ISO/IEC 27001 Mapping guide

Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013

Introduction

This document presents a mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013. It has been designed for guidance purposes only.

There are two groups of tables. The first group deals with ISMS requirements:

1. **New ISMS requirements**;
2. **A mapping between ISMS requirements in ISO/IEC 27001:2013 and ISO/IEC 27001:2005** where the requirement is essentially the same;
3. **The reverse mapping** (i.e. ISO/IEC 27001:2005 and ISO/IEC 27001:2013);
4. **Deleted requirements** (i.e. ISO/IEC 27001:2005 requirements that do not feature in ISO/IEC 27001:2013).

The second group deals with Annex A controls:

1. **New Annex A controls**;
2. **A mapping between Annex A controls in ISO/IEC 27001:2013 and ISO/IEC 27001:2005** where the Annex A control is essentially the same;
3. **The reverse mapping** (i.e. ISO/IEC 27001:2005 and ISO/IEC 27001:2013);
4. **Deleted controls** (ISO/IEC 27001:2005 Annex A control that do not feature in ISO/IEC 27001:2013).

Please note that Annex A controls are not ISMS requirements unless they are deemed by an organization to be applicable in its Statement of Applicability.

Continued >>

Group 1 - ISMS requirements

New ISMS requirements

Clause (in ISO/IEC 27001:2013)	Requirement
4.2(a)	the interested parties that are relevant to the information security management system; and
4.3(c)	interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.
5.1(b)	ensuring the integration of the information security management system requirements into the organization's business processes;
6.1.1(a)	ensure information security management system can achieve its intended outcome(s);
6.1.1(b)	prevent, or reduce, undesired effects; and
6.1.1(c)	achieve continual improvement.
6.1.2(a)	establishes and maintains information security risk criteria that include:
6.2(b)	be measurable (if practicable)
6.2(c)	take into account applicable information security requirements,
6.2(c)	and results from risk assessment and risk treatment;
6.2(f)	what will be done;
6.2(g)	what resources will be required;
6.2(h)	who will be responsible;
6.2(i)	when it will be completed; and
6.2(k)	how the results will be evaluated.
7.3(a)	the information security policy;
7.4(a)	on what to communicate;
7.4(b)	when to communicate;
7.4(c)	with whom to communicate;
7.4(d)	who shall communicate; and
7.4(e)	the processes by which communication shall be effected.
7.5.1(b)	documented information determined by the organization as being necessary for the effectiveness of the information security management system.
8.1	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1.
9.1(c)	when the monitoring and measuring shall be performed;
9.1(d)	who shall monitor and measure;
9.1(f)	who shall analyse and evaluate these results.
9.3(c)(4)	fulfilment of information security objectives;
10.1(a)	react to the nonconformity, and as applicable:
10.1(a)(1)	take action to control and correct it; and
10.1(a)(2)	deal with the consequences;
10.1(e)	make changes to the information security management system, if necessary.
10.1(f)	the nature of the nonconformities and any subsequent actions taken, and

Mapping of ISO/IEC 27001:2013 to ISO/IEC 27001:2005

Note that when looking at the mapping at an individual requirement level, one finds that some 2013 ISMS requirements actually map on to 2005 Annex A controls.

Clause (in ISO/IEC 27001:2013)	Requirement	ISO/IEC 27001:2005
4.1	The organization shall determine external and inte...	**8.3, 8.3(a), 8.3(e)**
4.2(a)	the interested parties that are relevant to the i...	**This is a new requirement**
4.2(b)	the requirements of these interested parties rele...	**5.2.1(c), 7.3(c)(4), 7.3(c)(5)**
4.3	The organization shall determine the boundaries an...	**4.2.1(a)**
4.3(a)	the external and internal issues referred to in 4...	**4.2.3(e)**
4.3(b)	the requirements referred to in 4.2; and	**4.2.3(e)**
4.3(c)	interfaces and dependencies between activities pe...	**This is a new requirement**
4.3(c)	The scope shall be available as documented informa...	**4.3.1(b)**
4.4	The organization shall establish, implement, maint...	**4.1, 5.2.1(a)**
5.1(a)	ensuring the information security policy and the ...	**4.2.1(b)(3)**
5.1(b)	ensuring the integration of the information secur...	**This is a new requirement**
5.1(c)	ensuring that the resources needed for the inform...	**5.1(e)**
5.1(d)	communicating the importance of effective informa...	**5.1(c)**
5.1(e)	ensuring that the information security management...	**5.1(b), 5.1(g), 5.1(h)**
5.1(f)	directing and supporting persons to contribute to...	**5.1(b), 5.1(g), 5.1(h)**
5.1(g)	promoting continual improvement; and	**5.1(c)**
5.1(h)	supporting other relevant management roles to dem...	**5.1**
5.2	Top management shall establish an information secu...	**4.2.1(b)(5), 5.1(a)**
5.2(a)	is appropriate to the purpose of the organization...	**4.2.1(b)**
5.2(b)	includes information security objectives (see 6.2...	**4.2.1(b)(1)**
5.2(c)	includes a commitment to satisfy applicable requi...	**4.2.1(b)(2), 4.3.3**
5.2(d)	includes a commitment to continual improvement of...	**5.1(c)**
5.2(e)	be available as documented information;	**4.3.1(a)**
5.2(f)	be communicated within the organization;	**5.1(c)**
5.2(g)	be available to interested parties, as appropriat...	**4.3.2(e)**
5.3	Top management shall ensure that the responsibilit...	**5.1(c)**
5.3(a)	ensuring that the information security management...	**4.3.3**
5.3(b)	reporting on the performance of the information s...	**4.3.3**
6.1.1	When planning for the information security managem...	**4.2.1(d), 8.3(a)**
6.1.1(a)	ensure information security management system can...	**This is a new requirement**
6.1.1(b)	prevent, or reduce, undesired effects; and	**This is a new requirement**
6.1.1(c)	achieve continual improvement.	**This is a new requirement**
6.1.1(d)	actions to address these risks and opportunities,...	**4.2.1(e)(4), 8.3(b), 8.3(c)**

Continued >>

Clause (in ISO/IEC 27001:2013)	Requirement	ISO/IEC 27001:2005
6.1.1(e)(1)	integrate and implement the actioninto its info...	**4.3.1(f), 8.3(c)**
6.1.1(e)(2)	evaluate the effectiveness of these actions.	**7.2(f)**
6.1.2	The organization shall define and apply an informa...	**4.2.1(c), 4.2.1(c)(1)**
6.1.2(a)	establishes and maintains information security ri...	**This is a new requirement**
6.1.2(a)(1)	the risk acceptance criteria; and	**4.2.1(b)(4), 4.2.1(c)(2), 5.1(f)**
6.1.2(a)(2)	criteria for performing information security risk...	**4.2.3(d)**
6.1.2(b)	ensures that repeated risk assessments shall prod...	**4.2.1(c)(2)**
6.1.2(c)	Identify the information security risks.	**4.2.1(d)**
6.1.2(c)(1)	apply the information security risk assessment pr...	**4.2.1(d)(1), 4.2.1(d)(2), 4.2.1(d)(3), 4.2.1(d)(4)**
6.1.2(c)(2)	identify the risk owners;	**4.2.1(d)(1)**
6.1.2(d)	analyses the information security risks:	**4.2.1(e)**
6.1.2(d)(1)	assess the potential consequences that would resu...	**4.2.1(e)(1)**
6.1.2(d)(2)	assess the realistic likelihood of the occurrence...	**4.2.1(e)(2)**
6.1.2(d)(3)	determine the levels of risk;	**4.2.1(e)(3)**
6.1.2(e)	evaluates the information security risks:	**4.2.1(e)(4)**
6.1.2(e)(1)	compare the results of risk analysis with the ris...	**4.2.1(e)(4)**
6.1.2(e)(2)	prioritise the analysed risks for risk treatment....	**4.2.1(e)(4)**
6.1.2(e)(2)	The organization shall retain documented informati...	**4.3.1(d), 4.3.1(e)**
6.1.3	The organization shall define and apply an informa...	**4.2.1(c)(1)**
6.1.3(a)	select appropriate information security risk trea...	**4.2.1(f), 4.2.1(f)(1), 4.2.1(f)(2), 4.2.1(f)(3), 4.2.1(f)(4)**
6.1.3(b)	determine all controls that are necessary to impl...	**4.2.1(g)**
6.1.3(c)	compare the controls determined in 6.1.3 b) above...	**4.2.1(j)(1), 4.2.1(j)(3)**
6.1.3(d)	produce a Statement of Applicability that contain...	**4.2.1(j), 4.2.1(j)(1), 4.2.1(j)(2), 4.2.1(j)(3), 4.3.1(i)**
6.1.3(e)	formulate an information security risk treatment ...	**4.2.2(a)**
6.1.3(f)	obtain risk owners' approval of the information s...	**4.2.1(h)**
6.1.3(f)	The organization shall retain documented informati...	**4.3.1(f)**
6.2	The organization shall establish information secur...	**5.1(b)**
6.2(a)	be consistent with the information security polic...	**5.1(c)**
6.2(b)	be measurable (if practicable)	**This is a new requirement**
6.2(c)	take into account applicable information security...	**This is a new requirement**
6.2(c)	and results from risk assessment and risk treatmen...	**This is a new requirement**
6.2(d)	be communicated, and	**5.1(c)**
6.2(e)	be updated as appropriate.	**4.2.3(b)**
6.2(e)	The organization shall retain documented informati...	**4.3.1(a)**
6.2(f)	what will be done;	**This is a new requirement**

Continued >>

Clause (in ISO/IEC 27001:2013)	Requirement	ISO/IEC 27001:2005
6.2(g)	what resources will be required;	**This is a new requirement**
6.2(h)	who will be responsible;	**This is a new requirement**
6.2(i)	when it will be completed; and	**This is a new requirement**
6.2(k)	how the results will be evaluated.	**This is a new requirement**
7.1	The organization shall determine and provide the r...	**4.2.2(g), 5.2.1**
7.2(a)	determine the necessary competence of person(s) d...	**5.2.2, 5.2.2(a)**
7.2(b)	ensure these persons are competent on the basis o...	**5.2.2**
7.2(c)	where applicable, take actions to acquire the nec...	**5.2.2(b), 5.2.2(c)**
7.2(d)	retain appropriate documented information as evid...	**5.2.2(d)**
7.3(a)	the information security policy;	**This is a new requirement**
7.3(b)	their contribution to the effectiveness of the in...	**4.2.2(e), 5.2.2(d)**
7.3(c)	the implications of not conforming with the infor...	**4.2.2(e), 5.2.2(d)**
7.4	The organization shall determine the need for inte...	**4.2.4(c), 5.1(c)**
7.4(a)	on what to communicate;	**This is a new requirement**
7.4(b)	when to communicate;	**This is a new requirement**
7.4(c)	with whom to communicate;	**This is a new requirement**
7.4(d)	who shall communicate; and	**This is a new requirement**
7.4(e)	the processes by which communication shall be eff...	**This is a new requirement**
7.5.1(a)	documented information required by this Internati...	**4.3.1(a), 4.3.1(b), 4.3.1(h), 4.3.1(i)**
7.5.1(b)	documented information determined by the organiza...	**This is a new requirement**
7.5.2(a)	identification and description (e.g. a title, dat...	**4.3.2(j)**
7.5.2(b)	format(e.g. language, software version, graphics)...	4.3.1(i)
7.5.2(c)	review and approval for suitability and adequacy.	**4.3.2(a), 4.3.2(b)**
7.5.3	Documented information required by the information...	4.3.2
7.5.3(a)	it is available and suitable for use, where and w...	**4.3.2(d)**
7.5.3(b)	it is adequately protected (e.g. from loss of con...	**4.3.3**
7.5.3(c)	distribution, access, retrieval and use;	**4.3.2(e), 4.3.2(h), 4.3.2(i)**
7.5.3(d)	storage and preservation, including preservation ...	**4.3.2(e), 4.3.3**
7.5.3(e)	control of changes (e.g. version control);	**4.3.2(c)**
7.5.3(f)	retention and disposition	**4.3.2(e)**
7.5.3(f)	Documented information of external origin determin...	**4.3.2(g)**
8.1	The organization shall plan, implement and control...	**This is a new requirement**
8.1	The organization shall also implement plans to ach...	**4.2.2(f)**
8.1	The organization shall keep documented information...	**4.3.3**
8.1	The organization shall control planned changes and...	**A.10.1.2, A.12.5.1, A.12.5.2, A.12.5.3**
8.1	review the consequences of unintended changes, tak...	**4.2.2(h), 8.3(b), 8.3(c)**

Continued >>

Clause (in ISO/IEC 27001:2013)	Requirement	ISO/IEC 27001:2005
8.1	The organization shall ensure that outsourced proc...	**A.10.2.1, A.10.2.2, A.10.2.3, A.12.5.5**
8.2	The organization shall perform information securit...	**4.2.3(d)**
8.2	The organization shall retain documented informati...	**4.3.1(e)**
8.3	The organization shall implement the information s...	**4.2.2(b), 4.2.2(c)**
8.3	The organization shall retain documented informati...	**4.3.3**
9.1	The organization shall evaluate the information se...	**4.2.3(a)(3), 4.2.3(b), 4.2.3(c), 4.2.3(e), 6(d)**
9.1(a)	what needs to be monitored and measured, including...	**4.2.2(d)**
9.1(b)	the methods for monitoring, measurement, analysis...	**4.2.2(d)**
9.1(c)	when the monitoring and measuring shall be perfor...	**This is a new requirement**
9.1(d)	who shall monitor and measure;	**This is a new requirement**
9.1(e)	when the results from monitoring and measurement ...	**4.2.3(b)**
9.1(f)	who shall analyse and evaluate these results.	**This is a new requirement**
9.1(f)	The organization shall retain appropriate document...	**4.3.1(f)**
9.2	The organization shall conduct internal audits at ...	**4.2.3(e), 6**
9.2(a)(1)	the organization's own requirements for its infor...	**6(b)**
9.2(a)(2)	the requirements of this International Standard.	**6(a)**
9.2(b)	is effectively implemented and maintained.	**6(c)**
9.2(c)	plan, establish, implement and maintain an audit ...	**6(d)**
9.2(d)	define the audit criteria and scope for each audi...	**6(d)**
9.2(e)	select auditors and conduct audits to ensure obje...	**6(d)**
9.2(f)	ensure that the results of the audits are reporte...	**6(d)**
9.2(g)	retain documented information as evidence of the ...	**4.3.1(h), 4.3.3**
9.3	Top management shall review the organization's inf...	**5.2.1(e), 7.1**
9.3(a)	the status of actions from previous management re...	**7.2(g)**
9.3(b)	changes in external and internal issues that are ...	**4.2.3(d)(1), 4.2.3(d)(2), 4.2.3(d)(3), 4.2.3(d)(4), 4.2.3(d)(5), 4.2.3(d)(6), 7.2(c), 7.2(e), 7.2(h)**
9.3(c)	feedback on the information security performance,...	**7.2(f)**
9.3(c)(1)	nonconformities and corrective actions;	**7.2(d)**
9.3(c)(2)	monitoring and measurement evaluation results;	**7.2(f)**
9.3(c)(3)	audit results; and	**7.2(a)**
9.3(c)(4)	fulfilment of information security objectives;	**This is a new requirement**
9.3(d)	feedback from interested parties;	**7.2(b)**
9.3(e)	results of risk assessment and status of risk tre...	7.2(e), 7.2(f)
9.3(f)	opportunities for continual improvement.	**7.2(i)**
9.3(f)	The outputs of the management review shall include...	**4.2.3(e), 7.1, 7.3(a)**

Continued >>

Clause (in ISO/IEC 27001:2013)	Requirement	ISO/IEC 27001:2005
9.3(f)	and any need for changes to the information securi...	**4.2.3(d)(1), 4.2.3(d)(2), 4.2.3(d)(3), 4.2.3(d)(5), 4.2.3(d)(6), 4.2.3(g), 7.1, 7.3(b), 7.3(c), 7.3(c)(1), 7.3(c)(2), 7.3(c)(3), 7.3(c)(4), 7.3(c)(5), 7.3(c) (6), 7.3(d), 7.3(e)**
9.3(f)	The organization shall retain documented informati...	**4.3.1(h), 7.1**
10.1(a)	react to the nonconformity, and as applicable:	**This is a new requirement**
10.1(a)(1)	take action to control and correct it; and	**This is a new requirement**
10.1(a)(2)	deal with the consequences;	**This is a new requirement**
10.1(b)	evaluate the need for action to eliminate the cau...	**8.2(c), 8.3(b)**
10.1(b)(1)	reviewing the nonconformity;	**8.2(a)**
10.1(b)(2)	determining the causes of the nonconformity;	**8.2(b)**
10.1(b)(3)	determining if similar nonconformities exist, or ...	**8.3(a)**
10.1(c)	implement any action needed;	**4.2.4(a), 8.2, 8.2(d)**
10.1(d)	review the effectiveness of any corrective action...	**8.2, 8.2(f)**
10.1(e)	make changes to the information security manageme...	**This is a new requirement**
10.1(e)	Corrective actions shall be appropriate to the eff...	**8.3**
10.1(f)	the nature of the nonconformities and any subsequ...	**This is a new requirement**
10.1(g)	the results of any corrective action.	**8.2(e)**
10.2	The organization shall continually improve the sui...	**4.2.4(a), 4.2.4(d), 5.2.1(f), 8.1**

Mapping of ISO/IEC 27001:2005 to ISO/IEC 27001:2013

Clause (in ISO/IEC 27001:2005)	Requirement	ISO/IEC 27001:2013
4.1	The organization shall establish, implement, opera...	**4.4**
4.2.1(a)	Define the scope and boundaries of the ISMS in te...	**4.3**
4.2.1(b)	Define an ISMS policy in terms of the characteris...	**5.2(a)**
4.2.1(b)(1)	includes a framework for setting objectives and e...	**5.2(b)**
4.2.1(b)(2)	takes into account business and legal or regulato...	**5.2(c)**
4.2.1(b)(3)	aligns with the organization's strategic risk man...	**5.1(a)**
4.2.1(b)(4)	establishes criteria against which risk will be e...	**6.1.2(a)(1)**
4.2.1(b)(5)	has been approved by management.	**5.2**
4.2.1(c)	Define the risk assessment approach of the organi...	**6.1.2**
4.2.1(c)(1)	Identify a risk assessment methodology that is su...	**6.1.2, 6.1.3**
4.2.1(c)(2)	Develop criteria for accepting risks and identify...	**6.1.2(a)(1)**
4.2.1(c)(2)	The risk assessment methodology selected shall ens...	**6.1.2(b)**
4.2.1(d)	Identify the risks.	**6.1.1, 6.1.2(c)**
4.2.1(d)(1)	Identify the assets within the scope of the ISMS,...	**6.1.2(c)(1), 6.1.2(c)(2)**
4.2.1(d)(2)	Identify the threats to those assets.	**6.1.2(c)(1)**
4.2.1(d)(3)	Identify the vulnerabilities that might be exploi...	**6.1.2(c)(1)**
4.2.1(d)(4)	Identify the impacts that losses of confidentiali...	**6.1.2(c)(1)**
4.2.1(e)	Analyse and evaluate the risks.	**6.1.2(d)**
4.2.1(e)(1)	Assess the business impact upon the organization ...	**6.1.2(d)(1)**
4.2.1(e)(2)	Assess the realistic likelihood of such a securit...	**6.1.2(d)(2)**
4.2.1(e)(3)	Estimate the levels of risks.	**6.1.2(d)(3)**
4.2.1(e)(4)	Determine whether the risk is acceptable or requi...	**6.1.1(d), 6.1.2(e), 6.1.2(e)(1), 6.1.2(e)(2)**
4.2.1(f)	Identify and evaluate options for the treatment o...	**6.1.3(a)**
4.2.1(f)(1)	applying appropriate controls;	**6.1.3(a)**
4.2.1(f)(2)	knowingly and objectively accepting risks, provid...	**6.1.3(a)**
4.2.1(f)(3)	avoiding risks; and	**6.1.3(a)**
4.2.1(f)(4)	transferring the associated business risks to oth...	**6.1.3(a)**
4.2.1(g)	Select control objectives and controls for the tr...	**6.1.3(b)**
4.2.1(g)	Controls objectives and controls shall be selected...	**6.1.3(b)**
4.2.1(g)	The control objectives and controls from Annex A s...	**This is a deleted requirement**
4.2.1(h)	Obtain management approval of the proposed residu...	**6.1.3(f)**
4.2.1(i)	Obtain management authorization to implement and ...	**This is a deleted requirement**
4.2.1(j)	A Statement of Applicability shall be prepared tha...	**6.1.3(d)**
4.2.1(j)(1)	the control objectives and controls, selected in ...	**6.1.3(c), 6.1.3(d)**
4.2.1(j)(2)	the control objectives and controls currently imp...	**6.1.3(d)**

Continued >>

Clause (in ISO/IEC 27001:2005)	Requirement	ISO/IEC 27001:2013
4.2.1(j)(3)	the exclusion of any control objectives and contr...	**6.1.3(c), 6.1.3(d)**
4.2.2(a)	Formulate a risk treatment plan that identifies t...	**6.1.3(e)**
4.2.2(b)	Implement the risk treatment plan in order to ach...	**8.3**
4.2.2(c)	Implement controls selected in 4.2.1g) to meet th...	**8.3**
4.2.2(d)	Define how to measure the effectiveness of the se...	**9.1(a), 9.1(b)**
4.2.2(e)	Implement training and awareness programmes (see ...	7.3(b), 7.3(c)
4.2.2(f)	Manage operations of the ISMS.	**8.1**
4.2.2(g)	Manage resources for the ISMS (see 5.2).	**7.1**
4.2.2(h)	Implement procedures and other controls capable o...	**8.1**
4.2.3(a)(1)	promptly detect errors in the results of processi...	**This is a deleted requirement**
4.2.3(a)(2)	promptly identify attempted and successful securi...	**This is a deleted requirement**
4.2.3(a)(3)	enable management to determine whether the securi...	**9.1**
4.2.3(a)(4)	help detect security events and thereby prevent s...	**This is a deleted requirement**
4.2.3(a)(5)	determine whether the actions taken to resolve a ...	**This is a deleted requirement**
4.2.3(b)	Undertake regular reviews of the effectiveness of...	**6.2(e), 9.1, 9.1(e)**
4.2.3(c)	Measure the effectiveness of controls to verify t...	**9.1**
4.2.3(d)	Review risk assessments at planned intervals and ...	**6.1.2(a)(2), 8.2**
4.2.3(d)(1)	the organization;	**9.3(b), 9.3(f)**
4.2.3(d)(2)	technology;	**9.3(b), 9.3(f)**
4.2.3(d)(3)	business objectives and processes;	**9.3(b), 9.3(f)**
4.2.3(d)(4)	identified threats;	**9.3(b)**
4.2.3(d)(5)	effectiveness of the implemented controls; and	**9.3(b), 9.3(f)**
4.2.3(d)(6)	external events, such as changes to the legal or ...	**9.3(b), 9.3(f)**
4.2.3(e)	Conduct internal ISMS audits at planned intervals...	**9.2**
4.2.3(e)	f) Undertake a management review of the ISMS on a...	**4.3(a), 4.3(b), 9.1**
4.2.3(e)	improvements in the ISMS process are identified (s...	**9.3(f)**
4.2.3(g)	Update security plans to take into account the fi...	**9.3(f)**
4.2.3(h)	Record actions and events that could have an impa...	**This is a deleted requirement**
4.2.4(a)	Implement the identified improvements in the ISMS...	**10.2**
4.2.4(a)	b) Take appropriate corrective and preventive act...	**10.1(c)**
4.2.4(a)	Apply the lessons learnt from the security experie...	**10.2**
4.2.4(c)	Communicate the actions and improvements to all i...	**7.4**
4.2.4(d)	Ensure that the improvements achieve their intend...	10.2
4.3.1	Documentation shall include records of management ...	**This is a deleted requirement**
4.3.1	It is important to be able to demonstrate the rela...	**This is a deleted requirement**
4.3.1(a)	documented statements of the ISMS policy (see 4.2...	**5.2(e), 6.2(e), 7.5.1(a)**
4.3.1(b)	the scope of the ISMS	**(see 4.2.1a));4.3(c), 7.5.1(a)**

Continued >>

Clause (in ISO/IEC 27001:2005)	Requirement	ISO/IEC 27001:2013
4.3.1(c)	procedures and controls in support of the ISMS;	**This is a deleted requirement**
4.3.1(d)	a description of the risk assessment methodology ...	**6.1.2(e)(2)**
4.3.1(e)	the risk assessment report (see 4.2.1c) to 4.2.1g...	**6.1.2(e)(2), 8.2**
4.3.1(f)	the risk treatment plan (see 4.2.2b));	**6.1.1(e)(1), 6.1.3(f)**
4.3.1(f)	g) documented procedures needed by the organizati...	**9.1(f)**
4.3.1(f)	and describe how to measure the effectiveness of c...	**9.1(f)**
4.3.1(h)	records required by this International Standard (...	**7.5.1(a), 9.2(g), 9.3(f)**
4.3.1(i)	the Statement of Applicability.	**6.1.3(d), 7.5.1(a)**
4.3.1(i)	NOTE 3: Documents and records may be in any form o...	**7.5.2(b)**
4.3.2	Documents required by the ISMS shall be protected ...	**7.5.3**
4.3.2	A documented procedure shall be established to def...	**This is a deleted requirement**
4.3.2(a)	approve documents for adequacy prior to issue;	**7.5.2(c)**
4.3.2(b)	review and update documents as necessary and re-a...	**7.5.2(c)**
4.3.2(c)	ensure that changes and the current revision stat...	**7.5.3(e)**
4.3.2(d)	ensure that relevant versions of applicable docum...	**7.5.3(a)**
4.3.2(e)	ensure that documents remain legible and readily ...	**7.5.3(d)**
4.3.2(e)	f) ensure that documents are available to those w...	**5.2(g), 7.5.3(c)**
4.3.2(e)	and are transferred, stored and ultimately	**7.5.3(f)**
4.3.2(e)	disposed of in accordance with the procedures appl...	**7.5.3(f)**
4.3.2(g)	ensure that documents of external origin are iden...	**7.5.3(f)**
4.3.2(h)	ensure that the distribution of documents is cont...	**7.5.3(c)**
4.3.2(i)	prevent the unintended use of obsolete documents;...	**7.5.3(c)**
4.3.2(j)	apply suitable identification to them if they are...	**7.5.2(a)**
4.3.3	Records shall be established and maintained to pro...	**9.2(g)**
4.3.3	They shall be protected and controlled.	**7.5.3(b)**
4.3.3	The ISMS shall take account of any relevant legal ...	**5.2(c)**
4.3.3	Records shall remain legible, readily identifiable...	**7.5.3(d)**
4.3.3	The controls needed for the identification, storag...	**This is a deleted requirement**
4.3.3	Records shall be kept of the performance of the pr...	**5.3(a), 5.3(b), 8.1, 8.3**
4.3.3	and of all occurrences of significant security inc...	**This is a deleted requirement**
5.1	Management shall provide evidence of its commitmen...	**5.1(h)**
5.1(a)	establishing an ISMS policy;	**5.2**
5.1(b)	ensuring that ISMS objectives and plans are estab...	**5.1(e), 5.1(f), 6.2**
5.1(c)	establishing roles and responsibilities for infor...	**5.3**
5.1(c)	d) communicating to the organization the importan...	**5.1(d), 5.2(f), 6.2(a), 6.2(d), 7.4**
5.1(c)	and the need for continual improvement;	**5.1(g), 5.2(d)**
5.1(e)	providing sufficient resources to establish, impl...	**5.1(c)**

Continued >>

Clause (in ISO/IEC 27001:2005)	Requirement	ISO/IEC 27001:2013
5.1(f)	deciding the criteria for accepting risks and for...	**6.1.2(a)(1)**
5.1(g)	ensuring that internal ISMS audits are conducted ...	**5.1(e), 5.1(f)**
5.1(h)	conducting management reviews of the ISMS (see 7)...	**5.1(e), 5.1(f)**
5.2.1	The organization shall determine and provide the r...	**7.1**
5.2.1(a)	establish, implement, operate, monitor, review, m...	**4.4**
5.2.1(b)	ensure that information security procedures suppo...	**This is a deleted requirement**
5.2.1(c)	identify and address legal and regulatory require...	**4.2(b)**
5.2.1(d)	maintain adequate security by correct application...	**This is a deleted requirement**
5.2.1(e)	carry out reviews when necessary, and to react ap...	**9.3**
5.2.1(f)	where required, improve the effectiveness of the ...	**10.2**
5.2.2	The organization shall ensure that all personnel w...	**7.2(a), 7.2(b)**
5.2.2(a)	determining the necessary competencies for person...	**7.2(a)**
5.2.2(b)	providing training or taking other actions (e.g. ...	**7.2(c)**
5.2.2(c)	evaluating the effectiveness of the actions taken...	**7.2(c)**
5.2.2(d)	maintaining records of education, training, skill...	**7.2(d)**
5.2.2(d)	The organization shall also ensure that all releva...	**7.3(b), 7.3(c)**
6	The organization shall conduct internal ISMS audit...	**9.2**
6(a)	conform to the requirements of this International...	**9.2(a)(2)**
6(b)	conform to the identified information security re...	**9.2(a)(1)**
6(c)	are effectively implemented and maintained; and	**9.2(b)**
6(d)	perform as expected.	**9.1**
6(d)	An audit programme shall be planned, taking into c...	**9.2(c)**
6(d)	The audit criteria, scope,	**9.2(d)**
6(d)	frequency and methods shall be defined.	**9.2(c)**
6(d)	Selection of auditors and conduct of audits shall ...	**9.2(e)**
6(d)	Auditors shall not audit their own work.	**9.2(e)**
6(d)	The responsibilities and requirements for planning...	**This is a deleted requirement**
6(d)	The management responsible for the area being audi...	**9.2(f)**
7.1	Management shall review the organization's ISMS at...	**9.3**
7.1	This review shall include assessing opportunities ...	**9.3(f)**
7.1	and the need for changes to the ISMS, including th...	**9.3(f)**
7.1	The results of the reviews shall be clearly docume...	**9.3(f)**
7.2(a)	results of ISMS audits and reviews;	**9.3(c)(3)**
7.2(b)	feedback from interested parties;	**9.3(d)**
7.2(c)	techniques, products or procedures, which could b...	**9.3(b)**
7.2(d)	status of preventive and corrective actions;	**9.3(c)(1)**
7.2(e)	vulnerabilities or threats not adequately address...	**9.3(b), 9.3(e)**

Continued >>

Clause (in ISO/IEC 27001:2005)	Requirement	ISO/IEC 27001:2013
7.2(f)	results from effectiveness measurements;	**6.1.1(e)(2), 9.3(c), 9.3(c)(2), 9.3(e)**
7.2(g)	follow-up actions from previous management review...	**9.3(a)**
7.2(h)	any changes that could affect the ISMS; and	**9.3(b)**
7.2(i)	recommendations for improvement.	**9.3(f)**
7.3(a)	Improvement of the effectiveness of the ISMS.	**9.3(f)**
7.3(b)	Update of the risk assessment and risk treatment ...	**9.3(f)**
7.3(c)	Modification of procedures and controls that effe...	**9.3(f)**
7.3(c)(1)	business requirements;	**9.3(f)**
7.3(c)(2)	security requirements ;	**9.3(f)**
7.3(c)(3)	business processes effecting the existing busines...	**9.3(f)**
7.3(c)(4)	regulatory or legal requirements;	**4.2(b), 9.3(f)**
7.3(c)(5)	contractual obligations; and	**4.2(b), 9.3(f)**
7.3(c)(6)	levels of risk and/or risk acceptance criteria.	**9.3(f)**
7.3(d)	Resource needs.	**9.3(f)**
7.3(e)	Improvement to how the effectiveness of controls ...	**9.3(f)**
8.1	The organization shall continually improve the eff...	**10.2**
8.2	The organization shall take action to eliminate th...	**10.1(c), 10.1(d)**
8.2	The documented procedure for corrective action sha...	**This is a deleted requirement**
8.2(a)	identifying nonconformities;	**10.1(b)(1)**
8.2(b)	determining the causes of nonconformities;	**10.1(b)(2)**
8.2(c)	evaluating the need for actions to ensure that no...	**10.1(b)**
8.2(d)	determining and implementing the corrective actio...	**10.1(c)**
8.2(e)	recording results of action taken (see 4.3.3); an...	**10.1(g)**
8.2(f)	reviewing of corrective action taken.	**10.1(d)**
8.3	The organization shall determine action to elimina...	**4.1**
8.3	Preventive actions taken shall be appropriate to t...	**10.1(e)**
8.3	The documented procedure for preventive action sha...	**This is a deleted requirement**
8.3(a)	identifying potential nonconformities and their c...	**4.1, 6.1.1, 10.1(b)(3)**
8.3(b)	evaluating the need for action to prevent occurre...	**6.1.1(d), 8.1, 10.1(b)**
8.3(c)	determining and implementing preventive action ne...	**6.1.1(d), 6.1.1(e)(1), 8.1**
8.3(d)	recording results of action taken (see 4.3.3); an...	**This is a deleted requirement**
8.3(e)	reviewing of preventive action taken.	**This is a deleted requirement**
8.3(e)	The organization shall identify changed risks and ...	**4.1**
8.3(e)	The priority of preventive actions shall be determ...	**This is a deleted requirement**

Deleted ISMS requirements

Clause (in ISO/IEC 27001:2005)	Deleted requirement
4.2.1(g)	The control objectives and controls from Annex A shall be selected as part of this process as suitable to cover these requirements.
4.2.1(i)	Obtain management authorization to implement and operate the ISMS.
4.2.3(a)(1)	promptly detect errors in the results of processing;
4.2.3(a)(2)	promptly identify attempted and successful security breaches and incidents;
4.2.3(a)(4)	help detect security events and thereby prevent security incidents by the use of indicators; and
4.2.3(a)(5)	determine whether the actions taken to resolve a breach of security were effective.
4.2.3(h)	Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3).
4.3.1	Documentation shall include records of management decisions, ensure that actions are traceable to management decisions and policies, and the recorded results are reproducible.
4.3.1	It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives.
4.3.1(c)	procedures and controls in support of the ISMS;
4.3.2	A documented procedure shall be established to define the management actions needed to:
4.3.3	The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented.
4.3.3	and of all occurrences of significant security incidents related to the ISMS.
5.2.1(b)	ensure that information security procedures support the business requirements;
5.2.1(d)	maintain adequate security by correct application of all implemented controls;
6(d)	The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.3.3) shall be defined in a documented procedure.
8.2	The documented procedure for corrective action shall define requirements for:
8.3	The documented procedure for preventive action shall define requirements for:
8.3(d)	recording results of action taken (see 4.3.3); and
8.3(e)	reviewing of preventive action taken.
8.3(e)	The priority of preventive actions shall be determined based on the results of the risk assessment.

Group 2 - Annex A controls

New Annex A controls

Annex A control (in ISO/IEC 27001:2013)		
A.6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of project.
A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.
A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development efforts.
A.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environment for system development and integration efforts that cover the entire system development lifecycle.
A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.
A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier access to organization's assets shall be documented.
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.
A.16.1.4	Assessment and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.
A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

Mapping of Annex A controls in ISO/IEC 27001:2013 to ISO/IEC 27001:2005

Annex A control (in ISO/IEC 27001:2013)		Annex A control (in ISO/IEC 27001:2005)
A.5.1.1	Policies for information security	**A.5.1.1**
A.5.1.2	Review of the policies for information security	**A.5.1.2**
A.6.1.1	Information security roles and responsibilities	**A.6.1.3, A.8.1.1**
A.6.1.2	Segregation of duties	**A.10.1.3**
A.6.1.3	Contact with authorities	**A.6.1.6**
A.6.1.4	Contact with special interest groups	**A.6.1.7**
A.6.1.5	Information security in project management	**This is a new Annex A control**
A.6.2.1	Mobile device policy	**A.11.7.1**
A.6.2.2	Teleworking	**A.11.7.2**
A.7.1.1	Screening	**A.8.1.2**
A.7.1.2	Terms and conditions of employment	**A.8.1.3**
A.7.2.1	Management responsibilities	**A.8.2.1**
A.7.2.2	Information security awareness, education and training	**A.8.2.2**
A.7.2.3	Disciplinary process	**A.8.2.3**
A.7.3.1	Termination or change of employment responsibilities	**A.8.3.1**
A.8.1.1	Inventory of assets	**A.7.1.1**
A.8.1.2	Ownership of assets	**A.7.1.2**
A.8.1.3	Acceptable use of assets	**A.7.1.3**
A.8.1.4	Return of assets	**A.8.3.2**
A.8.2.1	Classification of information	**A.7.2.1**
A.8.2.2	Labelling of information	**A.7.2.2**
A.8.2.3	Handling of assets	**A.10.7.3**
A.8.3.1	Management of removable media	**A.10.7.1**
A.8.3.2	Disposal of media	**A.10.7.2**
A.8.3.3	Physical media transfer	**A.10.8.3**
A.9.1.1	Access control policy	**A.11.1.1**
A.9.1.2	Access to networks and network services	**A.11.4.1**
A.9.2.1	User registration and de-registration	**A.11.2.1, A.11.5.2**
A.9.2.2	User access provisioning	**A.11.2.1**
A.9.2.3	Privilege management	**A.11.2.2**
A.9.2.4	Management of secret authentication information of users	**A.11.2.3**
A.9.2.5	Review of user access rights	**A.11.2.4**
A.9.2.6	Removal or adjustment of access rights	**A.8.3.3**
A.9.3.1	Use of secret authentication information	**A.11.3.1**

Continued >>

Annex A control (in ISO/IEC 27001:2013)		Annex A control (in ISO/IEC 27001:2005)
A.9.4.1	Information access restriction	**A.11.6.1**
A.9.4.2	Secure log-on procedures	**A.11.5.1, A.11.5.5, A.11.5.6**
A.9.4.3	Password management system	**A.11.5.3**
A.9.4.4	Use of privileged utility programs	**A.11.5.4**
A.9.4.5	Access control to program source code	**A.12.4.3**
A.10.1.1	Policy on the use of cryptographic controls	**A.12.3.1**
A.10.1.2	Key management	**A.12.3.2**
A.11.1.1	Physical security perimeter	**A.9.1.1**
A.11.1.2	Physical entry controls	**A.9.1.2**
A.11.1.3	Securing office, rooms and facilities	**A.9.1.3**
A.11.1.4	Protecting against external end environmental threats	**A.9.1.4**
A.11.1.5	Working in secure areas	**A.9.1.5**
A.11.1.6	Delivery and loading areas	**A.9.1.6**
A.11.2.1	Equipment siting and protection	**A.9.2.1**
A.11.2.2	Supporting utilities	**A.9.2.2**
A.11.2.3	Cabling security	**A.9.2.3**
A.11.2.4	Equipment maintenance	**A.9.2.4**
A.11.2.5	Removal of assets	**A.9.2.7**
A.11.2.6	Security of equipment and assets off-premises	**A.9.2.5**
A.11.2.7	Security disposal or re-use of equipment	**A.9.2.6**
A.11.2.8	Unattended user equipment	**A.11.3.2**
A.11.2.9	Clear desk and clear screen policy	**A.11.3.3**
A.12.1.1	Documented operating procedures	**A.10.1.1**
A.12.1.2	Change management	**A.10.1.2**
A.12.1.3	Capacity management	**A.10.3.1**
A.12.1.4	Separation of development, test and operational environments	**A.10.1.4**
A.12.2.1	Controls against malware	**A.10.4.1, A.10.4.2**
A.12.3.1	Information backup	**A.10.5.1**
A.12.4.1	Event logging	**A.10.10.1, A.10.10.2, A.10.10.5**
A.12.4.2	Protection of log information	**A.10.10.3**
A.12.4.3	Administrator and operator logs	**A.10.10.3, A.10.10.4**
A.12.4.4	Clock synchronisation	**A.10.10.6**
A.12.5.1	Installation of software on operational systems	**A.12.4.1**
A.12.6.1	Management of technical vulnerabilities	**A.12.6.1**
A.12.6.2	Restrictions on software installation	**This is a new Annex A control**
A.12.7.1	Information systems audit controls	**A.15.3.1**
A.13.1.1	Network controls	**A.10.6.1**

Continued >>

Annex A control (in ISO/IEC 27001:2013)		Annex A control (in ISO/IEC 27001:2005)
A.13.1.2	Security of network services	**A.10.6.2**
A.13.1.3	Segregation in networks	**A.11.4.5**
A.13.2.1	Information transfer policies and procedures	**A.10.8.1**
A.13.2.2	Agreements on information transfer	**A.10.8.2**
A.13.2.3	Electronic messaging	**A.10.8.4**
A.13.2.4	Confidentiality or non-disclosure agreements	**A.6.1.5**
A.14.1.1	Security requirements analysis and specification	**A.12.1.1**
A.14.1.2	Securing applications services on public networks	**A.10.9.1, A.10.9.3**
A.14.1.3	Protecting application services transactions	**A.10.9.2**
A.14.2.1	Secure development policy	**This is a new Annex A control**
A.14.2.2	System change control procedures	**A.12.5.1**
A.14.2.3	Technical review of applications after operating platform changes	**A.12.5.2**
A.14.2.4	Restrictions on changes to software packages	**A.12.5.3**
A.14.2.5	Secure system engineering principles	**This is a new Annex A control**
A.14.2.6	Secure development environment	**This is a new Annex A control**
A.14.2.7	Outsourced development	**A.12.5.5**
A.14.2.8	System security testing	**This is a new Annex A control**
A.14.2.9	System acceptance testing	**A.10.3.2**
A.14.3.1	Protection of test data	**A.12.4.2**
A.15.1.1	Information security policy for supplier relationships	**This is a new Annex A control**
A.15.1.2	Addressing security within supplier agreements	**A.6.2.3**
A.15.1.3	Information and communication technology supply chain	**This is a new Annex A control**
A.15.2.1	Monitoring and review of supplier services	**A.10.2.2**
A.15.2.2	Managing changes to supplier services	**A.10.2.3**
A.16.1.1	Responsibilities and procedures	**A.13.2.1**
A.16.1.2	Reporting information security events	**A.13.1.1**
A.16.1.3	Reporting information security weaknesses	**A.13.1.2**
A.16.1.4	Assessment and decision on information security events	**This is a new Annex A control**
A.16.1.5	Response to information security incidents	**This is a new Annex A control**
A.16.1.6	Learning from information security incidents	**A.13.2.2**
A.16.1.7	Collection of evidence	**A.13.2.3**
A.17.1.1	Planning information security continuity	**A.14.1.2**
A.17.1.2	Implementing information security continuity	**A.14.1.1, A.14.1.3, A.14.1.4**
A.17.1.3	Verify, review and evaluate information security continuity	**A.14.1.5**
A.17.2.1	Availability of information processing facilities	**This is a new Annex A control**
A.18.1.1	Identification of applicable legislation and contractual requirements	**A.15.1.1**
A.18.1.2	Intellectual property rights (IPR)	**A.15.1.2**

Continued >>

Annex A control (in ISO/IEC 27001:2013)		Annex A control (in ISO/IEC 27001:2005)
A.18.1.3	Protection of records	**A.15.1.3**
A.18.1.4	Privacy and protection of personally identifiable information	**A.15.1.4**
A.18.1.5	Regulation of cryptographic controls	**A.15.1.6**
A.18.2.1	Independent review of information security	**A.6.1.8**
A.18.2.2	Compliance with security policies and standards	**A.15.2.1**
A.18.2.3	Technical compliance review	**A.15.2.2**

Mapping of Annex A controls in ISO/IEC 27001:2005 to ISO/IEC 27001:2013

ISO/IEC 27001:2005		ISO/IEC 27001:2013
A.5.1.1	Information security policy document	**A.5.1.1**
A.5.1.2	Review of the information security policy	**A.5.1.2**
A.6.1.1	Management commitment to information security	**This is a deleted Annex A control**
A.6.1.2	Information security coordination	**This is a deleted Annex A control**
A.6.1.3	Allocation of information security responsibilities	**A.6.1.1**
A.6.1.4	Authorisation process for information processing facilities	**This is a deleted Annex A control**
A.6.1.5	Confidentiality agreements	**A.13.2.4**
A.6.1.6	Contact with authorities	**A.6.1.3**
A.6.1.7	Contact with special interest groups	**A.6.1.4**
A.6.1.8	Independent review of information security	**A.18.2.1**
A.6.2.1	Identification of risks related to external parties	**This is a deleted Annex A control**
A.6.2.2	Addressing security when dealing with customers	**This is a deleted Annex A control**
A.6.2.3	Addressing security in third party agreements	**A.15.1.2**
A.7.1.1	Inventory of assets	**A.8.1.1**
A.7.1.2	Ownership of assets	**A.8.1.2**
A.7.1.3	Acceptable use of assets	**A.8.1.3**
A.7.2.1	Classification guidelines	**A.8.2.1**
A.7.2.2	Information labeling and handling	**A.8.2.2**
A.8.1.1	Roles and responsibilities	**A.6.1.1**
A.8.1.2	Screening	**A.7.1.1**
A.8.1.3	Terms and conditions of employment	**A.7.1.2**
A.8.2.1	Management responsibilities	**A.7.2.1**

Continued >>

ISO/IEC 27001:2005		ISO/IEC 27001:2013
A.8.2.2	Information security awareness, education and training	**A.7.2.2**
A.8.2.3	Disciplinary process	**A.7.2.3**
A.8.3.1	Termination responsibilities	**A.7.3.1**
A.8.3.2	Return of assets	**A.8.1.4**
A.8.3.3	Removal of access rights	**A.9.2.6**
A.9.1.1	Physical security perimeter	**A.11.1.1**
A.9.1.2	Physical entry controls	**A.11.1.2**
A.9.1.3	Securing offices, rooms and facilities	**A.11.1.3**
A.9.1.4	Protecting against external and environmental threats	**A.11.1.4**
A.9.1.5	Working in secure areas	**A.11.1.5**
A.9.1.6	Public access, delivery and loading areas	**A.11.1.6**
A.9.2.1	Equipment sitting and protection	**A.11.2.1**
A.9.2.2	Supporting utilities	**A.11.2.2**
A.9.2.3	Cabling security	**A.11.2.3**
A.9.2.4	Equipment maintenance	**A.11.2.4**
A.9.2.5	Security of equipment off-premises	**A.11.2.6**
A.9.2.6	Secure disposal or re-use of equipment	**A.11.2.7**
A.9.2.7	Removal of property	**A.11.2.5**
A.10.1.1	Documented operating procedures	**A.12.1.1**
A.10.1.2	Change management	**8.1*, A.12.1.2**
A.10.1.3	Segregation of duties	**A.6.1.2**
A.10.1.4	Separation of development, test and operational facilities	**A.12.1.4**
A.10.2.1	Service delivery	**8.1***
A.10.2.2	Monitoring and review of third party services	**8.1*, A.15.2.1**
A.10.2.3	Managing changes to third party services	**8.1*, A.15.2.2**
A.10.3.1	Capacity management	**A.12.1.3**
A.10.3.2	System Acceptance	**A.14.2.9**
A.10.4.1	Controls against malicious code	**A.12.2.1**
A.10.4.2	Controls against mobile code	**A.12.2.1**
A.10.5.1	Information back-up	**A.12.3.1**
A.10.6.1	Network controls	**A.13.1.1**
A.10.6.2	Security of network services	**A.13.1.2**
A.10.7.1	Management of removable media	**A.8.3.1**
A.10.7.2	Disposal of Media	**A.8.3.2**
A.10.7.3	Information Handling procedures	**A.8.2.3**
A.10.7.4	Security of system documentation	**This is a deleted Annex A control**
A.10.8.1	Information exchange policies and procedures	**A.13.2.1**

Continued >>

ISO/IEC 27001:2005		ISO/IEC 27001:2013
A.10.8.2	Exchange agreements	**A.13.2.2**
A.10.8.3	Physical media in transit	**A.8.3.3**
A.10.8.4	Electronic messaging	**A.13.2.3**
A.10.8.5	Business Information Systems	**This is a deleted Annex A control**
A.10.9.1	Electronic commerce	**A.14.1.2**
A.10.9.2	Online-transactions	**A.14.1.3**
A.10.9.3	Publicly available information	**A.14.1.2**
A.10.10.1	Audit logging	**A.12.4.1**
A.10.10.2	Monitoring system use	**A.12.4.1**
A.10.10.3	Protection of log information	**A.12.4.2, A.12.4.3**
A.10.10.4	Administrator and operator logs	**A.12.4.3**
A.10.10.5	Fault logging	**A.12.4.1**
A.10.10.6	Clock synchronisation	**A.12.4.4**
A.11.1.1	Access control policy	**A.9.1.1**
A.11.2.1	User registration	**A.9.2.1, A.9.2.2**
A.11.2.2	Privilege management	**A.9.2.3**
A.11.2.3	User password management	**A.9.2.4**
A.11.2.4	Review of user access rights	**A.9.2.5**
A.11.3.1	Password use	**A.9.3.1**
A.11.3.2	Unattended user equipment	**A.11.2.8**
A.11.3.3	Clear desk and clear screen policy	**A.11.2.9**
A.11.4.1	Policy on use of network services	**A.9.1.2**
A.11.4.2	User authentication for external connections	**This is a deleted Annex A control**
A.11.4.3	Equipment identification in networks	**This is a deleted Annex A control**
A.11.4.4	Remote Diagnostic and configuration port protection	**This is a deleted Annex A control**
A.11.4.5	Segregation in Networks	**A.13.1.3**
A.11.4.6	Network Connection control	**This is a deleted Annex A control**
A.11.4.7	Network routing control	**This is a deleted Annex A control**
A.11.5.1	Secure log-on procedures	**A.9.4.2**
A.11.5.2	User identification and authentication	**A.9.2.1**
A.11.5.3	Password management system	**A.9.4.3**
A.11.5.4	Use of system utilities	**A.9.4.4**
A.11.5.5	Session time-out	**A.9.4.2**
A.11.5.6	Limitation of connection time	**A.9.4.2**
A.11.6.1	Information access restriction	**A.9.4.1**
A.11.6.2	Sensitive system isolation	**This is a deleted Annex A control**

Continued >>

ISO/IEC 27001:2005		ISO/IEC 27001:2013
A.11.7.1	Mobile computing and communications	**A.6.2.1**
A.11.7.2	Teleworking	**A.6.2.2**
A.12.1.1	Security requirements analysis and specification	**A.14.1.1**
A.12.2.1	Input data validation	**This is a deleted Annex A control**
A.12.2.2	Control of internal processing	**This is a deleted Annex A control**
A.12.2.3	Message integrity	**This is a deleted Annex A control**
A.12.2.4	Output data validation	**This is a deleted Annex A control**
A.12.3.1	Policy on the use of cryptographic controls	**A.10.1.1**
A.12.3.2	Key management	**A.10.1.2**
A.12.4.1	Control of operational software	**A.12.5.1**
A.12.4.2	Protection of system test data	**A.14.3.1**
A.12.4.3	Access control to program source code	**A.9.4.5**
A.12.5.1	Change control procedures	**8.1*, A.14.2.2**
A.12.5.2	Technical review of applications after operating system changes	**8.1*, A.14.2.3**
A.12.5.3	Restrictions on changes to software packages	**8.1*, A.14.2.4**
A.12.5.4	Information leakage	**This is a deleted Annex A control**
A.12.5.5	Outsourced software development	**8.1*, A.14.2.7**
A.12.6.1	Control of technical vulnerabilities	**A.12.6.1**
A.13.1.1	Reporting information security events	**A.16.1.2**
A.13.1.2	Reporting security weakness	**A.16.1.3**
A.13.2.1	Responsibilities and Procedures	**A.16.1.1**
A.13.2.2	Learning from information security incidents	**A.16.1.6**
A.13.2.3	Collection of evidence	**A.16.1.7**
A.14.1.1	Including information security in the business continuity management process	**A.17.1.2**
A.14.1.2	Business continuity and risk assessment	**A.17.1.1**
A.14.1.3	Developing and implementing continuity plans including formation security.	**A.17.1.2**
A.14.1.4	Business continuity planning framework	**A.17.1.2**
A.14.1.5	Testing, maintaining and re-assessing business continuity plans	**A.17.1.3**
A.15.1.1	Identification of applicable legislation	**A.18.1.1**
A.15.1.2	Intellectual property rights (IPR)	**A.18.1.2**
A.15.1.3	Protection of organisational records	**A.18.1.3**
A.15.1.4	Data protection and privacy of personal information	**A.18.1.4**
A.15.1.5	Prevention of misuse of information processing facilities	**This is a deleted Annex A control**
A.15.1.6	Regulation of cryptographic controls	**A.18.1.5**
A.15.2.1	Compliance with security policies and standards	**A.18.2.2**
A.15.2.2	Technical compliance checking	**A.18.2.3**
A.15.3.1	Information system audit controls	**A.12.7.1**
A.15.3.2	Protection of information systems audit tools	**This is a deleted Annex A control**

* These controls map (at least partially) onto ISMS requirements. For example, Clause 8.1 in ISO/IEC 27001:2013 requires organizations to ensure that outsourced processes are controlled.

Deleted Annex A controls

ISO/IEC 27001:2005 requirements that do not feature in ISO/IEC 27001:2013

A.6.1.1	Management commitment to information security
A.6.1.2	Information security coordination
A.6.1.4	Authorisation process for information processing facilities
A.6.2.1	Identification of risks related to external parties
A.6.2.2	Addressing security when dealing with customers
A.10.7.4	Security of system documentation
A.10.8.5	Business Information Systems
A.11.4.2	User authentication for external connections
A.11.4.3	Equipment identification in networks
A.11.4.4	Remote Diagnostic and configuration port protection
A.11.4.6	Network Connection control
A.11.4.7	Network routing control
A.11.6.2	Sensitive system isolation
A.12.2.1	Input data validation
A.12.2.2	Control of internal processing
A.12.2.3	Message integrity
A.12.2.4	Output data validation
A.12.5.4	Information leakage
A.15.1.5	Prevention of misuse of information processing facilities
A.15.3.2	Protection of information systems audit tools

Acknowledgement

These tables are based on work performed by David Brewer and Sabrina Feng and are reproduced by permission of IMS-Smart Limited.

BSI UK
Kitemark Court
Davy Avenue, Knowlhill
Milton Keynes, MK5 8PP
United Kingdom

T: +44 845 080 9000
E: certification.sales@bsigroup.com
bsigroup.com