of cloud computing. The process is mandatory for Public and non-Public Service departments as part of the robust information management process listed above, however, all State services agencies are expected to follow the process.

Endorsed as supporting NZ Govt (GCIO) Guidance on adoption and security risk assessment (certification) of Public Cloud services (IaaS, PaaS, SaaS)</td></tr>
<tr><td>Organisation(s)</td><td>Government CIO (GCIO) at the Department of Internal Affairs (DIA)
https://www.dia.govt.nz/</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th></tr>
<tr><td>Mandatory</td><td>X</td></tr>
</table>

*Applicable to public sector generally; though mandated for Public Service Agencies, Non-Public Service Departments and District Health Boards.</td></tr>
<tr><td>Comments</td><td>ISO/IEC 27001:2013 is also considered “best practice” by New Zealand private sector and industry.</td></tr>
</table>

4.13 Norway

"Information security" domain – Public sector	
Reference(s)	**Guideline: Internkontroll i praksis – informasjonssikkerhet for toppledere** https://internkontroll-infosikkerhet.difi.no/sites/sikkerhet/files/for_toppledere_-_internkontroll_informasjonssikkerhet.pdf Guidelines regarding information security for top management. ISO/IEC 27001 is a recommended standard for public sector.
Organisation(s)	Difi (Agency for Public Management and eGovernment)
Referenced standards associated to ISO/IEC 27001 family	**Degree of use** \ **Standards**: **ISO/IEC 27001** **Recommended**: **X**
Comments	-

"Privacy and protection" domain – Public and private sectors	
Reference(s)	**Guideline: Software development with Data Protection by Design and by Default** https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/ The Norwegian Data Protection Authority has developed these guidelines to help organisations understand and comply with the requirements of data protection by design and by default in article 25 of the General Data Protection Regulation.
Organisation(s)	Datatilsynet The Norwegian Data Protection Authority (DPA)
Referenced standards associated to ISO/IEC 27001 family	**Degree of use** \ **Standards**: **ISO/IEC 27001** **Recommended**: **X**
Comments	-

4.14 Peru

"Information security" domain – Public sector	
Reference(s)	➢ **Ministerial Resolution 129-2012-PCM (year 2012)** http://www.pcm.gob.pe/normaslegales/2012/RM-129-2012-PCM.pdf Approves the mandatory use of NTP-ISO/IEC 27001:2008 in all dependences of the Informatic National System. ➢ **Ministerial Resolution 004-2016-PCM (year 2016)** http://www.pcm.gob.pe/wpcontent/uploads/2016/01/RM_N_04-2016-PCM.pdf **[EDITORS NOTE: provided URL does not work anymore. Editors kindly request to PE experts to update the present section.]** Approves the mandatory use of NTP-ISO/IEC 27001:2014 in all dependences of the Informatic National System and replace to RM 129-2012-PCM.
Organisation(s)	Presidencia del Consejo de Ministros
Referenced standards associated to ISO/IEC 27001 family	<table><tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th></tr><tr><td>Mandatory</td><td>X</td></tr></table> *Applicable to all public sectors (all informatic offices in all levels of government – Local, regional and national).
Comments	-

"Privacy and protection" domain – Public and private sectors	
Reference(s)	**National Personal Data Protection Act, Regulation of Act 29733**
Organisation(s)	Government of Peru
Referenced standards associated to ISO/IEC 27001 family	<table><tr><th>Standards / Degree of use</th><th>ISO/IEC 27002</th></tr><tr><td>Recommended</td><td>X</td></tr></table> * Applicable nationally.
Comments	-

4.15 Poland

"Privacy and data protection" domain – Public sector	
Reference(s)	➢ **Regulation on National Interoperability Framework, minimal requirements for public registers and information exchange in electronic form, and minimal requirements for ICT systems, 12.04.2012** http://isap.sejm.gov.pl/DetailsServlet?id=WDU20120000526 ➢ **Regulation on baseline requirements for ICT systems; 20.07.2011** Only applicable for processing of classified information in any relevant organisation.
Organisation(s)	Polish Government https://www.premier.gov.pl/en.html
Referenced standards associated to ISO/IEC 27001 family	<table><tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27005</th></tr><tr><td>Recommended</td><td>X</td><td>X</td></tr></table> *Applicable to public administration, all entities performing public tasks.
Comments	-

"Information security" domain – Public sector	
Reference(s)	➢ **Regulation on chancellery instruction, unified classification of material records and instruction on organisation and scope of organisations' archives, 18.01.2011** http://isap.sejm.gov.pl/DetailsServlet?id=WDU20110140067 ➢ **Regulation on introducing Information Security Policy in the Ministry of Justice and courts of general jurisdiction, 27.06.2012** http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjixI2VjdLSAhVFLcAKHR1NDplQFggZMAA&url=http%3A%2F%2Fwww.bip.powiat.poznan.pl%2Fplik%2C20825%2C132-pdf.pdf&usg=AFQjCNHCfAIjvIFMkt16nPKkuyGcptM4EQ&sig2=T-ryoZv8TvvVwihAjcss8w&bvm=bv.149397726,d.ZGg ➢ **Recommendation for the methodology of cybersecurity risk management in information security management systems of governmental entities, 2015** http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwj--_p-LkNLSAhXlDsAKHfQGAqMQFggZMAA&url=http%3A%2F%2Fkrmc.mc.gov.pl%2Fdownload%2F50%2F12585%2FMetodykaZarzadzaniaRyzykiemCRP2015v18ZZKRMC.docx&usg=AFQjCNFOBQm-0_vlvNhITtkwzVFbNy_jdA&sig2=xe41_Zwu_ztQK7lt4ssBtg&bvm=bv.149397726,d.ZGg
Organisation(s)	➢ Prime Minister Office of Poland ➢ Minister of Justice

<table>
<tr><td></td><td>➢ Government Council for Digital Affairs</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th><th>ISO/IEC 27005</th></tr>
<tr><td>Recommended</td><td>X</td><td>X</td><td>X</td></tr>
</table>

*ISO/IEC 27001:2013 is applicable to all organisations from public, private sector, courts of general jurisdiction and departments of the Ministry of Justice.

ISO/IEC 27002:2013 is applicable to courts of general jurisdiction and departments of the Ministry of Justice.

ISO/IEC 27005:2011 is applicable to governmental agencies and units, courts of general jurisdiction and departments of the Ministry of Justice.</td></tr>
<tr><td>Comments</td><td>-</td></tr>
</table>

4.16 Sweden

"Privacy and data protection" domain – Public sector	
Reference(s)	**Regulation on data protection** https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/dataskyddsforordningen---fulltext/
Organisation(s)	Swedish Data Protection Authority http://www.datainspektionen.se/
Referenced standards associated to ISO/IEC 27001 family	<table><tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th></tr><tr><td>Recommended</td><td>X</td><td>X</td></tr></table> *Applicable to Swedish governmental agencies/authorities and recommended for all organisations handling personal data.
Assurance/Control mechanism	The Data Protection Authority performs audits based on ISO/IEC 27001:2013 and ISO/IEC 27002:2013.

"Information security" domain – Public sector	
Reference(s)	➢ **Regulations and general guidelines on government agencies' information security (MSB FS 2016:1 föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet)** https://www.msb.se/sv/Om-MSB/Lag-och-ratt/Gallande-regler/Krisberedskap-och-informationssakerhet/MSBFS-20161/ ➢ **Regulations and general guidelines on government agencies it-incident reporting (MSBFS 2016:2 Föreskrifter och allmänna råd om statliga myndigheters rapportering av it-incidenter)** https://www.msb.se/externdata/rs/f21ae5f7-b655-4462-a2e6-9939b952a751.pdf
Organisation(s)	The Swedish Civil Contingency Agency https://www.msb.se/en/
Referenced standards associated to ISO/IEC 27001 family	<table><tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th></tr><tr><td>Recommended</td><td>X</td><td>X</td></tr></table> *Applicable to Swedish governmental agencies/authorities.
Comments	-

<table>
<tr><th colspan="2">“Digitalization and electronic archiving” domain – Public sector</th></tr>
<tr><td>Reference(s)</td><td>Regulation of The Swedish National Archives
https://riksarkivet.se/rafs?pdf=rafs/RA-FS%202009-01.pdf</td></tr>
<tr><td>Organisation(s)</td><td>The Swedish National Archives
https://riksarkivet.se/startpage</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards
Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th></tr>
<tr><td>Recommended</td><td>X</td><td>X</td></tr>
</table>
*Applicable to Swedish governmental agencies/authorities.
</td></tr>
<tr><td>Comments</td><td>-</td></tr>
</table>

<table>
<tr><th colspan="2">“Information security” domain – Financial sector</th></tr>
<tr><td>Reference(s)</td><td>Finansinspektionen’s Regulatory Code, FFFS 2014:5
http://www.fi.se/contentassets/a8d558e3a0074cc796c4c23f6e6b3f53/fs1405_eng.pdf

This regulation includes provisions on how an undertaking is to manage information security, IT operations and deposit systems.</td></tr>
<tr><td>Organisation(s)</td><td>The Swedish financial supervisory authority "Finansinspektionen"
http://www.fi.se/en/</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards
Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th></tr>
<tr><td>Mandatory</td><td>X</td><td>X</td></tr>
</table>
*Applicable to financial sector in Sweden.
</td></tr>
<tr><td>Comments</td><td>Mandatory to implement an ISMS although they do not explicitly refer to the standards.</td></tr>
</table>

<table>
<tr><th colspan="2">“Privacy and data protection” domain – Health sector</th></tr>
<tr><td>Reference(s)</td><td>Om journalföring och behandling av personuppgifter i hälso- och sjukvård.
https://www.socialstyrelsen.se/sosfs/2016-40</td></tr>
<tr><td>Organisation(s)</td><td>The National Board of Health and Welfare</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th></tr>
<tr><td>Recommended</td><td>X</td><td>X</td></tr>
</table>
*Applicable to all health sector in Sweden.
</td></tr>
<tr><td>Comments</td><td>-</td></tr>
</table>

<table>
<tr><th colspan="2">“Privacy and data protection” domain – Public and private sectors</th></tr>
<tr><td>Reference(s)</td><td>Datainspektionens Allmänna råd, Säkerhet för personuppgifter
https://www.datainspektionen.se/globalassets/dokument/ovrigt/faktabroschyr-allmannarad-sakerhet.pdf</td></tr>
<tr><td>Organisation(s)</td><td>Swedish Data Protection Authority
http://www.datainspektionen.se/</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th></tr>
<tr><td>Recommended</td><td>X</td></tr>
</table>
</td></tr>
<tr><td>Comments</td><td>-</td></tr>
</table>

<table>
<tr><th colspan="2">“Information security” domain – Public and private sectors</th></tr>
<tr><td>Reference(s)</td><td>

Act on information security for operators of essential and digital services (MSBFS 2018:8 Föreskrifter och allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster)
https://www.msb.se/sv/regler/gallande-regler/krisberedskap-och-informationssakerhet/msbfs-20188/
Act on (Lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster)
https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174
Säkerhetspolisens vägledning i säkerhetsskydd – informationssäkerhet
https://www.sakerhetspolisen.se/download/18.7acd465e16b4e0e54c673/1560952186689/Vagledning-Informationssakerhet.pdf
Metodstöd för systematiskt informationssäkerhetsarbete
https://www.informationssakerhet.se/metodstodet/

</td></tr>
<tr><td>Organisation(s)</td><td>

Swedish Civil Contingencies Agency
https://www.msb.se/
Swedish Parliament
https://www.riksdagen.se/
Swedish Security Service
https://www.sakerhetspolisen.se/en/swedish-security-service.html
Swedish Civil Contingencies Agency
https://www.msb.se/

</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td>
<table>
<tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th></tr>
<tr><td>Recommended</td><td>X</td><td>X</td></tr>
</table>
</td></tr>
<tr><td>Comments</td><td>-</td></tr>
</table>

4.17 Switzerland

"Information security" domain – Public sector	
Reference(s)	➢ **Federal Act on Information Security (not in force yet)** http://www.vbs.admin.ch/de/themen/informationssicherheit/informationssicherheitsgesetz.detail.document.html/vbs-internet/de/documents/isg/Bundesgesetz-ISG-d.pdf.html ➢ **Bundesinformatikverordnung** (Ordinance) https://www.admin.ch/opc/de/classified-compilation/20081009/index.html ➢ **IKT-Grundschutz in der Bundesverwaltung (Guideline)** https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/sicherheit/si001-ikt-grundschutz_in_der_bundesverwaltung.html
Organisation(s)	➢ The Federal Assembly of the Swiss Confederation (Federal Act) ➢ The Swiss Federal Council (Ordinance) ➢ Federal IT Steering Unit (Guidelines) ➢ Federal Department of Defence Civil Protection and Sport (Guidelines)
Referenced standards associated to ISO/IEC 27001 family	

Standards / Degree of use	ISO/IEC 27001	ISO/IEC 27002
Mandatory	**X**	**X**

Comments	-

"Privacy and data protection" domain – Health sector	
Reference(s)	**Explanatory notes on the Ordinance on Electronic Patient Records** Erläuterungen zur Verordnung über das elektronische Patientendossier und zur Verordnung des EDI über das elektronische Patientendossier
Organisation(s)	Federal Office of Public Health
Referenced standards associated to ISO/IEC 27001 family	

Standards / Degree of use	ISO/IEC 27001	ISO/IEC 27002
Recommended	**X**	**X**

Assurance/Control mechanism	For the accomplishment of its legal tasks, the Federal Data Protection and Information Commissioner can investigate facts on its own initiative or at request of a third party. Based upon these investigations, the Federal Data Protection and Information Commissioner can issue recommendations.

<table>
<tr><th colspan="2">“Privacy and data protection” domain – Public and private sectors</th></tr>
<tr><td>Reference(s)</td><td>➢ Ordinance on Data Protection Certification
https://www.admin.ch/opc/en/classified-compilation/20071826/index.html

➢ Guidelines on the minimum requirements for the data protection management system
https://www.edoeb.admin.ch/datenschutz/00756/00974/index.html -> Zertifizierungsrichtlinien

[EDITORS NOTE: provided URL does not work anymore. Editors kindly request to CH experts to update the present section.]</td></tr>
<tr><td>Organisation(s)</td><td>➢ The Swiss Federal Council (Ordinance)

➢ Federal Data Protection and Information Commissioner (Guidelines)</td></tr>
<tr><td>Referenced standards associated to ISO/IEC 27001 family</td><td><table><tr><th>Standards
Degree of use</th><th>ISO/IEC 27002</th></tr><tr><td>Mandatory</td><td>X</td></tr></table>
*Applicable to all organizations that are getting certified or already have a certificate after the Ordinance on Data Protection Certification.</td></tr>
<tr><td>Assurance/Control mechanism</td><td>The implementation of the standard ISO/IEC 27001:2013 is supervised by the Swiss Accreditation Service. The Commissioner has to be notified about the detection of substantial changes in conditions for certification of the certified organization, as well as suspensions and withdrawals of certifications; he can monitor the compliance with the applicable laws and make recommendations.</td></tr>
<tr><td>Comments</td><td>The certification itself is not mandatory, though certain organizations have to get certified (health insurers to process specific categories of health data).</td></tr>
</table>

4.18 United Kingdom

"Information security" domain – Financial sector	
Reference(s)	**The Financial Conduct Authority's Handbook contains the complete record of FCA Legal Instruments and presents changes made in a single, consolidated view.** https://www.handbook.fca.org.uk/
Organisation(s)	Financial Conduct Authority https://www.fca.org.uk/
Referenced standards associated to ISO/IEC 27001 family	<table><tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th></tr><tr><td>**Mandatory**</td><td>**X**</td><td>**X**</td></tr></table>
Comments	The FCA has published an updated version of the FCA Handbook to show the rules that will apply at the end of the transition period. It has also set out details on how it intends to use the Temporary Transitional Power (TTP). "*The FCA intends to apply the TTP on a broad basis from the end of the transition period until 31 March 2022. This means firms and other regulated persons do not generally need to prepare now to meet the changes to their UK regulatory obligations brought about by onshoring*".

"Information security" domain – Energy sector	
Reference(s)	**Industry codes and standards establish rules that govern market operation and the terms for connection and access to energy networks.** https://www.ofgem.gov.uk/licences-industry-codes-and-standards
Organisation(s)	The Office of Gas and Electricity Markets, supporting the Gas and Electricity Markets Authority, is the government regulator for the electricity and downstream natural gas markets in Great Britain. https://www.ofgem.gov.uk/
Referenced standards associated to ISO/IEC 27001 family	<table><tr><th>Standards / Degree of use</th><th>ISO/IEC 27001</th><th>ISO/IEC 27002</th></tr><tr><td>**Recommended**</td><td>**X**</td><td>**X**</td></tr></table>
Comments	-

"Information security" domain – Communications & media/multimedia	
Reference(s)	**The Financial Conduct Authority's Handbook contains the complete record of FCA Legal Instruments and presents changes made in a single, consolidated view.** https://www.ofcom.org.uk/about-ofcom/policies-and-guidelines
Organisation(s)	The Office of Communications, commonly known as Ofcom, is the government-approved regulatory and competition authority for the broadcasting, telecommunications and postal industries of the United Kingdom https://www.ofcom.org.uk/home
Referenced standards associated to ISO/IEC 27001 family	

Standards / Degree of use	ISO/IEC 27001	ISO/IEC 27002
Recommended	**X**	**X**

Comments	-

"Privacy and data protection" domain – Public and private sectors	
Reference(s)	**The guide covers the Data Protection Act 2018 (DPA 2018), and the General Data Protection Regulation (GDPR) as it applies in the UK.** https://ico.org.uk/for-organisations/guide-to-data-protection/
Organisation(s)	Information Commissioner's Office https://ico.org.uk/
Referenced standards associated to ISO/IEC 27001 family	

Standards / Degree of use	ISO/IEC 27001	ISO/IEC 27002
Recommended	**X**	**X**

Comments	-

5 Overview of ISO/IEC 27001 family of standards references list

The following table provides an overview of standards from the ISO/IEC 27001 family, with the associated country, domain, sector and if the concerned ISO/IEC standard is mandatory or recommended for the defined use case.

ISO/IEC standards	Country	Domain	Sector	Applicability
ISO/IEC 27001	Australia	Privacy and data protection	Public	Recommended
	European Union	Information security	Financial	Mandatory
	Germany	Information security	Energy	Mandatory
		Information security	Communications & media/multimedia	Mandatory
	India	Information security	Financial	Recommended
		Information security	Public and Private	Recommended
	Italy	Privacy and data protection	Public	Recommended
	Luxembourg	Information security	Public	Recommended
		Digitalization and electronic archiving	Public and Private	Mandatory
	Malaysia	Information security	Communications & media/multimedia	Mandatory
	Mexico	Privacy and data protection	Public	Recommended
		Privacy and data protection	Private	Recommended
	New Zealand	Information security	Public	Mandatory
	Norway	Privacy and data protection	Public	Recommended
		Information security		Recommended
	Peru	Information security	Public	Mandatory
	Poland	Privacy and data protection	Public	Recommended
		Information security		Recommended
	Sweden	Privacy and data protection	Public	Recommended
		Information security		Recommended
		Digitalization and electronic archiving		Recommended
		Information security	Financial	Mandatory
		Privacy and data protection	Health	Recommended
		Privacy and data protection	Public and Private	Recommended
		Information security		Recommended
	Switzerland	Information security	Public	Mandatory

		Privacy and data protection	Health	Recommended
	United Kingdom	Information security	Financial	Mandatory
		Information security	Energy	Recommended
ISO/IEC 27001	United Kingdom	Information security	Communications & media/multimedia	Recommended
		Privacy and data protection	Public and Private	Recommended
ISO/IEC 27001:2017	Lithuania	Privacy and data protection	Public	Recommended
ISO/IEC 27002	Australia	Privacy and data protection	Public	Recommended
	European Union	Information security"	Financial	Mandatory
	Germany	Information security"	Energy	Mandatory
	Italy	Privacy and data protection	Public	-
	Luxembourg	Information security	Public	Recommended
		Digitalization and electronic archiving	Public and Private	Mandatory
	Malaysia	Information security	Communications & media /multimedia	Recommended
	Mexico	Privacy and data protection	Public	Recommended
		Privacy and data protection	Private	Recommended
	Peru	Privacy and data protection	Public and Private	Recommended
	Poland	Information security	Public	Recommended
	Sweden	Privacy and data protection	Public	Recommended
		Information security		Recommended
		Digitalization and electronic archiving		Recommended
		Information security	Financial	Mandatory
		Privacy and data protection	Health	Recommended
		Information security	Public and Private	Recommended
	Switzerland	Information security	Public	Mandatory
		Privacy and data protection	Health	Recommended
		Privacy and data protection	Public and Private	Mandatory
	United Kingdom	Information security	Financial	Mandatory
		Information security	Energy	Recommended
		Information security	Communications & media/multimedia	Recommended
		Privacy and data protection	Public and Private	Recommended
ISO/IEC 27004	Malaysia	Information security	Communications & media /multimedia	Recommended
ISO/IEC 27005	Malaysia	Information security	Communications & media /multimedia	Recommended
	Poland	Privacy and data protection	Public	Recommended

		Information security		Recommended
ISO/IEC 27011	Malaysia	Information security	Communications & media /multimedia	Recommended
ISO/IEC TR 27019	Germany	Information security	Energy	Mandatory
ISO/IEC 27035-1	Malaysia	Information security	Communications & media /multimedia	Recommended
ISO/IEC 27701:2019	Lithuania	Privacy and data protection	Public	Recommended