ISO 27001; 2013 transition checklist

ISO 27001: 2013 – requirements	**Comments and evidence**
0	**Introduction**
0.1	**General**
	There are some textural changes for example the new standard are ***“requirements”*** for an ISMS rather than ***“a model for”***. Generally these do not affect the purpose of the standard. The major change is the removal of the Plan-do-check-act cycle and the specific mention of the ***“process approach”***. This does not remove or prohibit the adoption of either, simply, gives the Organisation flexibility in the methods and models they use. Assessors should ensure that the ISMS ***“is part of and integrated with the organizations processes and overall management structure”***.
0.2	**Compatibility with other management system standards**
	The introduction also references Annex SL and the compatibility with other management system standards.
1	**Scope**
	Application does not state; ***“any exclusion of controls…needs to be justified and evidence needs to be provided that the associated risks have been accepted by accountable persons”***. An argument might therefore be made that the ISMS no longer needs to contain all controls within Annex A or justify exclusions or agree residual risks. This is now covered in section 6 Planning and therefore such arguments are **not** acceptable.
2	**Normative references**
	Reference to ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary.
3	**Terms and definitions**
	changed definitions include; • information security; the preservation of confidentiality, integrity and availability of information • risk; the effect of uncertainty on objectives
	Context of the Organisation
4.1	**Understanding the Organisation and its context**
	• Determine external and internal issues relevant to the information security management system
4.2	**Understanding the needs and expectations of interested parties**
	• Determine interested parties • Requirements of the parties
4.3	**Determining the scope of the information security management system**
	• Determine boundaries and applicability of the ISMS • Be available as documented information • The Organisation shall consider; external and internal issues, requirements of interested parties, interface and dependencies between activities performed by the Organisation and those performed by other organizations **The Scope is required Documented Information.**
4.4	**Information security management system**
	• The Organisation shall establish, implement, maintain and continually improve the ISMS
5	**Leadership**
5.1	**Leadership and commitment**
	a) Establish policy and objectives in line with strategic direction b) Ensure integration with organizations processes c) Ensure resources d) Communicate importance of management and conformity e) Ensure ISMS achieves intended outcomes f) Directing and supporting persons involved in the ISMS g) Promoting continual improvement h) Supporting other relevant managers
5.2	**Policy**

	a) Is appropriate to the purpose of the Organisation b) Includes information security objectives or provides the framework for setting information security objectives c) Includes a commitment to satisfy applicable requirements related to information security d) Includes a commitment to continual improvement of the information security management system e) Is available as documented information f) Be communicated within the Organisation g) Be available to interested parties **The Policy is required Documented Information.**
5.3	**Organizational roles, responsibilities and authorities**
	• Roles and authorities are assigned and communicated • Top management shall assign responsibilities for; ensuring the ISMS conforms to the standard, reporting on the performance to top management (and within the Organisation)
6	**Planning**
6.1	**Actions to address risks and opportunities**
6.1.1	**General**
	• The organizations shall consider; context of the Organisation, needs and expectations of interested parties. • Determine the risks and opportunities that need to be addressed; ISMS achieves intended outcomes, prevents or reduces undesired effects and achieves continual improvement • The Organisation shall plan; actions to address risks and opportunities and how to; integrate and implement actions into its ISMS and evaluate the effectiveness
6.1.2	**Information security risk assessments**
	• The Organisation shall define and apply a risk assessment approach that; establishes and maintains risk acceptance criteria and criteria for performing risk assessments • Ensures repeatability producing consistent, valid and comparable results • That identifies security risks associated with loss of Confidentiality, Integrity and Availability and identifies Risk Owners • Analyses risks; potential consequences, realistic likelihood, levels of risk • Evaluates risks; compares and priorities • The organizations shall retain documented information **Information on the Risk Assessment Process is required Documented Information.**
6.1.3	**Information security risk treatment**
	• The Organisation shall define and apply Information security risk treatment process to; select treatment options • Determine controls ***“from any source”*** • Compare controls with Annex A • Produce a Statement of Applicability • Formulate a treatment plan • Obtain owners approval of treatments and residual risks • Retain documented information **Information on the Risk Treatment Process is required Documented Information.** **The Statement of Applicability must be documented.**
6.2	**Information security objectives and planning to achieve them**
	• The Organisation shall establish objectives ***“at relevant functions and levels”***. • They shall be; consistent, measurable (where practicable), take into account requirements, assessment and treatments, communicated, updated • The Organisation shall retain documented information; what will be done, what resources will be required, who will be responsible, when it will be completed and how results will be evaluated **The Objectives are required Documented Information.**
7	**Support**
7.1	**Resources**
	• The Organisation shall provide resources
7.2	**Competence**
	• The organizations shall; determine the necessary competence, ensure it, take actions to acquire, retain documentation **Evidence of competence is required Documented Information.**
7.3	**Awareness**
	• Persons shall be aware of; the ISMS policy, their contributions to the ISMS, consequence of not conforming

7.4	**Communication**
	• The Organisation shall determine the need for internal and external communication
7.5	**Documented information**
7.5.1	**General**
	• The organizations ISMS shall include documented information required by the standard • Information deemed by the Organisation as required **Information Necessary for the effectiveness of the ISMS is required Documented Information.**
7.5.2	**Creating and updating**
	• When creating documented information the Organisation shall ensure appropriate; identification and description, format, review and approval
7.5.3	**Control of documented information**
	• Documented information shall be controlled to ensure; availability and suitability, protection • The Organisation shall address; distribution, access retrieval and use, storage and preservation, change control, retention and disposition • External documents **Documented Information of External Origin shall be controlled as other Documented Information.**
8	**Operation**
8.1	**Operational planning and control**
	• The Organisation shall plan, implement and control processes • The Organisation shall implement plans to achieve objectives • The Organisation shall control planned changes and review consequences of unplanned changes • The Organisation shall ensure outsourced processes are determined and controlled **Information necessary to have confidence that processes are being carried out as planned are required Documented Information.**
8.2	**Information security risk assessments**
	• The Organisation shall perform risk assessments at planned intervals or significant changes • The Organisation shall retain documented information **Information on Risk Assessments is required Documented Information.**
8.3	**Information security risk treatment**
	• The Organisation shall implement risk treatment plan and retain documentation **Results of Risk Treatment is required Documented Information.**
9	**Performance evaluation**
9.1	**Monitoring, measurement, analysis and evaluation**
	• The Organisation shall evaluate the ISMS performance and effectiveness **Evidence of Monitoring and Measuring is required Documented Information.**
9.2	**Internal audit**
	• The Organisation shall conduct internal audits. Auditors shall be selected and conduct audits ***"that ensure the objectivity and impartiality of the audit process"*** however the statement ***"auditors shall not audit their own work"*** is omitted. **The Audit Programme and Results are required Documented Information.**
9.3	**Management review**
	• Top management shall review the ISMS this shall include; Status of actions from previous meetings External and internal changes Feedback on performance Non-conformities and corrective actions Monitoring and measurement Audit results Fulfilment of objectives Feedback from interested parties Results of risk assessments and treatment plans Opportunities for continuous improvement **The results of Management Review are required Documented Information.**
10	**Improvements**
10.1	**Nonconformity and corrective actions**
	• The Organisation shall react to nonconformities, evaluate the need for actions, implement actions **Information on Non-conformances and actions are required Documented Information.**
10.2	**Continual improvement**
	• The organizational shall continually improve the ISMS

Table A.1 Control objectives and Controls

A.5	Information Security Policies **– title change**	
A.5.1	Management direction for information security **– title change**	Objective: to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. **No change in wording.**
A.5.1.1	Policies for information security **– title change**	Control – a set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties. **Wording changed; talk of policies rather than a single policy.**
A.5.1.2	Review of the policies for information security **– title change**	Control – the policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy and, effectiveness. **As above.**
A.6	Organization of Information security **– no change**	
A.6.1	Internal organization **– no change**	Objective: to establish a management framework to initiate and control the implementation and operation of information security within the organisation. **Wording change but not intention; *"initiate and control"* rather than *"establish"*.**
A.6.1.1 **– formerly A.8.1.1**	Information security roles and responsibilities	Control – all information security responsibilities shall be defined and allocated. **Wording change but not intention.**
A.6.1.2 **– formerly A.10.1.3**	Segregation of duties	Control – conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organizations assets. **Addition of the word *"conflicting"*.**
A.6.1.3 **– formerly A.6.1.6**	Contact with authorities	Control – appropriate contacts with relevant authorities shall be maintained. **No change.**
A.6.1.4 **- formerly A.6.1.7**	Contact with special interest groups	Control – appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained. **No change.**
A.6.1.5	Information security in project management **– new requirement**	Control – information security shall be addressed in project management, regardless of the type of the project. **Clarification but this was always implicit in the previous standard. New clause in the SOA but new controls may not be required.** **New requirement.**
A.6.2 **- formerly A.11.7**	Mobile devices and teleworking **– title change was *"computing"* not *"devices"***	Objective – to ensure the security of teleworking and use of mobile devices. **Wording change as previous.**
A.6.2.1 **- formerly A.11.7.1**	Mobile device policy **– was *"computing and communication"***	Control – a policy and supporting security measures shall be adopted to manage risks introduced by using mobile devices. **Wording change with more emphasis on devices.**
A.6.2.2 **– formerly A.11.7.2**	Teleworking **– no change**	Control – a policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites. **Wording change, emphasis on *"sites"* rather than *"activities"*.**
A.7 **– formerly A.8**	Human resource security **– no change**	
A.7.1 **– formerly A.8.1**	Prior to employment **– no change**	Objective – to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. **Wording change; no *"third party users"* or *"to reduce the risk of theft, fraud or misuse of facilities"*.**
A.7.1.1 **– formerly A.8.1.2**	Screening **– no change**	Control – background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to business requirements, the classification of the information to be accessed, and the perceived risks. **Wording changes; no *"contractors and third party users"*.**
A.7.1.2 **– formerly A.8.1.3**	Terms and conditions of employment **– no change**	Control – the contractual agreements with employees and contractors shall their and the organization's responsibility for information security. **Wording changes; no *"third party users"*.**
A.7.2 **– formerly A.8.2**	During employment **– no change**	Objective – to ensure that all employees and contractors are aware of and fulfil their information security responsibilities. **Wording changes; no *"third party users"*, *"Human error"* or *"normal work"*.**
A.7.2.1 **– formerly A.8.2.1**	Management responsibilities **– no change**	Control – management shall require employees and contractors to apply security in accordance with established policies and procedures of the organization. **Wording changes; no *"third party users"*.**

A.7.2.2 **– formerly A.8.2.2**	Information security awareness, education and training **– no change**	Control – all employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in the organizations policies and procedures, as relevant to their job function. **Wording changes; no *“third party users”***.
A.7.2.3 **– formerly A.8.2.3**	Disciplinary process **no change**	Control – there shall be a formal and communicated disciplinary process to take action against employees who have committed an information security breach. **Wording change; *“communicated”* and *“take action”***.
A.7.3 **– formerly A.8.3**	Termination and change of employment **- Wording change *“and”* rather than *“or”***	Objective – to protect the organisations interests as part of the process of changing or terminating employment. **Wording change *“protect the organisation”* rather than *“exit…or change employment in an orderly manner”*.**
A.7.3.1 **- formerly A.8.3.1**	Termination or change of employment responsibilities. **Wording change *“or change of”*.**	Control – information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced. **Wording change; emphasis on *“duties...after”* and *“enforced”*.**
A.8 **– formerly A.7**	Asset Management **– no change**	
A.8.1 **– formerly A.7.1**	Responsibility for Assets **– no change**	Objective – to identify organizational assets and define appropriate protection responsibilities. **Wording change; *“identifying … assets”* and *“define … responsibilities”***.
A.8.1.1 **- formerly A.7.1.1**	Inventory of Assets **- no changes**	Control – assets associated with information security and information processing facilities shall be identified and an inventory of these assets shall drawn up and maintained. **Wording change; *“all assets”*.** **The Inventory of Assets must be documented.**
A.8.1.2 **– formerly A.7.1.2**	Ownership of Assets **– no change**	Control –assets maintained in the inventory shall be owned. **Wording change; ownership is emphasized.**
A.8.1.3 **– formerly A.7.1.3**	Acceptable use of Assets **– no change**	Control – rules for the acceptable use of information and assets associated with information and information processing facilities shall be identified, documented and implemented. **Wording change; word *“and”*.** **The Rules for the Acceptable Use of Information and Assets must be documented.**
A.8.1.4 **– formerly A.8.3.2**	Return of assets **– no change**	Control – all employees and external party users shall return all of the organizations assets in their possession upon termination of their employment, contract or assignment. **Wording change; *“external party”*.**
A.8.2 **– formerly A.7.2**	Information Classification **– no change**	Objective – to ensure that information receives an appropriate level of protection in accordance with its importance to the organisation. **Wording change; last part of sentence added.**
A.8.2.1 **– formerly A.7.2.1**	Classification of information **– was *“guidelines”***	Control – information shall be classified in terms of its legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. **Wording change; *“unauthorized disclosure”* rather than *“the organisation”*.**
A.8.2.2 **– formerly A.7.2.2**	Labelling of Information **– wording included *“handling”***	Control – an appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. **Wording change; handling separated.**
A.8.2.3	Handling of assets	Control – procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organisation. **New requirement caused by dividing A.7.2.2 into 2 parts.**
A.8.3 **– formerly A.10.7**	Media handling **– no change**	Objective – to prevent unauthorized disclosure, modification, removal or destruction of information stored on media. **Wording change *“information”* rather than *“assets, and the interruption to business activities”***
A.8.3.1 **– formerly A.10.7.1**	Management of removable media **– wording change *“removable”* not *“mobile”***	Control - procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation. **Wording change; last part of sentence added.**

A.8.3.2 **– formerly A.10.7.2**	Disposal of media **– no change**	Control - Media shall be disposed of securely when no longer required, using formal procedures. **Wording change; *“and safely”* removed.**
A.8.3.3 **– formerly A.10.8.3**	Physical media in transit **– no change**	Control - Media containing information shall be protected against unauthorized access, misuse or corruption during transportation. **Wording change; removed *“beyond an organization’s physical boundaries”***.
A.9 **formerly A.11**	Access control	
A.9.1 **formerly A.11.1**	Business requirements of access control	Objective – to limit access to information and information processing facilities. **Wording change; to *“limit”* rather than *“control”* also *“information processing facilities”***
A.9.1.1 **formerly A.11.1.1**	Access control policy	Control - An access control policy shall be established, documented, and reviewed based on business and security requirements. **Wording change; removed the words *“for access”*.** **The Access Control Policy must be documented.**
A.9.1.2 **similar to A.11.2**	Access to networks and network services **similar to User access management)**	Control – Users shall only be provided with access to the network and network services that they have been specifically authorized to use. **Different wording but broadly similar requirement; *“To ensure authorized user access and to prevent unauthorized access to information systems”.***
A.9.2	User access management **– new section but broadly similar to A.11**	Objective – to ensure authorized user access and to prevent unauthorized access to systems and services. **See before.**
A.9.2.1 **formerly A.11.2.1**	User registration and de-registration **– added de-registration**	Control - a formal user registration and de-registration procedure in implemented to enable assignment of access rights. **Wording change but broadly similar.**
A.9.2.2 **formerly A.11.2.2**	User access provisioning **- formerly Privilege management**	Control – a formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. **Wording change formerly *“the allocation and use of privileges shall be restricted and controlled”*.**
A.9.2.3	Management of privileged access rights **– new control**	Control – the allocation and use of privileged access rights shall be restricted and controlled. **New requirement but similar to many in old A.11.**
A.9.2.4 **similar to A.11.2.3**	Management of secret authentication information of users **similar to User password management**	Control - The allocation of secrete authentication information shall be controlled through a formal management process. **Wording change; was *“passwords”*.**
A.9.2.5 **was A.11.2.4**	Review of user access rights	Control – Asset owners shall review users’ access rights at regular intervals. **Wording change; was *“Management”* and *“using a formal process”*.**
A.9.2.6 **similar to A.8.3.3**	Removal or adjustment of access rights **adds “adjustment”**	Control – The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change. **Wording changes; *“external party users”*.**
A.9.3 **similar to A.11.3.1**	User Responsibilities	Objective – to make users accountable for safeguarding their authentication information. **Similar control but emphasis is now on user.**
A.9.3.1	Use of secret authentication information. **Formerly *“Password use”*.**	Control - Users shall be required to follow the organisation’s practices in the use of secrete authentication information. **Wording change; following *“organisation practice”* rather than *“good security practices”* and replacement of *“passwords”*.**
A.9.4 **similar to 11.6**	System and application access control. **Also stated *“information”*.**	Objective – to prevent unauthorized access to systems and applications. ***Also stated “information”.***
A.9.4.1 **similar to A.11.6.1**	Information access restriction	Control - Access to information and application system functions shall be restricted in accordance with the access control policy. **Previously stated *“by users and support personnel”*.**
A.9.4.2 **similar to A.11.5.1**	Secure log-on procedures	Control – where required by the access control policy, access to systems and applications shall be controlled by secure log-on procedures. **Added *“where required”*.**
A.9.4.3 **similar to A.11.5.3**	Password management system	Control – password management systems shall be interactive and shall ensure quality passwords. **Wording change.**

A.9.4.4 **similar to A.11.5.4**	Use of privileged utility programs. **Was *“system utilities”*.**	Control - The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled. **No change.**
A.9.4.5 **was A.12.4.3**	Access control to program source code	Control - Access to program source code shall be restricted. **No change.**
A.10.1 **similar to A.12**	Cryptographic Controls	Objective - To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. **Change of word order.**
A.10.1.1 **was A.12.3.1**	Policy on the use of cryptographic controls	Control - A policy on the use of cryptographic controls for protection of information shall be developed and implemented. **No change.**
A.10.1.2 **was A.12.3.2**	Key management	Control – a policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented throughout their whole lifetime. **New policy required and *“lifetime”* of keys specifically needs to be considered.** **New Policy required.**
A.11	Physical and environmental security	
A.11.1	Secure areas	Objective – to prevent unauthorized physical access, damage and interference to the organizations information and information processing facilities. **Was *“premises and information”*.**
A.11.1.1 **was A.9.1.1**	Physical security perimeter	Control – security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities. **Wording previously gave examples; *“barriers such as walls, card control entry gates or manned reception desks”*.**
A.11.1.2 **was A.9.1.2**	Physical entry controls	Control – secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. **No change.**
A.11.1.3 **was A.9.1.3**	Securing offices, rooms and facilities	Control – physical security for offices, rooms and facilities shall be designed and applied. **No change.**
A.11.1.4 **was A.9.1.4**	Protecting against external and environmental threats	Control – physical protection against natural disasters, malicious attack or accidents shall be designed and applied. **Previously gave examples *“damage fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster”*.**
A.11.1.5 **was A.9.1.5**	Working in secure areas	Control – procedures for working in secure areas shall be designed and applied. **Previously said *“physical protection and guidelines”*.**
A.11.1.6 **was A.9.1.6**	Delivery and loading areas. **Previously said *“Public access”*.**	Control – access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. **Says *“could”* not *“may”*.**
A.11.2 **was A.9.2**	Equipment **was *“Equipment security”***	Objective – to prevent loss, damage, theft or compromise of assets and interruption to the organizations operations. **Wording change; was *“activities”*.**
A.11.2.1 **was A.9.2.1**	Equipment siting and protection	Control – equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. **Wording change *“and”* not *“or”*.**
A.11.2.2 **was A.9.2.2**	Supporting utilities	Control – equipment shall be protected from power failures or other disruptions caused by failures in supporting utilities. **No change.**
A.11.2.3 **was A.9.2.3**	Cabling security	Control – power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. **No change.**
A.11.2.4 **was A.9.2.4**	Equipment maintenance	Control – equipment shall be correctly maintained to ensure its continued availability and integrity. **No change.**
A.11.2.5 **was A.9.2.7**	Removal of assets	Control – equipment, information or software shall not be taken off-site without prior authorization. **No change.**
A.11.2.6 **was A.9.2.5**	Security of equipment and assets off-premises. **Added *“assets”* and was *“off-site”*.**	Control – security shall be applied to off-site assets taking into account the different risks of working outside the organization’s premises. **Wording change; was *“equipment”*.**

A.11.2.7 **was A.9.2.6**	Secure disposal or re-use of equipment	Control – all items of equipment containing storage media shall verified be to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. **Wording change; *“checked”* and *“data”* and added *“or re-use”*.**
A.11.2.8 **was A.11.3.2**	Unattended user equipment	Control - Users shall ensure that unattended equipment has appropriate protection. **No change.**
A.11.2.9 **was A.11.3.3**	Clear desk and clear screen policy	Control - A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted. **No change.**
A.12 **was A.10**	Operations security	
A.12.1 **was A.10.1**	Operational procedures and responsibilities	Objective – to ensure the correct and secure operation of information processing facilities. **No change.**
A.12.1.1 **was A.10.1.1**	Documented operating procedures	Control – operating procedures shall be documented, maintained and made available to all users who need them. **Wording change; *“shall”* not *“should”*.** **The Operating Procedures must be documented.**
A.12.1.2 **was A.10.1.2**	Change management	Control – changes to the organisation, business processes and information processing facilities and systems shall be controlled. **Wording change; added *“the organisation, business processes”* and *“shall”* not *“should”*.**
A.12.1.3 **was A.10.3.1**	Capacity management **was previously A.10.3 System planning and acceptance So emphasis of objective was *“to minimize the risk of systems failures”***	Control – the use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. **No change.**
A.12.1.4 **was A.10.1.4**	Separation of development, test and operational environments **was *“facilities”***	Control – development, test and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment. **Wording change; was *“facilities”* and *“systems”*.**
A.12.2 **similar to A.10.4**	Protection from malware **was *“malicious and mobile code”***	Objective – to ensure that information and information processing facilities are protected against malware. **Change of emphasis; was *“protect the integrity of software and information”*.**
A.12.2.1 **was A.10.4.1**	Controls against malware **was *“malicious code”***	Control – detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness. **Wording change; was *“malicious code”***
A.12.3 **was A.10.5**	Back up	Objective – protect against the loss of data. **Was *“to maintain the integrity and availability of information and information processing facilities”*.**
A.12.3.1 **was A.10.5.1**	Information back-up	Control – back-up copies of information, software and system images shall be taken and tested regularly in accordance with an agreed back-up policy. **Added *“and system images”*.**
A.12.4 **similar to A.10.10**	Logging and Monitoring **added *“Logging”***	Objectives – to record events and generate evidence. **Was *“detect unauthorized information processing activities”*.**
A.12.4.1 **was A.10.10.1 and A.10.10.5**	Event logging **was *“Audit logging”* and *“Fault logging”***	Control – event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed. **Was *“Audit”* and *“kept for an agreed period to assist in future investigations and access control monitoring”*.**
A.12.4.2 **was A.10.10.3**	Protection of log information	Control - Logging facilities and log information shall be protected against tampering and unauthorized access. **No change.**
A.12.4.3 **was A.10.10.4**	Administrator and operator logs	Control - System administrator and system operator activities shall be logged and the logs protected and regularly reviewed. **Added *“and the logs protected and regularly reviewed”*.**
A.12.4.4 **was A.10.10.6**	Clock synchronization	Control - The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source. **Was *“with an agreed accurate time source”*.**

A.12.5	Control of operational software **was previously a control under objective *"A.12.4 Security of system files"***	Objective – to ensure the integrity of operational systems. **Previous control objective was *"To ensure the security of system files"*.**
A.12.5.1 **was A.12.4.1**	Installation of software on operational systems **was *"Control of operational software"***	Control - procedures shall be in place to control the installation of software on operational systems. **Wording reordered.**
A.12.6	Technical vulnerability management	Objective – to prevent exploitation of technical vulnerabilities. **Previously *"To reduce risks resulting from exploitation of published technical vulnerabilities"*.**
A.12.6.1	Management of technical vulnerabilities **was *"Control"***	Control - information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. **Wording rearranged.**
A.12.6.2 **was A.12.4.1**	Restrictions on software installation **was *"Control of operational software"***	Control – rules governing the installation of software by users shall be established and implemented. **Was *"procedures"* and *"on operational systems"*. Also *"by users"* has been added.**
A.12.7 **was A.15.3**	Information system audit considerations	Objective – to minimize the impact of audit activities on operational systems. **Was *"to maximize the effectiveness of and to minimize interference to/from the information systems audit process"*.**
A.12.7.1 **was A.15.3.1**	Information systems audit controls	Control - Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes. **Was *"checks"*.**
A.13	Communications security	
A.13.1 **was A.10.6**	Network security management	Objective – to ensure the protection of information in networks and its supporting information processing facilities. **Was *"infrastructure"*.**
A.13.1.1 **was A.10.6.1**	Network controls	Control - Networks shall be managed and controlled, in order to be protected information in systems and applications. **Removed *"in transit"*, *"adequately"*, *"from threats"* and *"to maintain security for the systems and applications using the network"*.**
A.13.1.2 **was A.10.6.2**	Security of network services	Control – Security mechanisms, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced. **Was *"features"*.**
A.13.1.3 **was A.11.4.5**	Segregation in networks	Control - Groups of information services, users and information systems shall be segregated on networks. **No change.**
A.13.2 **was A.10.8**	Information transfer **was *"exchange of information"***	Objective – to maintain the security of information and software transferred within an organization and with any external entity. **Was *"exchanged"*.**
A.13.2.1 **was A.10.8.1**	Information transfer policies and procedures **was *"exchange"***	Control - Formal transfer policies, procedures, and controls shall be in place to protect the transfer of information through the use of all types of communication facilities. **Was *"exchange"*.**
A.13.2.2 **was A.10.8.2**	Agreements on information transfer	Control - Agreements shall be established for the secure transfer of business information and software between the organization and external parties. **Was *"exchange"* and added *"secure"* and *"business"*.**
A.13.2.3 **was A.10.8.4**	Electronic messaging	Control - Information involved in electronic messaging shall be appropriately protected. **No change.**
A.13.2.4 **was A.6.1.5**	Confidentiality or non-disclosure agreements **added *"or non-disclosure"***	Control – requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented. **Added *"and documented"*.** **The Confidentiality and Non- disclosure agreements <u>must be documented</u>.**
A.14 **was A.12**	System acquisition, development and maintenance	

A.14.1	Security requirements of information systems	Objective - To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks. **Last section has been added.**
A.14.1.1 **was A.12.1.1**	Information security requirements analysis and specification ***"information"* was added**	Control – the information security related requirements shall be included in the requirements for new information systems or enhancements to existing informations systems. **Was *"Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls"*.**
A.14.1.2 **was A.10.9.1**	Securing application services on public networks **was *"Electronic commerce"***	Control – information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthroised disclosure and modification. **Was *"electronic commerce"***
A.14.1.3 **was A.10.9.2**	Protecting application services transactions **was *"On-line transactions"***	Control - Information involved in service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. **Was *"on-line"* not *"service"*.**
A.14.2 **was A.12.5**	Security in development and support processes	Objective - To ensure that information security is designed and implemented within the development lifecycle of information systems. **Was *"to maintain the security of application system software and information"*.**
A.14.2.1	Secure development policy	Control – rules for the development of software and systems shall be established and applied to developments within the organisation. **this is a new requirement policy and rules.**
A.14.2.2 **was A.12.5.1**	System change control procedures	Control – changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures. **Was *"the implementation of changes"*.**
A.14.2.3 **was A.12.5.2**	Technical review of applications after operating platform changes **was *"system"***	Control - When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security. **Was *"system"*.**
A.14.2.4 **was A.12.5.3**	Restrictions on changes to software packages	Control - Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled. **No change.**
A.14.2.5	Secure system engineering principles	Control – principles for engineering secure systems shall be established, documented, maintained and applied to any information systems implementation efforts. **The Principles for Engineering Secure Systems <u>must be documented</u>.** **This is a New requirement.**
A.14.2.6 **was A.10.1.4**	Secure development environment **was *"Separation of development, test and operational facilities"***	Control – organizations shall establish and appropriately protect sure development environments for system development and integration efforts that cover the entire system development lifecycle. **Was *"development, test and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational systems"*.**
A.14.2.7 **was A.12.5.5**	Outsourced development	Control – the organisation shall supervise and monitor the activity of out-sourced systems development. **Was *"software development"*.**
A.14.2.8 **similar to A.10.3.2**	system security testing **similar to *"System acceptance"***	Control – testing of security functionality shall be carried out during development. **The similar control was *"acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance"*.** **This is a new Control.**
A.14.2.9 **similar to A.10.3.2**	System acceptance testing **similar to *"System acceptance"***	Control – acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions. **This is a new Control.**
A.14.3 **was A.12.4**	Test data **was *"Security of system files"***	Objective – To ensure the protection of data used for testing. **Was *"security of system files"*.**

A.14.3.1 **was A.12.4.2**	Protection of test data	Control - Test data shall be selected carefully, and protected and controlled. **No change.**
A.15	Supplier relationships	
A.15.1 **was A.10.2**	Information security in supplier relationships **was *“Third party service delivery management”***	Objective – to maintain an agreed level of information security and service delivery in-line with supplier agreements. **Previous had *“to implement”* and was *“an appropriate”* and *“third party”*.**
A.15.1.1	Information security policy for supplier relationships	Control – information security requirements for mitigating the risks associated with supplier’s access to the organization’s assets shall be agreed with the suppliers and documented. **The Policy for Supplier Relationships must be documented.** **This is a New requirement.**
A.15.1.2	Addressing security within supplier agreements	control – all relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation’s information. **This is a new requirement.**
A.15.1.3 **similar to A.10.2.1**	Information and communication technology supply chain **similar to *“Service delivery”***	Control – agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain. **Previous was *“it shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated and maintained by the third party”.***
A.15.2	Supplier service delivery management	Objective – to maintain an agreed level of information security and service delivery in line with supplier agreements.
A.15.2.1 **was A.10.2.2**	Monitoring and review of supplier services. **Was *“third party”***	Control – organizations shall regularly monitor, review and audit supplier delivery. **Was *“the services, reports and records provided by the third party shall be regularly monitored and reviewed and audits shall be carried out regularly”.***
A.15.2.2 **was A.10.2.3**	Managing changes to supplier services. **Was *“third party”***	Control – changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls shall be managed, taking account of the criticality of the business information and processes involved and the re-assessment of the risks. **Was *“systems”***
A.16 **was A.13**	Information security incident management	
A.16.1 **was A.13.2**	Management of information security incidents and improvements	Objective - To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. **Removed *“is applied”* and added last section.**
A.16.1.1 **was A.13.2.1**	Responsibilities and procedures	Control - Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents. **No change.**
A.16.1.2 **was A.13.1.1**	Reporting information security events	Control - Information security events shall be reported through appropriate management channels as quickly as possible. **No change.**
A.16.1.3 **was A.13.1.2**	Reporting information security weaknesses	Control – employees and contractors using the organisation’s information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services. **Removed word *“All”* and *“third party users”.***
A.16.1.4	Assessment of and decision on information security events	Control – information security events shall be assessed and it shall be decided if they are to be classified as information security incidents. **this is a new requirement.**
A.16.1.5	Response to information security incidents	Control – information security incidents shall be responded to in accordance with documented procedures. **this is a new requirement.**
A.16.1.6 **was A.13.2.2**	Learning from information security incidents	Control – knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents. **Was *“There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored”.***

A.16.1.7 **was A.13.2.3**	Collection of evidence	Control – the organisation shall define and apply procedures for the identification, collection, acquisition and preservation of information which can serve as evidence. **was *"Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s)".***
A.17 **was A.14**	Information security aspects of business continuity management. **Was *"Business continuity management"***	
A.17.1 **was A.14.1**	Information security continuity. **Was *"aspects of business continuity management".***	Objective – information security continuity shall be embedded in the organisation's business continuity management systems. **Was *"To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption".***
A.17.1.1 **was A.14.1.4**	Planning information security continuity. **Was *"Business continuity planning framework"***	Control – the organisation shall determine its requirements for information security and continuity of information security management in adverse situations, e.g. a crisis or disaster. **Was *"A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance".***
A.17.1.2 **was A.14.1.3**	Implementing information security continuity. **Was *"Developing and".***	Control – the organisation shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation. **Was *"Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes".*** **The Procedures to Ensure Continuity of Information must be documented.**
A.17.1.3 **was A.14.1.5**	Verify, review and evaluate information security continuity. **Was *"Testing, maintaining and reassessing business continuity plans".***	Control – the organisation shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. **Was *"Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective"?***
A.17.2	Redundancies	Objective – to ensure availability of information processing facilities.
A.17.2.1	Availability of information processing facilities	Control – information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. **this is a new requirement.**
A.18 **was A.15**	Compliance	
A.18.1 **was A.15.1**	Compliance with legal and contractual requirements. ***"Contractual"*** **added.**	Objective - To avoid breaches of any legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. **Changed *"law"* and added *"related to information security".***
A.18.1.1 **was A.15.1.1**	Identification of applicable legislation and contractual requirements. **Added last section.**	Control - All relevant legislative, statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization. **Was *"statutory"* and *"defined".*** **The Relevant Legislative, Statutory and Contractual Requirements must be documented.**
A.18.1.2 **was A.15.1.2**	Intellectual property rights. **Included *"(IPR)".***	Control - Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and on the use of proprietary software products. **Was *"on the use of material in respect of which there may be".***
A.18.1.3 **was A.15.1.3**	Protection of records. **Did include *"organizational".***	Control - records shall be protected from loss, destruction and falsification, in accordance with legislatory, regulatory, contractual, and business requirements. **Was *"Important"* and *"statutory".***

A.18.1.4 **was A.15.1.4**	Privacy and protection of personally identifiable information. **Was *“Data protection”* and added *“protection”* and *“personally identifiable”*.**	Control - privacy and protection of personally identifiable information shall be ensured as required in relevant legislation, regulations where applicable. **Was *“Data protection”* and added *“protection”* and *“personally identifiable”* removed *“if applicable, contractual clauses”*.**
A.18.1.5 **was A.15.1.6**	Regulation of cryptographic controls	Control - Cryptographic controls shall be used in compliance with all relevant agreements, legislation, and regulations. **Was *“laws”*.**
A.18.2 **was A.15.2**	Information security reviews. **Was *“Compliance with security polices and standards, and technical compliance”*.**	Objective – to ensure that the information security is implemented and operated in accordance with the organizational security policies and standards. **Was *“to ensure compliance of systems”* rather than *“implemented and operated”*.**
A.18.2.1 **was A.6.1.8**	Independent review of information security	Control – the organizations approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes occur. **Removed *“to the security implementation”*.**
A.18.2.2 **was A.15.2.1**	Compliance with security policies and standards	Control - Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security polices, standards and any other security requirements. **Was *“shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards”* and added *“any other security requirements”*.**
A.18.2.3 **was A.15.2.2**	Technical compliance review. **Was *“checking”*.**	Control - Information systems shall be regularly reviewed for compliance with the organisation’s information security policies and standards. **Was *“security implementation standards”* and *“checked”*.**