NIS2 a ISO/IEC 27001

Herramienta de correspondencia

La transición hacia el cumplimiento de la Directiva NIS2 tiene importantes implicaciones para las organizaciones que se rigen por ella. Esta transición suele durar de 1 a 3 años, lo que pone de manifiesto la necesidad de poner en marcha medidas esenciales con suficiente antelación. Para simplificar este proceso, hemos desarrollado una herramienta de evaluación fácil de usar que alinea los requisitos de la Directiva NIS2 con la norma ISO/IEC 27001:2022.

Nuestra herramienta utiliza la norma ISO/IEC 27001 como punto de partida y proporciona información útil sobre las prácticas de ciberseguridad de su organización. La norma ISO/IEC 27001 establece un marco de mejores prácticas, políticas, procedimientos y controles para minimizar el riesgo de brechas relacionadas con la seguridad de la información. Al establecer la relación entre las medidas de la Directiva NIS2 y la norma ISO/IEC 27001:2022, un enfoque clave se centra en el Anexo A, que proporciona información fundamental desde un punto de vista de control.

El Anexo A de la norma ISO/IEC 27001:2022 expone un conjunto de controles de seguridad fundamentales para demostrar la conformidad con la norma ISO/IEC 27001 6.1.3 (Tratamiento de los riesgos de seguridad de la información) y su Declaración de Aplicabilidad correspondiente.

Consulte la tabla siguiente para obtener una visión general de la Directiva NIS2 y la norma ISO/IEC 27001:2022. Nuestra herramienta está diseñada para simplificar el proceso de alineación, ayudando a las organizaciones a comprender las posibles superposiciones e identificar las discrepancias entre los requisitos de cumplimiento de la Directiva NIS2 y la norma ISO/IEC 27001:2022.

A medida que se adentra en el cumplimiento de la normativa, recuerde que nuestra herramienta de mapeo está a su disposición para ayudarle. Le animamos a que haga uso de este recurso para ampliar sus conocimientos y le invitamos a que se ponga en contacto con nosotros para obtener más ayuda. Trabajemos juntos para abordar con eficacia la transición y garantizar la seguridad de su información.

Póngase en contacto con nosotrospara que le ayudemos a cumplir con la normativa NIS2:
sales.es@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 managemen 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 5and 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