ISO 27001:2022

Information Security, Cybersecurity and Privacy Protection

COMPASS
ASSURANCE SERVICES

RECENT UPDATES

NEW NAME

PREVIOUSLY:
Information Technology – Security Techniques

NOW:
Information Security, Cybersecurity and Privacy Protection

4 ORGANISATIONAL CONTEXT

Addition to 4.2: The organisation shall determine **which stakeholder requirements will be addressed through the ISMS**

6 PLANNING

Addition to 6.2: The information security objectives shall be monitored and available as documented information

NEW REQUIREMENT – 6.3: **Planning of changes**: Changes to the ISMS shall be carried out in a planned manner when the organisation determines need for such changes addressed through the ISMS

7 SUPPORT

7.4 Communication: Points "who shall communicate" and "the process by which communication shall be effected" combined to just "how to communicate"

8 OPERATION

Addition to 8.1: Establishing criteria for process & implementing control of the processes in accordance with said criteria

9 PERFORMANCE EVALUATION

Requirement 9.3: Management Review has been split into 3 sub requirements

Addition to Management Review inputs: consideration of changes in needs and expectations of interested parties relevant to the ISMS

COMPASS

ASSURANCE SERVICES

ANNEX A - NEW CONTROLS

5.7 Threat intelligence	Collecting and analysing information relating to information security threats
5.23 Information security for use of cloud services	Establishing processes for acquiring, using, managing, and exiting from cloud services
5.30 ICT readiness for business continuity	Implementing processes so the organisation can continue operations as usual in case of a disruption that affects ICT
7.4 Physical security monitoring	Monitoring of physical premises for unauthorised physical access
8.9 Configuration management	Developing and documenting a consistent process for establishing the attributes of a product or service such that the output is consistent
8.10 Information deletion	Deleting information when no longer required, or as per local regulations
8.11 Data masking	Masking data to limit exposure of sensitive information such as PII in compliance with local regulations
8.12 Data leakage prevention	Putting measures in place in systems, networks and any other devices that process, store, or transmit sensitive information to prevent leakage of data
8.16 Monitoring activities	Monitoring networks, systems and applications for unusual behaviour and taking appropriate action to evaluate and prevent potential incidents
8.23 Web filtering	Managing or reducing access to specific external websites on company devices to reduce exposure of these devices to malware
8.28 Secure coding	Putting protective measures in place to ensure software is written in a secure environment to reduce vulnerabilities in the software. For organisations that develop software

MANDATORY DOCUMENTED INFORMATION

4.3 Scope	The organisation must document the **scope** of the Information Security Management System and have this available to relevant parties
5.2 Policy	The organisation must document the **policy** of the Information Security Management System and have this available to relevant parties
6.1.2 & 8.2 Information Security Risk Assessment	The Information Security risk **assessment** process & results from risk assessments must be documented
6.1.3 & 8.3 Information Security Risk Treatment	The Information Security risk **treatment** process & results from risk treatments must be documented The organisation must produce a Statement of Applicability (SoA) that contains necessary controls, justification of inclusion/exclusion and level of implementation of the controls
6.2 Information Security Objectives and Planning to Achieve them	The Information Security objectives shall be documented and available
7.2 Competence	The organisation must retain appropriate documented evidence of competence
8.1 Operational Planning and Control	Appropriate documentation shall be retained and available to the extent necessary to be confident that operational processes are carried out as intended
9.1 Monitoring, Measurement, Analysis and Evaluation	Evidence of the results from monitoring and measuring activities shall be retained as documented evidence
9.2 Internal Audit	Results and evidence of implementation of the internal audit program/process shall be documented and available
9.3 Management Review	Management review results shall be documented as evidence
10.2 Nonconformity and Corrective Action	When corrective actions are undertaken, the nature of the nonconformities & results of corrective actions shall be documented as evidence

CHANGES TO PREVIOUSLY REQUIRED MANDATORY DOCUMENTS

Mobile Device Policy	Information stored on or processed by user devices (including mobile devices) shall be protected. No explicit mention of a policy
Teleworking	Previously a Teleworking Policy was required. Now the organisation must have security measures in place to protect information when staff and contractors are working away from the office
Access Control Policy	**Rules** must be in place to control access to physical and technological information. This may or may not be in the form of a policy
Policy on the use of Cryptographic Controls, and Key Management	**Rules** must be defined and implemented regarding the effective use of cryptography, including cryptographic key management. This may or may not be in the form of a policy
Clear Desk and Clear Screen Policy	**Rules** must be defined and enforced regarding clear desks including papers and removable storage media as well as clear screen

MAPPING ANNEX A - 2013 TO 2022

ISO/IEC 27001:2022	ISO/IEC 27001:2013	Control name in 27001:2022
5. ORGANISATIONAL CONTROLS		
5.1	**5.1.1, 5.1.2**	Policies for information security
5.2	**6.1.1**	Information security roles and responsibilities
5.3	**6.1.2**	Segregation of duties
5.4	**7.2.1**	Management responsibilities
5.5	**6.1.3**	Contact with authorities
5.6	**6.1.4**	Contact with special interest groups
5.7	**New**	Threat intelligence
5.8	**6.1.5, 14.1.1**	Information security in project management
5.9	**8.1.1, 8.1.2**	Inventory of information and other associated assets
5.10	**8.1.3, 8.2.3**	Acceptable use of information and other associated assets
5.11	**8.1.4**	Return of assets
5.12	**8.2.1**	Classification of information
5.13	**8.2.2**	Labelling of information
5.14	**13.2.1, 13.2.2, 13.2.3**	Information transfer
5.15	**9.1.1, 9.1.2**	Access control
5.16	**9.2.1**	Identity management

5.17	**9.2.4, 9.3.1, 9.4.3**	Authentication information
5.18	**9.2.2, 9.2.5, 9.2.6**	Access rights
5.19	**15.1.1**	Information security in supplier relationships
5.20	**15.1.2**	Addressing information security within supplier agreements
5.21	**15.1.3**	Managing information security in the ICT supply chain
5.22	**15.2.1, 15.2.2**	Monitoring, review and change management of supplier services
5.23	**New**	Information security for use of cloud services
5.24	**16.1.1**	Information security incident management planning and preparation
5.25	**16.1.4**	Assessment and decision on information security events
5.26	**16.1.5**	Response to information security incidents
5.27	**16.1.6**	Learning from information security incidents
5.28	**16.1.7**	Collection of evidence
5.29	**17.1.1, 17.1.2, 17.1.3**	Information security during disruption
5.30	**New**	ICT readiness for business continuity
5.31	**18.1.1, 18.1.5**	Legal, statutory, regulatory and contractual requirements
5.32	**18.1.2**	Intellectual property rights
5.33	**18.1.3**	Protection of records
5.34	**18.1.4**	Privacy and protection of PII

5.35	**18.2.1**	Independent review of information security
5.36	**18.2.2, 18.2.3**	Compliance with policies, rules and standards for information security
5.37	**12.1.1**	Documented operating procedures
6. PEOPLE CONTROLS		
6.1	**7.1.1**	Screening
6.2	**7.1.2**	Terms and conditions of employment
6.3	**7.2.2**	Information security awareness, education and training
6.4	**7.2.3**	Disciplinary process
6.5	**7.3.1**	Responsibilities after termination or change of employment
6.6	**13.2.4**	Confidentiality or non-disclosure agreements
6.7	**6.2.2**	Remote working
6.8	**16.1.2, 16.1.3**	Information security event reporting
7. PHYSICAL CONTROLS		
7.1	**11.1.1**	Physical security perimeters
7.2	**11.1.2, 11.1.6**	Physical entry
7.3	**11.1.3**	Securing offices, rooms, and facilities
7.4	**New**	Physical security monitoring
7.5	**11.1.4**	Protecting against physical and environmental threats
7.6	**11.1.5**	Working in secure areas

7.7	**11.2.9**	Clear desk and clear screen
7.8	**11.2.1**	Equipment siting and protection
7.9	**11.2.6**	Security of assets off-premises
7.10	**8.3.1, 8.3.2, 8.3.3, 11.2.5**	Storage media
7.11	**11.2.2**	Supporting utilities
7.12	**11.2.3**	Cabling security
7.13	**11.2.4**	Equipment maintenance
7.14	**11.2.7**	Secure disposal or re-use of equipment
8. TECHNOLOGICAL CONTROLS		
8.1	**6.2.1, 11.2.8**	User endpoint devices
8.2	**9.2.3**	Privileged access rights
8.3	**9.4.1**	Information access restriction
8.4	**9.4.5**	Access to source code
8.5	**9.4.2**	Secure authentication
8.6	**12.1.3**	Capacity management
8.7	**12.2.1**	Protection against malware
8.8	**12.6.1, 18.2.3**	Management of technical vulnerabilities
8.9	**New**	Configuration management
8.10	**New**	Information deletion

8.11	**New**	Data masking
8.12	**New**	Data leakage prevention
8.13	**12.3.1**	Information backup
8.14	**17.2.1**	Redundancy of information processing facilities
8.15	**12.4.1, 12.4.2, 12.4.3**	Logging
8.16	**New**	Monitoring activities
8.17	**12.4.4**	Clock synchronization
8.18	**9.4.4**	Use of privileged utility programs
8.19	**12.5.1, 12.6.2**	Installation of software on operational systems
8.20	**13.1.1**	Networks security
8.21	**13.1.2**	Security of network services
8.22	**13.1.3**	Segregation of networks
8.23	**New**	Web filtering
8.24	**10.1.1, 10.1.2**	Use of cryptography
8.25	**14.2.1**	Secure development life cycle
8.26	**14.1.2, 14.1.3**	Application security requirements
8.27	**14.2.5**	Secure system architecture and engineering principles
8.28	**New**	Secure coding
8.29	**14.2.8, 14.2.9**	Security testing in development and acceptance

THANK YOU

Contact us for a quick quote to get a better idea of costs and timings. Visit our website

www.cas.com.au