



NIS2 vs. ISO/IEC 27001: mapping tool



Per le organizzazioni che rientrano nel campo di applicazione della Direttiva NIS2, raggiungere la conformità è un obiettivo prioritario, che richiede una conoscenza approfondita delle misure di cybersecurity e un approccio strutturato all'implementazione. Per esserti d'aiuto abbiamo sviluppato uno strumento facile da usare, che mette in relazione i requisiti NIS2 con lo standard ISO/IEC 27001:2022.

Il tool utilizza la norma ISO/IEC 27001 come punto di partenza per valutare e migliorare le pratiche di cybersecurity e si concentra sui controlli dell'Annex A per identificare sinergie e gap nella conformità. Questi controlli sono fondamentali per mitigare i rischi legati alla sicurezza delle informazioni e dimostrare la conformità sia alla ISO/IEC 27001 sia alla NIS2.

Poiché le tempistiche di implementazione dei requisiti della Direttiva NIS2 vanno in genere da 1 a 3 anni, è importante non perdere tempo. Il nostro tool è stato pensato per agevolare la comprensione e accelerare i passi avanti delle organizzazioni in qualunque fase del percorso di conformità si trovino, da quella iniziale a quella di perfezionamento delle pratiche in essere.

Ti invitiamo quindi a utilizzare questa risorsa per approfondire la conoscenza delle misure NIS2 e il loro allineamento con i processi esistenti: fai il prossimo passo verso la conformità NIS2 e gestisci efficacemente il processi e la sicurezza delle informazioni.

Contattaci per avere supporto
sulla conformità a 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	Redundancy of information processing facilities
	A.8.15	Logging
(D) Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	A.8.16	Monitoring activities
	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
(E) Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	A.5.22	Monitoring, review and change management of supplier services
	A.5.23	Information security for use of cloud services
	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 cyber-security certification schemes		
	Annex A	
	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>

