NL digital

Rapport

Mapping NIS2

Uitvoeringshandelingen en ISO27001:2022

Versie 1.3 | Januari 2025

Aangevuld op basis van concept ENISA Guidance t.b.v. uitvoeringshandelingen 2024/2690

Mapping NIS2, uitvoeringshandelingen en ISO27001:2022

Doel van dit document

Deze mapping is opgesteld door het bureau van NLdigital in samenwerking met haar leden. Het is de bedoeling om zo inzichtelijk te helpen maken welke zaken door reeds bestaande maatregelen voor ISO27001 ingevuld kunnen worden. Dit document maakt geen gap-analyse, omdat het per organisatie zal verschillen hoeveel ingevuld kan worden door bestaande maatregelen.

Versiegeschiedenis

- 1.0, november 2024 – Eerste versie door bureau NLdigital
- 1.1, december 2024 – Op basis van schriftelijke input van betrokken leden
- 1.2, december 2024 – Op basis van bespreking Commissie Cybersecurity
- 1.3, januari 2025 – Aangevuld op basis van concept ENISA guidance t.b.v. uitvoeringshandelingen 2024/2690

Belangrijke afkortingen en definities

- **NIS2**
  De tweede versie van de Europese Network & Information Security richtlijn EU 2022/2555[1].
- **Cbw / Cyberbeveiligingswet**
  De aanstaande Nederlandse implementatiewet ten behoeve van de NIS2.
- **Uitvoeringshandelingen**
  Hiermee doelen we op de aanvullende wetgeving op de NIS2 met kenmerk 2024/2690[2], deze geeft uitwerking aan artikelen 21 en 23 van de NIS2 en is in de gehele EU bindend voor de benoemde sectoren.
- **ISO 27001:2022**
  De internationaal veelgebruikte ISO-standaard voor informatiebeveiliging, specifiek de revisie uit 2022. De norm beschrijft hoe met het beveiligen van informatie procesmatig omgegaan moet worden, met als doel om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie zeker te stellen. Waar we verwijzen naar deze standaard met een getal betreft het een verwijzing naar een hoofdstuk, wanneer het getal voorafgegaan wordt door een “A” betreft het een verwijzing naar de controls uit Annex A van de standaard.

[1] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022
[2] Uitvoeringsverordening (EU) 2024/2690 van de Commissie van 17 oktober 2024

1. Risicoanalyse en beveiliging

NIS2, artikel 21 lid 2 sub a	
Beleid inzake risicoanalyse en beveiliging van informatiesystemen	
Uitvoeringshandelingen	**ISO27001:2022**
Hoofdstuk 1: • 1.1 Beleid inzake de beveiliging van netwerk- en informatiesystemen • 1.2 Taken, verantwoordelijkheden en bevoegdheden Hoofdstuk 2: • 2.1 Kader voor risicobeheer • 2.2 Toezicht op de naleving • 2.3 Onafhankelijke evaluatie van de informatie- en netwerkbeveiliging	Relevante hoofdstukken: • 5.2 Policy • 5.3 Organizational roles, responsibilities and authorities • 6.1 Actions to address risks and opportunities • 6.2 Information security objectives and planning to achieve them • 8.2 Information security risk assessment • 8.3 Information security risk treatment • 9.2 Internal audit • 9.3 Management review • 10.1 Continual improvement Relevante controls: • A5.1 Policies for information security • A5.2 Information security roles and responsibilities • A5.3 Segregation of duties • A5.4 Management responsibilities • A5.7 Threat intelligence • A5.8 Information security in project management • A5.19 Information security in supplier relationships • A5.20 Addressing information security within supplier agreements • A5.21 Managing information security in the information and communication technology (ICT) supply chain • A5.31 Legal, statutory, regulatory and contractual requirements • A5.35 Independent review of information security • A5.36 Compliance with policies, rules and standards • A5.37 Documented operating procedures • A8.34 Protection of information systems during audit testing

2. Incidentenbehandeling

NIS2, artikel 21 lid 2 sub b	
Incidentenbehandeling	
Uitvoeringshandelingen	**ISO27001:2022**
Hoofdstuk 3: • 3.1 Beleid inzake incidentenbehandeling • 3.2 Monitoring en logging • 3.3 Melding van gebeurtenissen • 3.4 Beoordeling en classificatie van gebeurtenissen • 3.5 Incidentrespons • 3.6 Evaluaties na incidenten	Relevante controls: • A5.5 Contact with authorities • A5.6 Contact with special interest groups • A5.24 Information security incident management planning and preparation • A5.25 Assessment and decision on information security events • A5.26 Response to information security incidents • A5.27 Learning from information security incidents • A5.28 Collection of evidence • A5.29 Information security during disruption • A6.8 Information security event reporting • A8.15 Logging • A8.16 Monitoring activities • A8.17 Clock synchronization

3. Bedrijfscontinuïteit en crisisbeheer

NIS2, artikel 21 lid 2 sub c	
Bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer	
Uitvoeringshandelingen	**ISO27001:2022**
Hoofdstuk 4: • 4.1 Bedrijfscontinuïteits- en noodvoorzieningenplan • 4.2 Back-up- en redundantiebeheer • 4.3 Crisisbeheersing Paragraaf: • 13.2 Bescherming tegen fysieke en milieudreigingen	Relevante controls: • A5.26 Response to information security incidents • A5.29 Information security during disruption • A5.30 ICT readiness for business continuity • A7.3 Securing offices, rooms and facilities • A7.5 Protecting against physical and environmental threats • A7.11 Supporting utilities • A8.13 Information backup • A8.14 Redundancy of information processing facilities

4. Supply-chain management

NIS2, artikel 21 lid 2 sub d	
Beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners	
Uitvoeringshandelingen	**ISO27001:2022**
Hoofdstuk 5: • 5.1 Beleid inzake de beveiliging van de toeleveringsketen • 5.2 Register van leveranciers en dienstverleners Paragraaf: • 13.1 Ondersteunende nutsbedrijven	Relevante controls: • A5.19 Information security in supplier relationships • A5.20 Addressing information security within supplier agreements • A5.21 Managing information security in the information and communication technology (ICT) supply chain • A5.22 Monitoring, review and change management of supplier services • A5.23 Information security for use of cloud services • A7.11 Supporting utilities • A8.30 Outsourced development

5. Security-by- design/inkoop/onderhoud

NIS2, artikel 21 lid 2 sub e	
Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden	
Uitvoeringshandelingen	**ISO27001:2022**
Hoofdstuk 6: • 6.1 Beveiliging bij het verwerven van ICT-diensten of ICT-producten • 6.2 Beveiligde ontwikkelingscyclus • 6.3 Configuratiebeheer • 6.4 Veranderingsbeheer, reparatie en onderhoud • 6.5 Beveiligingstests • 6.6 Beveiligingspatchbeheer • 6.7 Netwerkbeveiliging • 6.8 Netwerksegmentatie • 6.9 Bescherming tegen kwaadaardige en ongeoorloofde software • 6.10 Aanpak en openbaarmaking van kwetsbaarheden	Relevante hoofdstukken: • 6.3 Planning of changes • 8.1 Operational planning and control Relevante controls: • A5.7 Threat intelligence • A5.8 Information security in project management • A5.21 Managing information security in the information and communication technology (ICT) supply chain • A5.23 Information security for use of cloud services • A5.32 Intellectual property rights • A5.33 Protection of records • A7.11 Supporting utilities • A7.12 Cabling security • A7.13 Equipment maintenance • A8.1 User end point devices8.4 Access to source code • A8.6 Capacity management • A8.7 Protection against malware • A8.8 Management of technical vulnerabilities • A8.9 Configuration management • A8.10 Information deletion • A8.11 Data masking • A8.12 Data leakage prevention • A8.13 Information backup • A8.14 Redundancy of information processing facilities • A8.15 Logging • A8.16 Monitoring activities • A8.17 Clock synchronization • A8.18 Use of privileged utility programs • A8.19 Installation of software on operational systems • A8.20 Networks security • A8.21 Security of network services • A8.22 Segregation of networks • A8.23 Web filtering • A8.25 Secure development life cycle • A8.26 Application security requirements • A8.27 Secure system architecture and engineering principles

	• A8.28 Secure coding • A8.29 Security testing in development and acceptance • A8.30 Outsourced development • A8.31 Separation of development, test and production environments • A8.32 Change management • A8.33 Test information • A8.34 Protection of information systems during audit testing

6. Monitoring & PDCA

NIS2, artikel 21 lid 2 sub f	
Beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen	
Uitvoeringshandelingen	**ISO27001:2022**
Hoofdstuk 7	Relevante hoofdstukken: • 6.2 Information security risk assessment • 9.1 Monitoring, measurement, analysis and evaluation • 9.3 Management review Relevante controls: • A5.35 Independent review of information security • A5.36 Compliance with policies, rules and standards • A8.16 Monitoring activities

7. Cyberhygiëne & opleiding

NIS2, artikel 21 lid 2 sub g	
Basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging	
Uitvoeringshandelingen	**ISO27001:2022**
Hoofstuk 8: • 8.1 Bewustmaking en basispraktijken op het gebied van cyberhygiëne • 8.2 Beveiligingsopleiding	Relevante hoofdstukken: • 7.2 Competence • 7.3 Awareness Relevante controls: • A5.10 Acceptable use of information and other associated assets • A6.1 Screening • A6.2 Terms and conditions of employment • A6.3 Information security awareness, education and training • A6.4 Disciplinary process • A6.7 Remote working • A7.7 Clear desk and clear screen • A8.7 Protection against malware

8. Cryptografie

NIS2, artikel 21 lid 2 sub h	
Beleid en procedures inzake het gebruik van cryptografie en, in voor komend geval, encryptie	
Uitvoeringshandelingen	**ISO27001:2022**
Hoofdstuk 9	Relevante controls: • A5.31 Legal, statutory, regulatory and contractual requirements • A8.24 Use of cryptography

9. Veilig personeelsbeleid en apparatuur

NIS2, artikel 21 lid 2 sub i	
Beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa	
Uitvoeringshandelingen	**ISO27001:2022**
Hoofdstuk 10: • 10.1 Beveiligingsaspecten ten aanzien van personeel • 10.2 Verificatie van de achtergrond • 10.3 Beëindiging of wijziging van arbeidsprocedures • 10.4 Tuchtprocedure Hoofdstuk 11 (gedeeltelijk): • 11.1 Beleid inzake toegangscontrole • 11.2 Beheer van toegangsrechten • 11.3 Bevoorrechte accounts en systeembeheeraccounts • 11.4 Beheersystemen Hoofdstuk 12: • 12.1 Classificatie van activa • 12.2 Behandeling van activa • 12.3 Beleid inzake verwijderbare media • 12.4 Inventaris van activa • 12.5 Afgeven, teruggeven of verwijderen van activa bij beëindiging van het dienstverband Paragraaf: • 13.3 Controle van de perimeter en de fysieke toegang	Relevante hoofdstukken: • 7.1 Resources • 7.2 Competence Relevante controls: • A5.9 Inventory of information and other associated assets • A5.10 Acceptable use of information and other associated assets • A5.11 Return of assets • A5.12 Classification of information • A5.13 Labelling of information • A5.14 Information transfer • A5.15 Access control • A5.16 Identity management • A5.18 Access rights • A5.28 Collection of evidence • A6.1 Screening • A6.2 Terms and conditions of employment • A6.3 Information security awareness, education and training • A6.4 Disciplinary process • A6.5 Responsibilities after termination or change of employment • A6.6 Confidentiality or non-disclosure agreements • A6.7 Remote working • A6.8 Information security event reporting • A7.1 Physical security perimeters • A7.2 Physical entry • A7.3 Securing offices, rooms and fa cilities • A7.4 Physical security monitoring • A7.6 Working in secure areas • A7.7 Clear desk and clear screen • A7.8 Equipment siting and protection • A7.9 Secuirty of assets off-premises • A7.10 Storage media • A7.13 Equipment Maintenance • A7.14 Secure disposal or re-use of equipment • A8.2 Privileged access rights • A8.3 Information access restriction • A8.18 Use of privileged utility programs • A8.21 Security of network services • A8.24 Use of cryptography

10. Veilige authenticatie (mfa)

NIS2, artikel 21 lid 2 sub j	
Wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekst communicatie en beveiligde noodcommunicatiesystemen binnen de entiteit	
Uitvoeringshandelingen	**ISO27001:2022**
Hoofdstuk 11 (gedeeltelijk): • 11.5 Identificatie • 11.6 Authenticatie • 11.7 Multifactorauthenticatie	Relevante controls: • A5.16 Identity management • A5.17 Authentication information • A8.2 Privileged access rights • A8.5 Secure authentication