Mapping NIS 2 en NEN-EN-ISO/IEC 27002 (nl) / BIO

In de aanloop naar de implementatie van de NIS 2 is er soms onduidelijkheid over de specifieke maatregelen die in de NIS 2 genoemd worden. Soms wordt er ten onrechte aangegeven dat specifieke maatregelen verplicht zijn vanuit de NIS 2.

Deze inventarisatie is een aanzet om organisaties welke maatregelen er in de NIS 2 expliciet genoemd worden, of deze verplicht/optioneel/situationeel zijn, en hoe deze zich verhouden tot de NEN-EN-ISO/IEC 27002 (nl). De inventarisatie is geen beoordeling of en op welke punten met de huidige BIO invulling wordt gegeven aan de NIS 2.

Belangrijkste aandachtspunten die wij zien in de analyse die we hebben uitgevoerd:

1. NIS 2 gaat uit van een **risicogestuurde aanpak** van informatiebeveiliging van de organisatie. De beoogde informatiebeveiliging die NIS 2 beschrijft is **dus breder dan alleen maatregelen** uit de **NIS 2** genoemd worden.
2. De NIS 2 maakt voor de maatregelen **geen onderscheid in (type) systeem**, maar gaat uit van een **entiteit**.
3. Reageren op **incidenten** is essentieel onderdeel van het treffen van maatregelen.
4. Voor de **maatregelen** uit artikel 20 en 21 wordt **geen verschil gemaakt tussen essentiële en belangrijke entiteiten**.
5. De **(toeleverings)keten** komt duidelijk naar voren in de NIS 2.
6. **Bedrijfscontinuiteit** is expliciet onderdeel van de maatregelen, met de voorbeelden back-upbeheer, noodvoorzieningsplannen en crisisbeheer.
7. **Cyberhygiëne** is beschreven op verschillende manieren in de NIS 2 en vergt ook afweging van de organisatie zelf.

Een aantal verschillen tussen NIS2 en de huidige BIO (opmaat):

- **Incidentregistratie** kent aanvullende eisen ten opzichte van de BIO. De NIS is, **naast interne organisatie**, **ook** sterk gericht op **externe notificatie**.
- **Bedrijfscontinuiteit, crisis(beheer) en de (toeleverings)keten** heeft **meer aandacht in de NIS 2** dan nu in de BIO staat. De NIS2 vereist een meer actieve rol van de organisatie.
- **2FA**, **beveiligde spraak-/tekst- en videoverbindingen** en beveiligde **noodcommunicatiesystemen** moeten worden **ingezet wanneer gepast**.
- **NIS maakt geen onderscheid in type systemen** en is daarmee allesomvattend, **inclusief OT/procesautomatisering**. Uit de evaluatie van de BIO blijkt dat respondenten OT/procesautomatisering onvoldoende terug vinden komen in de BIO.

De volgende personen hebben bijgedragen aan de inventarisatie: Jeroen Gaiser, Kees Hintzbergen, David van Es en Max de Bruijn. Heb je opmerkingen of aanvullingen op het document, stuur dan een bericht via het contactformulier op https://www.digitaleoverheid.nl/contact/

Kleurenlegenda

De kleuren zijn bewust geselecteerd om zo toegankelijk mogelijk voor iedereen te zijn.

Groen dikgedrukt: Actor

Groen: Verplichte maatregel

Lavendel: Situatie, voorbeeld en/of niet verplicht

Roze: Mate waarin het ontbreekt in de ISO

Onderstreept: Geen aanvullende overheidsmaatregel in BIO

Artikel NIS 2	Wie	Situatie	Wat	Onderdeel baseline BIO
Artikel 20 Governance	**bestuursorganen** van essentiële en belangrijke entiteiten		genomen maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren	5.1 - Beleidsregels voor informatiebeveiliging
			toezien op de uitvoering ervan	5.1 Beleidsregels voor informatiebeveiliging 5.31 - Wettelijke, statutaire, regelgevende en contractuele eisen 5.34 - Privacy en bescherming van persoonsgegevens 5.35 - Onafhankelijke beoordeling van informatiebeveiliging 5.36 - Naleving van beleid, regels en normen voor informatiebeveiliging
			aansprakelijk kunnen worden gesteld voor inbreuken door de entiteiten	Uit de NIS 2: *"De toepassing van dit lid doet geen afbreuk aan het nationale recht met betrekking tot de aansprakelijkheidsregels die gelden voor overheidsinstanties en voor de aansprakelijkheid van ambtenaren en verkozen of benoemde overheidsfunctionarissen.*
	leden van de bestuursorganen van essentiële en belangrijke entiteiten		een opleiding moeten volgen	6.3 - Bewustwording van, opleiding en training in informatiebeveiliging
	essentiële en **belangrijke entiteiten**		regelmatig een soortgelijke opleiding aan hun werknemers aan te bieden	

	essentiële en **belangrijke entiteiten**	passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico's … te beheren … afgestemd op de risico's die zich voordoen	5.1 - Beleidsregels voor informatiebeveiliging
	essentiële en **belangrijke entiteiten**	passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico's … te beheren … afgestemd op de risico's die zich voordoen	5.1 - Beleidsregels voor informatiebeveiliging
Artikel 21 Maatregelen voor het beheer van cyber-beveiligingsrisico's	**essentiële** en **belangrijke entiteiten**		
21 a		beleid inzake risicoanalyse en beveiliging van informatiesystemen	5.1 - Beleidsregels voor informatiebeveiliging *Hangt sterk samen met NIS 2 20.2.*
21 b		incidentenbehandeling	5.24 - Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten 5.25 - Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen 5.26 – Reageren op informatiebeveiligingsincidenten 5.27 - Leren van informatiebeveiligingsincidenten 5.28 - Verzamelen van bewijsmateriaal
21 c		bedrijfscontinuïteit,	Niet expliciet in NEN-EN-ISO/IEC 27002 (nl)*, NIS 2 lijkt uit te gaan van een breder begrip van contiuiteit dan alleen informatiebeveiliging.*

			5.29 - Informatiebeveiliging tijdens een verstoring
	zoals	back-upbeheer	8.13 - Back-up van informatie 8.14 - Redundantie van informatieverwerkende faciliteiten
	zoals	noodvoorzieningenplannen	5.29 - Informatiebeveiliging tijdens een verstoring 5.30 - ICT-gereedheid voor bedrijfscontinuïteit 7.11 - Nutsvoorzieningen
	zoals	crisisbeheer	Niet expliciet in NEN-EN-ISO/IEC 27002 (nl), *NIS 2 noemt expliciet crisis (als type incident).* 5.24 - Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten 5.25 - Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen 5.26 - Reageren op informatiebeveiligingsincidenten 5.27 - Leren van informatiebeveiligingsincidenten 5.28 - Verzamelen van bewijsmateriaal 6.8 - Melden van informatiebeveiligingsgebeurtenissen 8.13 - Back-up van informatie 8.15 - Logging 8.16 - Monitoren van activiteiten

21 d	beveiliging van de toeleveringsketen	5.19 - Informatiebeveiliging in leveranciersrelaties 5.20 - Adresseren van informatiebeveiliging in leveranciersovereenkomsten 5.21- Beheren van informatiebeveiliging in de ICT-keten 5.22 - Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten 5.23 - Informatiebeveiliging voor het gebruik van clouddiensten (algemeen voor leveranciers uitgewerkt in 5.19, 5.20, 5.21)
21 d	beveiliging van de toeleveringsketen	5.19 - Informatiebeveiliging in leveranciersrelaties 5.20 - Adresseren van informatiebeveiliging in leveranciersovereenkomsten 5.21- Beheren van informatiebeveiliging in de ICT-keten 5.22 - Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten 5.23 - Informatiebeveiliging voor het gebruik van clouddiensten (algemeen voor leveranciers uitgewerkt in 5.19, 5.20, 5.21)
21 d	beveiliging van de toeleveringsketen	5.19 - Informatiebeveiliging in leveranciersrelaties 5.20 - Adresseren van informatiebeveiliging in leveranciersovereenkomsten 5.21- Beheren van informatiebeveiliging in de ICT-keten

			5.22 - Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten 5.23 - Informatiebeveiliging voor het gebruik van clouddiensten (algemeen voor leveranciers uitgewerkt in 5.19, 5.20, 5.21)
21 e		beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen	5.20 - Adresseren van informatiebeveiliging in leveranciersovereenkomsten 8.20 - Beveiliging netwerkcomponenten 8.21 - Beveiliging van netwerkdiensten
		respons op en bekendmaking van kwetsbaarheden	5.24 - Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten 6.8 - Melden van informatiebeveiligingsgebeurtenissen 8.8 - Beheer van technische kwetsbaarheden
21 f		beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen	5.35 - Onafhankelijke beoordeling van informatiebeveiliging 5.36 - Naleving van beveiligingsbeleid en -normen
21 g		basispraktijken op het gebied van cyberhygiëne	
Cyberhygiënebeleid omvat een gemeenschappelijke basisreeks van praktijken, met inbegrip van	software- en hardware-updates	8.9 - Configuratiebeheer	

	wijziging van wachtwoorden	5.17 - Systeem voor wachtwoordbeheer 5.18 - Toegangsrechten	
	beheer van nieuwe installaties	8.19 - Installeren van software op operationele systemen	
	beperking van toegangsaccounts op beheersniveau	8.2 - Speciale toegangsrechten 8.3 - Beperking toegang tot informatie	
	back-uppen van gegevens	8.13- Back-up van informatie	
	het maakt een proactief kader mogelijk met betrekking tot paraatheid en algemene veiligheid en beveiliging in geval van incidenten of cyberdreigingen.	Niet expliciet in NEN-EN-ISO/IEC 27002 (nl)	
Essentiële en **belangrijke entiteiten** moeten een breed scala aan basispraktijken op het gebied van	zoals	zero trust-beginselen,	Niet expliciet in NEN-EN-ISO/IEC 27002 (nl)

	cyberhygiëne toepassen,			
		zoals	software-updates,	8.9 - Configuratiebeheer
		zoals	configuratie van apparaten,	
		zoals	netwerksegmentatie,	8.22 - Netwerksegmentatie
		zoals	identiteits- en toegangsbeheer	5.15 - Toegangsbeveiliging 5.16 - Identiteitsbeheer 5.17 - Beheren van authenticatie-informatie 5.18 - Toegangsrechten
		zoals	gebruikersbewustzijn,	5.1- Beleidsregels voor informatiebeveiliging 6.3 - Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging 8.7 - Beheersmaatregelen tegen malware
		zoals	opleidingen voor hun personeel organiseren	
		zoals	het bewustzijn van cyberdreigingen, phishing of socialengineeringtechnieken vergroten	
21 h			beleid en procedures inzake het gebruik van cryptografie	8.24 - Gebruik van cryptografie
21 i		in voor-komend geval	encryptie	8.24 - Gebruik van cryptografie
			personeel	5.10 - Aanvaard gebruik van informatie en andere gerelateerde bedrijfsmiddelen 6.1 - Screening 6.2 - Arbeidsovereenkomst

			6.3 - Bewustwording van, opleiding en training in informatiebeveiliging 6.4 - Disciplinaire procedure 6.5 - Verantwoordelijkheden na beëindiging of wijziging van het dienstverband 6.6 - Vertrouwelijkheids- of geheimhoudingsovereenkomsten
		toegangsbeleid	5.15 - Toegangsbeveiliging 5.16 - Identiteitsbeheer 5.17 - Beheren van authenticatie-informatie 5.18 - Toegangsrechten
		beheer van activa	7.9 - Beveiligen van bedrijfsmiddelen buiten het terrein 5.9 - Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen 5.10 - Aanvaard gebruik van informatie en andere gerelateerde bedrijfsmiddelen 5.11 - Retourneren van bedrijfsmiddelen 7.1 – Fysieke beveiligingszones 7.14 - Veilig verwijderen of hergebruiken van apparatuur
	wanneer gepast	multifactor-authenticatie- of continue-authenticatieoplossingen	5.17 - Beheren van authenticatie-informatie
	wanneer gepast	het gebruik van, beveiligde spraak-, video- en tekstcommunicatie	5.21 - Beheren van informatiebeveiliging in de ICT-keten
	wanneer gepast	beveiligde noodcommunicatiesystemen	5.21 - Beheren van informatiebeveiliging in de ICT-keten
essentiële en **belangrijke entiteiten**		rekening houden met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener en met de	5.20 - Opnemen van beveiligingsaspecten in leveranciersovereenkomsten 5.22 - Monitoren, beoordelen en het

			algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners met inbegrip van hun veilige ontwikkelingsprocedures.	beheren van wijzigingen van leveranciersdiensten 8.30 - Uitbestede systeemontwikkeling
	entiteiten		rekening moeten houden uitgevoerde gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens	5.21 - Toeleveringsketen van informatie- en communicatietechnologie
Artikel 23 Rapportage-verplichtingen	**essentiële** en **belangrijke entiteiten**		elk incident dat aanzienlijke gevolgen heeft voor de verlening van hun diensten als bedoeld in lid 3 (significant incident) onverwijld meldt bij zijn CSIRT of, indien van toepassing, zijn bevoegde autoriteit overeenkomstig	Niet expliciet in NEN-EN-ISO/IEC 27002 (nl) 6.8 - Melden van informatiebeveiligingsgebeurtenissen
	essentiële en **belangrijke entiteiten**		ontvangers van hun diensten onverwijld in kennis van significante incidenten die een nadelige invloed kunnen hebben op de verlening van die diensten	Niet expliciet in NEN-EN-ISO/IEC 27002 (nl) 6.8 - Melden van informatiebeveiligingsgebeurtenissen
	essentiële en **belangrijke entiteiten**	Indien van toe-passing	ontvangers van hun diensten die mogelijkerwijs door een significante cyberdreiging worden getroffen, onverwijld meedelen welke maatregelen die ontvangers kunnen nemen in reactie op die dreiging	Niet expliciet in NEN-EN-ISO/IEC 27002 (nl) 6.8 - Melden van informatiebeveiligingsgebeurtenissen
	essentiële en **belangrijke entiteiten**	Indien nodig	Stellen ontvangers ook in kennis van de significante cyberdreiging zelf	Niet expliciet in NEN-EN-ISO/IEC 27002 (nl) 6.8 - Melden van informatiebeveiligingsgebeurtenissen

	betrokken entiteiten voor de in lid 1 bedoelde melding	bij het CSIRT of, indien van toepassing, de bevoegde autoriteit - onverwijld en in elk geval binnen 24 uur nadat zij kennis hebben gekregen van het significante incident, een vroegtijdige waarschuwing geven - onverwijld en in elk geval binnen 72 uur nadat zij kennis hebben gekregen van het significante incident, een incidentmelding indienen met, indien van toepassing, een update - op verzoek van het CSIRT of, indien van toepassing, de bevoegde autoriteit, een tussentijds verslag indienen - uiterlijk één maand na de indiening een eindverslag indienen indien het incident nog aan de gang is voortgangsverslag indienen en binnen één maand nadat zij het incident hebben afgehandeld, een eindverslag indienen.	Niet expliciet in NEN-EN-ISO/IEC 27002 (nl) 6.8 - Melden van informatiebeveiligingsgebeurtenissen
Artikel 24 Gebruik van Europese cyberbeveiligings-certificeringsregelingen	kunnen de **lidstaten** eisen dat **essentiële** en **belangrijke entiteiten**	bepaalde ICT-producten, ICT -diensten en ICT -processen gebruiken die zijn gecertificeerd in het kader van Europese cyberbeveiligingscertificeringsregelingen	Niet expliciet in NEN-EN-ISO/IEC 27002 (nl) 5.20 - Opnemen van beveiligingsaspecten in leveranciersovereenkomsten

	moedigen de lidstaten **essentiële** en **belangrijke entiteiten** aan	gekwalificeerde vertrouwensdiensten	5.14 - Overdragen van informatie, met verwijzing naar AdES-Baseline profiles.
Artikel 25 Normalisatie	**lidstaten**	moedigen het gebruik aan van Europese en internationale normen en technische specificaties die relevant zijn voor de beveiliging van netwerk- en informatiesystemen.	Niet expliciet in NEN-EN-ISO/IEC 27002 (nl), wel o.a. via Lijst open standaarden en Wdo art. 3.
	ENISA	adviezen en richtsnoeren op over de technische gebieden	Niet expliciet in NEN-EN-ISO/IEC 27002 (nl)