Advent IM Ltd

ISO/IEC 27001:2013 vs 2005

www.advent-im.co.uk
0121 559 6699
bestpractice@advent-im.co.uk

Key Findings ISO/IEC 27001:2013 vs. 2005 Controls

1) PDCA as a main driver is now gone with greater importance being placed setting objectives and monitoring performance.

2) Document control, internal audit and CAPA requirements as we would recognise them have gone, at least in their requirement to be documented procedures although the requirement for them as an output still remains i.e. you do not need written procedures but you still need records maintained of what you have done with regard to them.

3) Documents and records are now treated as one in the same.

4) The number of sections has increased from 11 to 14, however the number of controls has been reduced from 133 to 114.

5) The Business Continuity section is gone really in place of a less prescriptive service continuity section.

6) More importance is now placed on interested parties and their role within the organisations ISMS.

7) ISMS is now Clause 4-10. These are:
   - 4. Context of the organisation (essentially scoping);
   - 5. Leadership (management commitment, roles and responsibilities, IS Policy);
   - 6. Planning (new way of dealing with preventative actions and basically determining risk methodology and appetite etc… There is a direct link with Clause 8);
   - 7. Support (resources, awareness, communication, documentation);
   - 8. Operation (essentially actioning the RA and RT);
   - 9. Performance evaluation (essentially logs, auditing, management review); and
   - 10. Improvement (corrective action, non conformity, continual improvement).

8) Controls are no longer 'selected' but 'determined'.

9) Control objectives have increased to 14 and are:
- A.5 Information security policies;
- A.6 Organisation of information security;
- A.7 Human resource security;
- A. 8 Asset management;
- A.9 Access control;
- A.10 Cryptography;
- A.11 Physical and environmental security;
- A.12 Operations security;
- A.13 Communications security;
- A.14 System acquisition, development and maintenance;
- A.15 Supplier relationships;
- A.16 Information security incident management;
- A.17 Information security aspects of business continuity management; and
- A. 18 Compliance.

10) CAPA – There are no preventative actions anymore replaced by 'actions to address risks'. These are merged into the Risk Assessment and Risk Treatment areas. There is also a distinction between corrections that are carried out in direct response to a non-conformity, against corrective actions that are implemented to eliminate the cause of a non-conformity.

11) Risk assessment – The identification of assets, threats and vulnerabilities is no longer a pre-requisite for the identification of information security risks. It is only required for the identification of Confidentiality, Integrity and Availability. There will be no need for organisations already certified to change the way they do risk necessarily.

12) Management commitment is no longer a control as its implied with Clause 5.

13) The Annex A controls have not massively changed, there are a few new ones and some have been deleted but many are the same in general or have been merged.

14) Passwords seem to be referred to as secret authentication.

15) For those who have already certified or are going through the process with ISO/IEC 27001:2005, we are currently investigating the official position but it would seem logical to continue with this version until further notice as currently we understand there is no formal certification process for the new standard.

ISMS Clauses

www.advent-im.co.uk
0121 559 6699
bestpractice@advent-im.co.uk

ISO/IEC 27001:2013		ISO/IEC 27001:2005	
0	Introduction	**0**	Introduction
1	Scope	**1**	Scope
2	Normative references	**2**	Normative references
3	Terms and definitions	**3**	Terms and definitions
4.1	Understanding the organisation and its context	**8.3**	Preventive action
4.2	Understanding the needs and expectations of interested parties	**5.2.1 c)**	Identify and address legal and regulatory requirements and contractual security obligations
4.3	Determining the scope of the information security management system	**4.2.1 a)** **4.2.3 f)**	Define scope and boundaries Ensure the scope remains adequate
4.4	Information security management system	**4.1**	General requirements
5.1	Leadership and commitment	**5.1**	Management commitment
5.2	Policy	**4.2.1 b)**	Define and ISMS policy
5.3	Organisational roles, responsibilities and authorities	**5.1 c)**	Establishing roles and responsibilities for information security
6.1.1	Actions to address risks and opportunities - general	**8.3**	Preventive action
6.1.2	Information security risk assessment	**4.2.1 c)** **4.2.1 d)** **4.2.1 e)**	Define the risk assessment approach Identify the risks Analyse and evaluate the risks
6.1.3	Information security risk treatment	**4.2.1 f)** **4.2.1 g)** **4.2.1 h)** **4.2.1 j)** **4.2.1 j)** **4.2.2 a)**	Identify and evaluate options for the treatment of risks Select control objectives and controls for the treatment of risks Obtain management approval of the proposed residual risks Prepare Statement of Applicability Prepare Statement of Applicability Formulate risk treatment plan

ISMS Clauses

ISO/IEC 27001:2013		ISO/IEC 27001:2005	
6.2	Information security objectives and planning to achieve them	**5.1 b)**	Ensuring that ISMS objectives and plans are established
7.1	Resources	**4.2.2 g)** **5.2.1**	Manage resource for the ISMS Provision of resources
7.2	Competence	**5.2.2**	Training, awareness and competence
7.3	Awareness	**4.2.2 e)** **5.2.2**	Implement training and awareness programmes Training, awareness and competence
7.4	Communication	**4.2.4 c)** **5.1 d)**	Communicate the actions and improvements Communicating to the organisation
7.5	Documented information	**4.3**	Documentation requirements
8.1	Operational planning and control	**4.2.2 f)**	Manage operations of the ISMS
8.2	Information security risk assessment	**4.2.3 d)**	Review risk assessments at planned intervals
8.3	Information security risk treatment	**4.2.2 b)** **4.2.2 c)**	Implement the risk treatment plan Implement controls
9.1	Monitoring, measurement, analysis and evaluation	**4.2.2 d)** **4.2.3 b)** **4.2.3 c)**	Define how to measure effectiveness Undertake regular reviews of the effectiveness of the ISMS Measure the effectiveness of controls
9.2	Internal audit	**4.2.3 e)** **6**	Conduct internal ISMS audits Internal ISMS audits
9.3	Management review	**4.2.3 f)** **7**	Undertake a management review of ISMS Management review of ISMS
10.1	Nonconformity and corrective action	**4.2.4** **8.2**	Maintain and improve the ISMS Corrective action
10.2	Continual improvement	**4.2.4** **8.1**	Maintain and improve the ISMS Continual improvement

ISMS Controls

2013 vs 2005

www.advent-im.co.uk
0121 559 6699
bestpractice@advent-im.co.uk

New/changed Objectives and Controls

Clause	ISO/IEC 27001:2013 Objectives and Controls	Clause	ISO/IEC 27001:2005 Objectives and Controls
A.5	**Information security policies**	**A.5**	**Security policy**
A.5.1	*Management direction for information security*	*A.5.1*	*Information security policy*
A.5.1.1	Policies for information security	A.5.1.1	Information security policy document
A.5.1.2	Review of the policies for information security	A.5.1.2	Review of the information security policy
A.6	**Organisation of information security**	**A.6**	**Organisation of information security**
A.6.1	*Internal organisation*	*A.6.1*	*Internal Organisation*
A.6.1.1	Information security roles and responsibilities	A.6.1.3	Allocation of information security responsibilities
		A.8.1.1	Roles and responsibilities
A.6.1.2	Segregation of duties	A.10.1.3	Segregation of duties
A.6.1.3	Contact with authorities	A.6.1.6	Contact with authorities
A.6.1.4	Contact with special interest groups	A.6.1.7	Contact with special interest groups
A.6.1.5	Information security in project management		No direct mapping
A.6.2	*Mobile devices and teleworking*	*A.11.7*	*Mobile computing and teleworking*
A.6.2.1	Mobile device policy	A.11.7.1	Mobile computing and communications
A.6.2.2	Teleworking	A.11.7.2	Teleworking
A.7	**Human resources security**	**A.8**	**Human resources security**
A.7.1	*Prior to employment*	*A.8.1*	*Prior to employment*
A.7.1.1	Screening	A.8.1.2	Screening
A.7.1.2	Terms and conditions of employment	A.8.1.3	Terms and conditions of employment
A.7.2	*During employment*	*A.8.2*	*During employment*
A.7.2.1	Management responsibilities	A.8.2.1	Management responsibilities
A.7.2.2	Information security awareness, education and training	A.8.2.2	Information security awareness, education and training

ISMS Controls

2013 vs 2005

New/changed Objectives and Controls

Clause	ISO/IEC 27001:2013 Objectives and Controls	Clause	ISO/IEC 27001:2005 Objectives and Controls
A.7.2.3	Disciplinary process	A.8.2.3	Disciplinary process
A.7.3	*Termination and change of employment*	*A.8.3*	*Termination or change of employment*
A.7.3.1	Termination or change of employment responsibilities	A.8.3.1	Termination responsibilities
A.8	**Asset management**	**A.7**	**Asset management**
A.8.1	*Responsibility for assets*	*A.7.1*	*Responsibility for assets*
A.8.1.1	Inventory of assets	A.7.1.1	Inventory of assets
A.8.1.2	Ownership of assets	A.7.1.2	Ownership of assets
A.8.1.3	Acceptable use of assets	A.7.1.3	Acceptable use of assets
A.8.1.4	Return of assets	A.8.3.2	Return of assets
A.8.2	*Information classification*	*A.7.2*	*Information classification*
A.8.2.1	Classification of information	A.7.2.1	Classification guidelines
A.8.2.2	Labelling of information	A.7.2.2	Information labelling and handling
A.8.2.3	Handling of assets	A.10.7.3	Information handling procedures
A.8.3	*Media handling*	*A.10.7*	*Media handling*
A.8.3.1	Management of removable media	A.10.7.1	Management of removable media
A.8.3.2	Disposal of media	A.10.7.2	Disposal of media
A.8.3.3	Physical media transfer	A.10.8.3	Physical media in transit
A.9	**Access control**	**A.11**	**Access control**
A.9.1	*Business requirements of access control*	*A.11.1*	*Business requirement for access control*
A.9.1.1	Access control policy	A.11.1.1	Access control policy
A.9.1.2	Access to networks and network services	A.11.4.1	Policy on use of network services
A.9.2	*User access management*	*A.11.2*	*User access management*
A.9.2.1	User registration and de-registration	A.11.2.1	User registration
A.9.2.2	User access provisioning	A.11.2.1	User registration

ISMS Controls

2013 vs 2005

New/changed Objectives and Controls

Clause	ISO/IEC 27001:2013 Objectives and Controls	Clause	ISO/IEC 27001:2005 Objectives and Controls
A.9.2.3	Management of privileged access rights	A.11.2.2	Privilege management
A.9.2.4	Management of secret authentication information of users	A.11.2.3	User password management
A.9.2.5	Review of user access rights	A.11.2.4	Review of user access rights
A.9.2.6	Removal or adjustment of access rights	A.8.3.3	Removal of access rights
A.9.3	*User responsibilities*	*A.11.3*	*User responsibilities*
A.9.3.1	Use of secret authentication information	A.11.3.1	Password use
A.9.4	*System and application access control*	*A.11.6*	*Application and information access control*
A.9.4.1	Information access restriction	A.11.6.1	Information access restriction
A.9.4.2	Secure log-on procedures	A.11.5.1	Secure log-on procedures
A.9.4.3	Password management system	A.11.5.3	Password management system
A.9.4.4	Use of privileged utility programs	A.11.5.4	Use of system utilities
A.9.4.5	Access control to program source code	A.12.4.3	Access control to program source code
A.10	**Cryptography**		**Previously part of A.12 Information systems acquisition, development and maintenance**
A.10.1	*Cryptographic controls*	*A.12.3*	*Cryptographic controls*
A.10.1.1	Policy on the use of cryptographic controls	A.12.3.1	Policy on the use of cryptographic controls
A.10.1.2	Key management	A.12.3.2	Key management
A.11	**Physical and environmental security**	**A.9**	**Physical and environmental security**
A.11.1	*Secure areas*	*A.9.1*	*Secure areas*
A.11.1.1	Physical security perimeter	A.9.1.1	Physical security perimeter
A.11.1.2	Physical entry controls	A.9.1.2	Physical entry controls
A.11.1.3	Securing offices, rooms and facilities	A.9.1.3	Securing offices, rooms and facilities
A.11.1.4	Protecting against external and environmental threats	A.9.1.4	Protecting against external and environmental threats

ISMS Controls

2013 vs 2005

New/changed Objectives and Controls

Clause	ISO/IEC 27001:2013 Objectives and Controls	Clause	ISO/IEC 27001:2005 Objectives and Controls
A.11.1.5	Working in secure areas	A.9.1.5	Working in secure areas
A.11.1.6	Delivery and loading areas	A.9.1.6	Public access, delivery and loading areas
A.11.2	*Equipment*	*A.9.2*	*Equipment security*
A.11.2.1	Equipment siting and protection	A.9.2.1	Equipment siting and protection
A.11.2.2	Supporting utilities	A.9.2.2	Supporting utilities
A.11.2.3	Cabling security	A.9.2.3	Cabling security
A.11.2.4	Equipment maintenance	A.9.2.4	Equipment maintenance
A.11.2.5	Removal of assets	A.9.2.7	Removal of property
A.11.2.6	Security of equipment and assets off-premises	A.9.2.5	Security of equipment off-premises
A.11.2.7	Secure disposal or re-use of equipment	A.9.2.6	Secure disposal or re-use of equipment
A.11.2.8	Unattended user equipment	A.11.3.2	Unattended user equipment
A.11.2.9	Clear desk and screen policy	A.11.3.3	Clear desk and screen policy
A.12	**Operations security**		**Previously part of A.10 Communications and operations management**
A.12.1	*Operational procedures and responsibilities*	*A.10.1*	*Operational procedures and responsibilities*
A.12.1.1	Documented operating procedures	A.10.1.1	Documented operating procedures
A.12.1.2	Change management	A.10.1.2	Change management
A.12.1.3	Capacity management	A.10.3.1	Capacity management
A.12.1.4	Separation of development, testing and operational environments	A.10.1.4	Separation of development, test and operational facilities
A.12.2	*Protection from malware*	*A.10.4*	*Protection against malicious and mobile code*
A.12.2.1	Controls against malware	A.10.4.1	Controls against malicious code
		A.10.4.2	Controls against mobile code

ISMS Controls

2013 vs 2005

New/changed Objectives and Controls

Clause	ISO/IEC 27001:2013 Objectives and Controls	Clause	ISO/IEC 27001:2005 Objectives and Controls
A.12.3	*Backup*	*A.10.5*	*Backup*
A.12.3.1	Information backup	A.10.5.1	Information backup
A.12.4	*Logging and monitoring*	*A.10.10*	*Monitoring*
A.12.4.1	Event logging	A.10.10.1	Audit logging
A.12.4.2	Protection of log information	A.10.10.3	Protection of log information
A.12.4.3	Administrator and operator logs	A.10.10.4	Administrator and operator logs
A.12.4.4	Clock synchronisation	A.10.10.6	Clock synchronisation
A.12.5	*Control of operational software*		*Previously part of A.12 Security of system files*
A.12.5.1	Installation of software on operational systems	A.12.4.1	Control of operational software
A.12.6	*Technical vulnerability management*	*A.12.5*	*Technical vulnerability management*
A.12.6.1	Management of technical vulnerabilities	A.12.6.1	Control of technical vulnerabilities
A.12.6.2	Restrictions on software installation		No direct mapping
A.12.7	*Information systems audit considerations*	*A.15.3*	*Information Systems audit considerations*
A.12.7.1	Information systems audit controls	A.15.3.1	Information systems audit controls
A.13	**Communications security**		**Previously part of A.10 Communications and operations management**
A.13.1	*Network security management*	*A.10.6*	*Network security management*
A.13.1.1	Network controls	A.10.6.1	Network controls
A.13.1.2	Security of network services	A.10.6.2	Security of network services
A.13.1.3	Segregation in networks	A.11.4.5	Segregation in networks
A.13.2	*Information transfer*	*A.10.8*	*Exchange of information*
A.13.2.1	Information transfer policies and procedures	A.10.8.1	Information exchange policies and procedures

ISMS Controls

2013 vs 2005

New/changed Objectives and Controls

Clause	ISO/IEC 27001:2013 Objectives and Controls	Clause	ISO/IEC 27001:2005 Objectives and Controls
A.13.2.2	Agreements on information transfer	A.10.8.2	Exchange agreements
A.13.2.5	Electronic messaging	A.10.8.4	Electronic messaging
A.13.2.4	Confidentiality or non -disclosure agreements	A.6.1.5	Confidentiality agreements
A.14	**System acquisition, development and maintenance**	**A.12**	**System acquisition, development and maintenance**
A.14.1	*Security requirements of information systems*	*A.12.1*	*Security requirements of information systems*
A.14.1.1	Information security requirements analysis and specification	A.12.1.1	Security requirements in analysis and specification
A.14.1.2	Securing application services on public networks	A.10.9.1	Electronic commerce
A.14.1.3	Protecting application services transactions	A.10.9.2	On-line transactions
A.14.2	*Security in development and support processes*	*A.12.6*	*Security in development and support processes*
A.14.2.1	Secure development policy		No direct mapping
A.14.2.2	System change control procedures	A.12.5.1	Change control procedures
A.14.2.3	Technical review of applications after operating platform changes	A.12.5.2	Technical review of applications after operating systems changes
A.14.2.4	Restrictions on changes to software packages	A.12.5.3	Restrictions on changes to software packages
A.14.2.5	Secure system engineering principles		No direct mapping
A.14.2.6	Secure development environment		No direct mapping
A.14.2.7	Outsourced development	A.12.5.5	Outsourced software development
A.14.2.8	System security testing		No direct mapping
A.14.2.9	System acceptance testing	A.10.3.2	System acceptance

ISMS Controls

2013 vs 2005

New/changed Objectives and Controls

Clause	ISO/IEC 27001:2013 Objectives and Controls	Clause	ISO/IEC 27001:2005 Objectives and Controls
A.14.3	*Test Data*		*Previously included in A.12.4 Security of system files*
A.14.3.1	Protection of test data	A.12.4.2	Protection of system test data
A.15	**Supplier Relationships**		**Previously included in A.6.2 External parties**
A.15.1	*Information security in supplier relationships*		*No direct mapping*
A.15.1.1	Information security policy for supplier relationships	A.6.2.2	Addressing security when dealing with customers
A.15.1.2	Addressing security within supplier agreements	A.6.2.3	Addressing security in third party agreements
A.15.1.3	Information and communication technology supply chain	A.6.2.1	Identification of risks related to external parties
A.15.2	*Supplier service delivery management*	*A.10.2*	*Third party service delivery management*
A.15.2.1	Monitoring and review of supplier services	A.10.2.2	Monitoring and review of third party services
A.15.2.2	Managing changes to supplier services	A.10.2.3	Managing changes to third party services
A.16	**Information security incident management**	**A.13**	**Information security incident management**
A.16.1	*Management of information security incidents and improvements*	*A.13.2*	*Management of information security incidents and improvements*
A.16.1.1	Responsibilities and procedures	A.13.2.1	Responsibilities and procedures
A.16.1.2	Reporting information security events	A.13.1.1	Reporting information security events
A.16.1.3	Reporting information security weaknesses	A.13.1.2	Reporting of security weaknesses

ISMS Controls

2013 vs 2005

New/changed Objectives and Controls

Clause	ISO/IEC 27001:2013 Objectives and Controls	Clause	ISO/IEC 27001:2005 Objectives and Controls
A.16.1.4	Assessment of and decision on information security events		No direct mapping
A.15.15	Response to information security incidents		No direct mapping
A.16.1.6	Learning from information security incidents	A.13.2.2	Learning from information security incidents
A.16.1.7	Collection of evidence	A.13.2.3	Collection of evidence
A.17	**Information security aspects of business continuity management**	**A.14**	**Business Continuity Management**
A.17.1	*Information security continuity*	*A.14.1*	*Information security aspects of business continuity management*
A.17.1.1	Planning information security continuity	A.14.1.1	Including information security in the business continuity management process
		A.14.1.2	Business continuity and risk assessment
		A.14.1.4	Business continuity planning framework
A.17.1.2	Implementing information security continuity	A.14.1.3	Developing and implementing continuity plans
A.17.1.3	Verify, review and evaluate information security continuity	A.14.1.5	Testing, maintaining and re-assessing business continuity plans

ISMS Controls

2013 vs 2005

New/changed Objectives and Controls

Clause	ISO/IEC 27001:2013 Objectives and Controls	Clause	ISO/IEC 27001:2005 Objectives and Controls
A.17.2	*Redundancies*		*Previously part of A.14.1.2 Business continuity and risk assessment*
A.17.2.1	Availability of information processing facilities		Previously part of A.14.1.2 Business continuity and risk assessment
A.18	**Compliance**	**A.15**	**Compliance**
A.18.1	*Compliance with legal and contractual requirements*	*A.15.1*	*Compliance with legal requirements*
A.18.1.1	Identification of applicable legislation and contractual requirements	A.15.1.1	Identification of applicable legislation
A.18.1.2	Intellectual property rights	A.15.1.2	Intellectual property rights
A.18.1.3	Protection of records	A.15.1.3	Protecting organisational records
A.18.1.4	Privacy and protection of personally identifiable information	A.15.1.4	Data protection and privacy of personal information
A.18.1.5	Regulation of cryptographic controls	A.15.1.6	Regulation of cryptographic controls
A.18.2	*Information security reviews*	*A.15.2*	*Compliance with security policies and standards*
A.18.2.1	Independent review of information security	A.6.1.8	Independent review of information security
A.18.2.2	Compliance with security policies and standards	A.15.2.1	Compliance with security policies and standards
A.18.2.3	Technical compliance review	A.15.2.2	Technical compliance checking

Note:

This is Advent IM's subjective view of the control mapping from ISO27001:2013 to 2005. Many have been merged into other controls or become part of the ISMS clauses or been deleted.

ISMS Controls

2005 vs 2013

www.advent-im.co.uk

0121 559 6699
bestpractice@advent-im.co.uk

Old Objectives and Controls		New/changed Objectives and Controls	
Clause	**ISO/IEC 27001:2005 Objectives and Controls**	**Clause**	**ISO/IEC 27001:2013 Objectives and Controls**
A.5	**Security policy**	**A.5**	**Information security policies**
A.5.1	*Information security policy*	*A.5.1*	*Management direction for information security*
A.5.1.1	Information security policy document	A.5.1.1	Policies for information security
A.5.1.2	Review of the information security policy	A.5.1.2	Review of the policies for information security
A.6	**Organisation of information security**	**A.6**	**Organisation of information security**
A.6.1	*Internal Organisation*	*A.6.1*	*Internal organisation*
A.6.1.1	Management commitment to information security		Subsumed into Clause 5
A.6.1.2	Information security co-ordination		Subsumed into Clause 5
A.6.1.3	Allocation of information security responsibilities	A.6.1.1	Information security roles and responsibilities
A.6.1.4	Authorisation process for information processing facilities		Merged into other controls
A.6.1.5	Confidentiality agreements	A.13.2.4	Confidentiality or non -disclosure agreements
A.6.1.6	Contact with authorities	A.6.1.3	Contact with authorities
A.6.1.7	Contact with special interest groups	A.6.1.4	Contact with special interest groups
A.6.1.8	Independent review of information security	A.18.2.1	Independent review of information security
A.6.2	*External Parties*	**A.15**	**Supplier Relationships**
		A.15.1	*Information security in supplier relationships*

ISMS Controls

2005 vs 2013

Old Objectives and Controls		New/changed Objectives and Controls	
Clause	**ISO/IEC 27001:2005 Objectives and Controls**	**Clause**	**ISO/IEC 27001:2013 Objectives and Controls**
A.6.2.1	Identification of risks related to external parties	A.15.1.3	Information and communication technology supply chain
A.6.2.2	Addressing security when dealing with customers	A.15.1.1	Information security policy for supplier relationships
A.6.2.3	Addressing security in third party agreements	A.15.1.2	Addressing security within supplier agreements
A.7	**Asset management**	**A.8**	**Asset management**
A.7.1	*Responsibility for assets*	*A.8.1*	*Responsibility for assets*
A.7.1.1	Inventory of assets	A.8.1.1	Inventory of assets
A.7.1.2	Ownership of assets	A.8.1.2	Ownership of assets
A.7.1.3	Acceptable use of assets	A.8.1.3	Acceptable use of assets
A.7.2	*Information classification*	*A.8.2*	*Information classification*
A.7.2.1	Classification guidelines	A.8.2.1	Classification of information
A.7.2.2	Information labelling and handling	A.8.2.2	Labelling of information
A.8	**Human resources security**	**A.7**	**Human resources security**
A.8.1	*Prior to employment*	*A.7.1*	*Prior to employment*
A.8.1.1	Roles and responsibilities	A.6.1.1	Information security roles and responsibilities
A.8.1.2	Screening	A.7.1.1	Screening
A.8.1.3	Terms and conditions of employment	A.7.1.2	Terms and conditions of employment
A.8.2	*During employment*	*A.7.2*	*During employment*
A.8.2.1	Management responsibilities	A.7.2.1	Management responsibilities

ISMS Controls

2005 vs 2013

Old Objectives and Controls		New/changed Objectives and Controls	
Clause	**ISO/IEC 27001:2005 Objectives and Controls**	**Clause**	**ISO/IEC 27001:2013 Objectives and Controls**
A.8.2.2	Information security awareness, education and training	A.7.2.2	Information security awareness, education and training
A.8.2.3	Disciplinary process	A.7.2.3	Disciplinary process
A.8.3	*Termination or change of employment*	*A.7.3*	*Termination and change of employment*
A.8.3.1	Termination responsibilities	A.7.3.1	Termination or change of employment responsibilities
A.8.3.2	Return of assets	A.8.1.4	Return of assets
A.8.3.3	Removal of access rights	A.9.2.6	Removal or adjustment of access rights
A.9	**Physical and environmental security**	**A.11**	**Physical and environmental security**
A.9.1	*Secure areas*	*A.11.1*	*Secure areas*
A.9.1.1	Physical security perimeter	A.11.1.1	Physical security perimeter
A.9.1.2	Physical entry controls	A.11.1.2	Physical entry controls
A.9.1.3	Securing offices, rooms and facilities	A.11.1.3	Securing offices, rooms and facilities
A.9.1.4	Protecting against external and environmental threats	A.11.1.4	Protecting against external and environmental threats
A.9.1.5	Working in secure areas	A.11.1.5	Working in secure areas
A.9.1.6	Public access, delivery and loading areas	A.11.1.6	Delivery and loading areas
A.9.2	*Equipment security*	*A.11.2*	*Equipment*

ISMS Controls

2005 vs 2013

Old Objectives and Controls		New/changed Objectives and Controls	
Clause	**ISO/IEC 27001:2005 Objectives and Controls**	**Clause**	**ISO/IEC 27001:2013 Objectives and Controls**
A.9.2.1	Equipment siting and protection	A.11.2.1	Equipment siting and protection
A.9.2.2	Supporting utilities	A.11.2.2	Supporting utilities
A.9.2.3	Cabling security	A.11.2.3	Cabling security
A.9.2.4	Equipment maintenance	A.11.2.4	Equipment maintenance
A.9.2.5	Security of equipment off-premises	A.11.2.6	Security of equipment and assets off-premises
A.9.2.6	Secure disposal or re-use of equipment	A.11.2.7	Secure disposal or re-use of equipment
A.9.2.7	Removal of property	A.11.2.5	Removal of assets
A.10	**Communications and operations management**	**A.12**	**Operations security**
		A.13	**Communications security**
A.10.1	*Operational procedures and responsibilities*	*A.12.1*	*Operational procedures and responsibilities*
A.10.1.1	Documented operating procedures	A.12.1.1	Documented operating procedures
A.10.1.2	Change management	A.12.1.2	Change management
A.10.1.3	Segregation of duties	A.6.1.2	Segregation of duties
A.10.1.4	Separation of development, test and operational facilities	A.12.1.4	Separation of development, testing and operational environments
A.10.2	*Third party service delivery management*	*A.15.2*	*Supplier service delivery management*
A.10.2.1	Service delivery		Deleted
A.10.2.2	Monitoring and review of third party services	A.15.2.1	Monitoring and review of supplier services
A.10.2.3	Managing changes to third party services	A.15.2.2	Managing changes to supplier services
A.10.3	*System Planning & Acceptance*		*Merged into other control objectives*
A.10.3.1	Capacity management	A.12.1.3	Capacity management
A.10.3.2	System acceptance	A.14.2.9	System acceptance testing

ISMS Controls

2005 vs 2013

Old Objectives and Controls		New/changed Objectives and Controls	
Clause	**ISO/IEC 27001:2005 Objectives and Controls**	**Clause**	**ISO/IEC 27001:2013 Objectives and Controls**
A.10.4	*Protection against malicious and mobile code*	*A.12.2*	*Protection from malware*
A.10.4.1	Controls against malicious code	A.12.2.1	Controls against malware
A.10.4.2	Controls against mobile code	A.12.2.1	Controls against malware
A.10.5	*Backup*	*A.12.3*	*Backup*
A.10.5.1	Information backup	A.12.3.1	Information backup
A.10.6	*Network security management*	*A.13.1*	*Network security management*
A.10.6.1	Network controls	A.13.1.1	Network controls
A.10.6.2	Security of network services	A.13.1.2	Security of network services
A.10.7	*Media handling*	*A.8.3*	*Media handling*
A.10.7.1	Management of removable media	A.8.3.1	Management of removable media
A.10.7.2	Disposal of media	A.8.3.2	Disposal of media
A.10.7.3	Information handling procedures	A.8.2.3	Handling of assets
A.10.7.4	Security of system documentation		Deleted
A.10.8	*Exchange of information*	*A.13.2*	*Information transfer*
A.10.8.1	Information exchange policies and procedures	A.13.2.1	Information transfer policies and procedures
A.10.8.2	Exchange agreements	A.13.2.2	Agreements on information transfer
A.10.8.3	Physical media in transit	A.8.3.3	Physical media transfer
A.10.8.4	Electronic messaging	A.13.2.5	Electronic messaging
A.10.8.5	Business information systems		Deleted
A.10.9	*Electronic commerce services*		*Merged into other control objectives*
A.10.9.1	Electronic commerce	A.14.1.2	Securing application services on public networks

ISMS Controls

2005 vs 2013

Old Objectives and Controls		New/changed Objectives and Controls	
Clause	**ISO/IEC 27001:2005 Objectives and Controls**	**Clause**	**ISO/IEC 27001:2013 Objectives and Controls**
A.10.9.2	On-line transactions	A.14.1.3	Protecting application services transactions
A.10.9.3	Publicly available information		Merged into other controls
A.10.10	*Monitoring*	*A.12.4*	*Logging and monitoring*
A.10.10.1	Audit logging	A.12.4.1	Event logging
A.10.10.2	Monitoring system use		Subsumed into Clause 9
A.10.10.3	Protection of log information	A.12.4.2	Protection of log information
A.10.10.4	Administrator and operator logs	A.12.4.3	Administrator and operator logs
A.10.10.5	Fault Logging		Deleted
A.10.10.6	Clock synchronisation	A.12.4.4	Clock synchronisation
A.11	**Access control**	**A.9**	**Access control**
A.11.1	*Business requirement for access control*	*A.9.1*	*Business requirements of access control*
A.11.1.1	Access control policy	A.9.1.1	Access control policy
A.11.2	*User access management*	*A.9.2*	*User access management*
A.11.2.1	User registration	A.9.2.1	User registration and de-registration
		A.9.2.2	User access provisioning
A.11.2.2	Privilege management	A.9.2.3	Management of privileged access rights
A.11.2.3	User password management	A.9.2.4	Management of secret authentication information of users
A.11.2.4	Review of user access rights	A.9.2.5	Review of user access rights
A.11.3	*User responsibilities*	*A.9.3*	*User responsibilities*
A.11.3.1	Password use	A.9.3.1	Use of secret authentication information
A.11.3.2	Unattended user equipment	A.11.2.8	Unattended user equipment
A.11.3.3	Clear desk and screen policy	A.11.2.9	Clear desk and screen policy

ISMS Controls

2005 vs 2013

Old Objectives and Controls		New/changed Objectives and Controls	
Clause	**ISO/IEC 27001:2005 Objectives and Controls**	**Clause**	**ISO/IEC 27001:2013 Objectives and Controls**
A.11.4	*Network Access Control*		Merged into other controls
A.11.4.1	Policy on use of network services	A.9.1.2	Access to networks and network services
A.11.4.2	User authentication for external connections		Deleted
A.11.4.3	Equipment identification in networks		Deleted
A.11.4.4	Remote diagnostic and conguration port protection		Deleted
A.11.4.5	Segregation in networks	A.13.1.3	Segregation in networks
A.11.4.6	Network connection control		Deleted
A.11.4.7	Network routing control		Deleted
A.11.5	*Operating system access control*		Merged into other controls
A.11.5.1	Secure log-on procedures	A.9.4.2	Secure log-on procedures
A.11.5.2	User identification and authentication		Merged into other controls
A.11.5.3	Password management system	A.9.4.3	Password management system
A.11.5.4	Use of system utilities	A.9.4.4	Use of privileged utility programs
A.11.5.5	Session time-out		Deleted
A.11.5.6	Limitation of connection time		Deleted
A.11.6	*Application and information access control*	*A.9.4*	*System and application access control*
A.11.6.1	Information access restriction	A.9.4.1	Information access restriction
A.11.6.2	Sensitive system isolation		Deleted
A.11.7	*Mobile computing and teleworking*	*A.6.2*	*Mobile devices and teleworking*
A.11.7.1	Mobile computing and communications	A.6.2.1	Mobile device policy
A.11.7.2	Teleworking	A.6.2.2	Teleworking
A.12	**System acquisition, development and maintenance**	**A.14**	**System acquisition, development and maintenance**
		A.10	**Cryptography**
		A.12.5	*Control of operational software*

ISMS Controls

2005 vs 2013

Old Objectives and Controls		New/changed Objectives and Controls	
Clause	**ISO/IEC 27001:2005 Objectives and Controls**	**Clause**	**ISO/IEC 27001:2013 Objectives and Controls**
A.12.1	*Security requirements of information systems*	*A.14.1*	*Security requirements of information systems*
A.12.1.1	Security requirements in analysis and specification	A.14.1.1	Information security requirements analysis and specification
A.12.2	*Correct processing in applications*		*Deleted*
A.12.2.1	Input data validation		Deleted
A.12.2.2	Control of internal processing		Deleted
A.12.2.3	Message integrity		Deleted
A.12.2.4	Output data validation		Deleted
A.12.3	*Cryptographic controls*	*A.10.1*	*Cryptographic controls*
A.12.3.1	Policy on the use of cryptographic controls	A.10.1.1	Policy on the use of cryptographic controls
A.12.3.2	Key management	A.10.1.2	Key management
A.12.4	*Security of system files*	*A.14.3*	*Test Data*
A.12.4.1	Control of operational software	A.12.5.1	Installation of software on operational systems
A.12.4.2	Protection of system test data	A.14.3.1	Protection of test data
A.12.4.3	Access control to program source code	A.9.4.5	Access control to program source code
A.12.5	*Technical vulnerability management*	*A.12.6*	*Technical vulnerability management*
A.12.5.1	Change control procedures	A.14.2.2	System change control procedures
A.12.5.2	Technical review of applications after operating systems changes	A.14.2.3	Technical review of applications after operating platform changes
A.12.5.3	Restrictions on changes to software packages	A.14.2.4	Restrictions on changes to software packages
A.12.5.4	Information leakage		Deleted
A.12.5.5	Outsourced software development	A.14.2.7	Outsourced development
A.12.6	*Security in development and support processes*	*A.14.2*	*Security in development and support processes*
A.12.6.1	Control of technical vulnerabilities	A.12.6.1	Management of technical vulnerabilities
A.13	**Information security incident management**	**A.16**	**Information security incident management**

ISMS Controls

2005 vs 2013

Old Objectives and Controls		New/changed Objectives and Controls	
Clause	**ISO/IEC 27001:2005 Objectives and Controls**	**Clause**	**ISO/IEC 27001:2013 Objectives and Controls**
A.13.1	*Reporting information security events and weaknesses*		*Merged into other control objectives*
A.13.1.1	Reporting information security events	A.16.1.2	Reporting information security events
A.13.1.2	Reporting of security weaknesses	A.16.1.3	Reporting information security weaknesses
A.13.2	*Management of information security incidents and improvements*	*A.16.1*	*Management of information security incidents and improvements*
A.13.2.1	Responsibilities and procedures	A.16.1.1	Responsibilities and procedures
A.13.2.2	Learning from information security incidents	A.16.1.6	Learning from information security incidents
A.13.2.3	Collection of evidence	A.16.1.7	Collection of evidence
A.14	**Business Continuity Management**	**A.17**	**Information security aspects of business continuity management**
A.14.1	*Information security aspects of business continuity management*	*A.17.1*	*Information security continuity*
A.14.1.1	Including information security in the business continuity management process	A.17.1.1	Planning information security continuity
A.14.1.2	Business continuity and risk assessment	A.17.1.1	Planning information security continuity
A.14.1.3	Developing and implementing continuity plans	A.17.1.2	Implementing information security continuity
A.14.1.4	Business continuity planning framework	A.17.1.1	Planning information security continuity
A.14.1.5	Testing, maintaining and re-assessing business continuity plans	A.17.1.3	Verify, review and evaluate information security continuity
A.15	**Compliance**	**A.18**	**Compliance**
A.15.1	*Compliance with legal requirements*	*A.18.1*	*Compliance with legal and contractual requirements*
A.15.1.1	Identification of applicable legislation	A.18.1.1	Identification of applicable legislation and contractual requirements

ISMS Controls

2005 vs 2013

Old Objectives and Controls		New/changed Objectives and Controls	
Clause	**ISO/IEC 27001:2005 Objectives and Controls**	**Clause**	**ISO/IEC 27001:2013 Objectives and Controls**
A.15.1.2	Intellectual property rights	A.18.1.2	Intellectual property rights
A.15.1.3	Protecting organisational records	A.18.1.3	Protection of records
A.15.1.4	Data protection and privacy of personal information	A.18.1.4	Privacy and protection of personally identifiable information
A.15.1.5	Prevention of misuse of information processing facilities		Deleted
A.15.1.6	Regulation of cryptographic controls	A.18.1.5	Regulation of cryptographic controls
A.15.2	*Compliance with security policies and standards*	*A.18.2*	*Information security reviews*
A.15.2.1	Compliance with security policies and standards	A.18.2.2	Compliance with security policies and standards
A.15.2.2	Technical compliance checking	A.18.2.3	Technical compliance review
A.15.3	*Information systems audit considerations*	*A.12.7*	*Information systems audit considerations*
A.15.3.1	Information systems audit controls	A.12.7.1	Information systems audit controls
A.15.3.2	Protection of information systems audit tools		Deleted

ISMS Controls

2005 vs 2013

Old Objectives and Controls		New/changed Objectives and Controls	
Clause	**ISO/IEC 27001:2005 Objectives and Controls**	**Clause**	**ISO/IEC 27001:2013 Objectives and Controls**

The following are essentially new control objectives and controls:

	No direct mapping	A.6.1.5	Information security in project management
	No direct mapping	A.12.6.2	Restrictions on software installation
	No direct mapping	A.14.2.1	Secure development policy
	No direct mapping	A.14.2.5	Secure system engineering principles
	No direct mapping	A.14.2.6	Secure development environment
	No direct mapping	A.14.2.8	System security testing
	No direct mapping	A.16.1.4	Assessment of and decision on information security events
	No direct mapping	A.15.15	Response to information security incidents
	No direct mapping	*A.17.2*	*Redundancies*
	No direct mapping	A.17.2.1	Availability of information processing facilities

Note:

This is Advent IM's subjective view of those controls that have no direct mapping. Many have been merged into other controls or become part of the ISMS clauses or been deleted.

ISMS Controls

Deleted

www.advent-im.co.uk

0121 559 6699
bestpractice@advent-im.co.uk

Old Objectives and Controls		New/changed Objectives and Controls	
A.10.2.1	Service delivery		Deleted
A.10.7.4	Security of system documentation		Deleted
A.10.8.5	Business information systems		Deleted
A.10.10.5	Fault Logging		Deleted
A.11.4.2	User authentication for external connections		Deleted
A.11.4.3	Equipment identification in networks		Deleted
A.11.4.4	Remote diagnostic and conguration port protection		Deleted
A.11.4.6	Network connection control		Deleted
A.11.4.7	Network routing control		Deleted
A.11.5.5	Session time-out		Deleted
A.11.5.6	Limitation of connection time		Deleted
A.11.6.2	Sensitive system isolation		Deleted
A.12.2	*Correct processing in applications*		*Deleted*
A.12.2.1	Input data validation		Deleted
A.12.2.2	Control of internal processing		Deleted
A.12.2.3	Message integrity		Deleted
A.12.2.4	Output data validation		Deleted
A.12.5.4	Information leakage		Deleted
A.15.1.5	Prevention of misuse of information processing facilities		Deleted
A.15.3.2	Protection of information systems audit tools		Deleted

Note:

This is Advent IM's subjective view of those controls that have been deleted. Many have been merged into other controls or become part of the ISMS clauses.

Documents & Records

2013: Mandatory Documents & Records

www.advent-im.co.uk

0121 559 6699

bestpractice@advent-im.co.uk

Mandatory Documents Subjects	ISO 27001:2013 Clause/Control Number
Determination of the Scope of the ISMS	4.3
Management Establishment of Information Security Policy & Objectives with Planning to Achieve Them	5.2, 6.2
Information Security Risk Assessment and Risk Treatment Methodology	6.1.2, 6.1.3
Statement of Applicability	6.1.3 d)
Risk Treatment Plan	6.1.3 e), 6.2
Risk Assessment Report	6.1.2, 6.1.3, 8.2
Definition of Security Roles and Responsibilities	A.7.1.2
Inventory of Assets	A.8.1.1
Acceptable Use of Assets	A.8.1.3
Access Control Policy	A.9.1.1
Operating Procedures for the Information Processing Facilities	A.12.1.1
Requirement for Review of Confidentiality or Non-Disclosure documents	A.13.2.4
Secure System Engineering Principles	A.14.2.5
Supplier Security Policy	A.15.1.1
Response to Security Incident Procedures	A.16.1.5
Business Continuity Procedures	A.17.1.2
Identification of Legal, Regulatory, and Contractual Requirements	A.18.1.1

Documents & Records

Mandatory Documents Subjects	ISO 27001:2013 Clause/Control Number
Mandatory Records Contents	ISO 27001:2013 Clause/Control Number
Records of Training, Skills, Experience and Qualifications of Persons that Affect Information Security Performance	7.2
Monitoring and Measurement Results	9.1
Internal Audit Program	9.2
Results of Internal Audits	9.2
Results of the Management Review	9.3
Results of Corrective Actions	10.1g)
Logs of User Activities, Exceptions, and Security Events	A.12.4.1, A.12.4.3

Documents & Records

2013: Non Mandatory Documents

www.advent-im.co.uk

0121 559 6699
bestpractice@advent-im.co.uk

Non-Mandatory Documents Subjects	ISO 27001:2013 Clause/Control Number
Procedure for Document Control	7.5
Controls for Managing Records	7.5
Procedure for Internal Audit	9.2
Procedure for and Result of Corrective Action	10.1g)
Bring Your Own Device (BYOD) Policy	A.6.2.1
Mobile Device and Teleworking Policy	A.6.2.1
Information Classification Policy	A.8.2.1, A.8.2.2, A.8.2.3
Password Policy	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
Disposal and Destruction Policy	A.8.3.2, A.11.2.7
Procedures for Working in Secure Areas	A.11.1.5
Clear Desk and Clear Screen Policy	A.11.2.9
Change Management Policy	8.1, A.12.1.2, A.14.2.4
Backup Policy	A.12.3.1
Information Transfer Policy	A.13.2.1, A.13.2.2, A.13.2.3
Business Impact Analysis	A.17.1.1
Exercising and Testing Plan	A.17.1.3
Maintenance and Review Plan	A.17.1.3
Business Continuity Strategy	A.17.2.1

The above listed documents are commonly used and mentioned in the IEC/ISO 27001 standard but are not mandatory.