

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.

There are now CS controls instead of L114

In total there are

In total there are

new controls

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

Organisational

- 28 merged

-3 new

People

- 2 merged

-0 new

- 5 merged

Physical

-1 new

Technical

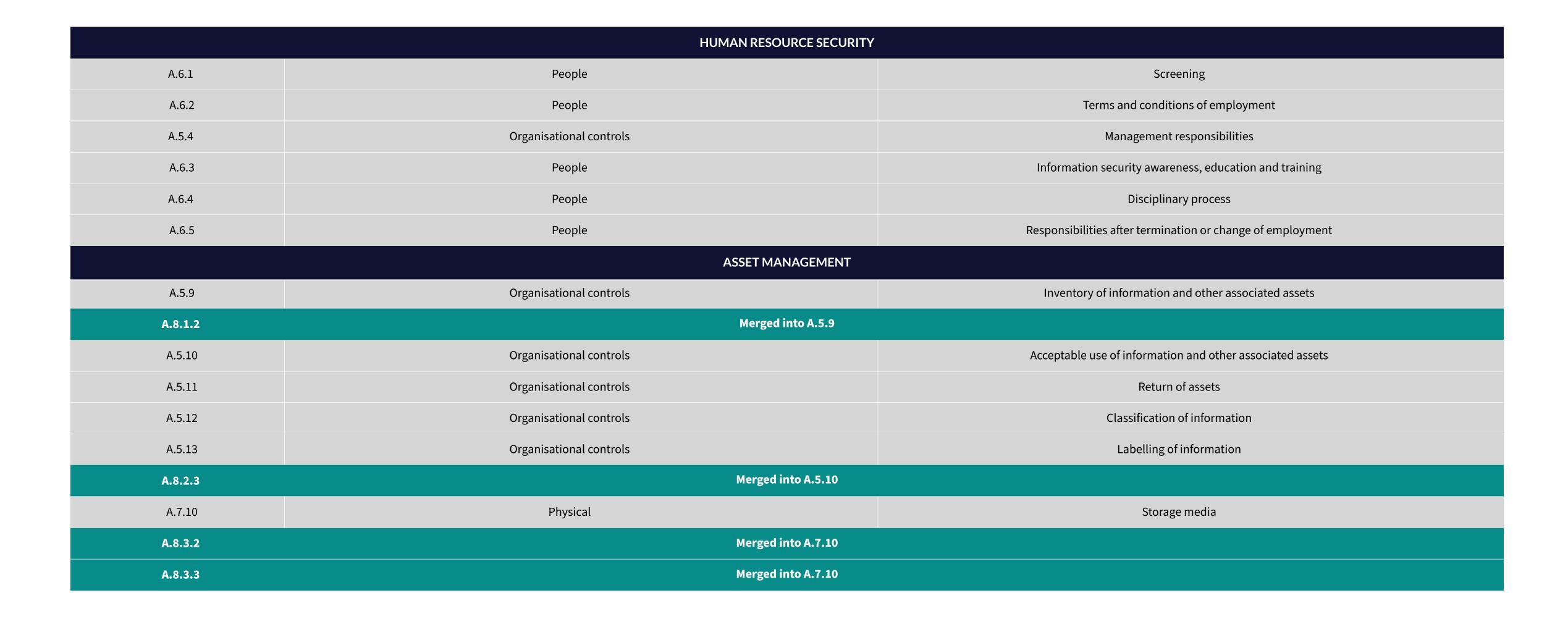
- 21 merged

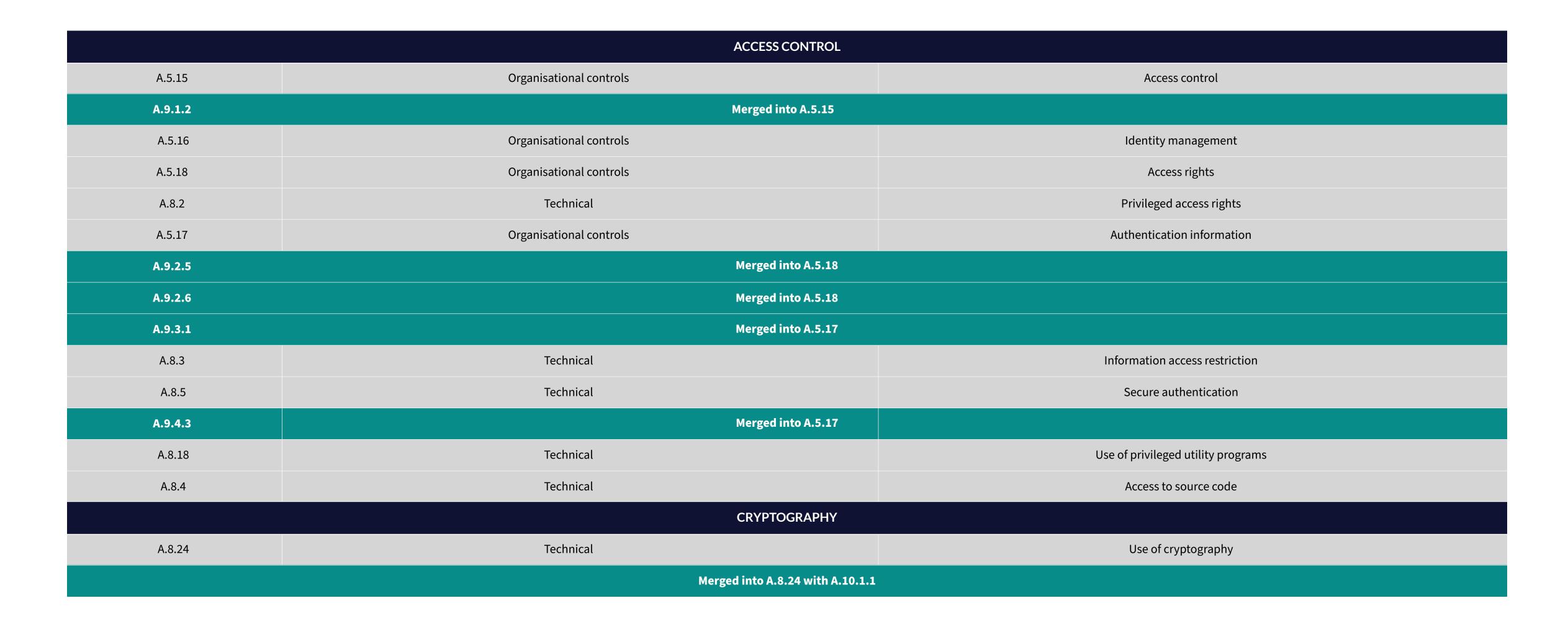
-7 new

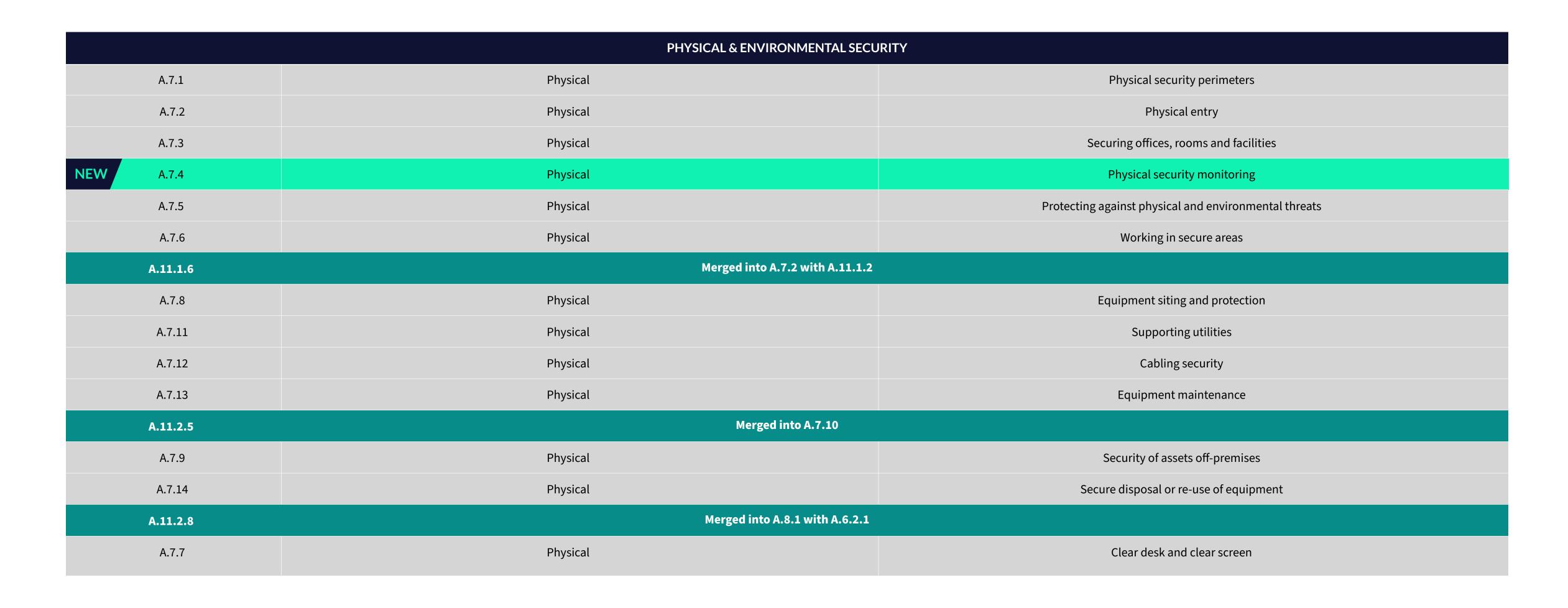
ISO 27001:2022 controls

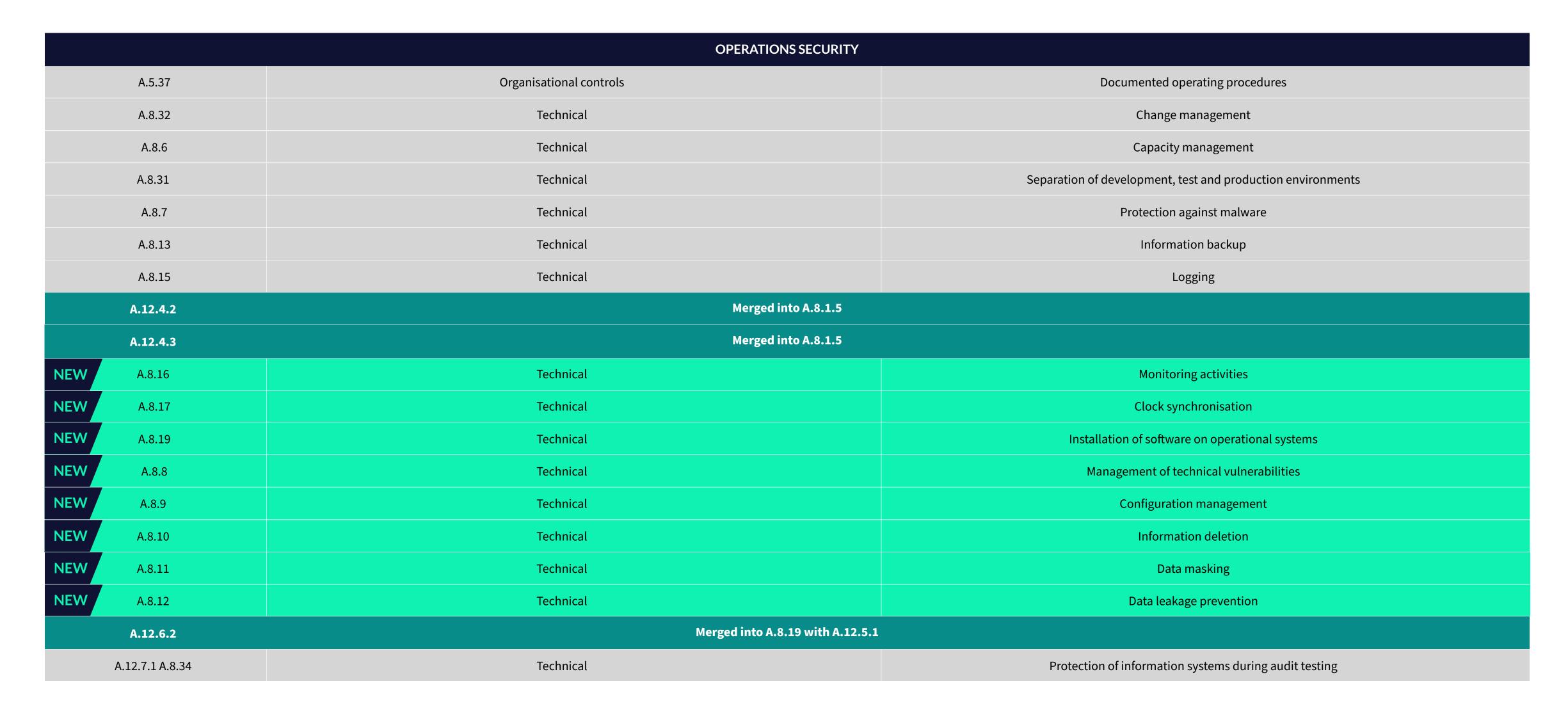
The controls outlined in ISO 27002:2022 will be included in ISO 27001:2022 Annex A – representing the most significant area of change in the new standard.

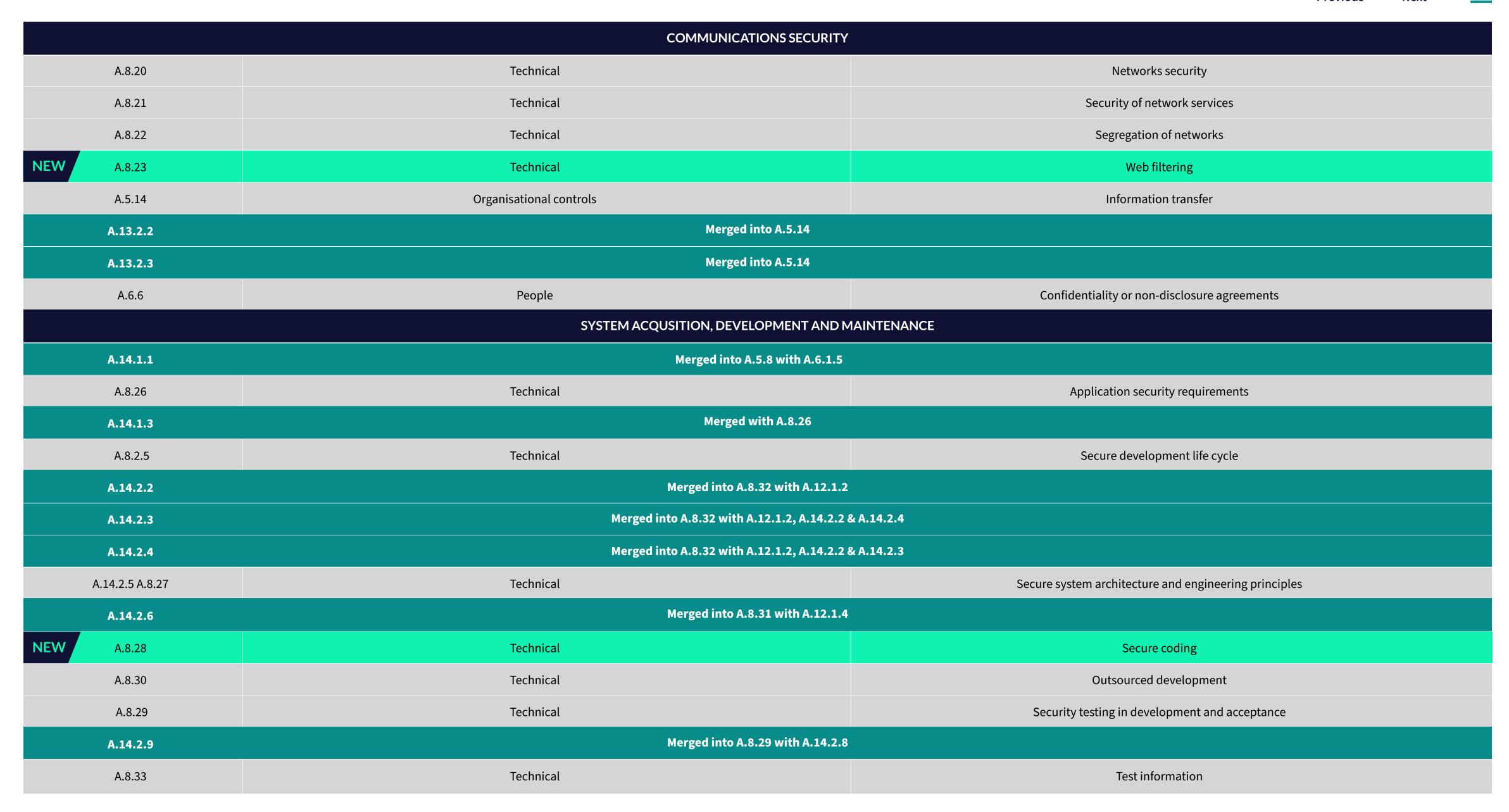
NEW ISO 27001:2022			
CONTROL	THEME (NEW)	TITLE	
INFORMATION SECURITY POLICIES			
A.5.1	Organisational controls	Policies for information security	
A.5.1.2	Merged into A.	5.1	
ORGANISATION OF INFORMATION			
A.5.2	Organisational controls	Information security roles and responsibilities	
A.5.3	Organisational 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	

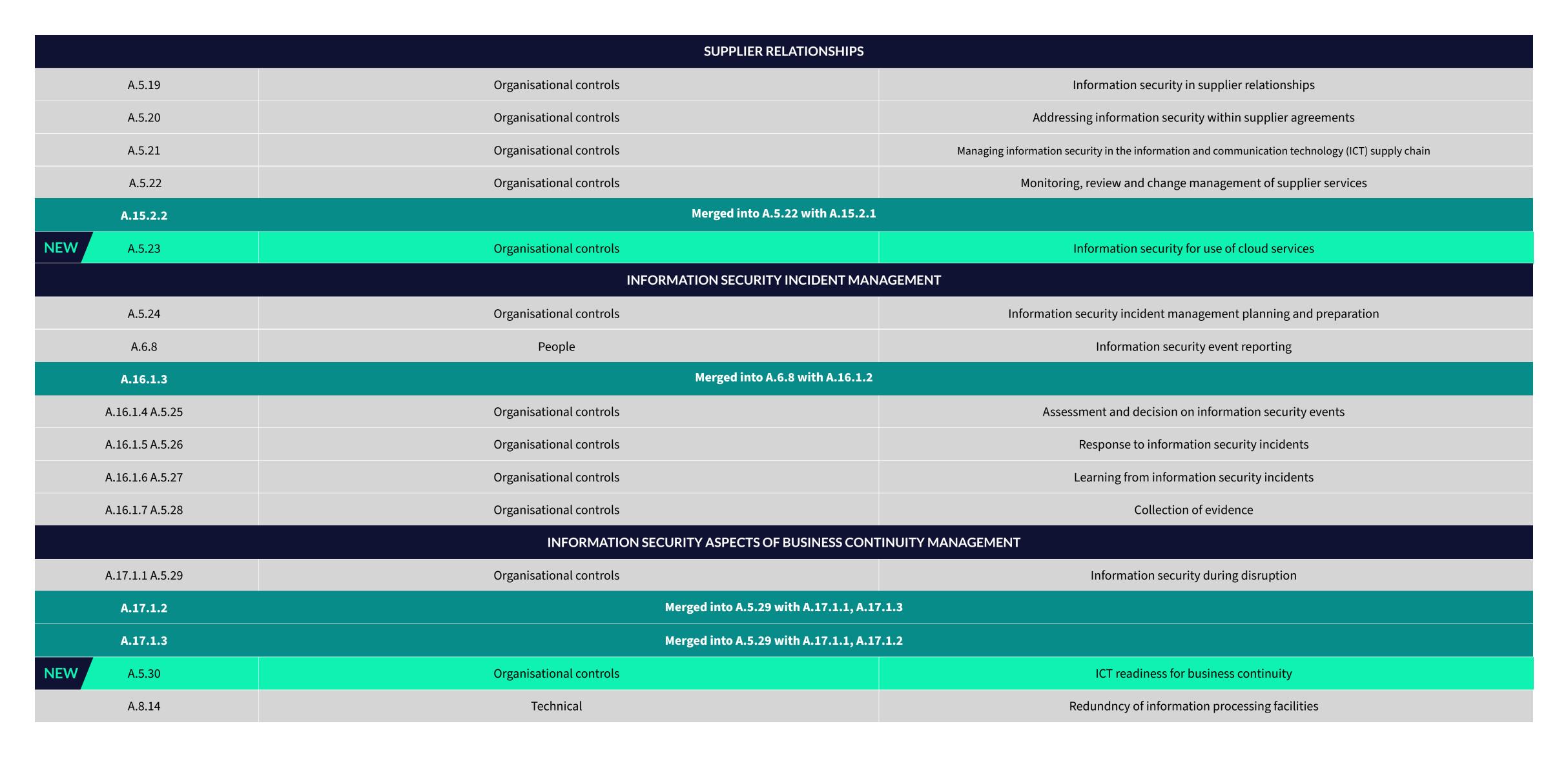












COMPLIANCE			
A.5.31	Organisational controls	Legal, statutory, regulatory and contractual requirements	
A.5.32	Organisational controls	Intellectual property rights	
A.5.33	Organisational controls	Protection of records	
A.5.34	Organisational controls	Privacy and protection of personal identifiable information (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		

\equiv

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 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/sg for more information, email enquiries.sg@lrqa.com or call +65 69904500







LRQA
460 Alexandra Road
mTower #15-01
Singapore 119963

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. © LRQA Group Limited 2023