Control Mapping

ISO 27002:2013			ISO 27002:2022		NIST SP 800-53	NIST CSF	CIS Critical Security Controls v8
Domain	**Control Objective**	**Control**	**Control Theme**	**Control ID**	**Control ID** Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control	**Control-ID**	**CIS Safeguard**
A.5 Information Security Policies	A.5.1 Management direction for information security	A.5.1.1 Policies for information security	Organisational Controls	5.1 Policies for information security	All XX-1 controls	ID.GV-1	15,2
A.5 Information Security Policies	A.5.1 Management direction for information security	A.5.1.2 Review of the policies for information security	Organisational Controls	5.1 Policies for information security	All XX-1 controls		15,2
A.6 Organization of information security	A.6.1 Internal organization	A.6.1.1 Information security roles and responsibilities	Organisational Controls	5.2 Information security roles and responsibilities	All XX-1 controls, CM-9, CP-2, PS-7, PS-9, SA-3, SA-9, PM-2, PM-10	ID.AM-6, ID.GV-2, PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5, DE.DP-1, RS.CO-1	17,5
A.6 Organization of information security	A.6.1 Internal organization	A.6.1.2 Segregation of duties	Organisational Controls	5.3 Segregation of duties	AC-5	PR.AC-4, PR.DS-5	6,8
A.6 Organization of information security	A.6.1 Internal organization	A.6.1.3 Contact with authorities	Organisational Controls	5.5 Contact with authorities	IR-6	RS.CO-2	17,2
A.6 Organization of information security	A.6.1 Internal organization	A.6.1.4 Contact with special interest groups	Organisational Controls	5.6 Contact with special interest groups	SI-5, PM-15	ID.RA-2, RS.CO-5, RC.CO-1	17,2
A.6 Organization of information security	A.6.1 Internal organization	A.6.1.5 Information security in project management	Organisational Controls	5.8 Information security in project management	SA-3, SA-9, SA-15	PR.IP-2	16,1
A.6 Organization of information security	A.6.2 Mobile devices and teleworking	A.6.2.1 Mobile device policy	Technological Controls	8.1 User endpoint devices	AC-17, AC-18, AC-19	PR.AC-3	3,1;3,6;4,1;4,5;4,11;4,12;9,1;10,1;10,7;12,7;13,5
A.6 Organization of information security	A.6.2 Mobile devices and teleworking	A.6.2.2 Teleworking	People Controls	6.7 Remote Working	AC-3, AC-17, PE-17	PR.AC-3	3,6;4,5;4,12;6,4;12,7;13,5
A.7 Human Resources Security	A.7.1 Prior to Employment	A.7.1.1 Screening	People Controls	6.1 Screening	PS-3, SA-21	PR.AC-6, PR.DS-5, PR.IP-11	
A.7 Human Resources Security	A.7.1 Prior to Employment	A.7.1.2 Terms and conditions of employment	People Controls	6.2 Terms and conditions of employment	PL-4, PS-6	PR.DS-5, PR.IP-11	
A.7 Human Resources Security	A.7.2 During employment	A.7.2.1 Management responsibilities	Organisational Controls	5.4 Management responsibilities	PL-4, PS-6, PS-7, SA-9	ID.GV-2, PR.AT-3, PR.IP-11	
A.7 Human Resources Security	A.7.2 During employment	A.7.2.2 Information security awareness, education, and training	People Controls	6.3 Information security awareness, education, and training	AT-2, AT-3, CP-3, IR-2, PM-13	PR.AT-1, PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5, PR.IP-11, DE.DP-1, RS.CO-1	14,1;14,3;14,5;14,7;14,8;14,9
A.7 Human Resources Security	A.7.2 During employment	A.7.2.3 Disciplinary process	People Controls	6.4 Disciplinary process	PS-8	PR.IP-11	
A.7 Human Resources Security	A.7.3 Termination and change of employment	A.7.3.1 Termination or change of employment responsibilities	People Controls	6.5 Responsibilities after termination or change of employment	PS-4, PS-5	PR.DS-5, PR.IP-11	6,2
A.8 Asset Management	A.8.1 Responsibility for assets	A.8.1.1 Inventory of assets	Organisational Controls	5.9 Inventory of information and other associated assets	CM-8	ID.AM-1, ID.AM-2	1,1;2,1;3,1;3.2;3,7
A.8 Asset Management	A.8.1 Responsibility for assets	A.8.1.2 Ownership of assets	Organisational Controls	5.9 Inventory of information and other associated assets	CM-8	ID.AM-1, ID.AM-2	1,1;2,1;3,1;3.2;3,7
A.8 Asset Management	A.8.1 Responsibility for assets	A.8.1.3 Acceptable use of assets	Organisational Controls	5.10 Acceptable use of assets and other associated information assets	PL-4		3,1;3,3;3,5;14,4;15,2
A.8 Asset Management	A.8.1 Responsibility for assets	A.8.1.4 Return of assets	Organisational Controls	5.11 Return of assets	PS-4, PS-5	PR.IP-11	
A.8 Asset Management	A.8.2 Information Classification	A.8.2.1 Classification of information	Organisational Controls	5.12 Classification of information	RA-2	ID.AM-5, PR.PT-2	3,7
A.8 Asset Management	A.8.2 Information Classification	A.8.2.2 Labelling of Information	Organisational Controls	5.13 Labelling of Information	MP-3, PE-22	PR.DS-5, PR.PT-2	3,7
A.8 Asset Management	A.8.2 Information Classification	A.8.2.3 Handling of Assets	Organisational Controls	5.10 Acceptable use of assets and other associated information assets	MP-2, MP-4, MP-5, MP-6, MP-7, PE-16, PE-18, PE- 20, SC-8, SC-28	PR.DS-1, PR.DS-2, PR.DS-3, PR.DS-5, PR.IP-6, PR.PT-2	3,1;3,3;3,5;14,4;15,2
A.8 Asset Management	A.8.3 Media Handling	A.8.3.1 Management of removable media	Physical Controls	7.10 Storage media	MP-2, MP-4, MP-5, MP-6, MP-7	PR.DS-3, PR.IP-6, PR.PT-2	3,5;3,6;3,9;10,3;10,4
A.8 Asset Management	A.8.3 Media Handling	A.8.3.2 Disposal of media	Physical Controls	7.10 Storage media	MP-6	PR.DS-3, PR.IP-6	3,5;3,6;3,9;10,3;10,4
A.8 Asset Management	A.8.3 Media Handling	A.8.3.3 Physical media transfer	Physical Controls	7.10 Storage media	MP-5	PR.DS-3, PR.PT-2	3,5;3,6;3,9;10,3;10,4
A.9 Access Control	A.9.1 Business requirement of access control	A.9.1.1 Access control policy	Organisational Controls	5.15 Access control	AC-1	PR.DS-5	3,3;5,4;5,5;5,6;6,1;6,3;6,8
A.9 Access Control	A.9.1 Business requirement of access control	A.9.1.2 Access to networks and network services	Organisational Controls	5.15 Access control	AC-3, AC-6	PR.AC-4, PR.DS-5, PR.PT-3	3,3;5,4;5,5;5,6;6,1;6,3;6,8
A.9 Access Control	A.9.2 User access management	A.9.2.1 User registration and de-registration	Organisational Controls	5.16 Identity management	AC-2, IA-2, IA-4, IA-5, IA-8	PR.AC-1, PR.AC-6, PR.AC-7	5,1;6,1;6,2
A.9 Access Control	A.9.2 User access management	A.9.2.2 User access provisioning	Organisational Controls	5.18 Access rights	AC-2	PR.AC-1	6,1;6,2;6,17
A.9 Access Control	A.9.2 User access management	A.9.2.3 Management of privileged access rights	Technological Controls	8.2 Privileged access rights	AC-2, AC-3, AC-6, CM-5	PR.AC-1, PR.AC-4, PR.DS-5	4,7;5,4;6,5;6,8
A.9 Access Control	A.9.2 User access management	A.9.2.4 Management of secret authentication information of users	Organisational Controls	5.17 Authentication of information	IA-5	PR.AC-1, PR.AC-7	5,2
A.9 Access Control	A.9.2 User access management	A.9.2.5 Review of user access rights	Organisational Controls	5.18 Access rights	AC-2		6,1;6,2;6,17
A.9 Access Control	A.9.2 User access management	A.9.2.6 Removal or adjustment of access rights	Organisational Controls	5.18 Access rights	AC-2	PR.AC-1	6,1;6,2;6,17
A.9 Access Control	A.9.3 User responsibilities	A.9.3.1 Use of secret authentication information	Organisational Controls	5.17 Authentication of information	IA-5	PR.AC-1, PR.AC-7	5,2
A.9 Access Control	A.9.4 System and application access control	A.9.4.1 Information access restriction	Technological Controls	8.3 Information access restriction	AC-3, AC-24	PR.AC-4, PR.DS-5	3,3;6,8;13,5
A.9 Access Control	A.9.4 System and application access control	A.9.4.2 Secure logon procedures	Technological Controls	8.5 Secure authentication	AC-7, AC-8, AC-9, IA-6	PR.AC-1, PR.AC-7	4,3;4,10;6,6
A.9 Access Control	A.9.4 System and application access control	A.9.4.3 Password management system	Organisational Controls	5.17 Authentication of information	IA-5	PR.AC-1, PR.AC-7	5,2
A.9 Access Control	A.9.4 System and application access control	A.9.4.4 Use of privileged utility programs	Technological Controls	8.18 Use of privileged utility programs	AC-3, AC-6	PR.AC-4, PR.DS-5	5,5
A.9 Access Control	A.9.4 System and application access control	A.9.4.5 Access control to program source code	Technological Controls	8.4 Access to source code	AC-3, AC-6, CM-5	PR.AC-4, PR.DS-5	3,3;16,1
A.10 Cryptography	A.10.1 Cryptographic controls	A.10.1.1 Policy on the use of cryptographic controls	Technological Controls	8.24 Use of cryptography	SC-13	PR.DS-5	
A.10 Cryptography	A.10.1 Cryptographic controls	A.10.1.2 Key Management	Technological Controls	8.24 Use of cryptography	SC-12, SC-17		
A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.1 Physical security perimeter	Physical Controls	7.1 Physical security perimeter	PE-3*	PR.AC-2, DE.CM-2	
A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.2 Physical entry controls	Physical Controls	7.2 Physical entry controls	PE-2, PE-3, PE-4, PE-5	PR.AC-2, PR.MA-1, DE.CM-2	
A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.3 Securing offices, rooms and facilities	Physical Controls	7.3 Securing offices, rooms and facilities	PE-3, PE-5	PR.AC-2, PR.DS-4	
A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.4 Protecting against external and environmental threats	Physical Controls	7.5 Protecting against physical and environmental threats	CP-6, CP-7, PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23	ID.BE-5, PR.AC-2, PR.DS-5, PR.IP-5	
A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.5 Working in secure areas	Physical Controls	7.6 Working in secure areas	AC-19(4), SC-42*	PR.AC-2, PR.DS-5	
A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.6 Delivery and loading areas	Physical Controls	7.2 Physical entry controls	PE-16	PR.AC-2	
A.11 Physical and environmental security	A.11.2 Equipment	A.11.2.1 Equipment siting and protection	Physical Controls	7.8 Equipment siting and protection	PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23	PR.AC-2, PR.DS-5, PR.IP-5	
A.11 Physical and environmental security	A.11.2 Equipment	A.11.2.2 Supporting utilities	Physical Controls	7.11 Supporting utilities	CP-8, PE-9, PE-10, PE-11, PE-12, PE-14, PE-15	PR.IP-5	
A.11 Physical and environmental security	A.11.2 Equipment	A.11.2.3 Cabling security	Physical Controls	7.12 Cabling security	PE-4, PE-9	ID.BE-4, PR.AC-2, PR.IP-5	
A.11 Physical and environmental security	A.11.2 Equipment	A.11.2.4 Equipment maintenance	Physical Controls	7.13 Equipment maintenance	MA-2, MA-6	ID.BE-4, PR.DS-7, PR.DS-8, PR.MA-1, PR.MA-2	
A.11 Physical and environmental security	A.11.2 Equipment	A.11.2.5 Removal of assets		DELETED	MA-2, MP-5, PE-16	ID.AM-4, PR.AC-2, PR.DS-3, PR.MA-1	
A.11 Physical and environmental security	A.11.2 Equipment	A.11.2.6 Security of equipment and assets off-premises	Physical Controls	7.9 Security of assets off-premises	AC-19, AC-20, MP-5, PE-17	PR.AC-2, PR.AC-3, PR.MA-1	

Control Mapping

ISO 27002:2013			ISO 27002:2022		NIST SP 800-53	NIST CSF	CIS Critical Security Controls v8
Domain	**Control Objective**	**Control**	**Control Theme**	**Control ID**	**Control ID** Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control	**Control-ID**	**CIS Safeguard**
A.11 Physical and environmental security	A.11.2 Equipment	A.11.2.7 Secure disposal or reuse of equipment	Physical Controls	7.14 Secure disposal or reuse of equipment	MP-6	PR.AC-2, PR.DS-3, PR.IP-6	3,5
A.11 Physical and environmental security	A.11.2 Equipment	A.11.2.8 Unattended user equipment		8.1 User endpoint devices	AC-11	PR.AC-2	3,1;3,6;4,1;4,5;4,11;4,12;9,1;10,1;10,7;12,7;13,5
A.11 Physical and environmental security	A.11.2 Equipment	A.11.2.9 Clear desk and clear screen policy	Physical Controls	7.7 Clear desk and clear screen policy	AC-11, MP-2, MP-4	PR.PT-2	
A.12 Operations security	A.12.1 Operational procedures and responsibilities	A.12.1.1 Documented operating procedures	Organisational Controls	5.37 Documented operating procedures	All XX-1 controls, SA-5	DE.AE-1	
A.12 Operations security	A.12.1 Operational procedures and responsibilities	A.12.1.2 Change management	Technological Controls	8.32 Change management	CM-3, CM-5, SA-10	PR.IP-1, PR.IP-3, DE.AE-1	
A.12 Operations security	A.12.1 Operational procedures and responsibilities	A.12.1.3 Capacity management	Technological Controls	8.6 Capacity management	AU-4, CP-2(2), SC-5(2)	ID.BE-4	8,3
A.12 Operations security	A.12.1 Operational procedures and responsibilities	A.12.1.4 Separation of development, testing, and operational environments	Technological Controls	8.31 Separation of development, test, and production environments	CM-4(1), CM-5*	PR.DS-7	16,8
A.12 Operations security	A.12.2 Protection from malware	A.12.2.1 Controls against malware	Technological Controls	8.7 Protection against malware	AT-2, SI-3	PR.AT-1, PR.DS-6, DE.CM-4, RS.MI-1, RS.MI-2	2,5;9,3;9,7;10,1;10,2;10,4;10,5;10,6;14,2
A.12 Operations security	A.12.3 Backup	A.12.3.1 Information backup	Technological Controls	8.13 Information backup	CP-9	PR.IP-4	11,1;11,2;11,3;11,4;11,5
A.12 Operations security	A.12.4 Logging and monitoring	A.12.4.1 Event logging	Technological Controls	8.15 Logging	AU-3, AU-6, AU-11, AU-12, AU-14	PR.PT-1, DE.AE-2, DE.AE-3, DE.CM-3, DE.CM-7, RS.AN-1	3,14;8,1;8,2;8,5;8,8;13,1;13,6
A.12 Operations security	A.12.4 Logging and monitoring	A.12.4.2 Protection of log information	Technological Controls	8.15 Logging	AU-9	PR.PT-1	3,14;8,1;8,2;8,5;8,8;13,1;13,6
A.12 Operations security	A.12.4 Logging and monitoring	A.12.4.3 Administrator and operator logs	Technological Controls	8.15 Logging	AU-9, AU-12	PR.PT-1, DE.CM-3, RS.AN-1	3,14;8,1;8,2;8,5;8,8;13,1;13,6
A.12 Operations security	A.12.4 Logging and monitoring	A.12.4.4 Clock synchronization	Technological Controls	8.17 Clock synchronization	AU-8	PR.PT-1	8,4
A.12 Operations security	A.12.5 Control of operational software	A.12.5.1 Installation of software on operational systems	Technological Controls	8.19 Installation of software on operational systems	CM-5, CM-7(4), CM-7(5), CM-11	ID.AM-2, PR.DS-6, PR.IP-1, PR.IP-3, DE.CM-5	2,5;2,6
A.12 Operations security	A.12.6 Technical vulnerability management	A.12.6.1 Management of technical vulnerabilities	Technological Controls	8.8 Management of technical vulnerabilities	RA-3, RA-5, SI-2, SI-5	ID.RA-1, ID.RA-5, PR.IP-12, DE.CM-8, RS.MI-3	1,1;7,1;7,2;7,3;7,4;7,5;7,6;7,7;13,7;13,8;13,9;13,10;16,2;16,3;16,6;16,7;16,13;18,1;18,2;18,3;18,4;18,5
A.12 Operations security	A.12.6 Technical vulnerability management	A.12.6.2 Restrictions on software installation	Technological Controls	8.19 Installation of software on operational systems	CM-11	PR.IP-1, PR.IP-3, DE.CM-5	2,5;2,6
A.12 Operations security	A.12.7 Information systems audit considerations	A.12.7.1 Information systems audit controls	Technological Controls	8.34 Protection of information systems during audit testing	AU-5*	PR.PT-1	
A.13 Communications security	A.13.1 Network security management	A.13.1.1 Network controls	Technological Controls	8.20 Network controls	AC-3, AC-17, AC-18, AC-20, SC-7, SC-8, SC-10	PR.AC-3, PR.AC-5, PR.DS-2, PR.DS-5, PR.PT-4, DE.AE-1	3,12;8,2
A.13 Communications security	A.13.1 Network security management	A.13.1.2 Security of network services	Technological Controls	8.21 Security of network services	CA-3, SA-9	DE.AE-1	12,3;12,6;12,7;13,3
A.13 Communications security	A.13.1 Network security management	A.13.1.3 Segregation in networks	Technological Controls	8.23 Segregation in networks	AC-4, SC-7	PR.AC-5, PR.DS-5	9,2;9,3
A.13 Communications security	A.13.2 Information transfer	A.13.2.1 Information transfer policies and procedures	Organisational Controls	5.14 Information transfer	AC-4, AC-17, AC-18, AC-19, AC-20, CA-3, PE-17, SC-7, SC-8, SC-15	ID.AM-3, PR.AC-3, PR.AC-5, PR.DS-2, PR.DS-5, PR.PT-4	3,8;3,9;3,10;3,13
A.13 Communications security	A.13.2 Information transfer	A.13.2.2 Agreements on information transfer	Organisational Controls	5.14 Information transfer	CA-3, PS-6, SA-9	ID.AM-3	3,8;3,9;3,10;3,13
A.13 Communications security	A.13.2 Information transfer	A.13.2.3 Electronic messaging	Organisational Controls	5.14 Information transfer	SC-8	PR.DS-2, PR.DS-5	3,8;3,9;3,10;3,13
A.13 Communications security	A.13.2 Information transfer	A.13.2.4 Confidentiality or nondisclosure agreements	People Controls	6.6 Confidentiality or nondisclosure agreements	PS-6	PR.DS-5	
A.14 System acquisition, development and maintenance	A.14.1 Security requirements of information systems	A.14.1.1 Information security requirements analysis and specification	Organisational Controls	5.8 Information security in project management	PL-2, PL-7, PL-8, SA-3, SA-4	PR.IP-2	16,1
A.14 System acquisition, development and maintenance	A.14.1 Security requirements of information systems	A.14.1.2 Securing application services on public networks	Technological Controls	8.26 Application security requirements	AC-3, AC-4, AC-17, SC-8, SC-13	PR.AC-5, PR.DS-2, PR.DS-5, PR.DS-6	16,4;16,5;16,11
A.14 System acquisition, development and maintenance	A.14.1 Security requirements of information systems	A.14.1.3 Protecting application services transactions	Technological Controls	8.26 Application security requirements	AC-3, AC-4, SC-7, SC-8, SC-13	PR.AC-5, PR.DS-2, PR.DS-5, PR.DS-6, PR.PT-4	16,4;16,5;16,11
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.1 Secure development policy	Technological Controls	8.25 Secure development lifecycle	SA-3, SA-15, SA-17	PR.IP-2	16,1;16,11;16,12
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.2 System change control procedures	Technological Controls	8.32 Change management	CM-3, SA-10, SI-2	PR.IP-1, PR.IP-3	
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.3 Technical review of applications after operating platform changes	Technological Controls	8.32 Change management	CM-3, CM-4, SI-2	PR.IP-1, PR.IP-3, PR.IP-12	
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.4 Restrictions on changes to software packages	Technological Controls	8.32 Change management	CM-3, SA-10	PR.DS-6, PR.IP-1, PR.IP-3	
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.5 Secure system engineering principles	Technological Controls	8.27 Secure system architecture and engineering principles	SA-8	PR.IP-2	16,10
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.6 Secure development environment	Technological Controls	8.31 Separation of development, test, and production environments	SA-3*		16,8
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.7 Outsourced development	Technological Controls	8.30 Outsourced development	SA-4, SA-10, SA-11, SA-15, SR-2, SR-4	DE.CM-6, DE.CM-7	16,4
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.8 System security testing	Technological Controls	8.29 Security testing in development and acceptance	CA-2, SA-11	DE.DP-3	16,12;16,13;16,14
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.9 System acceptance testing	Technological Controls	8.29 Security testing in development and acceptance	SA-4, SR-5(2)		
A.14 System acquisition, development and maintenance	A.14.3 Test data	A.14.3.1 Protection of test data	Technological Controls	8.33 Test information	SA-15(9)*		
A.15 Supplier Relationships	A.15.1 Information security in supplier relationships	A.15.1.1 Information security policy for supplier relationships	Organisational Controls	5.19 Information security policy for supplier relationships	SR-1	ID.BE-1, ID.GV-2, ID.SC-1, ID.SC-3, PR.MA-2	15,1;15,2;15,3;15,5;15,6;15,7
A.15 Supplier Relationships	A.15.1 Information security in supplier relationships	A.15.1.2 Address security within supplier agreements	Organisational Controls	5.20 Address security within supplier agreements	SA-4, SR-3	ID.BE-1, ID.SC-1, ID.SC-3	15,2;15,4;15,6;15,7;17,2
A.15 Supplier Relationships	A.15.1 Information security in supplier relationships	A.15.1.3 Information and communication technology supply chain	Organisational Controls	5.21 Managing information security in the ICT supply chain	SR-3, SR-5	ID.BE-1, ID.SC-1, ID.SC-3	15,4;15,6
A.15 Supplier Relationships	A.15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	Organisational Controls	5.22 Monitoring, review, and change management of supplier services	SA-9, SR-6	ID.BE-1, ID.SC-1, ID.SC-2, ID.SC-4, PR.MA-2, DE.CM-6, DE.CM-7	15,5;15,6
A.15 Supplier Relationships	A.15.2 Supplier service delivery management	A.15.2.2 Managing changes to supplier services	Organisational Controls	5.22 Monitoring, review, and change management of supplier services	RA-9, SA-9, SR-7	ID.BE-1, ID.SC-1, ID.SC-2, ID.SC-4	15,5;15,6

Control Mapping

ISO 27002:2013			ISO 27002:2022		NIST SP 800-53	NIST CSF	CIS Critical Security Controls v8
Domain	**Control Objective**	**Control**	**Control Theme**	**Control ID**	**Control ID** Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control	**Control-ID**	**CIS Safeguard**
A.16 Information security incident management	A.16.1 Managing of information security incidents and improvements	A.16.1.1 Responsibilities and procedures	Organisational Controls	5.24 Information security incident management planning and preparation	IR-8	PR.IP-9, DE.AE-2, RS.CO-1	17,1;17,2;17,4;17,5;17,6;17,8;17,9
A.16 Information security incident management	A.16.1 Managing of information security incidents and improvements	A.16.1.2 Reporting information security events	People Controls	6.8 Information security event reporting	AU-6, IR-6	DE.DP-4, RS.CO-2, RS.CO-3	14,6;17,3
A.16 Information security incident management	A.16.1 Managing of information security incidents and improvements	A.16.1.3 Reporting information security weaknesses	People Controls	6.8 Information security event reporting	SI-2	PR.IP-12, DE.DP-4	14,6;17,3
A.16 Information security incident management	A.16.1 Managing of information security incidents and improvements	A.16.1.4 Assessment of and decision on information security events	Organisational Controls	5.25 Assessment and decision on information security events	AU-6, IR-4	DE.AE-2, DE.AE-4, DE.AE-5, RS.AN-2, RS.AN-4	8,11;17,9
A.16 Information security incident management	A.16.1 Managing of information security incidents and improvements	A.16.1.5 Response to information security incidents	Organisational Controls	5.26 Response to information security incidents	IR-4	RS.RP-1, RS.AN-1, RS.MI-1, RS.MI-2, RC.RP-1	17,4
A.16 Information security incident management	A.16.1 Managing of information security incidents and improvements	A.16.1.6 Learning from information security incidents	Organisational Controls	5.27 Learning from information security incidents	IR-4	ID.RA-4, PR.IP-7, PR.IP-8, DE.DP-5, RS.AN-2, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2	17,8
A.16 Information security incident management	A.16.1 Managing of information security incidents and improvements	A.16.1.7 Collection of evidence	Organisational Controls	5.28 Collection of evidence	AU-4, AU-9, AU-10(3), AU-11*	DE.AE-3, RS.AN-3	8,5;8,10
A.17 Information security aspects of business continuity management	A.17.1 Information security continuity	A.17.1.1 Planning information security continuity	Organisational Controls	5.29 Information security during disruption	CP-2	ID.BE-5, PR.IP-9	
A.17 Information security aspects of business continuity management	A.17.1 Information security continuity	A.17.1.2 Implementing information security continuity	Organisational Controls	5.29 Information security during disruption	CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13	ID.BE-5, PR.IP-4, PR.IP-9, PR.PT-5	
A.17 Information security aspects of business continuity management	A.17.1 Information security continuity	A.17.1.3 Verify, review, and evaluate information security continuity	Organisational Controls	5.29 Information security during disruption	CP-4	PR.IP-4, PR.IP-9, PR.IP-10	
A.17 Information security aspects of business continuity management	A.17.2 Redundancies	A.17.2.1 Availability of information processing facilities		8.14 Redundancy of information processing facilities	CP-2,CP-6, CP-7	ID.BE-5, PR.DS-4, PR.PT-5	
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.1 Identification of applicable legislation and contractual requirements	Organisational Controls	5.31 Identification of applicable legislation and contractual requirements	All XX-1 controls	ID.GV-3	
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.2 Intellectual property rights	Organisational Controls	5.32 Intellectual property rights	CM-10	ID.GV-3	
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.3 Protection of records	Organisational Controls	5.33 Protection of records	AC-3, AC-23, AU-9, AU-10, CP-9, SC-8, SC-8(1), SC-13, SC-28, SC-28(1)	ID.GV-3, PR.IP-4	3,4;3,7;3,11
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.4 Privacy and protection of personal information	Organisational Controls	5.34 Privacy and protection of PII	Appendix J Privacy controls	ID.GV-3, PR.AC-7, DE.DP-2	
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.5 Regulation of cryptographic controls	Organisational Controls	5.31 Identification of applicable legislation and contractual requirements	IA-7, SC-12, SC-13, SC-17	ID.GV-3	
A.18 Compliance	A.18.2 Information security reviews	A.18.2.1 Independent review of information security	Organisational Controls	5.35 Independent review of information security	CA-2(1), SA-11(3)		
A.18 Compliance	A.18.2 Information security reviews	A.18.2.2 Compliance with security policies and standards	Organisational Controls	5.36 Compliance with security policies and standards	All XX-1 controls, CA-2	PR.IP-12, DE.DP-2	
A.18 Compliance	A.18.2 Information security reviews	A.18.2.3 Technical compliance review	Organisational Controls	5.36 Compliance with security policies and standards 8.8 Management of technical vulnerabilities	CA-2	ID.RA-1, PR.IP-12, DE.DP-2	1,1
		NEW	Organisational Controls	5.7 Threat intelligence			13,11
		NEW	Physical Controls	7.4 Physical security monitoring			
		NEW	Technological Controls	8.16 Monitoring activities			13,2;13,3;13,4;13,6
		NEW	Technological Controls	8.9 Configuration management			4,1;4,2;4,3;4,7;4,8
		NEW	Technological Controls	8.10 Information deletion			4,11
		NEW	Technological Controls	8.11 Data masking			
		NEW	Technological Controls	8.12 Data leakage prevention			3,7;3,13;11,3
		NEW	Technological Controls	8.22 Web filtering			3,12;12,2;12,8;13,4
		NEW	Technological Controls	8.28 Secure coding			16,1;16,9;16,12
		NEW	Organisational Controls	5.23 Information security for use of cloud services			15,2;15,4;15,5
		NEW	Organisational Controls	5.30 ICT readiness for business continuity			17,7