INFORMATION SECURITY: ISO 27001 HAS BEEN UPDATED

“ARE YOU READY?”

Controls comparison guide - ISO 27001:2013 and ISO 27001:2022

LRQA

Key changes

In February 2022, ISO 27002:2022 – the standard which provides the best practice controls that organizations can implement to improve security – was updated. As a result, a new version of ISO 27001 – the international standard which outlines the requirements of an information security management system (ISMS) – was also published on October 25, 2022.

The new version of the standard features the controls outlined by ISO 27002:2022, and organizations will need to revisit their risk assessment to determine whether updates or new risk treatments need to be implemented.

Organizations with existing ISO 27001:2013 certification will have three years to transition to the new standard.

There are now **93** controls

instead of **114**

In total there are **11** new controls

56 controls from ISO 27001:2013 have now been merged into 24 controls in ISO 27001:2022

The majority of controls are subject to some form of text change which could impact how the standard is interpreted and implemented

Controls are now split across four 'new' themes

Organizational	People	Physical	Technical
- 28 merged	- 2 merged	- 5 merged	- 21 merged
- 3 new	- 0 new	- 1 new	- 7 new

Controls Comparison: ISO 27001:2013 (Annex A) vs ISO 27001:2022 (Annex A)

The controls outlined in ISO 27002:2022 will be included in ISO 27001:2022 Annex A – representing the most significant area of change in the new standard. The tables below provide a useful comparison of all available controls and how they correspond to those in the previous version – including any new controls and merges which are highlighted.

PREVIOUS **ISO 27001:2013**			NEW **ISO 27001:2022**		
CONTROL	TITLE		CONTROL	THEME (NEW)	TITLE
INFORMATION SECURITY POLICIES					
A5.1.1	Policies for information security	→	A.5.1	Organizational controls	Policies for information security
A.5.1.2	Review of the policies for information security	→	**Merged into A.5.1**		
ORGANISATION OF INFORMATION					
A.6.1.1	Information security roles and responsibilities	→	A5.2	Organizational controls	Information security roles and responsibilities
A.6.1.2	Segregation of duties	→	A.5.3	Organizational controls	Segregation of duties
A.6.1.3	Contact with authorities	→	A.5.5	Organizational controls	Contact with authorities
A.6.1.4	Contact with special interest groups	→	A.5.6	Organizational controls	Contact with special interest groups
NEW			A.5.7	Organizational controls	Threat intelligence
A.6.1.5	Information security in project management	→	A.5.8	Organizational controls	Information security in project management
A.6.2.1	Mobile device policy	→	A.8.1	Technical	User end point devices
A.6.2.2	Teleworking	→	A.6.7	People	Remote working

Previous Next

HUMAN RESOURCE SECURITY					
A.7.1.1	Screening	→	A.6.1	People	Screening
A.7.1.2	Terms and conditions of employment	→	A.6.2	People	Terms and conditions of employment
A.7.2.1	Management responsibilities	→	A.5.4	Organisational controls	Management responsibilities
A.7.2.2	Information security awareness, education and training	→	A.6.3	People	Information security awareness, education and training
A.7.2.3	Disciplinary process	→	A.6.4	People	Disciplinary process
A.7.3.1	Termination or change of employment responsibilities	→	A.6.5	People	Responsibilities after termination or change of employment
ASSET MANAGEMENT					
A.8.1.1	Inventory of assets	→	A.5.9	Organisational controls	Inventory of information and other associated assets
A.8.1.2	Ownership of assets	→	**Merged into A.5.9**		
A.8.1.3	Acceptable use of assets	→	A.5.10	Organisational controls	Acceptable use of information and other associated assets
A.8.1.4	Return of assets	→	A.5.11	Organisational controls	Return of assets
A.8.2.1	Classification of information	→	A.5.12	Organisational controls	Classification of information
A.8.2.2	Labelling of information	→	A.5.13	Organisational controls	Labelling of information
A.8.2.3	Handling of assets	→	**Merged into A.5.10**		
A.8.3.1	Management of removable media	→	A.7.10	Physical	Storage media
A.8.3.2	Disposal of media	→	**Merged into A.7.10**		
A.8.3.3	Physical media transfer	→	**Merged into A.7.10**		

ACCESS CONTROL					
A.9.1.1	Access control policy	→	A.5.15	Organizational controls	Access control
A.9.1.2	Access to networks and network services	→	Merged into A.5.15		
A.9.2.1	User registration and de-registration	→	A.5.16	Organizational controls	Identity management
A.9.2.2	User access provisioning	→	A.5.18	Organizational controls	Access rights
A.9.2.3	Management of privileged access rights	→	A.8.2	Technical	Privileged access rights
A.9.2.4	Management of secret authentication information of users	→	A.5.17	Organizational controls	Authentication information
A.9.2.5	Review of user access rights	→	Merged into A.5.18		
A.9.2.6	Removal or adjustment of access rights	→	Merged into A.5.18		
A.9.3.1	Use of secret authentication information	→	Merged into A.5.17		
A.9.4.1	Information access restriction	→	A.8.3	Technical	Information access restriction
A.9.4.2	Secure log-on procedures	→	A.8.5	Technical	Secure authentication
A.9.4.3	Password management system	→	Merged into A.5.17		
A.9.4.4	Use of privileged utility programs	→	A.8.18	Technical	Use of privileged utility programs
A.9.4.5	Access control to program source code	→	A.8.4	Technical	Access to source code
CRYPTOGRAPHY					
A.10.1.1	Policy on the use of cryptographic controls	→	A.8.24	Technical	Use of cryptography
A.10.1.2	Key management	→	Merged into A.8.24 with A.10.1.1		

PHYSICAL & ENVIRONMENTAL SECURITY					
A.11.1.1	Physical security perimeter	→	A.7.1	Physical	Physical security perimeters
A.11.1.2	Physical entry controls	→	A.7.2	Physical	Physical entry
A.11.1.3	Securing offices, rooms and facilities	→	A.7.3	Physical	Securing offices, rooms and facilities
NEW			A.7.4	Physical	Physical security monitoring
A.11.1.4	Protecting against external and environmental threats	→	A.7.5	Physical	Protecting against physical and environmental threats
A.11.1.5	Working in secure areas	→	A.7.6	Physical	Working in secure areas
A.11.1.6	Delivery and loading areas	→	**Merged into A.7.2 with A.11.1.2**		
A.11.2.1	Equipment siting and protection	→	A.7.8	Physical	Equipment siting and protection
A.11.2.2	Supporting utilities	→	A.7.11	Physical	Supporting utilities
A.11.2.3	Cabling security	→	A.7.12	Physical	Cabling security
A.11.2.4	Equipment maintenance	→	A.7.13	Physical	Equipment maintenance
A.11.2.5	Removal of assets	→	**Merged into A.7.10**		
A.11.2.6	Security of equipment and assets off-premises	→	A.7.9	Physical	Security of assets off-premises
A.11.2.7	Secure disposal or reuse of equipment	→	A.7.14	Physical	Secure disposal or re-use of equipment
A.11.2.8	Unattended user equipment	→	**Merged into A.8.1 with A.6.2.1**		
A.11.2.9	Clear desk and clear screen policy	→	A.7.7	Physical	Clear desk and clear screen

OPERATIONS SECURITY					
A.12.1.1	Documented operating procedures	→	A.5.37	Organisational controls	Documented operating procedures
A.12.1.2	Change management	→	A.8.32	Technical	Change management
A.12.1.3	Capacity management	→	A.8.6	Technical	Capacity management
A.12.1.4	Separation of development, testing and operational environments	→	A.8.31	Technical	Separation of development, test and production environments
A.12.2.1	Controls against malware	→	A.8.7	Technical	Protection against malware
A.12.3.1	Information backup	→	A.8.13	Technical	Information backup
A.12.4.1	Event logging	→	A.8.15	Technical	Logging
A.12.4.2	Protection of log information	→	**Merged into A.8.1.5**		
A.12.4.3	Administrator and operator logs	→	**Merged into A.8.1.5**		
NEW		→	A.8.16	Technical	Monitoring activities
A.12.4.4	Clock synchronisation	→	A.8.17	Technical	Clock synchronisation
A.12.5.1	Installation of software on operational systems	→	A.8.19	Technical	Installation of software on operational systems
A.12.6.1	Management of technical vulnerabilities	→	A.8.8	Technical	Management of technical vulnerabilities
NEW		→	A.8.9	Technical	Configuration management
NEW		→	A.8.10	Technical	Information deletion
NEW		→	A.8.11	Technical	Data masking
NEW		→	A.8.12	Technical	Data leakage prevention
A.12.6.2	Restrictions on software installation	→	**Merged into A.8.19 with A.12.5.1**		
A.12.7.1	Information systems audit controls	→	A.8.34	Technical	Protection of information systems during audit testing

COMMUNICATIONS SECURITY					
A.13.1.1	Network controls	→	A.8.20	Technical	Networks security
A.13.1.2	Security of network services	→	A.8.21	Technical	Security of network services
A.13.1.3	Segregation in networks	→	A.8.22	Technical	Segregation of networks
NEW		→	A.8.23	Technical	Web filtering
A.13.2.1	Information transfer policies and procedures	→	A.5.14	Organizational controls	Information transfer
A.13.2.2	Agreements on information transfer	→	**Merged into A.5.14**		
A.13.2.3	Electronic messaging	→	**Merged into A.5.14**		
A.13.2.4	Confidentiality or nondisclosure agreements	→	A.6.6	People	Confidentiality or non-disclosure agreements
SYSTEM ACQUSITION, DEVELOPMENT AND MAINTENANCE					
A.14.1.1	Information security requirements analysis and specification	→	**Merged into A.5.8 with A.6.1.5**		
A.14.1.2	Securing application services on public networks	→	A.8.26	Technical	Application security requirements
A.14.1.3	Protecting application services transactions	→	**Merged with A.8.26**		
A.14.2.1	Secure development policy	→	A.8.2.5	Technical	Secure development life cycle
A.14.2.2	System change control procedures	→	**Merged into A.8.32 with A.12.1.2**		
A.14.2.3	Technical review of applications after operating platform changes	→	**Merged into A.8.32 with A.12.1.2, A.14.2.2 & A.14.2.4**		
A.14.2.4	Restrictions on changes to software packages	→	**Merged into A.8.32 with A.12.1.2, A.14.2.2 & A.14.2.3**		
A.14.2.5	Secure system engineering principles	→	A.8.27	Technical	Secure system architecture and engineering principles
A.14.2.6	Secure development environment	→	**Merged into A.8.31 with A.12.1.4**		
NEW		→	A.8.28	Technical	Secure coding
A.14.2.7	Outsourced development	→	A.8.30	Technical	Outsourced development
A.14.2.8	System security testing	→	A.8.29	Technical	Security testing in development and acceptance
A.14.2.9	System acceptance testing	→	**Merged into A.8.29 with A.14.2.8**		
A.14.3.1	Protection of test data	→	A.8.33	Technical	Test information

SUPPLIER RELATIONSHIPS					
A.15.1.1	Information security policy for supplier relationships	→	A.5.19	Organizational controls	Information security in supplier relationships
A.15.1.2	Addressing security within supplier agreements	→	A.5.20	Organizational controls	Addressing information security within supplier agreements
A.15.1.3	Information and communication technology supply chain	→	A.5.21	Organizational controls	Managing information security in the information and communication technology (ICT) supply chain
A.15.2.1	Monitoring and review of supplier services	→	A.5.22	Organizational controls	Monitoring, review and change management of supplier services
A.15.2.2	Managing changes to supplier services	→	**Merged into A.5.22 with A.15.2.1**		
NEW			A.5.23	Organizational controls	Information security for use of cloud services
INFORMATION SECURITY INCIDENT MANAGEMENT					
A.16.1.1	Responsibilities and procedures	→	A.5.24	Organizational controls	Information security incident management planning and preparation
A.16.1.2	Reporting information security events	→	A.6.8	People	Information security event reporting
A.16.1.3	Reporting information security weaknesses	→	**Merged into A.6.8 with A.16.1.2**		
A.16.1.4	Assessment of and decision on information security events	→	A.5.25	Organizational controls	Assessment and decision on information security events
A.16.1.5	Response to information security incidents	→	A.5.26	Organizational controls	Response to information security incidents
A.16.1.6	Learning from information security incidents	→	A.5.27	Organizational controls	Learning from information security incidents
A.16.1.7	Collection of evidence	→	A.5.28	Organizational controls	Collection of evidence
INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT					
A.17.1.1	Planning information security continuity	→	A.5.29	Organizational controls	Information security during disruption
A.17.1.2	Implementing information security continuity	→	**Merged into A.5.29 with A.17.1.1, A.17.1.3**		
A.17.1.3	Verify, review and evaluate information security continuity	→	**Merged into A.5.29 with A.17.1.1, A.17.1.2**		
NEW			A.5.30	Organizational controls	ICT readiness for business continuity
A.17.2.1	Availability of information processing facilities	→	A.8.14	Technical	Redundancy of information processing facilities

COMPLIANCE					
A.18.1.1	Identification of applicable legislation and contractual requirements	→	A.5.31	Organizational controls	Legal, statutory, regulatory and contractual requirements
A.18.1.2	Intellectual property rights	→	A.5.32	Organizational controls	Intellectual property rights
A.18.1.3	Protection of records	→	A.5.33	Organizational controls	Protection of records
A.18.1.4	Privacy and protection of personally identifiable information	→	A.5.34	Organizational controls	Privacy and protection of personal identifiable information (PII)
A.18.1.5	Regulation of cryptographic controls	→	**Merged into A.5.31 with A.18.1.1**		
INFORMATION SECURITY REVIEWS					
A.18.2.1	Independent review of information security	→	A.5.35	Organizational controls	Independent review of information security
A.18.2.2	Compliance with security policies and standards	→	A.5.36	Organizational controls	Compliance with policies, rules and standards for information security
A.18.2.3	Technical compliance review	→	**Merged into A.5.36 with A.18.2.2**		

Our ISO 27001:2022 training and audit services

Training

Build your knowledge of ISO 27001:2022 with a range of courses designed for different experience levels – delivered via multiple learning styles.

Gap analysis

An optional service where one of our expert auditors will help you identify any critical, high-risk, or weak areas of your system prior to your transition audit.

Transition audit

We'll assess your ISMS in line with the requirements of ISO 27001:2022 – with a particular focus on the Annex A controls and how they impact your system.

Integrated audits

If you've implemented multiple management systems, you could benefit from an integrated audit and surveillance program which is more efficient and cost-effective.

Working with you to target every aspect of cybersecurity

Our deep experience in assurance, combined with award-winning cybersecurity services and threat-led intelligence, enables us to deliver bespoke insights into – and protection from – the unique threats facing your business. Keeping you one step ahead of cyber risk, today, tomorrow and beyond.

We provide audit, training and certification services against the world's leading international standards and schemes, complemented by a wide range of advanced cybersecurity services delivered by our specialists, Nettitude.

We work collaboratively with your business – helping you to identify the specific threats you face and build strategies to mitigate them. We'll work with you to certify your systems, identify vulnerabilities, and help prevent attacks and incidents that could impact your brand integrity, finances and operations.

Information security

Our compliance and certification services help you protect business-critical information and demonstrate internationally recognised best practices.

Find out more ›

Operational resilience

Be ready to prevent, respond and recover from disruption with our certification, training and governance, risk and compliance services.

Find out more ›

Cyber threat protection

Stay one step ahead of cyber threats, with tailored solutions that provide a first line of defence and response to all types of cyber attack.

Find out more ›

LRQA

YOUR FUTURE. OUR FOCUS.

About LRQA:

Bringing together unrivaled expertise in certification, brand assurance and training, LRQA is one of the world's leading providers of food safety and assurance solutions. Working together with farms, fisheries, food manufacturers, restaurants, hotels, and global retailers, we help manage food safety and sustainability risks throughout supply chains and have become a leading global assurance provider.

We're proud of our heritage, but it's who we are today that really matters, because that's what shapes how we partner with our clients tomorrow. By combining strong values, decades of experience in risk management and mitigation and a keen focus on the future, we're here to support our clients as they build safer, more secure, more sustainable businesses.

From independent auditing, certification and training; to technical advisory services; to real-time assurance technology; to data-driven supply chain transformation, our innovative end-to-end solutions help our clients negotiate a rapidly changing risk landscape – making sure they're shaping their own future, rather than letting it shape them.

Get in touch

Visit **www.lrqa.com/u**s for more information, email **inquiries-usa@lrqa.com** or call **866 971 5772**

LRQA
2101 Citywest Blvd., Suite 100
Houston TX 77042
United States

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.

For more information on LRQA, click **here**.