



NIS2 vs. ISO/IEC 27001: mapping tool



Gestire il passaggio al NIS2 ha implicazioni significative per le organizzazioni che rientrano nell'ambito della direttiva. Questa transizione spesso dura da 1 a 3 anni, evidenziando la necessità di avviare le misure essenziali con largo anticipo. Per semplificare questo processo, abbiamo sviluppato uno strumento di assessment facile da usare che mette in relazione i requisiti NIS2 con lo standard ISO/IEC 27001:2022.

Il nostro mapping tool utilizza lo standard ISO/IEC 27001 come comodo punto di partenza, offrendo utili informazioni sulle pratiche di cybersecurity dell'organizzazione. ISO/IEC 27001 stabilisce un framework di best practice, politiche, procedure e controlli per ridurre al minimo il rischio di violazioni della sicurezza delle informazioni. Quando si mettono in relazione le misure NIS2 con lo standard ISO/IEC 27001:2022, l'attenzione si concentra sull'Allegato A, che fornisce approfondimenti fondamentali dal punto di vista dei controlli.

L'Annex A dello standard ISO/IEC 27001:2022 delinea una serie di controlli di sicurezza fondamentali per dimostrare la conformità al punto 6.1.3 della ISO/IEC 27001 (Tratta-

mento dei rischi per la sicurezza delle informazioni) e alla relativa Dichiarazione di Applicabilità (Statement of Applicability).

Nella tabella sottostante è riportata la mappatura tra NIS2 e ISO/IEC 27001:2022. Il nostro tool è disegnato per semplificare il processo di allineamento, aiutando le organizzazioni a comprendere le sovrapposizioni e a identificare i gap tra i requisiti di conformità NIS2 e ISO/IEC 27001:2022.

Lavoriamo insieme per affrontare efficacemente la transizione e garantire la sicurezza del patrimonio informativo delle organizzazioni. Oltre alle risorse documentali, mettiamo a disposizione la nostra expertise: contattaci per ulteriori approfondimenti.

Contattarci, per avere supporto nella conformità NIS2:

marketing.italy@bsigroup.com

NIS2 Measures	ISO/IEC 27001	
Article 20: Governance		
	Annex A	
	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		
(A) 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
	Annex A	
	A.5.1	Policies for information security
(B) Incident handling	Annex A	
	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	
Article 21: Cyber security risk management measures (cont.)		
(C) Business continuity, such as backup management and disaster recovery, and crisis management	Annex A	
	A.5.29	Information security during disruption
	A.5.30	ICT readiness for business continuity
	A.8.13	Information backup
	A.8.14	Information backup
	A.8.15	Logging
A.8.16	Monitoring activities	
(D) Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	Annex A	
	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
A.5.23	Information security for use of cloud services	
(E) Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	Annex A	
	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	
Article 21: Cyber security risk management measures (cont.)		
(F) 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
	Annex A	
	A.5.35	Independent review of information security
	A.5.36	Compliance with policies, rules and standards for information security
(G) Basic cyber hygiene practices and cybersecurity training	7.3	Awareness
	7.4	Communication
	Annex A	
	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	
Article 21: Cyber security risk management measures (cont.)		
(H) Policies and procedures regarding the use of cryptography and, where appropriate, encryption	Annex A	
	A.8.24	Use of cryptography
(I) Human resources security, access control policies and asset management	Annex A	
	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	
(J) 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	Annex A	
	A.5.14	Information transfer
	A.5.16	Identity management
A.5.17	Authentication information	
Article 23: Reporting obligations		
	Annex A	
	A.5.14	Information transfer
	A.6.8	Information security event reporting
Article 24: Use of European cybersecurity certification schemes		
	Annex A	
	A.5.20	Addressing information security within supplier agreements