De norm voor de NIS2 toeleveringsketen

Artikel 21.2d van de Europese NIS2-richtlijn legt cyberhygiëne vereisten op aan kritieke industrie, diensten en infrastructuur. Essentiële en belangrijke bedrijven dienen daarom samen te werken met hun directe leveranciers om de beveiliging van de toeleveringsketen te waarborgen. Het NIS2 Quality Mark biedt hiervoor een geschikte norm met drie niveaus (Basic, Substantial en High), zodat de maatregelen passen bij het dreigingsniveau.

NIS2-Quality Mark Basic: NIS2-QM10		Mapping* met ISO27001
1. Organisatorische beheersmaatregelen		
1.2	**Beleidsvorming voor informatiebeveiliging en bestuurlijke goedkeuring:** Formuleer een cybersecurity strategie en borg deze. Het formuleren van een informatiebeveiligings-en governancebeleid vereist het opstellen van gedetailleerde richtlijnen. Deze dienen minimaal een basis cyberhygiënebeleid te bevatten, inclusief standaardpraktijken zoals updates, wachtwoordwijzigingen, installatiebeheer, het beperken van toegangsniveaus en data-back-ups, ondersteunend aan proactieve paraatheid en beveiliging tegen incidenten of dreigingen. De verantwoordelijkheden voor het initiëren en beslissen over alle cybersecurity maatregelen moeten duidelijk zijn. Zorg altijd voor formele bestuurlijke goedkeuring.	5.1
1.3	**Toewijzing wie verantwoordelijk is bij informatiebeveiliging:** Elke medewerker krijgt specifieke taken en verantwoordelijkheden toegewezen in het kader van informatiebeveiliging. Het is cruciaal om een aangewezen persoon te hebben die verantwoordelijk is voor informatiebeveiliging.	5.2
1.6.1	**Overzicht van informatie:** Creëer een overzichtelijke lijst van alle organisatiegegevens, zoals klantinformatie en contracten. Wijs tevens een eigenaar/beheerder aan voor specifieke informatie.	5.9
1.6.2	**Overzicht van ICT-bedrijfsmiddelen:** Stel een gedetailleerde lijst op van alle organisatie-ICT-middelen met software, servers, dataopslagsystemen en firewalls. Benoem ook een verantwoordelijke eigenaar/beheerder per bedrijfsmiddel.	5.9
1.8	**Het inleveren van bedrijfsmiddelen na gebruik:** Bij vertrek leveren medewerkers bedrijfsmiddelen in, zoals computers en smartphones, om vertrouwelijke informatie te waarborgen. Stel een procedure en checklist op voor een correcte teruggave.	5.11
1.14	**Verlening en beheer van toegangsbevoegdheden:** Bij nieuwe medewerkers of functiewijzigingen is er risico op ongeoorloofde toegangsrechten. Controleer bij beëindiging van een dienstverband of accounts correct worden afgesloten. Registreer wie toegang heeft, definieer logische en fysieke toegangsrechten en noteer de beëindigingsdatum.	5.18
1.23	**Voorbereiding en optimalisatie van ICT voor het bedrijfscontinuïteitsproces:** Bij onverwachte gebeurtenissen, zoals een cyberaanval, is het cruciaal om snel operationeel te zijn. Formuleer doelen en bijbehorende continuïteitseisen, zoals een proces inclusief back-upbeheer, de noodvoorzieningenplannen en crisisbeheer inclusief cyberveiligheid. Zet de continuïteitseisen in een plan.	5.30

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken.*

De norm voor de NIS2 toeleveringsketen

NIS2-Quality Mark Basic: NIS2-QM10		Mapping* met ISO27001
1. Organisatorische beheersmaatregelen		
1.26	**Samen de toeleveringsketen beveiligen:** Voer een grondige risico-inventarisatie uit voor belangrijke leveranciers en maak gezamenlijke afspraken over digitale beveiliging. Zorg dat ontvangers (personen of organisaties) tijdig geïnformeerd zijn over de beheersmaatregelen die ze kunnen nemen bij een significante cyberdreiging in de organisatie. Significante cyberdreiging: een dreiging die, gezien de technische kenmerken, ernstige schade (materieel of immaterieel) aan organisaties, systemen of dienstgebruikers kan veroorzaken.	n/a**
2. Mensgerichte beheersmaatregelen		
2.2	**Educatie van bestuurders en medewerkers en bewustwording voor het beveiligen van informatie:** Zorg dat directie en bestuurders een opleiding of een cursus volgen zodat ze cyberbeveiligingsrisico's kunnen identificeren en beoordelen. Het is belangrijk dat iedereen in de organisatie de risico's van informatieverwerking begrijpt. Gebruik bijvoorbeeld video-trainingsmodules voor medewerkers over digitale veiligheid. Zorg voor opleidingen die passen bij de verschillende functies. Medewerkers moeten worden getest op hun kennis en naleving van het beleid.	6.3
2.6	**Thuis- of hybride werken op een veilige manier:** Werken buiten de organisatie vergroot het cyberincidentrisico. Formuleer regels voor veilige informatieverwerking op externe locaties en zorg dat alle medewerkers deze kennen en naleven.	6.7
2.7	**Registratie en rapportage van gebeurtenissen met betrekking tot informatiebeveiliging:** Maak afspraken om een snelle melding van bedreigingen voor de informatieveiligheid te waarborgen. Gebruik interne communicatiekanalen zoals e-mail, WhatsApp en bij voorkeur telefonie voor directe respons. Overweeg een digitaal meldsysteem of app voor uitgebreidere rapportage.	6.8
3. Fysieke beheersmaatregelen		
3.9	**Beveiligingsmaatregelen voor toegang:** Voorkom ongeautoriseerde toegang tot bedrijfsmiddelen met gevoelige informatie. Formuleer heldere toegangsregels, met bijzondere aandacht voor de beveiliging van essentiële bedrijfsmiddelen.	5.15
4. Technologische beheersmaatregelen		
4.1	**Beveiliging en beheer gebruikersapparaten:** Beveilig medewerkersapparaten, zoals laptops en telefoons, tegen cyberincidenten. Implementeer maatregelen zoals laptopversleuteling en beperking van adminrechten. Onderhoud en verspreid een actuele lijst met regels, inclusief vereisten voor sterke wachtwoorden en pincodes.	8.1
4.4	**Bestrijding en preventie van malware:** Malware kan schade aanrichten en gevoelige informatie blootleggen. Bescherm de digitale omgeving met anti-malwaresoftware, een virusscanner en een spamfilter. Overweeg encryptie voor belangrijke documenten.	8.7

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken.*
*** N/a: Not available, niet van toepassing. Er is geen corresponderende maatregel in ISO27001.*

NIS2-Quality Mark Basic: NIS2-QM10		Mapping* met ISO27001
4. Technologische beheersmaatregelen		
4.5	**Informatiebehoud: back-up en herstel:** Voorkom dataverlies met een back-up plan (volgens de 3-2-1-systematiek), maak regelmatig back-ups van belangrijke data en systemen en test deze periodiek op betrouwbaarheid.	8.13
4.7	**Software op computers en apparaten up-to-date houden:** Houd computers en apparaten veilig met regelmatige updates. Installeer direct alle updates volgens de vastgestelde procedures voor veilig updaten op alle apparaten.	8.19
4.10	**Authenticatie op cruciale systemen:** Zorg ervoor dat bij authenticatie- en communicatiesystemen gebruik wordt gemaakt van multifactor-authenticatie (MFA) of continue-authenticatieoplossingen, alsmede beveiligde spraak-, video- en tekstcommunicatie en veilige noodcommunicatiesystemen. Gebruik authenticatiemethoden (zoals wachtwoorden of MFA) die in lijn zijn met de gevoeligheid van de informatie die men probeert te benaderen. Implementeer MFA voor accounts met beheerdersrechten en voor alle toegang tot systemen met bedrijfsgevoelige informatie. Bovendien dienen gebruikers die via het internet inloggen ook MFA te gebruiken.	8.5

**Mapping: Deze norm is vergelijkbaar, maar niet identiek aan ISO27001. Elk normeringsstelsel heeft zijn eigen specifieke kenmerken.*

Copyright

Toelichting op mapping

Onze norm voor cybersecurity is het resultaat van een uitgebreide samenwerking tussen een divers team van experts op het gebied van cyberbeveiliging. Dit multidisciplinaire team bestond uit vertegenwoordigers van NIS2 organisaties, mkb-bedrijven, onafhankelijke cybersecurityspecialisten en auditoren. Door deze gevarieerde samenstelling hebben we ervoor gezorgd dat onze norm een breed scala aan perspectieven en expertise omvat, wat heeft geleid tot een unieke en uiterst waardevolle benadering van cybersecurity.

Hoewel onze norm mogelijk enige overlap vertoont met andere cybersecuritynormen op bepaalde punten, moeten gebruikers begrijpen dat onze norm een op zichzelf staand product is, dat is ontwikkeld met het oog op de specifieke behoeften en uitdagingen van moderne bedrijven. De inhoud en aanpak van onze norm kunnen daarom verschillen van die van andere normen, zelfs als er enige gelijkenis bestaat.

Het is belangrijk om te benadrukken dat onze norm is ontworpen om de best practices op het gebied van cybersecurity te omvatten, gebaseerd op de inzichten en ervaringen van onze diverse teamleden. Daarom moeten gebruikers onze norm beschouwen als een uniek instrument dat is ontwikkeld met het oog op maximale toegevoegde waarde en effectiviteit voor organisaties die streven naar verbeterde cybersecurity.

Disclaimer