NIS 2 Directive and ISO 27001:2022

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov

NIS 2 Directive	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
	https://eur-lex.europa.eu/eli/dir/2022/2555/oj
ISO 27001	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
	https://www.iso.org/standard/27001

From the NIS 2 Directive:

(77) **Responsibility for ensuring the security of network and information system lies**, to a great extent, **with essential and important entities**. A culture of risk management, involving risk assessments and the implementation of cybersecurity risk-management measures appropriate to the risks faced, should be promoted and developed.

(78) Cybersecurity risk-management measures should take into account the degree of dependence of the essential or important entity on network and information systems and include measures to identify any risks of incidents, to prevent, detect, respond to and recover from incidents and to mitigate their impact. The security of network and information systems should include the security of stored, transmitted and processed data. Cybersecurity risk-management measures should provide for systemic analysis, taking into account the human factor, in order to have a complete picture of the security of the network and information system.

(79) As threats to the security of network and information systems can have different origins, cybersecurity risk-management measures should be based on an all-hazards approach, which aims to protect network and information systems and the physical environment of those systems from events such as theft, fire, flood, telecommunication or power failures, or unauthorised physical access and damage to, and interference with, an essential or important entity's information and information processing facilities, which could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. The cybersecurity risk-management measures should therefore also address the physical and environmental security of network and information systems by including measures to protect such systems from system failures, human error, malicious acts or natural phenomena, in line with European and international standards, such as those included in **the ISO/IEC 27000 series**. In that regard, essential and important entities should, as part of their cybersecurity risk-management measures, also address human resources security and have in place appropriate access control policies. Those measures should be consistent with **Directive (EU) 2022/2557 _[Directive on the resilience of critical entities]_.**

(80) For the purpose of demonstrating compliance with cybersecurity risk-management measures and in the absence of appropriate European cybersecurity certification schemes adopted in accordance with Regulation (EU) 2019/881 of the European Parliament and of the Council (18), Member States should, in consultation with the Cooperation Group and the European Cybersecurity Certification Group, **promote the use of relevant European and international standards by essential and important entities or may require entities to use certified ICT products, ICT services and ICT processes**.

(81) In order to avoid imposing a disproportionate financial and administrative burden on essential and important entities, the **cybersecurity risk-management measures should be proportionate to the risks** posed to the network and information system concerned, **taking into account the state-of-the-art of such measures**, and, where applicable, **relevant European and international standards, as well as the cost for their implementation**.

(82) Cybersecurity risk-management measures should be proportionate to the degree of the essential or important entity's exposure to risks and to the societal and economic impact that an incident would have. When establishing cybersecurity risk-management measures adapted to essential and important entities, due account should be taken of the divergent risk exposure of essential and important entities, such as the criticality of the entity, the risks, including societal risks, to which it is exposed, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

(83) Essential and important entities should ensure the security of the network and information systems which they use in their activities. Those systems are primarily private network and information systems managed by the essential and important entities' internal IT staff or the security of which has been outsourced. The cybersecurity risk-management measures and reporting obligations laid down in this Directive should apply to the relevant essential and important entities regardless of whether those entities maintain their network and information systems internally or outsource the maintenance thereof.

(84) Taking account of their cross-border nature, DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, of online search engines and of social networking services platforms, and trust service providers should be subject to a high degree of harmonisation at Union level. The implementation of cybersecurity risk-management measures with regard to those entities should therefore be facilitated by an implementing act.

(85) Addressing risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security service providers and software editors, is particularly important given the prevalence of incidents where entities have been the victim of cyberattacks and where malicious perpetrators were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. Essential and important entities should therefore assess and take into account the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers.

(86) Among service providers, managed security service providers in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to prevent, detect, respond to or recover from incidents. Managed security service providers have however also themselves been the target of cyberattacks and, because of their close integration in the operations of entities pose a particular risk. Essential and important entities should therefore exercise increased diligence in selecting a managed security service provider.

(87) The competent authorities, in the context of their supervisory tasks, may also benefit from cybersecurity services such as security audits, penetration testing or incident responses.

(88) Essential and important entities should also address risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem, including with regard to countering industrial espionage and protecting trade secrets. In particular, those entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular. Similarly, given the importance and value of data for the activities of essential and important entities, when relying on data transformation and data analytics services from third parties, those entities should take all appropriate cybersecurity risk-management measures.

(89) Essential and important entities should adopt a wide range of **basic cyber hygiene practices**, such as **zero-trust principles**, **software updates**, **device configuration**, **network segmentation**, **identity and access management** or **user awareness**, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, those entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems.

…

Article 20. Governance
1. Member States shall ensure that **the management bodies** of essential and important entities **approve the cybersecurity risk-management measures** taken by those entities in order to comply with Article 21, **oversee its implementation and can be held liable for infringements by the entities** of that Article.

The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.

2. Member States shall ensure that the members of the management bodies of essential and important entities are required to **follow training**, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Article 21. Cybersecurity risk-management measures
1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account **the state-of-the-art** and, where applicable, **relevant European and international standards**, as well as **the cost of implementation**, **the measures** referred to in the first subparagraph sh**all ensure a level of security of network and information systems appropriate to the risks posed**. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

2. **The measures** referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and **shall include at least the following**:

(a) **policies on risk analysis and information system security**;

(b) **incident handling**;

(c) **business continuity**, such as backup management and disaster recovery, and crisis management;

(d) **supply chain security**, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) **security in network and information systems** acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) **policies and procedures to assess the effectiveness** of cybersecurity risk-management measures;

(g) **basic cyber hygiene practices and cybersecurity training**;

(h) policies and procedures regarding the use of **cryptography** and, where appropriate, encryption;

(i) **human resources security, access control policies and asset management**;

(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.

3. Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their **secure development procedures**. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

4. Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, **appropriate and proportionate corrective measures**.

NIS 2 Directive and ISO 27001:2022
2.0 (extended), 19.01.2024

NIS 2 Cybersecurity risk-management measures mapping to ISO 27001:2022

NIS 2 Directive	ISO 27001:2022
Article 20. Governance	5.1 Leadership and commitment 5.3 Organizational roles, responsibilities and authorities 7.1 Resources 7.2 Competence 7.3 Awareness 9.3 Management review A.5.4. Management responsibilities
General measures (21.2)	
Article 21.2 a) Policies on risk analysis and information system security	4. Context of the organization 5.2 Policy 5.3 Organizational roles, responsibilities and authorities 6.1.2 Information security risk assessment 6.1.3 Information security risk treatment 7.4 Communication 7.5 Documented information 8.2 Information security risk assessment 8.3 Information security risk treatment A.5.1 Policies for information security A.5.2 Information security roles and responsibilities A.5.4 Management responsibilities A.5.5 Contact with authorities A.5.6 Contact with special interest groups A.5.7 Threat intelligence A.5.31 Legal, statutory, regulatory and contractual requirements A.5.37 Documented operating procedures
Article 21.2 b) Incident handling Note: See also Article 23 (Reporting obligation)	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.8.15 Logging A.8.16 Monitoring activities A.8.17 Clock synchronization
Article 21.2 c) Business continuity, such as backup management and disaster recovery, and crisis management	A.5.29 Information security during disruption A.5.30 ICT readiness for business continuity A.5.37 Documented operating procedures A.7.11 Supporting utilities A.8.6 Capacity management A.8.13 Information backup A.8.14 Redundancy of information processing facilities
Article 21.2 d) Supply chain security, including security-related aspects concerning the	8.1 Operational planning and control A.5.8 Information security in project management A.5.19 Information security in supplier relationships A.5.20 Addressing information security within supplier agreements

relationships between each entity and its direct suppliers or service providers Note: See also Article 21.3 and Article 22 (Union level coordinated security risk assessments of critical supply chains)	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
Article 21.2 e) Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	A.5.37 Documented operating procedures A.8.8 Management of technical vulnerabilities A.8.9 Configuration management A.8.19 Installation of software on operational systems A.8.20 Network security A.8.21 Security of network services A.8.22 Segregation of networks A.8.23 Web filtering
Article 21.2 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 A.5.35 Independent review of information security A.5.36 Compliance with policies, rules and standards for information security
Article 21.2 g) Basic computer hygiene practices and cybersecurity training	7.2 Competence 7.3 Awareness 7.4 Communication A.6.3 Information security awareness, education and training A.7.7 Clear desk and clear screen Note: See also NIS 2 (89) A.5.15 Access control A.5.16 Identity management A.5.17 Authentication information A.5.18 Access rights A.8.8 Management of technical vulnerabilities A.8.9 Configuration management A.8.19 Installation of software on operational systems A.8.22 Segregation of networks
Article 21.2 h) Policies and procedures regarding the use of cryptography and, where appropriate, encryption	Annex A. Information security controls reference: A.5.37 Documented operating procedures A.8.24 Use of cryptography
Article 21.2 i) Human resources security, access control policies and asset management	7.2 Competence A.5.2 Information security roles and responsibilities A.5.3 Segregation of duties A.6.1 Screening A.6.2 Terms and conditions of employment A.6.3 Information security awareness, education and training A.6.4 Disciplinary process A.6.5 Responsibilities after termination or change of employment

	A.6.6 Confidentiality or non-disclosure agreements
	A.6.7 Remote working
	A.5.15 Access control
	A.5.16 Identity management
	A.5.17 Authentication information
	A.5.18 Access rights
	A.8.2 Privileged access rights
	A.8.3 Information access restriction
	A.8.4 Access to source code
	A.8.5 Secure authentication
	A.8.18 Use of privileged utility programs
	Note: Physical controls should also be here (7.1-7.8, 7.12, 7.13), see NIS 2 (30, 31, 79)
	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.7.9 Security of assets off-premises
	A.7.10 Storage media
	A.7.14 Secure disposal or re-use of equipment
	A.8.1 User endpoint devices
	A.8.7 Protection against malware
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	A.5.14 Information transfer A.5.16 Identity management A.5.17 Authentication information A.8.5 Secure authentication A.8.12 Data leakage prevention
Other	
Article 21.3 *Secure development procedures…*	A.8.25 Secure development life cycle A.8.26 Application security requirements A.8.27 Secure system architecture and engineering principles A.8.28 Secure coding A.8.29 Security testing in development and acceptance A.8.30 Outsourced development A.8.31 Separation of development, test and production environments A.8.32 Change management A.8.33 Test information A.8.34 Protection of information systems during audit testing
Article 21.4 *Appropriate and proportionate corrective measures (if not comply)*	6.3 Planning of changes 10. Improvement

See also: *ISMS Implementation Toolkit (ISO 27001)-*
www.patreon.com/posts/47806655

ISO 27001:2022 and NIS 2 Directive. IS controls to focus on

5. Organizational controls

5.1. Policies for information security
5.2. Information security roles and responsibilities
5.3. Segregation of duties
5.4. Management responsibilities
5.5. Contact with authorities
5.6. Contact with special interest groups
5.7. Threat intelligence
5.8. Information security in project management
5.9. Inventory of information and other associated assets
5.10. Acceptable use of information and other associated assets
5.11. Return of assets
5.12. Classification of information
5.13. Labelling of information
5.14. Information transfer
5.15. Access control
5.16. Identity management
5.17. Authentication information
5.18. Access rights
5.19. Information security in supplier relationships
5.20. Addressing information security within supplier agreements
5.21. Managing information security in the ICT supply chain
5.22. Monitoring, review and change management of supplier services
5.23. Information security for use of cloud services
5.24. Information security incident management planning and preparation
5.25. Assessment and decision on information security events
5.26. Response to information security incidents
5.27. Learning from information security incidents
5.28. Collection of evidence
5.29. Information security during disruption
5.30. ICT readiness for business continuity
5.31. Legal, statutory, regulatory and contractual requirements
5.32. Intellectual property rights
5.33. Protection of records
5.34. Privacy and protection of PII
5.35. Independent review of information security
5.36. Compliance with policies, rules and standards for information security
5.37. Documented operating procedures

6. People controls

6.1. Screening
6.2. Terms and conditions of employment
6.3. Information security awareness, education and training
6.4. Disciplinary process
6.5. Responsibilities after termination or change of employment
6.6. Confidentiality or non-disclosure agreements
6.7. Remote working
6.8. Information security event reporting

7. Physical controls

7.1. Physical security perimeter
7.2. Physical entry
7.3. Securing offices, rooms and facilities
7.4. Physical security monitoring
7.5. Protecting against physical and environmental threats
7.6. Working in secure areas
7.7. Clear desk and clear screen
7.8. Equipment siting and protection
7.9. Security of assets off-premises
7.10. Storage media
7.11. Supporting utilities
7.12. Cabling security
7.13. Equipment maintenance
7.14. Secure disposal or re-use of equipment

ISMS Requirements (ISO 27001)

4. Context of the organization
4.1 Understanding the organization and its context / 4.2 Understanding the needs and expectations of interested parties / 4.3 Determining the scope of the ISMS / 4.4 ISMS

5. Leadership
5.1 Leadership and commitment / 5.2 Policy / 5.3 Organizational roles, responsibilities and authorities

6. Planning
6.1 Actions to address risks and opportunities / 6.2 Information security objectives and planning to achieve them / 6.3 Planning of changes

7. Support
7.1 Resources / 7.2 Competence / 7.3 Awareness / 7.4 Communication / 7.5 Documented information

8. Operation
8.1 Operational planning and control / 8.2 Information security risk assessment / 8.3 Information security risk treatment

9. Performance evaluation
9.1 Monitoring, measurement, analysis and evaluation / 9.2 Internal audit / 9.3 Management review

10. Improvement
10.1 Continual improvement / 10.2 Nonconformity and corrective action

8. Technological controls

8.1. User endpoint devices
8.2. Privileged access rights
8.3. Information access restriction
8.4. Access to source code
8.5. Secure authentication
8.6. Capacity management
8.7. Protection against malware
8.8. Management of technical vulnerabilities
8.9. Configuration management
8.10. Information deletion
8.11. Data masking
8.12. Data leakage prevention
8.13. Information backup
8.14. Redundancy of information processing facilities
8.15. Logging
8.16. Monitoring activities
8.17. Clock synchronization
8.18. Use of privileged utility programs
8.19. Installation of software on operational systems
8.20. Network security
8.21. Security of network services
8.22. Segregation of networks
8.23. Web filtering
8.24. Use of cryptography
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
8.34. Protection of information systems during audit testing

Control: measure that maintains and/or modifies risk