PEERS QUALITY ASSURANCE LIMITED
GAP ANALYSIS – ISO/IEC 27001:2013 TO ISO/IEC 27001:2022

PEERS QUALITY ASSURANCE LTD

Clause	Requirement of ISO/IEC 27001:2013	Clause	Requirement of ISO/IEC 27001:2022	Comments
Standard Name	Information technology — Security techniques	Standard Name	Information security, cybersecurity and privacy protection	Name of the Standard has been updated
4.1	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009	4.1	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system. NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.4.1 of ISO 31000:2018	Change to the referenced standard
4.2	The organization shall determine: a) interested parties that are relevant to the information security management system and b) the requirements of these interested parties relevant to information security.	4.2	The organization shall determine: a) interested parties that are relevant to the information security management system b) the relevant requirements of these interested parties c) which of these requirements will be addressed through the information security management system.	Now requires an analysis of which of the interested party requirements must be addressed through the ISMS
4.3	The organization shall determine the boundaries and applicability of the information security management system to establish its scope When determining this scope, the organization shall consider: a) the external and internal issues referred to in 4.1 b) the requirements referred to in 4.2 and c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations. The scope shall be available as documented information	4.3	The organization shall determine the boundaries and applicability of the information security management system to establish its scope When determining this scope, the organization shall consider: a) the external and internal issues referred to in 4.1 b) the requirements referred to in 4.2 c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations. The scope shall be available as documented information	

4.4	The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard	4.4	The organization 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	Now requires planning for processes and their interactions, as part of the ISMS Now refers to the International Standard as a Document
5.1	Top management shall demonstrate leadership and commitment with respect to the information security management system by: a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization b) ensuring the integration of the information security management system requirements into the organization's processes c) ensuring that the resources needed for the information security management system are available d) communicating the importance of effective information security management and of conforming to the information security management system requirements e) ensuring that the information security management system achieves its intended outcome(s) f) directing and supporting persons to contribute to the effectiveness of the information security management system g) promoting continual improvement and h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility	5.1	Top management shall demonstrate leadership and commitment with respect to the information security management system by: a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization b) ensuring the integration of the information security management system requirements into the organization's processes c) ensuring that the resources needed for the information security management system are available d) communicating the importance of effective information security management and of conforming to the information security management system requirements e) ensuring that the information security management system achieves its intended outcome(s) f) directing and supporting persons to contribute to the effectiveness of the information security management system g) promoting continual improvement and h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility. NOTE Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence	
5.2	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives	5.2	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives	

	c) includes a commitment to satisfy applicable requirements related to information security and d) includes a commitment to continual improvement of the information security management system. The information security policy shall: e) be available as documented information f) be communicated within the organization and g) be available to interested parties, as appropriate		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. The information security policy shall: e) be available as documented information f) be communicated within the organization g) be available to interested parties, as appropriate.	
5.3	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. Top management shall assign the responsibility and authority for: a) ensuring that the information security management system conforms to the requirements of this International Standard and b) reporting on the performance of the information security management system to top management. NOTE Top management may also assign responsibilities and authorities for reporting performance of the information security management system within the organization	5.3	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization. Top management shall assign the responsibility and authority for: a) ensuring that the information security management system conforms to the requirements of this document b) reporting on the performance of the information security management system to top management. NOTE Top management can also assign responsibilities and authorities for reporting performance of the information security management system within the organization.	There is an addition to clarify that the communication of roles is done internally within the organization
6.1.1	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s) b) prevent, or reduce, undesired effects and c) achieve continual improvement. The organization shall plan: d) actions to address these risks and opportunities and	6.1.1	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s) b) prevent, or reduce, undesired effects c) achieve continual improvement. The organization shall plan: d) actions to address these risks and opportunities and	

	e) how to 1) integrate and implement the actions into its information security management system processes and 2) evaluate the effectiveness of these actions.		e) how to 1) integrate and implement the actions into its information security management system processes and 2) evaluate the effectiveness of these actions.	
6.1.2	The organization shall define and apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria and 2) criteria for performing information security risk assessments b) ensures that repeated information security risk assessments produce consistent, valid and comparable results c) identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system and 2) identify the risk owners d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1) and 3) determine the levels of risk e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a) and 2) prioritize the analysed risks for risk treatment.	6.1.2	The organization shall define and apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria and 2) criteria for performing information security risk assessments b) ensures that repeated information security risk assessments produce consistent, valid and comparable results c) identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system and 2) identify the risk owners d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1) and 3) determine the levels of risk e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a) and 2) prioritize the analysed risks for risk treatment.	

	The organization shall retain documented information about the information security risk assessment process.		The organization shall retain documented information about the information security risk assessment process.	
6.1.3	The organization shall define and apply an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen NOTE Organizations can design controls as required, or identify them from any source. c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked. NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed. d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A e) formulate an information security risk treatment plan and f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization shall retain documented information about the information security risk treatment process. NOTE The information security risk assessment and treatment process in this International Standard aligns with the principles and generic guidelines provided in ISO 31000.	6.1.3	The organization shall define and apply an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen NOTE 1 Organizations can design controls as required, or identify them from any source. c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted NOTE 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked. NOTE 3 The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed. d) produce a Statement of Applicability that contains: — the necessary controls (see 6.1.3 b) and c)) — justification for their inclusion — whether the necessary controls are implemented or not and — the justification for excluding any of the Annex A controls. e) formulate an information security risk treatment plan and f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization shall retain documented information about the information security risk treatment process.	Now references Annex A as containing "a list of possible information security controls". This is a change from it containing "a comprehensive list of control objectives".

			NOTE 4 The information security risk assessment and treatment process in this document aligns with the principles and generic guidelines provided in ISO 31000.	
6.2	The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: a) be consistent with the information security policy b) be measurable (if practicable) c) take into account applicable information security requirements, and results from risk assessment and risk treatment d) be communicated and e) be updated as appropriate. The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine: f) what will be done g) what resources will be required h) who will be responsible i) when it will be completed and j) how the results will be evaluated.	6.2	The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: a) be consistent with the information security policy b) be measurable (if practicable) c) take into account applicable information security requirements, and results from risk assessment and risk treatment d) be monitored e) be communicated f) be updated as appropriate g) be available as documented information. The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine: h) what will be done i) what resources will be required j) who will be responsible k) when it will be completed and l) how the results will be evaluated.	Refined to require objectives to be monitored
		6.3	Planning of changes When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner	A new addition, requiring that any change in the ISMS needs to be conducted in a planned manner. Considering factors such as: the purpose of the change and the potential consequences, how it may impact the ISMS,

				the availability of resources, and the allocation or reallocation of responsibilities and authorities
7.1	The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	7.1	The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	
7.2	The organization shall: a) determine the necessary competence of person(s) doing work under its control that affects its information security performance b) ensure that these persons are competent on the basis of appropriate education, training, or experience c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken and d) retain appropriate documented information as evidence of competence. NOTE Applicable actions may include, for example: the provision of training to, the mentoring of, or the reassignment of current employees; or the hiring or contracting of competent persons.	7.2	The organization shall: a) determine the necessary competence of person(s) doing work under its control that affects its information security performance b) ensure that these persons are competent on the basis of appropriate education, training, or experience c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken and d) retain appropriate documented information as evidence of competence. NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the re-assignment of current employees; or the hiring or contracting of competent persons.	
7.3	Persons doing work under the organization’s control shall be aware of: a) the information security policy b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance and c) the implications of not conforming with the information security management system requirements.	7.3	Persons doing work under the organization’s control shall be aware of: a) the information security policy b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance and c) the implications of not conforming with the information security management system requirements.	
7.4	The organization shall determine the need for internal and external communications relevant to the information security management system including:	7.4	The organization shall determine the need for internal and external communications relevant to the information security management system including:	The requirement for setting up processes for communication has been removed

	a) on what to communicate b) when to communicate c) with whom to communicate d) who shall communicate and e) the processes by which communication shall be effected.		a) on what to communicate b) when to communicate c) with whom to communicate d) how to communicate.	
7.5.1	The organization's information security management system shall include: a) documented information required by this International Standard and b) documented information determined by the organization as being necessary for the effectiveness of the information security management system. NOTE The extent of documented information for an information security management system can differ from one organization to another due to: 1) the size of organization and its type of activities, processes, products and services 2) the complexity of processes and their interactions and 3) the competence of persons.	7.5.1	The organization's information security management system shall include: a) documented information required by this document and b) documented information determined by the organization as being necessary for the effectiveness of the information security management system. NOTE The extent of documented information for an information security management system can differ from one organization to another due to: 1) the size of organization and its type of activities, processes, products and services 2) the complexity of processes and their interactions and 3) the competence of persons.	
7.5.2	When creating and updating documented information the organization shall ensure appropriate: a) identification and description (e.g. a title, date, author, or reference number) b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic) and c) review and approval for suitability and adequacy.	7.5.2	When creating and updating documented information the organization shall ensure appropriate: a) identification and description (e.g. a title, date, author, or reference number) b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic) and c) review and approval for suitability and adequacy.	

7.5.3	Documented information required by the information security management system and by this International Standard shall be controlled to ensure: a) it is available and suitable for use, where and when it is needed and b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity). For the control of documented information, the organization shall address the following activities, as applicable: c) distribution, access, retrieval and use d) storage and preservation, including the preservation of legibility e) control of changes (e.g. version control) and f) retention and disposition. Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled. NOTE Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.	7.5.3	Documented information required by the information security management system and by this document shall be controlled to ensure: a) it is available and suitable for use, where and when it is needed and b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity). For the control of documented information, the organization shall address the following activities, as applicable: c) distribution, access, retrieval and use d) storage and preservation, including the preservation of legibility e) control of changes (e.g. version control) and f) retention and disposition. Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled. NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.	
8.1	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2. The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.	8.1	The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined 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.	New requirements added for establishing criteria for security processes, and for implementing processes according to those criteria. The requirement to implement plans for achieving objectives has been removed

	The organization shall ensure that outsourced processes are determined and controlled.		The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.	
8.2	The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). The organization shall retain documented information of the results of the information security risk assessments.	8.2	The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). The organization shall retain documented information of the results of the information security risk assessments.	
8.3	The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.	8.3	The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.	
9.1	The organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall determine: a) what needs to be monitored and measured, including information security processes and controls b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results NOTE The methods selected should produce comparable and reproducible results to be considered valid. c) when the monitoring and measuring shall be performed d) who shall monitor and measure e) when the results from monitoring and measurement shall be analysed and evaluated and	9.1	The organization shall determine: a) what needs to be monitored and measured, including information security processes and controls b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid c) when the monitoring and measuring shall be performed d) who shall monitor and measure e) when the results from monitoring and measurement shall be analysed and evaluated f) who shall analyse and evaluate these results. Documented information shall be available as evidence of the results.	Methods of monitoring, measuring, analysing and evaluating the effectiveness of the ISMS now need to be comparable and reproducible

	f) who shall analyse and evaluate these results. The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.		The organization shall evaluate the information	
9.2	The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system: a) conforms to 1) the organization’s own requirements for its information security management system and 2) the requirements of this International Standard b) is effectively implemented and maintained. The organization shall: c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits d) define the audit criteria and scope for each audit e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process f) ensure that the results of the audits are reported to relevant management and g) retain documented information as evidence of the audit programme(s) and the audit results.	9.2.1	The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system: a) conforms to 1) the organization’s own requirements for its information security management system 2) the requirements of this document b) is effectively implemented and maintained.	This has been split into separate parts, for ease of reading
		9.2.2	Internal audit programme The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits. The organization shall: a) define the audit criteria and scope for each audit b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process c) ensure that the results of the audits are reported to relevant management Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.	
9.3	Top management shall review the organization’s information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.	9.3.1	Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.	This has been split into separate parts, for ease of reading

	The management review shall include consideration of: a) the status of actions from previous management reviews b) changes in external and internal issues that are relevant to the information security management system c) feedback on the information security performance, including trends in: 1) nonconformities and corrective actions 2) monitoring and measurement results 3) audit results and 4) fulfilment of information security objectives d) feedback from interested parties e) results of risk assessment and status of risk treatment plan and f) opportunities for continual improvement. The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. The organization shall retain documented information as evidence of the results of management reviews.	9.3.2	Management review inputs The management review shall include consideration of: a) the status of actions from previous management reviews b) changes in external and internal issues that are relevant to the information security management system c) changes in needs and expectations of interested parties that are relevant to the information security management system d) feedback on the information security performance, including trends in: 1) nonconformities and corrective actions 2) monitoring and measurement results 3) audit results 4) fulfilment of information security objectives e) feedback from interested parties f) results of risk assessment and status of risk treatment plan g) opportunities for continual improvement.	It now clarifies that inputs from interested parties need to be about their needs and expectations, and relevant to the ISMS
		9.3.3	Management review results The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. Documented information shall be available as evidence of the results of management reviews.	
10.1	When a nonconformity occurs, the organization shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it and 2) deal with the consequences	10.2	When a nonconformity occurs, the organization shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it 2) deal with the consequences	Clauses 10.1 and 10.2 have switched places

	b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity 2) determining the causes of the nonconformity and 3) determining if similar nonconformities exist, or could potentially occur c) implement any action needed d) review the effectiveness of any corrective action taken and e) make changes to the information security management system, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of: f) the nature of the nonconformities and any subsequent actions taken, and g) the results of any corrective action		b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity 2) determining the causes of the nonconformity and 3) determining if similar nonconformities exist, or could potentially occur c) implement any action needed d) review the effectiveness of any corrective action taken and e) make changes to the information security management system, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. Documented information shall be available as evidence of: f) the nature of the nonconformities and any subsequent actions taken g) the results of any corrective action.	
10.2	The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system	10.1	The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.	Clauses 10.1 and 10.2 have switched places

2013 ANNEX A CONTROLS VERSES 2022 ANNEX A CONTROLS

Control Group in 2013	Annex A Clause 2013	2013 Control	Annex A Clause 2022	2022 Control	Difference
Information security policies	A 5.1.1	Policies for information security	A 5.1	Policies for information security	Merged Control
Information security policies	A 5.1.2	Review of the policies for information security	A 5.1	Policies for information security	Merged Control
Organization of information security	A 6.1.1	Information security roles and responsibilities	A 5.2	Information security roles and responsibilities	Re-Numbered Control
Organization of information security	A 6.1.2	Segregation of duties	A 5.3	Segregation of duties	Re-Numbered Control
Organization of information security	A 6.1.3	Contact with authorities	A 5.5	Contact with authorities	Re-Numbered Control
Organization of information security	A 6.1.4	Contact with special interest groups	A 5.6	Contact with special interest groups	Re-Numbered Control
Organization of information security	A 6.1.5	Information security in project management	A 5.8	Information security in project management	Merged Control
Organization of information security	A 6.2.1	Mobile device policy	A 8.1	User end point devices	Merged Control
Organization of information security	A 6.2.2	Teleworking	A 6.7	Remote working	Renamed Control
Human resource security	A 7.1.1	Screening	A 6.1	Screening	Re-Numbered Control
Human resource security	A 7.1.2	Terms and conditions of employment	A 6.2	Terms and conditions of employment	Re-Numbered Control
Human resource security	A 7.2.1	Management responsibilities	A 5.4	Management responsibilities	Re-Numbered Control
Human resource security	A 7.2.2	Information security awareness, education and training	A 6.3	Information security awareness, education and training	Re-Numbered Control
Human resource security	A 7.2.3	Disciplinary process	A 6.4	Disciplinary process	Re-Numbered Control

2013 ANNEX A CONTROLS VERSES 2022 ANNEX A CONTROLS

Control Group in 2013	Annex A Clause 2013	2013 Control	Annex A Clause 2022	2022 Control	Difference
Human resource security	A 7.3.1	Termination or change of employment responsibilities	A 6.5	Responsibilities after termination or change of employment	Renamed Control
Asset management	A 8.1.1	Inventory of assets	A 5.9	Inventory of information and other associated assets	Merged Control
Asset management	A 8.1.2	Ownership of assets	A 5.9	Inventory of information and other associated assets	Merged Control
Asset management	A 8.1.3	Acceptable use of assets	A 5.10	Acceptable use of information and other associated assets	Merged Control
Asset management	A 8.1.4	Return of assets	A 5.11	Return of assets	Re-Numbered Control
Asset management	A 8.2.1	Classification of information	A 5.12	Classification of information	Re-Numbered Control
Asset management	A 8.2.2	Labelling of information	A 5.13	Labelling of information	Re-Numbered Control
Asset management	A 8.2.3	Handling of assets	A 5.10	Acceptable use of information and other associated assets	Merged Control
Asset management	A 8.3.1	Management of removable media	A 7.10	Storage media	Merged Control
Asset management	A 8.3.2	Disposal of media	A 7.10	Storage media	Merged Control
Asset management	A 8.3.3	Physical media transfer	A 7.10	Storage media	Merged Control
Access control	A 9.1.1	Access control policy	A 5.15	Access control	Merged Control
Access control	A 9.1.2	Access to networks and network services	A 5.15	Access control	Merged Control
Access control	A 9.2.1	User registration and de-registration	A 5.16	Identity management	Renamed Control
Access control	A 9.2.2	User access provisioning	A 5.18	Access rights	Merged Control

2013 ANNEX A CONTROLS VERSES 2022 ANNEX A CONTROLS

Control Group in 2013	Annex A Clause 2013	2013 Control	Annex A Clause 2022	2022 Control	Difference
Access control	A 9.2.3	Management of privileged access rights	A 8.2	Privileged access rights	Renamed Control
Access control	A 9.2.4	Management of secret authentication information of users	A 5.17	Authentication information	Merged Control
Access control	A 9.2.5	Review of user access rights	A 5.18	Access rights	Merged Control
Access control	A 9.2.6	Removal or adjustment of access rights	A 5.18	Access rights	Merged Control
Access control	A 9.3.1	Use of secret authentication information	A 5.17	Authentication information	Merged Control
Access control	A 9.4.1	Information access restriction	A 8.3	Information access restriction	Re-Numbered Control
Access control	A 9.4.2	Secure log-on procedures	A 8.5	Secure authentication	Renamed Control
Access control	A 9.4.3	Password management system	A 5.17	Authentication information	Merged Control
Access control	A 9.4.4	Use of privileged utility programs	A 8.18	Use of privileged utility programs	Re-Numbered Control
Access control	A 9.4.5	Access control to program source code	A 8.4	Access to source code	Renamed Control
Cryptography	A 10.1.1	Policy on the use of cryptographic controls	A 8.24	Use of cryptography	Merged Control
Cryptography	A 10.1.2	Key management	A 8.24	Use of cryptography	Merged Control
Physical and environmental security	A 11.1.1	Physical security perimeter	A 7.1	Physical security perimeters	Renamed Control
Physical and environmental security	A 11.1.2	Physical entry controls	A 7.2	Physical entry	Merged Control
Physical and environmental security	A 11.1.3	Securing offices, rooms and facilities	A 7.3	Securing offices, rooms and facilities	Re-Numbered Control

2013 ANNEX A CONTROLS VERSES 2022 ANNEX A CONTROLS

Control Group in 2013	Annex A Clause 2013	2013 Control	Annex A Clause 2022	2022 Control	Difference
Physical and environmental security	A 11.1.4	Protecting against external and environmental threats	A 7.5	Protecting against external and environmental threats	Re-Numbered Control
Physical and environmental security	A 11.1.5	Working in secure areas	A 7.6	Working in secure areas	Re-Numbered Control
Physical and environmental security	A 11.1.6	Delivery and loading areas	A 7.2	Physical entry	Merged Control
Physical and environmental security	A 11.2.1	Equipment siting and protection	A 7.8	Equipment siting and protection	Re-Numbered Control
Physical and environmental security	A 11.2.2	Supporting utilities	A 7.11	Supporting utilities	Re-Numbered Control
Physical and environmental security	A 11.2.3	Cabling security	A 7.12	Cabling security	Re-Numbered Control
Physical and environmental security	A 11.2.4	Equipment maintenance	A 7.13	Equipment maintenance	Re-Numbered Control
Physical and environmental security	A 11.2.5	Removal of assets	A 7.10	Storage media	Merged Control
Physical and environmental security	A 11.2.6	Security of equipment and assets off-premises	A 7.9	Security of assets off-premises	Renamed Control
Physical and environmental security	A 11.2.7	Secure disposal or re-use of equipment	A 7.14	Secure disposal or re-use of equipment	Re-Numbered Control
Physical and environmental security	A 11.2.8	Unattended user equipment	A 8.1	User end point devices	Merged Control
Physical and environmental security	A 11.2.9	Clear desk and clear screen policy	A 7.7	Clear desk and clear screen	Renamed Control
Operations security	A 12.1.1	Documented operating procedures	A 5.37	Documented operating procedures	Re-Numbered Control
Operations security	A 12.1.2	Change management	A 8.32	Change management	Merged Control
Operations security	A 12.1.3	Capacity management	A 8.6	Capacity management	Re-Numbered Control

2013 ANNEX A CONTROLS VERSES 2022 ANNEX A CONTROLS

Control Group in 2013	Annex A Clause 2013	2013 Control	Annex A Clause 2022	2022 Control	Difference
Operations security	A 12.1.4	Separation of development, testing and operational environments	A 8.31	Separation of development, test and production environments	Merged Control
Operations security	A 12.2.1	Controls against malware	A 8.7	Protection against malware	Renamed Control
Operations security	A 12.3.1	Information backup	A 8.13	Information backup	Re-Numbered Control
Operations security	A 12.4.1	Event logging	A 8.15	Logging	Merged Control
Operations security	A 12.4.2	Protection of log information	A 8.15	Logging	Merged Control
Operations security	A 12.4.3	Administrator and operator logs	A 8.15	Logging	Merged Control
Operations security	A 12.4.4	Clock synchronization	A 8.17	Clock synchronization	Re-Numbered Control
Operations security	A 12.5.1	Installation of software on operational systems	A 8.19	Installation of software on operational systems	Merged Control
Operations security	A 12.6.1	Management of technical vulnerabilities	A 8.8	Management of technical vulnerabilities	Merged Control
Operations security	A 12.6.2	Restrictions on software installation	A 8.19	Installation of software on operational systems	Merged Control
Operations security	A 12.7.1	Information systems audit controls	A 8.34	Protection of information systems during audit testing	Renamed Control
Communications security	A 13.1.1	Network controls	A 8.20	Networks security	Renamed Control
Communications security	A 13.1.2	Security of network services	A 8.21	Security of network services	Re-Numbered Control
Communications security	A 13.1.3	Segregation in networks	A 8.22	Segregation of networks	Renamed Control
Communications security	A 13.2.1	Information transfer policies and procedures	A 5.14	Information transfer	Merged Control

2013 ANNEX A CONTROLS VERSES 2022 ANNEX A CONTROLS

Control Group in 2013	Annex A Clause 2013	2013 Control	Annex A Clause 2022	2022 Control	Difference
Communications security	A 13.2.2	Agreements on information transfer	A 5.14	Information transfer	Merged Control
Communications security	A 13.2.3	Electronic messaging	A 5.14	Information transfer	Merged Control
Communications security	A 13.2.4	Confidentiality or non-disclosure agreements	A 6.6	Confidentiality or non-disclosure agreements	Re-Numbered Control
System acquisition, devt & maintenance	A 14.1.1	Information security requirements analysis and specification	A 5.8	Information security in project management	Merged Control
System acquisition, devt & maintenance	A 14.1.2	Securing application services on public networks	A 8.26	Application security requirements	Merged Control
System acquisition, devt & maintenance	A 14.1.3	Protecting application services transactions	A 8.26	Application security requirements	Merged Control
System acquisition, devt & maintenance	A 14.2.1	Secure development policy	A 8.25	Secure development life cycle	Renamed Control
System acquisition, devt & maintenance	A 14.2.2	System change control procedures	A 8.32	Change management	Merged Control
System acquisition, devt & maintenance	A 14.2.3	Technical review of applications after operating platform changes	A 8.32	Change management	Merged Control
System acquisition, devt & maintenance	A 14.2.4	Restrictions on changes to software packages	A 8.32	Change management	Merged Control
System acquisition, devt & maintenance	A 14.2.5	Secure system engineering principles	A 8.27	Secure system architecture and engineering principles	Renamed Control
System acquisition, devt & maintenance	A 14.2.6	Secure development environment	A 8.31	Separation of development, test and production environments	Merged Control
System acquisition, devt & maintenance	A 14.2.7	Outsourced development	A 8.30	Outsourced development	Re-Numbered Control
System acquisition, devt & maintenance	A 14.2.8	System security testing	A 8.29	Security testing in development and acceptance	Merged Control
System acquisition, devt & maintenance	A 14.2.9	System acceptance testing	A 8.29	Security testing in development and acceptance	Merged Control

2013 ANNEX A CONTROLS VERSES 2022 ANNEX A CONTROLS

Control Group in 2013	Annex A Clause 2013	2013 Control	Annex A Clause 2022	2022 Control	Difference
System acquisition, devt & maintenance	A 14.3.1	Protection of test data	A 8.33	Test information	Renamed Control
Supplier relationships	A 15.1.1	Information security policy for supplier relationships	A 5.19	Information security in supplier relationships	Renamed Control
Supplier relationships	A 15.1.2	Addressing security within supplier agreements	A 5.20	Addressing information security within supplier agreements	Renamed Control
Supplier relationships	A 15.1.3	Information and communication technology supply chain	A 5.21	Managing information security in the ICT supply chain	Renamed Control
Supplier relationships	A 15.2.1	Monitoring and review of supplier services	A 5.22	Monitoring, review and change management of supplier services	Merged Control
Supplier relationships	A 15.2.2	Managing changes to supplier services	A 5.22	Monitoring, review and change management of supplier services	Merged Control
Inf Sec incident management	A 16.1.1	Responsibilities and procedures	A 5.24	Information security incident management planning and preparation	Renamed Control
Inf Sec incident management	A 16.1.2	Reporting information security events	A 6.8	Information security event reporting	Merged Control
Inf Sec incident management	A 16.1.3	Reporting information security weaknesses	A 6.8	Information security event reporting	Merged Control
Inf Sec incident management	A 16.1.4	Assessment of and decision on information security events	A 5.25	Assessment and decision on information security events	Renamed Control
Inf Sec incident management	A 16.1.5	Response to information security incidents	A 5.26	Response to information security incidents	Re-Numbered Control
Inf Sec incident management	A 16.1.6	Learning from information security incidents	A 5.27	Learning from information security incidents	Re-Numbered Control
Inf Sec incident management	A 16.1.7	Collection of evidence	A 5.28	Collection of evidence	Re-Numbered Control
Inf Sec aspects of business continuity management	A 17.1.1	Planning information security continuity	A 5.29	Information security during disruption	Merged Control
Inf Sec aspects of business continuity management	A 17.1.2	Implementing information security continuity	A 5.29	Information security during disruption	Merged Control

2013 ANNEX A CONTROLS VERSES 2022 ANNEX A CONTROLS

Control Group in 2013	Annex A Clause 2013	2013 Control	Annex A Clause 2022	2022 Control	Difference
Inf Sec aspects of business continuity management	A 17.1.3	Verify, review and evaluate information security continuity	A 5.29	Information security during disruption	Merged Control
Inf Sec aspects of business continuity management	A 17.2.1	Availability of information processing facilities	A 8.14	Redundancy of information processing facilities	Renamed Control
Compliance	A 18.1.1	Identification of applicable legislation and contractual requirements	A 5.31	Legal, statutory, regulatory and contractual requirements	Merged Control
Compliance	A 18.1.2	Intellectual property rights	A 5.32	Intellectual property rights	Re-Numbered Control
Compliance	A 18.1.3	Protection of records	A 5.33	Protection of records	Re-Numbered Control
Compliance	A 18.1.4	Privacy and protection of personally identifiable information	A 5.34	Privacy and protection of PII	Renamed Control
Compliance	A 18.1.5	Regulation of cryptographic controls	A 5.31	Legal, statutory, regulatory and contractual requirements	Merged Control
Compliance	A 18.2.1	Independent review of information security	A 5.35	Independent review of information security	Re-Numbered Control
Compliance	A 18.2.2	Compliance with security policies and standards	A 5.36	Conformance with policies, rules and standards for information security	Merged Control
Compliance	A 18.2.3	Technical compliance review	A 5.36	Conformance with policies, rules and standards for information security	Merged Control
			A 8.8	Management of technical vulnerabilities	Merged Control
Not in 2013 Version	N/A	N/A	A 5.7	Threat intelligence	New Control
Not in 2013 Version	N/A	N/A	A 5.23	Information security for use of cloud services	New Control
Not in 2013 Version	N/A	N/A	A 5.30	ICT readiness for business continuity	New Control
Not in 2013 Version	N/A	N/A	A 7.4	Physical security monitoring	New Control

2013 ANNEX A CONTROLS VERSES 2022 ANNEX A CONTROLS

Control Group in 2013	Annex A Clause 2013	2013 Control	Annex A Clause 2022	2022 Control	Difference
Not in 2013 Version	N/A	N/A	A 8.9	Configuration management	New Control
Not in 2013 Version	N/A	N/A	A 8.10	Information deletion	New Control
Not in 2013 Version	N/A	N/A	A 8.11	Data masking	New Control
Not in 2013 Version	N/A	N/A	A 8.12	Data leakage prevention	New Control
Not in 2013 Version	N/A	N/A	A 8.16	Monitoring activities	New Control
Not in 2013 Version	N/A	N/A	A 8.23	Web filtering	New Control
Not in 2013 Version	N/A	N/A	A 8.28	Secure coding	New Control

2022 ANNEX A CONTROLS VERSES 2013 ANNEX A CONTROLS

Theme Clauses in 2022	Annex A Clause 2022	2022 Control	Difference	Annex A Clause 2013	2013 Control
Organizational control	A 5.1	Policies for information security	Merged Control	A 5.1.1 A 5.1.2	Policies for information security Review of the policies for information security
Organizational control	A 5.2	Information security roles and responsibilities	Re-Numbered Control	A 6.1.1	Information security roles and responsibilities
Organizational control	A 5.3	Segregation of duties	Re-Numbered Control	A 6.1.2	Segregation of duties
Organizational control	A 5.4	Management responsibilities	Re-Numbered Control	A 7.2.1	Management responsibilities
Organizational control	A 5.5	Contact with authorities	Re-Numbered Control	A 6.1.3	Contact with authorities
Organizational control	A 5.6	Contact with special interest groups	Re-Numbered Control	A 6.1.4	Contact with special interest groups
Organizational control	A 5.7	Threat intelligence	New Control	N/A	N/A
Organizational control	A 5.8	Information security in project management	Merged Control	A 6.1.5 A 14.1.1	Information security in project management Information security requirements analysis and specification
Organizational control	A 5.9	Inventory of information and other associated assets	Merged Control	A 8.1.1 A 8.1.2	Inventory of assets Ownership of assets
Organizational control	A 5.10	Acceptable use of information and other associated assets	Merged Control	A 8.1.3 A 8.2.3	Acceptable use of assets Handling of assets
Organizational control	A 5.11	Return of assets	Re-Numbered Control	A 8.1.4	Return of assets
Organizational control	A 5.12	Classification of information	Re-Numbered Control	A 8.2.1	Classification of information
Organizational control	A 5.13	Labelling of information	Re-Numbered Control	A 8.2.2	Labelling of information
Organizational control	A 5.14	Information transfer	Merged Control	A 13.2.1 A 13.2.2 A 13.2.3	Information transfer policies and procedures Agreements on information transfer Electronic messaging

2022 ANNEX A CONTROLS VERSES 2013 ANNEX A CONTROLS

Theme Clauses in 2022	Annex A Clause 2022	2022 Control	Difference	Annex A Clause 2013	2013 Control
Organizational control	A 5.15	Access control	Merged Control	A 9.1.1 A 9.1.2	Access control policy Access to networks and network services
Organizational control	A 5.16	Identity management	Renamed Control	A 9.2.1	User registration and de-registration
Organizational control	A 5.17	Authentication information	Merged Control	A 9.2.4 A 9.3.1 A 9.4.3	Management of secret authentication information of users Use of secret authentication information Password management system
Organizational control	A 5.18	Access rights	Merged Control	A 9.2.2 A 9.2.5 A 9.2.6	User access provisioning Review of user access rights Removal or adjustment of access rights
Organizational control	A 5.19	Information security in supplier relationships	Renamed Control	A 15.1.1	Information security policy for supplier relationships
Organizational control	A 5.20	Addressing information security within supplier agreements	Renamed Control	A 15.1.2	Addressing security within supplier agreements
Organizational control	A 5.21	Managing information security in the ICT supply chain	Renamed Control	A 15.1.3	Information and communication technology supply chain
Organizational control	A 5.22	Monitoring, review and change management of supplier services	Merged Control	A 15.2.1 A 15.2.2	Monitoring and review of supplier services Managing changes to supplier services
Organizational control	A 5.23	Information security for use of cloud services	New Control	N/A	N/A
Organizational control	A 5.24	Information security incident management planning and preparation	Renamed Control	A 16.1.1	Responsibilities and procedures
Organizational control	A 5.25	Assessment and decision on information security events	Renamed Control	A 16.1.4	Assessment of and decision on information security events
Organizational control	A 5.26	Response to information security incidents	Re-Numbered Control	A 16.1.5	Response to information security incidents
Organizational control	A 5.27	Learning from information security incidents	Re-Numbered Control	A 16.1.6	Learning from information security incidents
Organizational control	A 5.28	Collection of evidence	Re-Numbered Control	A 16.1.7	Collection of evidence

2022 ANNEX A CONTROLS VERSES 2013 ANNEX A CONTROLS

Theme Clauses in 2022	Annex A Clause 2022	2022 Control	Difference	Annex A Clause 2013	2013 Control
Organizational control	A 5.29	Information security during disruption	Merged Control	A 17.1.1 A 17.1.2 A 17.1.3	Planning information security continuity Implementing information security continuity Verify, review and evaluate information security continuity
Organizational control	A 5.30	ICT readiness for business continuity	New Control	N/A	N/A
Organizational control	A 5.31	Legal, statutory, regulatory and contractual requirements	Merged Control	A 18.1.1 A 18.1.5	Identification of applicable legislation and contractual requirements Regulation of cryptographic controls
Organizational control	A 5.32	Intellectual property rights	Re-Numbered Control	A 18.1.2	Intellectual property rights
Organizational control	A 5.33	Protection of records	Re-Numbered Control	A 18.1.3	Protection of records
Organizational control	A 5.34	Privacy and protection of PII	Renamed Control	A 18.1.4	Privacy and protection of personally identifiable information
Organizational control	A 5.35	Independent review of information security	Re-Numbered Control	A 18.2.1	Independent review of information security
Organizational control	A 5.36	Conformance with policies, rules and standards for information security	Merged Control	A 18.2.2 A 18.2.3	Compliance with security policies and standards Technical compliance review
Organizational control	A 5.37	Documented operating procedures	Re-Numbered Control	A 12.1.1	Documented operating procedures
People control	A 6.1	Screening	Re-Numbered Control	A 7.1.1	Screening
People control	A 6.2	Terms and conditions of employment	Re-Numbered Control	A 7.1.2	Terms and conditions of employment
People control	A 6.3	Information security awareness, education and training	Re-Numbered Control	A 7.2.2	Information security awareness, education and training
People control	A 6.4	Disciplinary process	Re-Numbered Control	A 7.2.3	Disciplinary process
People control	A 6.5	Responsibilities after termination or change of employment	Renamed Control	A 7.3.1	Termination or change of employment responsibilities

2022 ANNEX A CONTROLS VERSES 2013 ANNEX A CONTROLS

Theme Clauses in 2022	Annex A Clause 2022	2022 Control	Difference	Annex A Clause 2013	2013 Control
People control	A 6.6	Confidentiality or non-disclosure agreements	Re-Numbered Control	A 13.2.4	Confidentiality or non-disclosure agreements
People control	A 6.7	Remote working	Renamed Control	A 6.2.2	Teleworking
People control	A 6.8	Information security event reporting	Merged Control	A 16.1.2 A 16.1.3	Reporting information security events Reporting information security weaknesses
Physical control	A 7.1	Physical security perimeters	Renamed Control	A 11.1.1	Physical security perimeter
Physical control	A 7.2	Physical entry	Merged Control	A 11.1.2 A 11.1.6	Physical entry controls Delivery and loading areas
Physical control	A 7.3	Securing offices, rooms and facilities	Re-Numbered Control	A 11.1.3	Securing offices, rooms and facilities
Physical control	A 7.4	Physical security monitoring	New Control	N/A	N/A
Physical control	A 7.5	Protecting against external and environmental threats	Re-Numbered Control	A 11.1.4	Protecting against external and environmental threats
Physical control	A 7.6	Working in secure areas	Re-Numbered Control	A 11.1.5	Working in secure areas
Physical control	A 7.7	Clear desk and clear screen	Renamed Control	A 11.2.9	Clear desk and clear screen policy
Physical control	A 7.8	Equipment siting and protection	Re-Numbered Control	A 11.2.1	Equipment siting and protection
Physical control	A 7.9	Security of assets off-premises	Renamed Control	A 11.2.6	Security of equipment and assets off-premises
Physical control	A 7.10	Storage media	Merged Control	A 8.3.1 A 8.3.2 A 8.3.3 A 11.2.5	Management of removable media Disposal of media Physical media transfer Removal of assets
Physical control	A 7.11	Supporting utilities	Re-Numbered Control	A 11.2.2	Supporting utilities

2022 ANNEX A CONTROLS VERSES 2013 ANNEX A CONTROLS

Theme Clauses in 2022	Annex A Clause 2022	2022 Control	Difference	Annex A Clause 2013	2013 Control
Physical control	A 7.12	Cabling security	Re-Numbered Control	A 11.2.3	Cabling security
Physical control	A 7.13	Equipment maintenance	Re-Numbered Control	A 11.2.4	Equipment maintenance
Physical control	A 7.14	Secure disposal or re-use of equipment	Re-Numbered Control	A 11.2.7	Secure disposal or re-use of equipment
Technological control	A 8.1	User end point devices	Merged Control	A 6.2.1 A 11.2.8	Mobile device policyUnattended user equipment
Technological control	A 8.2	Privileged access rights	Renamed Control	A 9.2.3	Management of privileged access rights
Technological control	A 8.3	Information access restriction	Re-Numbered Control	A 9.4.1	Information access restriction
Technological control	A 8.4	Access to source code	Renamed Control	A 9.4.5	Access control to program source code
Technological control	A 8.5	Secure authentication	Renamed Control	A 9.4.2	Secure log-on procedures
Technological control	A 8.6	Capacity management	Re-Numbered Control	A 12.1.3	Capacity management
Technological control	A 8.7	Protection against malware	Renamed Control	A 12.2.1	Controls against malware
Technological control	A 8.8	Management of technical vulnerabilities	Merged Control	A 12.6.1 A 18.2.3	Management of technical vulnerabilities Technical compliance review
Technological control	A 8.9	Configuration management	New Control	N/A	N/A
Technological control	A 8.10	Information deletion	New Control	N/A	N/A
Technological control	A 8.11	Data masking	New Control	N/A	N/A
Technological control	A 8.12	Data leakage prevention	New Control	N/A	N/A

2022 ANNEX A CONTROLS VERSES 2013 ANNEX A CONTROLS

Theme Clauses in 2022	Annex A Clause 2022	2022 Control	Difference	Annex A Clause 2013	2013 Control
Technological control	A 8.13	Information backup	Re-Numbered Control	A 12.3.1	Information backup
Technological control	A 8.14	Redundancy of information processing facilities	Renamed Control	A 17.2.1	Availability of information processing facilities
Technological control	A 8.15	Logging	Merged Control	A 12.4.1 A 12.4.2 A 12.4.3	Event logging Protection of log information Administrator and operator logs
Technological control	A 8.16	Monitoring activities	New Control	N/A	N/A
Technological control	A 8.17	Clock synchronization	Re-Numbered Control	A 12.4.4	Clock synchronization
Technological control	A 8.18	Use of privileged utility programs	Re-Numbered Control	A 9.4.4	Use of privileged utility programs
Technological control	A 8.19	Installation of software on operational systems	Merged Control	A 12.5.1 A 12.6.2	Installation of software on operational systems Restrictions on software installation
Technological control	A 8.20	Networks security	Renamed Control	A 13.1.1	Network controls
Technological control	A 8.21	Security of network services	Re-Numbered Control	A 13.1.2	Security of network services
Technological control	A 8.22	Segregation of networks	Renamed Control	A 13.1.3	Segregation in networks
Technological control	A 8.23	Web filtering	New Control	N/A	N/A
Technological control	A 8.24	Use of cryptography	Merged Control	A 10.1.1 A 10.1.2	Policy on the use of cryptographic controls Key management
Technological control	A 8.25	Secure development life cycle	Renamed Control	A 14.2.1	Secure development policy
Technological control	A 8.26	Application security requirements	Merged Control	A 14.1.2 A 14.1.3	Securing application services on public networks Protecting application services transactions

2022 ANNEX A CONTROLS VERSES 2013 ANNEX A CONTROLS

Theme Clauses in 2022	Annex A Clause 2022	2022 Control	Difference	Annex A Clause 2013	2013 Control
Technological control	A 8.27	Secure system architecture and engineering principles	Renamed Control	A 14.2.5	Secure system engineering principles
Technological control	A 8.28	Secure coding	New Control	N/A	N/A
Technological control	A 8.29	Security testing in development and acceptance	Merged Control	A 14.2.8 A 14.2.9	System security testing System acceptance testing
Technological control	A 8.30	Outsourced development	Re-Numbered Control	A 14.2.7	Outsourced development
Technological control	A 8.31	Separation of development, test and production environments	Merged Control	A 12.1.4 A 14.2.6	Separation of development, testing and operational environments Secure development environment
Technological control	A 8.32	Change management	Merged Control	A 12.1.2 A 14.2.2 A 14.2.3 A 14.2.4	Change management System change control procedures Technical review of applications after operating platform changes Restrictions on changes to software packages
Technological control	A 8.33	Test information	Renamed Control	A 14.3.1	Protection of test data
Technological control	A 8.34	Protection of information systems during audit testing	Renamed Control	A 12.7.1	Information systems audit controls