



# NIS2 to ISO/IEC 27001 Mapping Tool



**Achieving compliance with the NIS2 Directive is a priority for organizations within its scope. This process requires a thorough understanding of cybersecurity measures and a structured approach to implementation. To support your efforts, we've developed an easy-to-use mapping tool that connects NIS2 requirements with the ISO/IEC 27001:2022 standard.**

Our tool uses ISO/IEC 27001 as the basis for assessing and improving cybersecurity practices, focusing on Annex A controls to identify synergies and gaps in compliance. These controls are critical to mitigating information security risks and demonstrating compliance with both ISO/IEC 27001 and NIS2.

It's important to start preparing for NIS2 compliance early, as implementation of the directive's requirements typically takes 1 to 3 years. Whether you're starting your compliance journey or refining existing practices, this resource is designed to simplify the process and accelerate your progress.

We encourage you to use our mapping tool to gain a clearer understanding of the NIS2 measures and how they align with your existing processes.

Take the next step towards NIS2 compliance, manage your compliance journey effectively and protect your information assets.

Contact us to get NIS2  
compliance support:  
[marketing.italy@bsigroup.com](mailto:marketing.italy@bsigroup.com)

NIS2 Measures	ISO/IEC 27001	
Article 20: Governance		
	<b>Annex A</b>	
	A.5.1	Policies for information security
	A.5.31	Legal, statutory, regulatory and contractual requirements
	A.5.34	Privacy and protection of personal Identifiable information (PII)
	A.5.35	Independent review of information security
	A.5.36	Compliance with policies, rules and standards for information security
	A.6.3	Information security awareness, education and training
Article 21: Cyber security risk management measures		
<b>(A)</b> Policies on risk analysis and information system security	5.2	Information security policy
	6.1.2	Information security risk assessment process
	6.1.3	Information security risk treatment process
	8.2	Information security risk assessment
	8.3	Information security risk treatment
	<b>Annex A</b>	
	A.5.1	Policies for information security
<b>(B)</b> Incident handling	<b>Annex A</b>	
	A.5.24	Information security incident management planning and preparation
	A.5.25	Assessment and decision on information security events
	A.5.26	Response to information security incidents
	A.5.27	Learning from information security incidents
	A.5.28	Collection of evidence
	A.6.8	Information security event reporting
	A.8.16	Monitoring activities

NIS2 Measures	ISO/IEC 27001	
<b>Article 21: Cyber security risk management measures (cont.)</b>		
<b>(C)</b> Business continuity, such as backup management and disaster recovery, and crisis management	<b>Annex A</b>	
	A.5.29	Information security during disruption
	A.5.30	ICT readiness for business continuity
	A.8.13	Information backup
	A.8.14	Redundancy of information processing facilities
	A.8.15	Logging
<b>(D)</b> Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	<b>Annex A</b>	
	A.5.19	Information security in supplier relationships
	A.5.20	Addressing information security within supplier agreements
	A.5.21	Managing information security in the ICT supply chain
	A.5.22	Monitoring, review and change management of supplier services
<b>(E)</b> Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	<b>Annex A</b>	
	A.5.20	Addressing information security within supplier agreements
	A.5.24	Information security incident management planning and preparation
	A.5.37	Documented operating procedures
	A.6.8	Information security event reporting
	A.8.8	Management of technical vulnerabilities
	A.8.9	Configuration management
	A.8.20	Network security
	A.8.21	Security of network services

NIS2 Measures	ISO/IEC 27001	
<b>Article 21: Cyber security risk management measures (cont.)</b>		
<b>(F)</b> Policies and procedures to assess the effectiveness of cybersecurity risk- management measures	9.1	Monitoring, measurement, analysis and evaluation
	9.2	Internal audit
	9.3	Management review
	<b>Annex A</b>	
	A.5.35	Independent review of information security
	A.5.36	Compliance with policies, rules and standards for information security
<b>(G)</b> Basic cyber hygiene practices and cybersecurity training	7.3	Awareness
	7.4	Communication
	<b>Annex A</b>	
	A.5.15	Access control
	A.5.16	Identity management
	A.5.18	Access rights
	A.5.24	Information security incident management planning and preparation
	A.6.3	Information security awareness, education and training
	A.6.5	Responsibilities after termination of change of employment
	A.6.8	Information security event reporting
	A.8.2	Privileged access rights
	A.8.3	Information access restriction
	A.8.5	Secure authentication
	A.8.7	Protection against malware
	A.8.9	Configuration management
	A.8.13	Information backup
	A.8.15	Logging
	A.8.19	Installation of software on operational systems
	A.8.22	Segregation of networks

NIS2 Measures	ISO/IEC 27001	
<b>Article 21: Cyber security risk management measures (cont.)</b>		
<b>(H)</b> Policies and procedures regarding the use of cryptography and, where appropriate, encryption	<b>Annex A</b>	
	A.8.24	Use of cryptography
<b>(I)</b> Human resources security, access control policies and asset management	<b>Annex A</b>	
	A.5.9	Inventory of information and other associated assets
	A.5.10	Acceptable use of information and other associated assets
	A.5.11	Return of assets
	A.5.15	Access control
	A.5.16	Identity management
	A.5.17	Authentication information
	A.5.18	Access rights
	A.6.1	Screening
	A.6.2	Terms and conditions of employment
	A.6.4	Disciplinary process
	A.6.5	Responsibilities after termination or change of employment
	A.6.6	Confidentiality or non-disclosure agreements
<b>(J)</b> The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate	<b>Annex A</b>	
	A.5.14	Information transfer
	A.5.16	Identity management
	A.5.17	Authentication information
<b>Article 23: Reporting obligations</b>		
	<b>Annex A</b>	
	A.5.14	Information transfer
	A.6.8	Information security event reporting
<b>Article 24: Use of European cyber-security certification schemes</b>		
	<b>Annex A</b>	
	A.5.20	Addressing information security within supplier agreements

Hunt & Hackett ISO Mapping tool:  
<https://www.huntandhackett.com/blog/iso-mapping-tool>

DNV's NIS2 and IEC 62443 Guidance:  
<https://www.dnv.com/cybersecurity/cyber-insights/leverage-iec-62443-for-eu-nis2-directive-compliance.html>