

ISOQAR



ISO 27001:2022 INFORMATION SECURITY MANAGEMENT SYSTEMS

TRANSITION GAP ANALYSIS

A document to help you transition from
ISO 27001:2013 to ISO 27001:2022 including
details of changes to controls in Annex A

To find out more visit
alcumus.com/isoqar

CHANGES - THE ISO 27001 STANDARD

This first section highlights where there are differences between the main clauses of the 2013 and 2022 versions of the standard and where new requirements have been implemented. **Text is highlighted in blue to emphasise changes in wording which you might otherwise miss.**

Clauses of the 2013 standard may appear to be out of sequence; this is because they have been put in an order that best relates to the sequence of equivalent clauses in the 2022 version.

You can make your own notes in the ACTION REQUIRED and COMPLETED columns.

2013 CLAUSE	2013 REQUIREMENT	2022 CLAUSE	2022 REQUIREMENT	CHANGES	ACTION REQUIRED	COMPLETED
4.1 Context	No change to this clause.	4.1 Context	No change to this clause.	The note on this clause makes reference to Clause 5.4.1 of ISO 31000: 2018 rather than the previous 2009 version.		
4.2 Understanding the needs and expectations of interested parties	No additional requirements.	4.2 Understanding the needs and expectations of interested parties	There is an additional requirement to be determined: c) which of these requirements will be addressed through the information security management system.	This is to clarify the ISMS requirements.		
4.4 Information security management system	The organisation shall establish, implement, maintain and continually improve an information security management system in accordance with the requirements of this International Standard.	4.4 Information security management system	The organisation shall establish, implement, maintain and continually improve an information security management system including the processes needed and their interactions, in accordance with the requirements of this document.	Rewritten but fundamentally similar.		
6.1.3 Information security risk treatment	Minor changes to the numbering of the Notes.	6.1.3 Information security risk treatment	Minor changes to the numbering of the Notes.	The reference to “control objectives” in Annex A is gone and now the term “information security controls” is used rather than “controls”. This is in line with the changes to the Annex A.		

2013 CLAUSE	2013 REQUIREMENT	2022 CLAUSE	2022 REQUIREMENT	CHANGES	ACTION REQUIRED	COMPLETED
6.2 Information security objectives and planning to achieve them	The organisation shall retain documented information on the information security objectives.	6.2 Information security objectives and planning to achieve them	d) be monitored g) be available as documented information The organisation shall retain documented information on the information security objectives.	Monitor changes and additional requirement for monitoring of objectives.		
NEW (No equivalent 2013 requirement)		6.3 Planning of changes	When the organisation determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.	A new clause and requirement.		
7.4 Communication	d) who shall communicate; and e) the processes by which communication shall be effected	7.4 Communication	d) how to communicate	<i>How to communicate</i> added and who shall communicate removed.		
8.1 Operational planning and control	in 6.1. The organisation shall also implement plans to achieve information security objectives determined in 6.2. The organisation shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. The organisation shall ensure that outsourced processes are determined and controlled.	8.1 Operational planning and control	in Clause 6, by: - establishing criteria for the processes; - implementing control of the processes in accordance with the criteria. Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned. The organisation shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.	Rewritten but fundamentally similar.		

2013 CLAUSE	2013 REQUIREMENT	2022 CLAUSE	2022 REQUIREMENT	CHANGES	ACTION REQUIRED	COMPLETED
9.1 Monitoring, measurement, analysis and evaluation	The organisation shall evaluate the information security performance and the effectiveness of the information security management system. NOTE The methods selected should produce comparable and reproducible results to be considered valid.	9.1 Monitoring, measurement, analysis and evaluation	Some minor differences.	2022 has some additions such as determining who shall monitor and when analysis and evaluation shall be done but fundamentally the clause is similar.		
9.2 Internal audit	Some minor differences.	9.2 Internal audit	Some minor differences.	The structure of the clauses is different but has no new or different requirements.		
9.3 Management review	No additional requirements.	9.3 Management review	c) changes in needs and expectations of interested parties that are relevant to the information security management system	The clauses are renumbered. Also need to review needs and expectations of interested parties.		
10 Improvement	Minor renumbering of clauses but no significant change.	10 Improvement	Minor renumbering of clauses but no significant change.			

CHANGES - ANNEX A CONTROLS

This section focuses on Annex A Controls. It highlights where there are differences between the 2022 and 2013 versions and where new requirements have been added. **Text is highlighted in blue to emphasise changes in wording which you might otherwise miss.**

You can make your own notes in the ACTION REQUIRED and COMPLETED columns.

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
5. ORGANISATIONAL CONTROLS						
A.5.1.1 Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	A.5.1 Policies for information security	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	The main change is a means to show that acknowledgement of policies needs to be in place.		
A.5.1.2 Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness.					
A.6.1.1 Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	A.5.2 Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organisation's needs.	In practice the difference is not significant.		
A.6.1.2 Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	A.5.3 Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	2013 gives justification but the difference is not significant.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.7.2.1 Management responsibilities	Management shall require employees and contractors to apply security in accordance with established policies and procedures of the organisation.	A.5.4 Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic specific policies and procedures of the organisation.	Some clarification but the difference is not significant.		
A.6.1.3 Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	A.5.5 Contact with authorities	The organisation shall establish and maintain contact with relevant authorities.	The clause has been rewritten but the difference is not significant.		
A.6.1.4 Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	A.5.6 Contact with special interest groups	The organisation shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	The clause has been rewritten but the difference is not significant.		
NEW (No equivalent 2013 requirement)		A.5.7 Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	A new requirement. It could be linked with the risk assessments and also management review item on external changes.		
A.6.1.5 Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	A.5.8 Information security in project management	Information security shall be integrated into project management.	The clause has been rewritten but the difference is not significant.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.8.1.1 Inventory of assets	Information, other assets associated with information security and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	A.5.9 Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	There is a stronger focus on Information as an asset and equipment being “other associated”. Organisations will need to create information registers.		
A.8.1.2 Ownership of assets	Assets maintained in the inventory shall be owned.			The definition of assets is given as “3.1.2 asset - anything that has value to the organisation.”		
A.8.2.3 Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.			Note 1 to entry: In the context of information security, two kinds of assets can be distinguished: PRIMARY ASSETS: • information • business processes (3.1.27) and activities SUPPORTING ASSETS (on which the primary assets rely) of all types, for example: • hardware • software • network • personnel (3.1.20) • site • organisation's structure		
A.11.2 Equipment	To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.					
A.11.2.5 Removal of assets	Equipment, information or software shall not be taken off-site without prior authorisation.					
A.8.1.3 Acceptable use of assets	Rules for the acceptable use of information and assets associated with information and information processing facilities shall be identified, documented and implemented.	A.5.10 Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	The wording flips the emphasis from the physical assets to the information.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.8.1.4 Return of assets	All employees and external party users shall return all of the organisation's assets in their possession upon termination of their employment, contract or assignment .	A.5.11 Return of assets	Personnel and other interested parties as appropriate shall return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement .	The clause has been rewritten but the difference is not significant.		
A.8.2.1 Classification of information	Information shall be classified in terms of its legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification .	A.5.12 Classification of information	Information shall be classified according to the information security needs of the organisation based upon confidentiality, integrity, availability and relevant interested party requirements .	There is a specific reference to confidentiality, integrity and availability (CIA).		
A.8.2.2 Labelling of Information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.	A.5.13 Labelling of information	No change.	No change to the requirement wording.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.13.2.1 Information transfer policies and procedures	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.	A.5.14 Information transfer	Information transfer rules, procedures or agreements shall be in place for all types of transfer facilities within the organisation and between the organisation and other parties.	The clause has been rewritten but the difference is not significant.		
A.13.2.2 Agreements on information transfer	Agreements shall be established for the secure transfer of business information and software between the organisation and external parties.					
A.13.2.3 Electronic messaging	Information involved in electronic messaging shall be appropriately protected.					
A.14.1.2 Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.					
A.14.1.3 Protecting application services transactions	Information involved in service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.					

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.9.1.1 Access control policy	An access control policy shall be established, documented, and reviewed based on business and security requirements. Appropriate contacts with relevant authorities shall be maintained.	A.5.15 Access control	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy on and rules for access control.	The specific requirement for a policy has been removed. There is also an emphasis on physical and logical security controls.		
		A.5.16 Identity management	The full life cycle of identities shall be managed.	While it has links with passwords and access control, requirements are more detailed, especially the full life cycle.		
A.9.2.4 Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	A.5.17 Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel of appropriate handling of authentication information.	The word "secret" has been removed, perhaps widening the application of the clause. Also there is an additional requirement to provide advice. Organisations may be required to have additional training or requirements in staff handbooks. This could also be extended to 3rd parties, clients/ customers or temporary issuing of access.		
		A.5.18 Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organisation's topic specific policy on and rule for access control.	Similar to A.9.3. The emphasis on rights may be significant.		
A.15.1.1 Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets shall be agreed with the suppliers and documented.	A.5.19 Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Some clarification but the difference is not significant.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.15.1.2 Addressing security within supplier agreements	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.	A.5.20 Addressing security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	This does not limit the need for relationships to certain activities but also implies not all suppliers need agreements. In practice the difference is probably minor.		
A.15.1.3 Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	A.5.21 Managing information security in the ICT supply chain	Processes and procedures shall be defined and implemented to manage information security risks associated with ICT products and services supply chain.	Significant rewrite of this clause. In practice the effect may not be significant.		
A.15.2.1 Monitoring and review of supplier services	Organisations shall regularly monitor, review and audit supplier delivery.	A.5.22 Monitoring, review and change management of supplier services	The organisation shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Change management has been added and audit removed.		
A.15.1 Information security in supplier relationship	[Objective] – To maintain an agreed level of information security and service delivery in line with supplier agreements.					
A.15.2 Supplier service delivery management	[Objective] – To maintain an agreed level of information security and service delivery in line with supplier agreements.					
NEW (No equivalent 2013 requirement)		A.5.23 Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organisation's information security requirements.	New requirement. Cloud is a significant new feature since 2013.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.16.1 Management of information security incidents and improvements	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	A.5.24 Information security incident management planning and preparation	The organisation shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management process, roles and responsibilities.	Major re-write including roles and responsibilities but no mention of communicating security events and weaknesses.		
A.16.1.4 Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	A.5.25 Assessment and decisions on information security events	The organisation shall assess information security events and decide if they are to be categorised as information security incidents	Significant rewrite of this clause. In practice the effect may not be significant.		
A.16.1.5 Response to information security incidents	Information security incidents shall be responded to in accordance with documented procedures.	A.5.26 Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	No differences.		
A.16.1.6 Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	A.5.27 Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	The change is essentially from “reducing likelihood or impact” to “strengthen and improve”.		
A.16.1.1 Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.					
A.16.1.3 Reporting information security weaknesses	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.					

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.16.1.7 Collection of evidence	The organisation shall define and apply procedures for the identification, collection, acquisition and preservation of information which can serve as evidence .	A.5.28 Collection of evidence	The organisation shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events .	Fundamentally the same but with a new emphasis on actual evidence.		
A.17.1 Information security continuity	Information security continuity shall be embedded in the organisation's business continuity management systems.	A.5.29 Information security during disruption	The organisation shall plan how to maintain information security at an appropriate level during disruption.	Fundamentally the same requirements.		
A.17.1.1 Planning information security continuity	The organisation shall determine its requirements for information security and continuity of information security management in adverse situations e.g. a crisis or disaster.					
A.17.1.2 Implementing information security continuity	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.					
A.17.1.3 Verify, review and evaluate information security continuity	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.					
NEW (No equivalent 2013 requirement)		A.5.30 ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Emphasis is now on the ICT systems.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.18.1 Compliance with legal and contractual requirements	[Objective] - To avoid breaches of any legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.	A.5.31 Legal, statutory, regulatory and contractual requirements	Legal, statutory and contractual requirements relevant to information security and the organisation's approach to meet these requirements shall be identified, documented and kept up to date.	Fundamentally the same requirements.		
A.18.1.1 Identification of applicable legislation and contractual requirements	All relevant legislative, statutory, regulatory and contractual requirements and the organisation's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organisation.					
A.18.1.2 Intellectual property rights	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.	A.5.32 Intellectual property rights	The organisation shall implement appropriate procedures to protect intellectual property rights.	Fundamentally the same requirements.		
A.18.1.3 Protection of records	Records shall be protected from loss, destruction and falsification, in accordance with legislative, regulatory, contractual, and business requirements.	A.5.33 Protection of records	Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release.	The reference to legislative, regulatory, contractual and business requirements has been removed but "unauthorised access" and "unauthorised release" have been added.		
A.18.1.4 Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation, regulations where applicable.	A.5.34 Privacy and protection of personally identifiable information (PII)	The organisation shall identify and meet requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual	Fundamentally the same requirements.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.18.2.1 Independent review of information security	The organisation's 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.	A.5.35 Independent review of information security	The organisation's approach to managing information security and its implementation including people, process and technologies shall be reviewed independently at planned intervals or when significant changes occur.	Fundamentally the same requirements.		
A.18.2.3 Technical compliance review	Information systems shall be regularly reviewed for compliance with the organisation's information security policies and standards.					
A.12.7.1 Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise the risk of disruptions to business processes.					
A.18.2.2 Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	A.5.36 Compliance with policies, rules and standards for information security	Compliance with the organisation's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	Emphasis is away from managers and processing.		
A.12.1.1 Documented operating procedures	Operating procedures shall be documented, maintained and made available to all users who need them.	A.5.37 Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	The new requirement for information processing facilities does not materially affect the clause.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
6. PEOPLE CONTROLS						
A.7.1.1 Screening	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.	A.6.1 Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organisation and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Addition of “prior to joining the organisation and on an ongoing basis”. Organisations will need to ensure persons are both screened prior to starting on an ongoing basis.		
A.7.1.2 Terms and conditions of employment	The contractual agreements with employees and contractors shall their and the organisation’s responsibility for information security.	A.6.2 Terms and conditions of employment	The employment contractual agreements shall state the personnel and the organisation’s responsibilities for information security.	The requirement is expanded from employees and contractors.		
A.7.2.2 Information security awareness, education and training	All employees of the organisation and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in the organisation’s policies and procedures, as relevant to their job function.	A.6.3 Information security awareness, education and training	Personnel of the organisation and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organisation’s information security policy, topic-specific policies and procedures, as relevant for their job functions.	The persons who might require the awareness, education and training is expanded. This might now include clients, customers, visitors etc.		
A.7.2.3 Disciplinary process	There shall be a formal and communicated disciplinary process to take action against employees who have committed an information security breach .	A.6.4 Disciplinary process	A disciplinary process shall be formalised and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation .	Again this has been expanded to other interested parties. Issues are also expanded from just breaches.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.7.3.1 Termination or change of employment responsibilities	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.	A.6.5 Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties .	Again this has been expanded to include others who may not simply be employees.		
A.13.2.4 Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed and documented.	A.6.6 Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties .	Again the requirement is broadened. Key requirement is that they are <i>signed</i> .		
A.6.2.2 Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites .	A.6.7 Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.	The change from "teleworking" to "remote" is to broaden the range of activities and works covered.		
A.6.2.1 Mobile device policy	A policy and supporting security measures shall be adopted to manage risks introduced by using mobile devices.					
A.16.1.2 Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible .	A.6.8 Information security event reporting	The organisation shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	The emphasis is more on the organisation and less on managers.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
7. PHYSICAL CONTROLS						
A.11.1.1 Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	A.7.1 Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	“Information processing facilities” is replaced by “other associated assets”. This might result in a broadening of requirements or cover cloud, data centre or other facilities.		
A.11.1.6 Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorised persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.					
A.11.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	A.7.2 Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	The emphasis is broadened from simply preventing unauthorised personnel.		
A.11.1 Secure areas	To prevent unauthorised physical access, damage and interference to the organisation’s information and information processing facilities.					
A.11.1.3 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	A.7.3 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	“Applied” is changed to “implemented” but in practice the control is the same.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
NEW (No equivalent 2013 requirement)		A.7.4 Physical security monitoring	Premises shall be continuously monitored for unauthorised physical access.	A new requirement for monitoring and this states “continuously”.		
A.11.1.4 Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	A.7.5 Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Specific emphasis is made on <i>intentional or unintentional threats</i> .		
A.11.1.5 Working in secure areas	Procedures for working in secure areas shall be designed and applied.	A.7.6 Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	The word “applied” is changed to “implemented”.		
A.11.2.9 Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	A.7.7 Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Requirement for a policy has gone and replaced by “rules”.		
A.11.2.8 Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.					
A.11.2.1 Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.	A.7.8 Equipment siting and protection	Equipment shall be sited securely and protected.	The reasons for the siting have been removed to broaden the potential solutions.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.11.2.6 Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organisation's premises.	A.7.9 Security of assets off-premises	Off-site assets shall be protected.	The requirement to take into account different risks has been removed.		
A.8.3.1 Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.	A.7.10 Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organisation's classification scheme and handling requirements.	The emphasis and term has been changed from removable media to all potential storage media.		
A.8.3.3 Physical media in transit	Media containing information shall be protected against unauthorised access, misuse or corruption during transportation.					
A.11.2.2 Supporting utilities	Equipment shall be protected from power failures or other disruptions caused by failures in supporting utilities.	A.7.11 Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Facilities, not just equipment, must be protected.		
A.11.2.3 Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	A.7.12 Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	Broadening of the types of cabling and also requirement to protect from interference.		
A.11.2.4 Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	A.7.13 Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Addition of confidentiality.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.8.3.2 Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	A.7.14 Secure disposal or re-use of equipment	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Reference to verification and also licensed software.		
A.11.2.7 Secure disposal or re-use of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.					
8. TECHNOLOGICAL CONTROLS						
A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	A.8.1 User endpoint devices	Information stored on, processed by or accessible via user endpoint devices shall be protected.	The control is to allow for the variety of equipment used by organisations.		
		A.8.2 Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	Change from controlled to managed.		
A.9.4.1 Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	A.8.3 Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	The emphasis changes to other associated assets and topic-specific policies.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.9.4.5 Access control to program source code	Access to program source code shall be restricted .	A.8.4 Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed .	The control is specific to read and write but broadened to include development tools and software libraries.		
A.9.2.1 User registration and de-registration	A formal user registration and de-registration procedure is implemented to enable assignment of access rights.					
A.9.2.2 User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.					
A.9.2.5 Review of user access rights	Asset owners shall review users' access rights at regular intervals.					
A.9.2.6 Removal or adjustment of access rights	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.					
A.9.3.1 Use of secret authentication information	Users shall be required to follow the organisation's practices in the use of secret authentication information.	A.8.5 Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and topic-specific policy on access control.	The control is broadened to include technologies.		
A.9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by secure log-on procedures.					
A.9.4.3 Password management system	Password management systems shall be interactive and shall ensure quality passwords.					

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.12.1.3 Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	A.8.6 Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Rewritten but fundamentally similar.		
A.12.2.1 Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	A.8.7 Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	Rewritten but fundamentally similar.		
A.12.6.1 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	A.8.8 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organisation's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Rewritten but fundamentally the same.		
NEW (No equivalent 2013 requirement)		A.8.9 Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Configurations need to be recorded and monitored.		
NEW (No equivalent 2013 requirement)		A.8.10 Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Procedures, linked with documentary information, need to cover deletion. This is linked to GDPR and DPA 2018 requirements.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
NEW (No equivalent 2013 requirement)		A.8.11 Data masking	Data masking shall be used in accordance with the organisation's topic-specific policy on access control and other related topic-specific, and business requirements, taking applicable legislation into consideration.	Pseudonymisation and anonymisation requirements, often of PII, and to ensure privacy linked with GDPR and DPA 2018.		
NEW (No equivalent 2013 requirement)		A.8.12 Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	The requirement is supportive of GDPR and DPA 2018 requirements.		
A.12.3.1 Information back-up	Back-up copies of information, software and system images shall be taken and tested regularly in accordance with an agreed back-up policy.	A.8.13 Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Rewritten but basically similar.		
A.17.2.1 Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	A.8.14 Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	No changes except in the title.		
A.17.2 Redundancies	To ensure availability of information processing facilities.					

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.12.4.1 Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	A.8.15 Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	Logs should be analysed rather than simply reviewed.		
A.12.4.2 Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorised access.					
A.12.4.3 Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.					
NEW (No equivalent 2013 requirement)		A.8.16 Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	The additional monitoring requirements are new.		
A.12.4.4 Clock synchronization	The clocks of all relevant information processing systems within an organisation or security domain shall be synchronized to a single reference time source.	A.8.17 Clock synchronization	The clocks of information processing systems used by the organisation shall be synchronised to approved time sources.	Requirement for a single source has been removed.		
A.9.4.4 Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	A.8.18 Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	No change.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.12.5.1 Installation of software on operational systems	Procedures shall be in place to control the installation of software on operational systems.	A.8.19 Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Rewritten but fundamentally similar.		
A.12.6.2 Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.					
A.14.2.4 Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.					
A.13.1.1 Network controls	Networks shall be managed and controlled to protect information in systems and applications.	A.8.20 Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	Rewritten but fundamentally similar.		
A.13.1.2 Security of network services	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.	A.8.21 Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Rewritten but similar requirements.		
A.9.1.2 Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.					

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.13.1.3 Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	A.8.22 Segregation of networks	Groups of information services, users and information systems shall be segregated in the organisation's networks.	Fundamentally similar.		
NEW (No equivalent 2013 requirement)		A.8.23 Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	This is a requirement to prevent access to “unsuitable” sites that might compromise the ISMS.		
A.10.1.1 Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	A.8.24 Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Fundamentally similar.		
A.10.1 Cryptographic Controls	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.					
A.18.1.5 Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation, and regulations.					
A.10.1.2 Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented throughout their whole lifetime.					
A.14.2.1 Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organisation.					
		A.8.25 Secure development life cycle	Rules for the secure development of software and systems shall be established and applied.	The removal of “within the organisation” expands the application to include outsourced development.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.14.1.1 Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems	A.8.26 Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Fundamentally similar.		
A.14.2.3 Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organisational operations or security.					
A.14.2.5 Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	A.8.27 Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information systems development activities.	Fundamentally similar.		
NEW (No equivalent 2013 requirement)		A.8.28 Secure coding	Secure coding principles shall be applied to software development.	While this is similar to existing controls the emphasis is stronger.		
A.14.2.9 System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	A.8.29 Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	While this is similar to existing controls the emphasis is stronger.		
A.14.2.7 Outsourced development	The organisation shall supervise and monitor the activity of out-sourced systems development.	A.8.30 Outsourced development	The organisation shall direct , monitor and review the activities related to outsourced system development.	The requirement for review has been added.		

2013 OBJECTIVE & CONTROL		2022 OBJECTIVE & CONTROL		CHANGES	ACTION REQUIRED	COMPLETED
A.12.1.4 Separation of development, test and operational environments	Development, test and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment .	A.8.31 Separation of development, test and production environments	Development, testing and production environments shall be separated and secured .	The term “secured” has been added.		
A.14.2.6 Secure development environment	Organisations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.					
A.12.1.2 Change management	Changes to the organisation, business processes and information processing facilities and systems shall be controlled .	A.8.32 Change management	Changes to information processing facilities and information systems shall be subject to change management procedures .	Change management procedures are now specifically required, rather than simple control.		
A.14.2.2 System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.					
A.14.3.1 Protection of test data	Test data shall be selected carefully, and protected and controlled .	A.8.33 Test information	Test information shall be appropriately selected, protected and managed .	Rewritten but similar requirements.		
A.14.3 Test data	[Objective] – To ensure the protection of data used for testing.					
A.14.2.8 System security testing	Testing of security functionality shall be carried out during development.	A.8.34 Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Rewritten but similar requirements.		

ALCUMUS

To find out more visit
alcumus.com/isoqar

