ISO 27002 - ISO 27017 - ISO 27018 - ISO 27701 MAPPING

INFORMATION SECURITY CODE OF PRACTICE — ISO 27002

CLOUD SERVICES — ISO/IEC 27017

PERSONAL INFORMATION IN THE CLOUD — ISO/IEC 27018

PRIVACY INFORMATION MANAGEMENT — ISO/IEC 27701

CLAUSE	SUMMARY	CLOUD SERVICE CUSTOMER	CLOUD SERVICE PROVIDER	CLOUD SERVICE PROVIDER		CONTROLLER	PROCESSOR
5			**INFORMATION SECURITY POLICIES**				
5.1	**Information Security Policy**	No change	No change	No change	6.2.1	No change	
5.1.1	Policies for Information Security	Additional implementation guidance for information security policy with a cloud service customer topic	Additional implementation guidance for information security policy as a cloud service provider	Additional implementation guidance	6.2.1.1	Additional implementation guidance	
5.1.2	Review of the policies for information security	No change	No change	No change	6.2.1.1	No change	
6			**ORGANIZATION OF INFORMATION SECURITY**				
6.1	**Internal Organisation**	No change	No change	No change	6.3.1	No change	
6.1.1	Information security roles and responsibilities	Additional implementation guidance to agree roles and responsibilities with cloud service provider	Additional implementation guidance to agree roles and responsibilities with cloud service customers	Additional implementation guidance	6.3.1.1	Additional implementation guidance	
6.1.2	Segregation of duties	No change	No change	No change	6.3.1.2	No change	
6.1.3	Contact with authorities	Additional implementation guidance to identify authorities relevant to both customer and provider	Additional guidance to inform customers of geographical locations of data hosting	No change	6.3.1.3	No change	
6.1.4	Contact with special interest groups	No change	No change	No change	6.3.1.4	No change	
6.1.5	Information security in project management	No change	No change	No change	6.3.1.5	No change	
6.2	**Mobile devices and teleworking**	No change	No change	No change	6.3.2	No change	
6.2.1	Mobile device policy	No change	No change	No change	6.3.2.1	Additional implementation guidance	
6.2.2	Teleworking	No change	No change	No change	6.3.2.2	Additional implementation guidance	
6.3		Relationship between cloud service customer and cloud service provider					
6.3.1		New control to ensure cloud service users are aware of their roles and responsibilities	New control to ensure customers are aware of cloud security functions and their role in using them				
7			**HUMAN RESOURCE SECURITY**				
7.1	**Prior to employment**	No change	No change	No change	6.4.1	No change	
7.1.1	Screening	No change	No change	No change	6.4.1.1	No change	
7.1.2	Terms and conditions of employment	No change	No change	No change	6.4.1.2	No change	
7.2	During employment	No change	No change	No change	6.4.2	No change	
7.2.1	Management responsibilities	No change	No change	No change	6.4.2.1	No change	
7.2.2	Information security awareness, education and training	Additional implementation guidance for raising awareness of the use of cloud services	Additional implementation guidance to raise awareness of customer data handling	Additional implementation guidance	6.4.2.2	No change	
7.2.3	Disciplinary process	No change	No change	No change	6.4.2.3	No change	
7.3	**Termination and change of employment**	No change	No change	No change	6.4.3	No change	
7.3.1	Termination or change of employment responsibilities	No change	No change	No change	6.4.3.1	No change	
8			**ASSET MANAGEMENT**				
8.1	**Responsibility for assets**	No change	No change	No change	6.5.1	No change	
8.1.1	Inventory of assets	Additional implementation guidance for cloud data assets	Additional implementation guidance for identifying customer data and cloud-derived data	No change	6.5.1.2	No change	
8.1.2	Ownership of assets	No change	No change	No change	6.5.1.3	No change	
8.1.3	Acceptable use of assets	No change	No change	No change	6.5.1.4	No change	
8.1.4	Return of assets	No change	No change	No change	6.5.1.5	No change	
		New control to request documented information regarding termination of services	New control regarding return and removal of assets on termination of service				
8.2	**Information classification**	No change	No change	No change	6.5.2	No change	
8.2.1	Classification guidelines	No change	No change	No change	6.5.2.1	Additional implementation guidance	
8.2.2	Labelling of information	Additional implementation guidance for labelling assets in cloud locations	Additional implementation guidance for making labelling functionality available to customers	No change	6.5.2.2	Additional implementation guidance	
8.2.3	Handling of assets	No change	No change	No change	6.5.2.3	No change	
8.3	**Media handling**	No change	No change	No change	6.5.3	No change	
8.3.1	Management of removable media	No change	No change	No change	6.5.3.1	Additional implementation guidance	
8.3.2	Disposal of media	No change	No change	No change	6.5.3.2	Additional implementation guidance	
8.3.3	Physical media transfer	No change	No change	No change	6.5.3.3	Additional implementation guidance	
9			**ACCESS CONTROL**				
9.1	**Business requirement of access control**	No change	No change	No change	6.6.1	No change	
9.1.1	Access control policy	No change	No change	No change	6.6.1.1	No change	
9.1.2	Access to networks and network services	Additional implementation guidance for access control policy	No change	No change	6.6.1.2	No change	
9.2	**User access management**	No change	No change	Additional implementation guidance	6.6.2	No change	
9.2.1	User registration and de-registration	No change	Additional guidance for the provision of user registration and de-registration	Additional implementation guidance	6.6.2.1	Additional implementation guidance	
9.2.2	User access provisioning	No change	Additional guidance for managing customer access rights	No change	6.6.2.2	Additional implementation guidance	
9.2.3	Management of privileged access rights	Additional implementation guidance for authenticating administrators to cloud services	Additional implementation guidance providing extra authentication of customer administrators	No change	6.6.2.3	No change	
9.2.4	"Management of secret authentication information of users"	Additional implementation guidance for assuring that the provider meets the customer's requirements	Additional implementation guidance for providing information on secret authentication to customers	No change	6.6.2.4	No change	
9.2.5	Review of user access rights	No change	No change	No change	6.6.2.5	No change	
9.2.6	"Removal or adjustment of access rights"	No change	No change	No change	6.6.2.6	No change	
9.3	**User responsibilities**	No change	No change	No change	6.6.3	No change	
9.3.1	"Use of secret authentication information"	No change	No change	No change	6.6.3.1	No change	
9.4	**System and application access control**	No change	No change	No change	6.6.4	No change	
9.4.1	Information access restriction	Additional implementation guidance to ensure cloud information access is restricted	Additional implementation guidance for providing access controls to customers	No change	6.6.4.1	No change	
9.4.2	Secure log-on procedures	No change	No change	Additional implementation guidance	6.6.4.2	Additional implementation guidance	
9.4.3	Password management system	No change	No change	No change	6.6.4.3	No change	
9.4.4	Use of privileged utility programs	Additional implementation guidance to ensure utility programes do not interfere with the cloud service provider's controls	Additional guidance to control the use of utility programs	No change	6.6.4.4	No change	
9.4.5	Access control to program source code	No change	No change	No change	6.6.4.5	No change	
9.5		Access control of cloud service customer data in a shared virtual environment					
9.5.1		No control	New control to enforce logical segregation in cloud environments				
9.5.2		New control to ensure hardening of services	New control to ensure hardening of services				
10			**CYPTOGRAPHY**				
10.1	**Cryptographic controls**	No change	No change	No change	6.7.1	No change	
10.1.1	Policy on the use of cryptographic controls	Additional implementation guidance for cryptographic controls in the cloud environment	No change	Additional implementation guidance	6.7.1.1	Additional implementation guidance	
10.1.2	Key management	Additional implementation guidance for key mangement in cloud environments	No change	No change	6.7.1.2	No change	
11			**PHYSICAL AND ENVIRONMENTAL SECURITY**				
11.1	**Secure areas**	No change	No change	No change	6.8.1	No change	
11.1.1	Physical security perimeter	No change	No change	No change	6.8.1.1	No change	
11.1.2	Physical entry controls	No change	No change	No change	6.8.1.2	No change	
11.1.3	Securing offices, rooms and facilities	No change	No change	No change	6.8.1.3	No change	
11.1.4	Protecting against external and environmental threats	No change	No change	No change	6.8.1.4	No change	
11.1.5	Working in secure areas	No change	No change	No change	6.8.1.5	No change	
11.1.6	Delivery and loading areas	No change	No change	No change	6.8.1.6	No change	
11.2	**Equipment security**	No change	No change	No change	6.8.2	No change	
11.2.1	Equipment siting and protection	No change	No change	No change	6.8.2.1	No change	
11.2.2	Supporting utilities	No change	No change	No change	6.8.2.2	No change	
11.2.3	Cabling security	No change	No change	No change	6.8.2.3	No change	
11.2.4	Equipment maintenance	No change	No change	No change	6.8.2.4	No change	
11.2.5	Removal of assets	No change	No change	No change	6.8.2.5	No change	
11.2.6	Security of equipment off-premises	No change	No change	No change	6.8.2.6	No change	
11.2.7	Secure disposal or re-use of equipment	Additional implementation guidance for ensuring cloud service provider has disposal procedures	Additional implementation guidance for timely disposal	Additional implementation guidance	6.8.2.7	Additional implementation guidance	
11.2.8	Unattended user equipment	No change	No change	No change	6.8.2.8	No change	
11.2.9	Clear desk and clear screen policy	No change	No change	No change	6.8.2.9	Additional implementation guidance	
12			**OPERATIONS SECURITY**				
12.1	**Operational procedures and responsibilities**	No change	No change	No change	6.9.1	No change	
12.1.1	Documented operating procedures	No change	No change	No change	6.9.1.1	No change	
12.1.2	Change management	Additional implementation guidance to include cloud services in change management	Additional implementation guidance for customer notifications of changes	No change	6.9.1.2	No change	
12.1.3	Capacity planning	Additional implementation guidance to include capacity management for cloud services	Additional implementation to include capacity monitoring to prevent security incidents	No change	6.9.1.3	No change	
12.1.4	Separation of development and operational environments	No change	No change	Additional implementation guidance	6.9.1.4	No change	
		New requirement to document procedures for critical failures	New requirement to provide information about critical operations to customers				
12.2	**Protection from malware**	No change	No change	No change	6.9.2	No change	
12.2.1	Controls against malware	No change	No change	No change	6.9.2.1	No change	
12.3	**Backup**	No change	No change	No change	6.9.3	No change	
12.3.1	Information backup	Additional implementation guidance for backup within cloud services	Additional implementation guidance for providing backup specifications to customers	Additional implementation guidance	6.9.3.1	Additional implementation guidance	
12.4	**Logging and monitoring**	No change	No change	No change	6.9.4	No change	
12.4.1	Event logging	Additional implementation guidance for defining logging requirements	Additional guidance for the provision of logging capabilities	Additional implementation guidance	6.9.4.1	Additional implementation guidance	Additional Guidance for processors
12.4.2	Protection of log information	No change	No change	Additional implementation guidance	6.9.4.2	Additional implementation guidance	
12.4.3	Administrator and operator logs	Additional implementation guidance for logging capabilities and obtaining assurance from provider	No change	No change	6.9.4.3	No change	
12.4.4	Clock synchronisation	Additional implementation guidance to request clock information from provider	Additional implementation guidance about providing clock information to customers	No change	6.9.4.4	No change	
		New control for requesting service monitoring information from provider	New control for providing capabilities to monitor service aspects				
12.5	**Control of operational software**	No change	No change	No change	6.9.5	No change	
12.5.1	Control of operational software	No change	No change	No change	6.9.5.1	No change	
12.6	**Technical vulnerability management**	No change	No change	No change	6.9.6	No change	
12.6.1	Control of technical vulnerabilities	Additional implementation guidance about obtaining technical vulnerability management information from providers	Additional implementation guidance regarding the provision of technical vulnerability management information to customers	No change	6.9.6.1	No change	
12.6.2	Restrictions on software installation	No change	No change	No change	6.9.6.2	No change	
12.7	**Information systems audit considerations**	No change	No change	No change	6.9.7	No change	
12.7.1	Information systems audit controls	No change	No change	No change	6.9.7.1	No change	
13			**COMMUNICATIONS SECURITY**				
13.1	**Network security management**	No change	No change	No change	6.10.1	No change	
13.1.1	Network controls	No change	No change	No change	6.10.1.1	No change	
13.1.2	Security of network services	No change	No change	No change	6.10.1.2	No change	
13.1.3	Segregation in networks	Additional implementation guidance for the defining segregation requirements	Additional implementation guidance for enforcing segregation	No change	6.10.1.3	No change	
		No new control	New control for a policy for virtual network configuration				
13.2	**Exchange of information**	No change	No change	No change	6.10.2	No change	
13.2.1	Information exchange policies and procedures	No change	No change	Additional implementation guidance	6.10.2.1	Additional implementation guidance	
13.2.2	Agreement on information transfer	No change	No change	No change	6.10.2.2	No change	
13.2.3	Electronic messaging	No change	No change	No change	6.10.2.3	No change	
13.2.4	"Confidentiality or nondisclosure agreements"	No change	No change	No change	6.10.2.4	Additional implementation guidance	
14			**SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE**				
14.1	**Security requirements of information systems**	No change	No change	No change	6.11.1	No change	
14.1.1	Security requirements analysis and specification	Additional implementation guidance for cloud security requirements analysis	Additional implementation guidance about information to be provided to customers about security capabilities	No change	6.11.1.1	No change	
14.1.2	Securing application services on public networks	No change	No change	No change	6.11.1.2	Additional implementation guidance	
14.1.3	Protecting application services transactions	No change	No change	No change	6.11.1.3	No change	
14.2	**Security in development and support processes**	No change	No change	No change	6.11.2	No change	
14.2.1	Secure development policy	Additional implementation guidance for requesting information about providers secure development practices	Additional impementation guidance about providing customers with information about secure development practices	No change	6.11.2.1	Additional implementation guidance	
14.2.2	System change control procedures	No change	No change	No change	6.11.2.2	No change	
14.2.3	Technical review of applications after operating platform changes	No change	No change	No change	6.11.2.3	No change	
14.2.4	Restrictions on changes to software packages	No change	No change	No change	6.11.2.4	No change	
14.2.5	"Secure system engineering principles"	No change	No change	No change	6.11.2.5	Additional implementation guidance	
14.2.6	Secure development environment	No change	No change	No change	6.11.2.6	No change	
14.2.7	Outsourced software development	No change	No change	No change	6.11.2.7	Additional implementation guidance	
14.2.8	System security testing	No change	No change	No change	6.11.2.8	No change	
14.2.9	System acceptance testing	No change	No change	No change	6.11.2.9	No change	
14.3	**Test data**	No change	No change	No change	6.11.3	No change	
14.3.1	Protection of system test data	No change	No change	No change	6.11.3.1	Additional implementation guidance	
15			**SUPPLIER RELATIONSHIPS**				
15.1	**Information security in supplier relationships**	No change	No change	No change	6.12.1	No change	
15.1.1	Information security policy for supplier relationships	Additional implementation guidance for including provider in list of suppliers	No change	No change	6.12.1.1	No change	
15.1.2	"Addressing security within supplier agreements"	Additional implementation guidance for security service agreement	Additional implementation guidance for specifying security measures provided in the service	No change	6.12.1.2	Additional implementation guidance	Additional Guidance for processors
15.1.3	Information and communication technology supply chain	No change	Additional implementation guidance where the provider is a peer or user of other providers	No change	6.12.1.3	No change	
15.2	**Supplier service delivery management**	No change	No change	No change	6.12.2	No change	
15.2.1	Monitoring and review of supplier services	No change	No change	No change	6.12.2.1	No change	
15.2.2	Managing changes to supplier services	No change	No change	No change	6.12.2.2	No change	
16			**INFORMATION SECURITY INCIDENT MANAGEMENT**				
16.1	**Management of information security incidents and improvements**	No change	No change	Additional implementation guidance	6.13.1	No change	
16.1.1	Responsibilities and procedures	Additional implementation guidance to ensure provider allocates incident management responsibilities	Additional implementation guidance for information to be provided to customers regarding information security incident management	Additional implementation guidance	6.13.1.1	Additional implementation guidance	
16.1.2	Reporting information security events	Additional implementation guidance about reporting flows between customer and provider and vice versa	Additional implementation guidance about reporting to customers	No change	6.13.1.2	No change	
16.1.3	Reporting security weaknesses	No change	No change	No change	6.13.1.3	No change	
16.1.4	Assessment of and decision on information security events	No change	No change	No change	6.13.1.4	No change	
16.1.5	Response to information security incidents	No change	No change	No change	6.13.1.5	Additional implementation guidance	Additional Guidance for processors
16.1.6	Learning from information security incidents	No change	No change	No change	6.13.1.6	No change	
16.1.7	Collection of evidence	Additional implementation guidance regarding exchange of evidence	Additional implementation guidance regarding exchange of evidence	No change	6.13.1.7	No change	
17			**INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT**				
17.1	**Information security continuity**	No change	No change	No change	6.14.1	No change	
17.1.1	Planning information security continuity	No change	No change	No change	6.14.1.1	No change	
17.1.2	"Implementing information security continuity"	No change	No change	No change	6.14.1.2	No change	
17.1.3	Verify, review and evaluate information security continuity	No change	No change	No change	6.14.1.3	No change	
17.2	**Redundacies**	No change	No change	No change	6.14.2	No change	
17.2.1	Availability of information processing facilities	No change	No change	No change	6.14.2.1	No change	
18			**COMPLIANCE**				
18.1	**Compliance with legal and contractual requirements**	No change	No change	No change	6.15.1	No change	
18.1.1	Identification of applicable legislation and contractual requirements	Additional implementation guidance for identifying applicable legislation for where data is held	Additional implementation guidance for informing customers of legal jurisdictions	No change	6.15.1.1	Additional implementation guidance	
18.1.2	Intellectual property rights	Additional implementation guidance for software licensing	Additional implementation guidance for responding to IPR complaints	No change	6.15.1.2	No change	
18.1.3	Protection of records	Additional implementation guidance for request information about protection of records	Additional implementation guidance for providing customers with information about protection of records	No change	6.15.1.3	Additional implementation guidance	
18.1.4	Privacy and protection of personally identifiable information	No change	No change	No change	6.15.1.4	No change	
18.1.5	Regulation of cryptographic controls	Additional implementation guidance for assurance on crypto compliance	Additional implementation guidance about providing customers with crypto assurance	No change	6.15.1.5	No change	
18.2	**Information security reviews**	No change	No change	No change	6.15.2	No change	
18.2.1	Independent review of information security	Additional implementation guidance for requesting information about independent security reviews from providers	Additional implementation guidance to provide customers with assurance of security controls	Additional implementation guidance	6.15.2.1	Additional implementation guidance	
18.2.2	Compliance with security policies and standards	No change	No change	No change	6.15.2.2	No change	
18.2.3	Technical compliance review	No change	No change	No change	6.15.2.3	No change	