PEERS QUALITY ASSURANCE LIMITED
ISO/IEC 27001:2022 UPDATE

PEERS QUALITY ASSURANCE LTD

A NEW VERSION OF ISO/IEC 27001 HAS BEEN RELEASED

As you may already be aware, the new ISO/IEC 27001:2022 version was released on 25th October 2022, replacing the 2013/2017 version.

Certified Companies will have until 31st October 2025 (36 months) to update their ISMS and transition their Certification to ISO/IEC 27001:2022.

All ISO/IEC 27001:2013 certificates will cease to be valid after 31st October 2025

A Certification Body (such as PQAL) will need to conduct a transition assessment within this time period and issue an updated Certificate.

The transition assessment will determine whether a company has updated their ISMS to the new requirements of ISO/IEC 27001:2022, including the changes to Annex A controls.

Transitions can take place at the time of a Surveillance Audit, a Recertification Audit, or even as a stand-alone Audit. Typically, a transition will require additional Audit Time.

It is anticipated that most Certified Companies will choose to conduct their implementation of the new requirements prior to their next audit, to be in line with stakeholder expectations

THE CHANGES WITHIN CLAUSES 4 TO 10 OF ISO/IEC 27001:2022

The Management System part of ISO/IEC 27001:2022 (Clauses 4 to 10) contains only minor refinements, additions, and rewrites to align it with Annex SL.

The changes in the Management System part of the standard are only small and will require only slight changes in the documentation and processes.

CLAUSE	TITLE	CHANGES
4.2	Understanding the Needs and Expectations of Interested Parties	Now requires an analysis of which of the interested party requirements must be addressed through the ISMS
4.4	Information Security Management System	Now requires planning for processes and their interactions, as part of the ISMS
5.3	Organizational Roles, Responsibilities and Authorities	There is an addition to clarify that the communication of roles is done internally within the organization
6.1.3	Risk Treatment	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*".
6.2	Information Security Objectives and Planning to Achieve Them	Refined to require objectives to be monitored

6.3	Change Management	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
7.4	Communication	The requirement for setting up processes for communication has been removed
8.1	Operational Planning and Control	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
9.1	Monitoring, Measurement, Analysis and Evaluation	Methods of monitoring, measuring, analysing and evaluating the effectiveness of the ISMS now need to be comparable and reproducible
9.2	Internal Audit	This has been split into separate parts, for ease of reading
9.3	Management Review	This has been split into separate parts, for ease of reading It now clarifies that inputs from interested parties need to be about their needs and expectations, and relevant to the ISMS
10.1	Continual Improvement	These two clauses have switched places
10.2	Nonconformity and Corrective Action	

THE CHANGES WITHIN THE ANNEX A CONTROLS OF ISO/IEC 27001:2022

Changes within the Annex A controls are moderate and can be mostly dealt with by adding the new controls to the existing documentation

The Annex A controls of ISO/IEC 27001:2013 contained 114 controls, divided over 14 **Control Groups**.

This has now been restructured in ISO/IEC 27001:2022 to contain 93 controls, divided over 4 **Theme Clauses**, to align it with ISO/IEC 27002

THEME CLAUSES		DESCRIPTION
5	**Organizational Controls**	Contains 37 controls related to various organizational issues
6	**People Controls**	Contains 8 controls related to human resources security
7	**Physical Controls**	Contains 14 controls related to the physical environment
8	**Technological Controls**	Contains 34 controls related to technological solutions

PEERS QUALITY ASSURANCE LIMITED
ISO/IEC 27001:2022 UPDATE

Within the Annex A controls there are 11 new controls and no deletions.

Many of the existing controls have now been renamed, re-numbered, merged together or split, so they might require some tweaking of your existing implementation – if you wish to include them in your Statement of Applicability, of course

- 35 of the controls have stayed the same and been re-numbered
- 23 of the controls have only been renamed
- 57 of the controls have been merged (this has reduced the overall number of controls, but the requirements within those controls have remained almost the same)
- 1 of the controls has been split into 2 separate controls (while the requirements have stayed the same).
- 11 of the controls are new, these were needed because of the trends in IT and security

A full list and a comparison of the control changes appears at the end of this document as:

- **2022 Annex A Controls Verses 2013 Annex A Controls**
- **2013 Annex A Controls Verses 2022 Annex A Controls**

THE SIMPLIFIED PATH TO TRANSITION OF YOUR CERTIFICATION TO ISO/IEC 27001:2022		
1	Understand the changes to ISO/IEC 27001:2022	You will need to obtain a copy of the revised Standard and review this
2	Check the impact on your organization	You will need to perform a gap analysis against the changes identified in the new version of ISO/IEC 27001 to see how these will affect your Management System and Controls
3	Implement the changes	You will need to justify the inclusion or exclusion of the necessary controls of ISO/IEC 27001:2022, and then update your Statement of Applicability to reflect this. Look through your Risk Treatment Plan. Implement the applicable changes and new controls, and be sure to make sure that these have been effectively implemented
4	Transition your certificate	Let your Certification Body (PQAL) and Auditor know that you have updated your management system and that you believe that you are ready to be transitioned to ISO/IEC 27001:2011 during your next Audit

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

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 7.11	Supporting utilities	Re-Numbered Control	A 11.2.2	Supporting utilities
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

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 8.11	Data masking	New Control	N/A	N/A
Technological control	A 8.12	Data leakage prevention	New Control	N/A	N/A
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

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 8.25	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
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

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

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 9.2.2	User access provisioning	A 5.18	Access rights	Merged Control
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

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 11.1.2	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
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

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 12.1.1	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
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

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 13.1.1	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
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

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 14.2.5	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
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

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 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
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

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
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
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