

**ISO/IEC 27001:2022**

# **Start your transition**

**New controls**

**LRQA**



# Key changes

In February 2022, ISO 27002:2022 – the standard which provides the best practice controls that organisations 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) – is also expected to be published in the final quarter of 2022.

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

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



# ISO 27001:2022 controls

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.


NEW ISO 27001:2022		
CONTROL	THEME (NEW)	TITLE
INFORMATION SECURITY POLICIES		
A.5.1	Organisational controls	Policies for information security
A.5.1.2	Merged into A.5.1	
ORGANISATION OF INFORMATION		
A.5.2	Organisational controls	Information security roles and responsibilities
A.5.3	Organisational controls	Segregation of duties
A.5.5	Organisational controls	Contact with authorities
A.5.6	Organisational controls	Contact with special interest groups
NEW A.5.7	Organisational controls	Threat intelligence
A.5.8	Organisational controls	Information security in project management
A.8.1	Technical	User end point devices
A.6.7	People	Remote working

HUMAN RESOURCE SECURITY		
A.6.1	People	Screening
A.6.2	People	Terms and conditions of employment
A.5.4	Organisational controls	Management responsibilities
A.6.3	People	Information security awareness, education and training
A.6.4	People	Disciplinary process
A.6.5	People	Responsibilities after termination or change of employment
ASSET MANAGEMENT		
A.5.9	Organisational controls	Inventory of information and other associated assets
A.8.1.2 Merged into A.5.9		
A.5.10	Organisational controls	Acceptable use of information and other associated assets
A.5.11	Organisational controls	Return of assets
A.5.12	Organisational controls	Classification of information
A.5.13	Organisational controls	Labelling of information
A.8.2.3 Merged into A.5.10		
A.7.10	Physical	Storage media
A.8.3.2 Merged into A.7.10		
A.8.3.3 Merged into A.7.10		

ACCESS CONTROL		
A.5.15	Organisational controls	Access control
A.9.1.2 Merged into A.5.15		
A.5.16	Organisational controls	Identity management
A.5.18	Organisational controls	Access rights
A.8.2	Technical	Privileged access rights
A.5.17	Organisational controls	Authentication information
A.9.2.5 Merged into A.5.18		
A.9.2.6 Merged into A.5.18		
A.9.3.1 Merged into A.5.17		
A.8.3	Technical	Information access restriction
A.8.5	Technical	Secure authentication
A.9.4.3 Merged into A.5.17		
A.8.18	Technical	Use of privileged utility programs
A.8.4	Technical	Access to source code
CRYPTOGRAPHY		
A.8.24	Technical	Use of cryptography
Merged into A.8.24 with A.10.1.1		

PHYSICAL & ENVIRONMENTAL SECURITY			
A.7.1	Physical	Physical security perimeters	
A.7.2	Physical	Physical entry	
A.7.3	Physical	Securing offices, rooms and facilities	
NEW A.7.4	Physical	Physical security monitoring	
A.7.5	Physical	Protecting against physical and environmental threats	
A.7.6	Physical	Working in secure areas	
A.11.1.6 Merged into A.7.2 with A.11.1.2			
A.7.8	Physical	Equipment siting and protection	
A.7.11	Physical	Supporting utilities	
A.7.12	Physical	Cabling security	
A.7.13	Physical	Equipment maintenance	
A.11.2.5 Merged into A.7.10			
A.7.9	Physical	Security of assets off-premises	
A.7.14	Physical	Secure disposal or re-use of equipment	
A.11.2.8 Merged into A.8.1 with A.6.2.1			
A.7.7	Physical	Clear desk and clear screen	

OPERATIONS SECURITY			
	A.5.37	Organisational controls	Documented operating procedures
	A.8.32	Technical	Change management
	A.8.6	Technical	Capacity management
	A.8.31	Technical	Separation of development, test and production environments
	A.8.7	Technical	Protection against malware
	A.8.13	Technical	Information backup
	A.8.15	Technical	Logging
A.12.4.2		Merged into A.8.1.5	
A.12.4.3		Merged into A.8.1.5	
NEW	A.8.16	Technical	Monitoring activities
NEW	A.8.17	Technical	Clock synchronisation
NEW	A.8.19	Technical	Installation of software on operational systems
NEW	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		Merged into A.8.19 with A.12.5.1	
	A.12.7.1 A.8.34	Technical	Protection of information systems during audit testing

				Previous	Next	
COMMUNICATIONS SECURITY						
A.8.20		Technical			Networks security	
A.8.21		Technical			Security of network services	
A.8.22		Technical			Segregation of networks	
NEW	A.8.23	Technical			Web filtering	
A.5.14		Organisational controls			Information transfer	
A.13.2.2		Merged into A.5.14				
A.13.2.3		Merged into A.5.14				
A.6.6		People			Confidentiality or non-disclosure agreements	
SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE						
A.14.1.1		Merged into A.5.8 with A.6.1.5				
A.8.26		Technical			Application security requirements	
A.14.1.3		Merged with A.8.26				
A.8.2.5		Technical			Secure development life cycle	
A.14.2.2		Merged into A.8.32 with A.12.1.2				
A.14.2.3		Merged into A.8.32 with A.12.1.2, A.14.2.2 & A.14.2.4				
A.14.2.4		Merged into A.8.32 with A.12.1.2, A.14.2.2 & A.14.2.3				
A.14.2.5 A.8.27		Technical			Secure system architecture and engineering principles	
A.14.2.6		Merged into A.8.31 with A.12.1.4				
NEW	A.8.28	Technical			Secure coding	
A.8.30		Technical			Outsourced development	
A.8.29		Technical			Security testing in development and acceptance	
A.14.2.9		Merged into A.8.29 with A.14.2.8				
A.8.33		Technical			Test information	



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

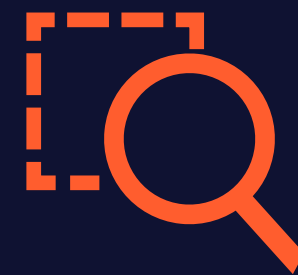
COMPLIANCE			
A.5.31		Organisational controls	Legal, statutory, regulatory and contractual requirements
A.5.32		Organisational controls	Intellectual property rights
A.5.33		Organisational controls	Protection of records
A.5.34		Organisational controls	Privacy and protection of personal identifiable information (PII)
A.18.1.5		Merged into A.5.31 with A.18.1.1	
INFORMATION SECURITY REVIEWS			
A.5.35		Organisational controls	Independent review of information security
A.5.36		Organisational controls	Compliance with policies, rules and standards for information security
A.18.2.3		Merged into A.5.36 with A.18.2.2	

# Our ISO 27001:2022 training and audit services

[Previous](#)[Next](#)

## 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 programme 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 >](#)

# Discover ThreatWatcher



LRQA Nettitude's ThreatWatcher service provides a managed assessment using advanced reconnaissance and analytics to identify previously unknown threats that could be used in a cyberattack. Security intelligence from ThreatWatcher can highlight weaknesses in user education and help to identify digital attack surface like never before. Nettitude's Threat Watcher is delivered by our team of highly skilled and experienced Threat Intelligence analysts and powered by the Recorded Future platform.

## ThreatWatcher and ISO 27001:2022

One of the new organisational controls, A.5.7 Threat intelligence, requires organisations to collect, analyse and produce threat intelligence regarding information security threats.

The goal of this new control is to provide organisations with a deeper understanding of cyber threats by collecting, analysing, and contextualising data about current and future cyber attacks. The new control is also designed to help organisations understand how hackers might hack them and inform companies about what types of data attackers are seeking.

ThreatWatcher provides these exact solutions, helping organisations demonstrate compliance with the new threat intelligence control.

Contact our experts for more information about ThreatWatcher and other LRQA Nettitude services that can help demonstrate compliance with the new requirements and controls introduced in ISO 27001:2022.

[Find out more →](#)





YOUR FUTURE. OUR FOCUS.

About LRQA:

Bringing together unrivalled 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/au](http://www.lrqa.com/au) for more information, email [enquiries.au@lrqa.com](mailto:enquiries.au@lrqa.com) or call +61 37 004 3410



LRQA  
Office 115, Level 18,  
120 Spencer St, Melbourne 3000  
Australia