NIS2 vs ISO 27001:2022 vs CIS v8

NIS 2	ISO 27001:2022	CIS Controls v8			
Legislation article	ISMS and/or Annex A	CIS Safe-guard	Asset Type	Security Function	Title
Article 21.2 a) **Policies on risk analysis and information system security**	**ISMS:** 5.2 Policy	1,1	Devices	**Identify**	Establish and Maintain Detailed Enterprise Asset Inventory
	6.1.2 Information security risk assessment	1,2	Devices	Respond	Address Unauthorized Assets
	6.1.3 Information security risk treatment	2,1	Applications	Identify	Establish and Maintain a Software Inventory
	8.2 Information security risk assessment	2,2	Applications	Identify	Ensure Authorized Software is Currently Supported
	8.3 Information security risk treatment	2,3	Applications	Respond	Address Unauthorized Software
	Annex A. Information security controls reference:	3,1	Data	Identify	Establish and Maintain a Data Management Process
	· 5.1 Policies for information security	3,2	Data	Identify	Establish and Maintain a Data Inventory
	· 5.2 Information security roles and responsibilities	4,1	Applications	Protect	Establish and Maintain a Secure Configuration Process
	· 5.7 Threat intelligence	4,2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure
	· 5.37 Documented operating procedures	7,1	Applications	Protect	Establish and Maintain a Vulnerability Management Process
		7,2	Applications	Respond	Establish and Maintain a Remediation Process
		8,1	Network	Protect	Establish and Maintain an Audit Log Management Process
		11,1	Data	Recover	Establish and Maintain a Data Recovery Process
		14,1	N/A	Protect	Establish and Maintain a Security Awareness Program
		15,2	N/A	Identify	Establish and Maintain a Service Provider Management Policy
		16,1	Applications	Protect	Establish and Maintain a Secure Application Development Process
		17,4	N/A	Respond	Establish and Maintain an Incident Response Process
		18,1	N/A	Identify	Establish and Maintain a Penetration Testing Program
Article 21.2 b) **Incident handling**	**Annex A. Information security controls reference:**	17,1	N/A	Respond	Designate Personnel to Manage Incident Handling
	· 5.24 Information security incident management planning and preparation	17,2	N/A	Respond	Establish and Maintain Contact Information for Reporting Security Incidents
	· 5.25 Assessment and decision on information security events	17,3	N/A	Respond	Establish and Maintain an Enterprise Process for Reporting Incidents
	· 5.26 Response to information security incidents	17,4	N/A	Respond	Establish and Maintain an Incident Response Process
	· 5.27 Learning from information security incidents	17,5	N/A	Respond	Assign Key Roles and Responsibilities
	· 5.28 Collection of evidence	17,6	N/A	Respond	Define Mechanisms for Communicating During Incident Response
	· 6.8 Information security event reporting	17,7	N/A	Recover	Conduct Routine Incident Response Exercises
	· 8.15 Logging	17,8	N/A	Recover	Conduct Post-Incident Reviews
	· 8.16 Monitoring activities	17,9	N/A	Recover	Establish and Maintain Security Incident Thresholds
		8,2	Network	Detect	Collect Audit Logs
		8,5	Network	Detect	Collect Detailed Audit Logs
		8,9	Network	Detect	Centralize Audit Logs
		8,1	Network	Protect	Retain Audit Logs
Article 21.2 c) **Business continuity, such as backup management and disaster recovery, and crisis management**	**Annex A. Information security controls reference:**	11,1	Data	Recover	Establish and Maintain a Data Recovery Process
	· 5.29 Information security during disruption	11,2	Data	Recover	Perform Automated Backups
	· 5.30 ICT readiness for business continuity	11,3	Data	Protect	Protect Recovery Data
	· 5.37 Documented operating procedures	11,4	Data	Recover	Establish and Maintain an Isolated Instance of Recovery Data
	· 8.13 Information backup	11,5	Data	Recover	Test Data Recovery
	· 8.14 Redundancy of information processing facilities	17,1	N/A	Respond	Designate Personnel to Manage Incident Handling
		17,4	N/A	Respond	Establish and Maintain an Incident Response Process
		17,5	N/A	Respond	Assign Key Roles and Responsibilities
		17,6	N/A	Respond	Define Mechanisms for Communicating During Incident Response
Article 21.2 d) **Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers**	**Annex A. Information security controls reference:**	8,12	Data	Detect	Collect Service Provider Logs

NIS2 vs ISO 27001:2022 vs CIS v8

NIS 2	ISO 27001:2022	CIS Controls v8			
	· 5.19 Information security in supplier relationships	15,1	N/A	Identify	Establish and Maintain an Inventory of Service Providers
	· 5.20 Addressing information security within supplier agreements	15,2	N/A	Identify	Establish and Maintain a Service Provider Management Policy
	· 5.21 Managing information security in the ICT supply chain	15,3	N/A	Identify	Classify Service Providers
	· 5.22 Monitoring, review and change management of supplier services	15,4	N/A	Protect	Ensure Service Provider Contracts Include Security Requirements
	· 5.23 Information security for use of cloud services	15,5	N/A	Identify	Assess Service Providers
		15,6	Data	Detect	Monitor Service Providers
		15,7	Data	Protect	Securely Decommission Service Providers
Article 21.2 e) **Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure**	**Annex A. Information security controls reference:**	4,1	Applications	Protect	Establish and Maintain a Secure Configuration Process
	· 5.37 Documented operating procedures	4,2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure
	· 8.8 Management of technical vulnerabilities	4,3	Users	Protect	Configure Automatic Session Locking on Enterprise Assets
	· 8.9 Configuration management	4,4	Devices	Protect	Implement and Manage a Firewall on Servers
	· 8.19 Installation of software on operational systems	4,5	Devices	Protect	Implement and Manage a Firewall on End-User Devices
	· 8.20 Network security	4,6	Network	Protect	Securely Manage Enterprise Assets and Software
	· 8.21 Security of network services	4,7	Users	Protect	Manage Default Accounts on Enterprise Assets and Software
		4,8	Devices	Protect	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
		4,9	Devices	Protect	Configure Trusted DNS Servers on Enterprise Assets
		4,10	Devices	Respond	Enforce Automatic Device Lockout on Portable End-User Devices
		4,11	Devices	Protect	Enforce Remote Wipe Capability on Portable End-User Devices
		4,12	Devices	Protect	Separate Enterprise Workspaces on Mobile End-User Devices
		7,1	Applications	Protect	Establish and Maintain a Vulnerability Management Process
		7,2	Applications	Respond	Establish and Maintain a Remediation Process
		7,3	Applications	Protect	Perform Automated Operating System Patch Management
		7,4	Applications	Protect	Perform Automated Application Patch Management
		7,5	Applications	Identify	Perform Automated Vulnerability Scans of Internal Enterprise Assets
		7,6	Applications	Identify	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
		7,7	Applications	Respond	Remediate Detected Vulnerabilities
		12,1	Network	Protect	Ensure Network Infrastructure is Up-to-Date
		12,2	Network	Protect	Establish and Maintain a Secure Network Architecture
		12,3	Network	Protect	Securely Manage Network Infrastructure
		12,6	Network	Protect	Use of Secure Network Management and Communication Protocols
		12,7	Devices	Protect	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure
		12,8	Devices	Protect	Establish and Maintain Dedicated Computing Resources for All Administrative Work
		13,1	Network	Detect	Centralize Security Event Alerting
		13,2	Devices	Detect	Deploy a Host-Based Intrusion Detection Solution
		13,3	Network	Detect	Deploy a Network Intrusion Detection Solution
		13,4	Network	Protect	Perform Traffic Filtering Between Network Segments
		13,5	Devices	Protect	Manage Access Control for Remote Assets
		13,6	Network	Detect	Collect Network Traffic Flow Logs
Article 21.2 f) **Policies and procedures to assess the effectiveness of cybersecurity risk-management measures**	**ISMS:** 9.1 Monitoring, measurement, analysis and evaluation	18,1	N/A	Identify	Establish and Maintain a Penetration Testing Program

NIS2 vs ISO 27001:2022 vs CIS v8

NIS 2	ISO 27001:2022	CIS Controls v8			
	9.2 Internal audit	18,2	Network	Identify	Perform Periodic External Penetration Tests
	9.3 Management review	18,3	Network	Protect	Remediate Penetration Test Findings
	Annex A. Information security controls reference:	18,4	Network	Protect	Validate Security Measures
	· 5.35 Independent review of information security	18,5	N/A	Identify	Perform Periodic Internal Penetration Tests
	· 5.36 Compliance with policies, rules and standards for information security	16,3	Applications	Protect	Perform Root Cause Analysis on Security Vulnerabilities
		11,5	Data	Recover	Test Data Recovery
Article 21.2 g) **Basic computer hygiene practices and cybersecurity training**	**ISMS:** 7.2 Competence	1,1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory
	7.3 Awareness	1,2	Devices	Respond	Address Unauthorized Assets
	7.4 Communication	2,1	Applications	Identify	Establish and Maintain a Software Inventory
	Annex A. Information security controls reference:	2,2	Applications	Identify	Ensure Authorized Software is Currently Supported
	· 6.3 Information security awareness, education and training	2,3	Applications	Respond	Address Unauthorized Software
		3,2	Data	Identify	Establish and Maintain a Data Inventory
		3,3	Data	Protect	Configure Data Access Control Lists
		4,1	Applications	Protect	Establish and Maintain a Secure Configuration Process
		4,2	Network	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure
		4,3	Users	Protect	Configure Automatic Session Locking on Enterprise Assets
		4,4	Devices	Protect	Implement and Manage a Firewall on Servers
		4,5	Devices	Protect	Implement and Manage a Firewall on End-User Devices
		4,6	Network	Protect	Securely Manage Enterprise Assets and Software
		5,1	Users	Identify	Establish and Maintain an Inventory of Accounts
		5,2	Users	Protect	Use Unique Passwords
		5,3	Users	Respond	Disable Dormant Accounts
		5,4	Users	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts
		6,1	Users	Protect	Establish an Access Granting Process
		6,2	Users	Protect	Establish an Access Revoking Process
		6,3	Users	Protect	Require MFA for Externally-Exposed Applications
		6,4	Users	Protect	Require MFA for Remote Network Access
		6,5	Users	Protect	Require MFA for Administrative Access
		8,2	Network	Detect	Collect Audit Logs
		9,1	Applications	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients
		9,2	Network	Protect	Use DNS Filtering Services
		10,1	Devices	Protect	Deploy and Maintain Anti-Malware Software
		10,2	Devices	Protect	Configure Automatic Anti-Malware Signature Updates
		10,3	Devices	Protect	Disable Autorun and Autoplay for Removable Media
		11,1	Data	Recover	Establish and Maintain a Data Recovery Process
		11,2	Data	Recover	Perform Automated Backups
		14,1	N/A	Protect	Establish and Maintain a Security Awareness Program
		14,9	N/A	Protect	Conduct Role-Specific Security Awareness and Skills Training
Article 21.2 h) **Policies and procedures regarding the use of cryptography and, where appropriate, encryption**	**Annex A. Information security controls reference:**	3,6	Devices	Protect	Encrypt Data on End-User Devices
	· 8.24 Use of cryptography	3,9	Data	Protect	Encrypt Data on Removable Media
		3,10	Data	Protect	Encrypt Sensitive Data in Transit
		3,11	Data	Protect	Encrypt Sensitive Data at Rest
		4,9	Devices	Protect	Configure Trusted DNS Servers on Enterprise Assets
		12,3	Network	Protect	Securely Manage Network Infrastructure
		12,6	Network	Protect	Use of Secure Network Management and Communication Protocols

NIS2 vs ISO 27001:2022 vs CIS v8

NIS 2	ISO 27001:2022	CIS Controls v8			
		12,7	Devices	Protect	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure
Article 21.2 i) **Human resources security, access control policies and asset management**	ISMS:	5,1	Users	Identify	Establish and Maintain an Inventory of Accounts
	Annex A. Information security controls reference:	5,2	Users	Protect	Use Unique Passwords
	· 5.2 Information security roles and responsibilities	5,3	Users	Respond	Disable Dormant Accounts
	· 5.3 Segregation of duties	5,4	Users	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts
	· 6.1 Screening	5,5	Users	Identify	Establish and Maintain an Inventory of Service Accounts
	· 6.2 Terms and conditions of employment	5,6	Users	Protect	Centralize Account Management
	· 6.3 Information security awareness, education and training	6,1	Users	Protect	Establish an Access Granting Process
	· 6.4 Disciplinary process	6,2	Users	Protect	Establish an Access Revoking Process
	· 6.5 Responsibilities after termination or change of employment	6,3	Users	Protect	Require MFA for Externally-Exposed Applications
	· 6.6 Confidentiality or non-disclosure agreements	6,4	Users	Protect	Require MFA for Remote Network Access
	· 6.7 Remote working	6,5	Users	Protect	Require MFA for Administrative Access
	· 7.7 Clear desk and clear screen	6,6	Users	Identify	Establish and Maintain an Inventory of Authentication and Authorization Systems
		6,7	Users	Protect	Centralize Access Control
	· 5.15 Access control	6,8	Data	Protect	Define and Maintain Role-Based Access Control
	· 5.16 Identity management	13,9	Devices	Protect	Deploy Port-Level Access Control
	· 5.17 Authentication information				
	· 5.18 Access rights				
	· 8.2 Privileged access rights				
	· 8.3 Information access restriction				
	· 8.4 Access to source code				
	· 8.5 Secure authentication				
	· 5.9 Inventory of information and other associated assets				
	· 5.10 Acceptable use of information and other associated assets				
	· 5.11 Return of assets				
	· 7.9 Security of assets off-premises				
	· 7.10 Storage media				
	· 7.14 Secure disposal or re-use of equipment				
	· 8.1 User endpoint devices				
Article 21.2 j) **The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems within the entity, where appropriate**	**Annex A. Information security controls reference:**	6,3	Users	Protect	Require MFA for Externally-Exposed Applications
	· 5.14 Information transfer	6,4	Users	Protect	Require MFA for Remote Network Access
	· 5.16 Identity management	6,5	Users	Protect	Require MFA for Administrative Access
	· 5.17 Authentication information	6,6	Users	Identify	Establish and Maintain an Inventory of Authentication and Authorization Systems
	· 8.5 Secure authentication	6,7	Users	Protect	Centralize Access Control
		17,6	N/A	Respond	Define Mechanisms for Communicating During Incident Response
Other					
Article 21.3 **Secure development procedures…**	**Annex A. Information security controls reference:**				
	· 8.25 Secure development life cycle				
	· 8.26 Application security requirements				
	· 8.27 Secure system architecture and engineering principles				
	· 8.28 Secure coding				
	· 8.29 Security testing in development and acceptance				
	· 8.30 Outsourced development				
	· 8.31 Separation of development, test and production environments				
	· 8.32 Change management				
	· 8.33 Test information				
Article 21.4 Appropriate and proportionate corrective measures (if not comply)	10.2 Nonconformity and corrective action				

By: Harry van der Plas, CISO, LA 27001
www.management-projects.nl

Sources: Andrey Prozorov,
www.patreon.com

Laura Kata & Tom Moester
www.huntandhackett.com

ISO organisation
Enisa EU, NIS2

NIS2 vs ISO 27001:2022 vs CIS v8

NIS 2	ISO 27001:2022	CIS Controls v8