ISO 27002:2017 - ISO 27002:2022 MAPPING TOOL

The below mapping document outlines the relationship between the previous ISO 27002 controls and their 2022 counterparts.

INFORMATION SECURITY CODE OF PRACTICE ISO 27002:2017			INFORMATION SECURITY CODE OF PRACTICE ISO 27002:2022	
5	**INFORMATION SECURITY POLICY**	**MERGED ISO27002:2017 CONTROLS**	**CONTROL REFERENCE**	
5.1.1	Policies for Information Security	5.1.1, 5.1.2	5.1	Policies for information security
5.1.2	Review of the policies for information security	5.1.1, 5.1.2	5.1	Policies for information security
6.1	**Internal Organisation**			
6.1.1	Information security roles and responsibilities		5.2	Information security roles and responsibilities
6.1.2	Segregation of duties		5.3	Segregation of duties
6.1.3	Contact with authorities		5.5	Contact with authorities
6.1.4	Contact with special interest groups		5.6	Contact with special interest groups
			5.7 (new)	Threat intelligence
6.1.5	Information security in project management	6.1.5, 14.1.1	5.8	Information security in project management
6.2	**Mobile devices and teleworking**			
6.2.1	Mobile device policy		8.1	User endpoint devices
6.2.2	Teleworking		6.7	Remote working
7.1	**Prior to employment**			
7.1.1	Screening		6.1	Screening
7.1.2	Terms and conditions of employment		6.2	Terms and conditions of employment
7.2	**During employment**			
7.2.1	Management responsibilities		5.4	Management responsibilities
7.2.2	Information security awareness, education and training		6.3	Information security awareness, education and training
7.2.3	Disciplinary process		6.4	Disciplinary process
7.3	Termination and change of employment			
7.3.1	Termination or change of employment responsibilities		6.5	Responsibilities after termination or change of employment
8.1	**Responsibility for assets**			
8.1.1	Inventory of assets	8.1.1, 8.1.2	5.9	Inventory of information and other associated assets
8.1.2	Ownership of assets	8.1.1, 8.1.2	5.9	Inventory of information and other associated assets
8.1.3	Acceptable use of assets	8.1.3, 8.2.3	5.10	Acceptable use of information and other associated assets
8.1.4	Return of assets		5.11	Return of assets
8.2	**Information classification**			
8.2.1	Classification guidelines		5.12	Classification of information
8.2.2	Labelling of information		5.13	Labelling of information
8.2.3	Handling of assets	8.1.3, 8.2.3	5.10	Acceptable use of information and other associated assets
8.3	**Media handling**			
8.3.1	Management of removable media	8.3.1, 8.3.2, 8.3.3, 11.2.5	7.10	Storage media
8.3.2	Disposal of media	8.3.1, 8.3.2, 8.3.3, 11.2.5	7.10	Storage media
8.3.3	Physical media transfer	8.3.1, 8.3.2, 8.3.3, 11.2.5	7.10	Storage media
9.1	**Business requirement of access control**			
9.1.1	Access control policy	9.1.1, 9.1.2	5.15	Access control
9.1.2	Access to networks and network services	9.1.1, 9.1.2	5.15	Access control
9.2	**User access management**			
9.2.1	User registration and de-registration		5.16	Identity management
9.2.2	User access provisioning	9.2.2, 9.2.5, 9.2.6	5.18	Access rights
9.2.3	Management of privileged access rights		8.2	Privileged access rights
9.2.4	Management of secret authentication information of users	9.2.4, 9.3.1, 9.4.3	5.17	Authentication information
9.2.5	Review of user access rights	9.2.2, 9.2.5, 9.2.6	5.18	Access rights
9.2.6	Removal or adjustment of access rights	9.2.2, 9.2.5, 9.2.6	5.18	Access rights
9.3	**User responsibilities**			
9.3.1	Use of secret authentication information	9.2.4, 9.3.1, 9.4.3	5.17	Authentication information
9.4	**System and application access control**			
9.4.1	Information access restriction		8.3	Information access restriction
9.4.2	Secure log-on procedures		8.5	Secure authentication
9.4.3	Password management system	9.2.4, 9.3.1, 9.4.3	5.17	Authentication information
9.4.4	Use of privileged utility programs		8.18	Use of privileged utility programs
9.4.5	Access control to program source code		8.4	Access to source code
10.1	**Cryptographic controls**			
10.1.1	Policy on the use of cryptographic controls	10.1.1, 10.1.2	8.24	Use of cryptography
10.1.2	Key management	10.1.1, 10.1.2	8.24	Use of cryptography
11.1	**Secure areas**			
11.1.1	Physical security perimeter		7.1	Physical security perimeters
11.1.2	Physical entry controls	11.1.2, 11.1.6	7.2	Physical entry
11.1.3	Securing offices, rooms and facilities		7.3	Securing offices, rooms and facilities
			7.4 (new)	Physical security monitoring
11.1.4	Protecting against external and environmental threats		7.5	Protecting against physical and environmental threats
11.1.5	Working in secure areas		7.6	Working in secure areas
11.1.6	Delivery and loading areas	11.1.2, 11.1.6	7.2	Physical entry
11.2	**Equipment security**			
11.2.1	Equipment siting and protection		7.8	Equipment siting and protection
11.2.2	Supporting utilities		7.11	Supporting utilities
11.2.3	Cabling security		7.12	Cabling security
11.2.4	Equipment maintenance		7.13	Equipment maintenance
11.2.5	Removal of assets	8.3.1, 8.3.2, 8.3.3, 11.2.5	7.10	Storage media
11.2.6	Security of equipment off-premises		7.9	Security of assets off-premises
11.2.7	Secure disposal or re-use of equipment		7.14	Secure disposal or re-use of equipment
11.2.8	Unattended user equipment		8.1	User endpoint devices
11.2.9	Clear desk and clear screen policy		7.7	Clear desk and clear screen
12.1	**Operational procedures and responsibilities**			
12.1.1	Documented operating procedures		5.37	Documented operating procedures
			8.10 (new)	Information deletion
12.1.2	Change management	12.1.2, 14.2.2, 14.2.3, 14.2.4	8.32	Change management
12.1.3	Capacity planning		8.6	Capacity management
12.1.4	Separation of development and operational environments		8.31	Separation of development, test and production environments
12.2	**Protection from malware**			
12.2.1	Controls against malware		8.7	Protection against malware
12.3	**Backup**			
12.3.1	Information backup		8.13	Information backup
12.4	**Logging and monitoring**			
12.4.1	Event logging	12.4.1, 12.4.2, 12.4.3	8.15	Logging
12.4.2	Protection of log information	12.4.1, 12.4.2, 12.4.3	8.15	Logging
12.4.3	Administrator and operator logs	12.4.1, 12.4.2, 12.4.3	8.15	Logging
			8.16 (new)	Monitoring activities
12.4.4	Clock synchronisation		8.17	Clock synchronization
12.5	**Control of operational software**			
12.5.1	Control of operational software		8.19	Installation of software on operational systems
12.6	**Technical vulnerability management**			
12.6.1	Control of technical vulnerabilities		8.8	Management of technical vulnerabilities
			8.9 (new)	Configuration management
12.6.2	Restrictions on software installation		8.19	Installation of software on operational systems
12.7	**Information systems audit considerations**			
12.7.1	Information systems audit controls		8.34	Protection of information systems during audit testing
13.1	**Network security management**			
13.1.1	Network controls		8.20	Networks security
13.1.2	Security of network services		8.21	Security of network services
13.1.3	Segregation in networks		8.22	Segregation of networks
			8.23 (new)	Webfiltering
13.2	**Exchange of information**			
13.2.1	Information exchange policies and procedures	13.2.1, 13.2.2, 13.2.3	5.14	Information transfer
13.2.2	Agreement on information transfer	13.2.1, 13.2.2, 13.2.3	5.14	Information transfer
13.2.3	Electronic messaging	13.2.1, 13.2.2, 13.2.3	5.14	Information transfer
13.2.4	"Confidentiality or nondisclosure agreements"		6.6	Confidentiality or non-disclosure agreements
14.1	**Security requirements of information systems**			
14.1.1	Security requirements analysis and specification	6.1.5, 14.1.1	5.8	Information security in project management
14.1.2	Securing application services on public networks	14.1.2, 14.1.3	8.26	Application security requirements
14.1.3	Protecting application services transactions	14.1.2, 14.1.3	8.26	Application security requirements
14.2	**Security in development and support processes**			
14.2.1	Secure development policy		8.25	Secure development life cycle
14.2.2	System change control procedures	12.1.2, 14.2.2, 14.2.3, 14.2.4	8.32	Change management
14.2.3	Technical review of applications after operating platform changes	12.1.2, 14.2.2, 14.2.3, 14.2.4	8.32	Change management
14.2.4	Restrictions on changes to software packages	12.1.2, 14.2.2, 14.2.3, 14.2.4	8.32	Change management
14.2.5	Secure system engineering principles		8.27	Secure system architecture and engineering principles
			8.28 (new)	Secure coding
14.2.6	Secure development environment		8.31	Separation of development, test and production environments
14.2.7	Outsourced software development		8.30	Outsourced development
14.2.8	System security testing	14.2.8, 14.2.9	8.29	Security testing in development and acceptance
14.2.9	System acceptance testing	14.2.8, 14.2.9	8.29	Security testing in development and acceptance
14.3	**Test data**			
14.3.1	Protection of system test data		8.33	Test information
15.1	**Information security in supplier relationships**			
15.1.1	Information security policy for supplier relationships		5.19	Information security in supplier relationships
15.1.2	"Addressing security within supplier agreements"		5.20	Addressing information security within supplier agreements
15.1.3	Information and communication technology supply chain		5.21	Managing information security in the ICT supply chain
15.2	**Supplier service delivery management**			
15.2.1	Monitoring and review of supplier services	15.2.1, 15.2.2	5.22	Monitoring, review and change management of supplier services
15.2.2	Managing changes to supplier services	15.2.1, 15.2.2	5.22	Monitoring, review and change management of supplier services
			5.23 (new)	Information security for use of cloud services
16.1	**Management of information security incidents and improvements**			
16.1.1	Responsibilities and procedures		5.24	Information security incident management planning and preparation
16.1.2	Reporting information security events	16.1.2, 16.1.3	6.8	Information security event reporting
16.1.3	Reporting security weaknesses	16.1.2, 16.1.3	6.8	Information security event reporting
16.1.4	Assessment of and decision on information security events		5.25	Assessment and decision on information security events
16.1.5	Response to information security incidents		5.26	Response to information security incidents
16.1.6	Learning from information security incidents		5.27	Learning from information security incidents
16.1.7	Collection of evidence		5.28	Collection of evidence
17.1	**Information security continuity**			
17.1.1	Planning information security continuity	17.1.1, 17.1.2, 17.1.3	5.29	Information security during disruption
17.1.2	Implementing information security continuity	17.1.1, 17.1.2, 17.1.3	5.29	Information security during disruption
17.1.3	Verify, review and evaluate information security continuity	17.1.1, 17.1.2, 17.1.3	5.29	Information security during disruption
			5.30 (new)	ICT readiness for business continuity
17.2	**Redundancies**			
17.2.1	Availability of information processing facilities		8.14	Redundancy of information processing facilities
18.1	**Compliance with legal and contractual requirements**			
18.1.1	Identification of applicable legislation and contractual requirements	18.1.1, 18.1.5	5.31	Legal, statutory, regulatory and contractual requirements
18.1.2	Intellectual property rights		5.32	Intellectual property rights
18.1.3	Protection of records		5.33	Protection of records
			8.12 (new)	Data leakage prevention
18.1.4	Privacy and protection of personally identifiable information		5.34	Privacy and protection of PII
			8.11 (new)	Data masking
18.1.5	Regulation of cryptographic controls	18.1.1, 18.1.5	5.31	Legal, statutory, regulatory and contractual requirements
18.2	**Information security reviews**			
18.2.1	Independent review of information security		5.35	Independent review of information security
18.2.2	Compliance with security policies and standards	18.2.2, 18.2.3	5.36	Compliance with policies, rules and standards for information security
18.2.3	Technical compliance review	18.2.2, 18.2.3	5.36	Compliance with policies, rules and standards for information security

NQA, Warwick House, Houghton Hall Park, Houghton Regis, Dunstable, Bedfordshire LU5 5ZX, United Kingdom
T: 0800 052 2424 E: info@nqa.com @nqaglobal