

Control Mapping

ISO 27002:2013			ISO 27002:2022	NIST SP 800-53	NIST CSF	CIS Critical Security Controls v8
Domain	Control Objective	Control	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	8.24 Use of cryptography	SC-13	PR.DS-5	
A.10 Cryptography	A.10.1 Cryptographic controls	A.10.1.2 Key Management	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	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	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	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	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	7.6 Working in secure areas	AC-19(4), SC-42*	PR.AC-2, PR.DS-5	