

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 High: NIS2-QM30		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
1.4	Asset management, toegang en management controle: Houd personeels-, toegangs- en activabeheer actief up-to-date en in naleving door regelmatige controles via de PDCA-cyclus en managementrapportages. De directie dient te waarborgen dat alle medewerkers binnen de organisatie betrokken zijn en bekend zijn met de vereisten die aan hen worden gesteld.	5.4
1.5	Beoordeling en inzicht van beveiligingsdreigingen: Voor het verkrijgen van inzicht in potentiële bedreigingen is het essentieel om niet enkel informatie hieromtrent te verzamelen, maar tevens grondig onderzoek te verrichten en een gedegen beoordeling uit te voeren.	5.7
1.6.1	Overzicht van informatie, activa en assets: Zorg voor beleidsdocumenten waarin de beschrijving van activa (inclusief personeel, machines, apparatuur en gebouwen als onderdeel van het productieproces) wordt opgenomen, samen met een overzicht van alle organisatiegegevens, zoals klantinformatie en contracten.	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
1.7	Informatie en aanverwante bedrijfsmiddelen acceptabel gebruiken: Er dienen voorschriften te worden opgesteld voor veilig gebruik van informatie. Dit omvat tevens ICT-middelen die gerelateerd zijn aan informatie, zoals netwerkapparatuur en clouddiensten.	5.10

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

NIS2-Quality Mark High: NIS2-QM30		Mapping* met ISO27001
1. Organisatorische beheersmaatregelen		
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
1.9	Informatie indelen: Met behulp van een opgesteld classificatieschema wordt informatie geclassificeerd door middel van labeling, waarbij bijvoorbeeld wordt vastgesteld dat een kopie van een paspoort onderdeel is van de categorie personeelsgegevens. Dit verschaft medewerkers die met informatie werken een beknopt overzicht van hoe zij de informatie dienen te behandelen en te beschermen.	5.12
1.11	Het overbrengen van informatie binnen de organisatie en aan derden: De voorschriften en procedures met betrekking tot het veilig overbrengen van informatie dragen bij aan het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie tijdens het overdrachtsproces. Het opstellen van deze voorschriften en procedures en het communiceren ervan naar alle medewerkers, en indien nodig naar externe partijen, is essentieel.	5.14
1.13	Authenticatieprocessen en regulering van identiteitsgegevens: De identiteit van het personeel dient vastgelegd te worden, en er dient beleid te zijn en een procedure geïmplementeerd te worden waarin beschreven staat hoe deze gegevens geregistreerd, aangepast en verwijderd moeten worden (de "levenscyclus").	5.16
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
1.15	Bescherming van informatie in samenwerking met leveranciers: Er dient een inventarisatie te worden gemaakt van de risico's die zich voordoen bij de leveranciers, waarna deze worden beoordeeld en er maatregelen worden genomen om de risico's te beperken.	5.19
1.16	Borgen van informatieveiligheid in overeenkomsten met leveranciers: Zorg ervoor dat de beveiligingseisen en verantwoordelijkheden in een overeenkomst vastliggen. Stel specifieke afspraken op met leveranciers. Documenteer welke maatregelen gezamenlijk genomen kunnen worden om de bestaande cyberrisico's te mitigeren.	5.20
1.17	Managen van informatieveiligheid in de toeleveringsketen van ICT-producten en -diensten: Het is van belang dat duidelijk is welke risico's er bij de ICT-leveranciers spelen, zodat hier op een passende manier mee omgegaan kan worden.	5.21
1.18	Toezicht, evaluatie en wijzigingsbeheer van leveranciersdiensten: Controleer of de contractuele beveiligingseisen worden uitgevoerd en effectief zijn via een eigen controle of audit door externen. Zorg ervoor dat het duidelijk is welke maatregelen leveranciers moeten treffen op het gebied van informatiebeveiliging.	5.22

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

NIS2-Quality Mark High: NIS2-QM30		Mapping* met ISO27001
1. Organisatorische beheersmaatregelen		
1.19	Informatie veilig houden bij het gebruik van cloudservices: Indien de organisatie gebruik maakt van clouddiensten, is het van belang om vast te leggen hoe deze worden aangeschaft, gebruikt, beheerd en beëindigd.	5.23
1.20	Richtlijnen voor de aanpak van informatiebeveiligingsincidenten (cybersecurityincidenten): Er dient een plan te worden opgesteld met betrekking tot hoe de organisatie omgaat met informatiebeveiligingsincidenten, zoals een inbreuk die beschikbaarheid, integriteit of vertrouwelijkheid van informatie bedreigt. Hierbij wordt duidelijk aangegeven wie verantwoordelijk is voor welke taken.	5.24
1.21	Registratie, beoordeling en afhandeling van beveiligingsincidenten inclusief rapportage aan het management: Zorg voor evaluatie en besluitvorming over gebeurtenissen met betrekking tot informatiebeveiliging. Bespreek elke ongebruikelijke gebeurtenis. Niet elke cybergebeurtenis is onmiddellijk een incident. Beoordeel bij elke gebeurtenis wat het inhoudt en bepaal of actie noodzakelijk is.	5.25
1.22	Melden van en handelen bij incidenten rondom informatieveiligheid: Incidenten met aanzienlijke gevolgen moeten worden gemeld bij het CSIRT en de bevoegde autoriteiten. Het gaat dan om incidenten die zware operationele verstoring of financiële schade voor de entiteit of materiële/immateriële schade aan andere organisaties (kunnen) veroorzaken. Indien zich een cyberincident voordoet, is het essentieel om adequaat te handelen. Leg vast welke stappen ondernomen moeten worden, ook buiten reguliere werktijden, en communiceer dit met medewerkers.	5.26
1.23	Vorbereiding 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
1.24	Objectieve toetsing en bewijsvoering van informatiebeveiliging en bedrijfscontinuïteit: Organiseer regelmatig een onafhankelijke beoordeling, zoals een externe audit, om te checken of de organisatie voldoet aan de eisen op het gebied van informatiebeveiliging en bedrijfscontinuïteit.	5.35
1.25	Handhaven van voorschriften, regelgeving en standaarden voor informatiebeveiliging: Zorg voor beveiligingsbeleid en een meldingsprocedure van kwetsbaarheden en test op actualiteit en naleving. Om te voldoen aan een adequaat niveau van informatiebeveiliging, is het van essentieel belang dat alle overeengekomen procedures zoals uiteengezet in het informatiebeveiligingsbeleid (inclusief de 'Richtlijnen voor de beveiliging van informatie' en de 'Toewijzing van verantwoordelijkheden voor informatiebeveiliging') strikt worden nageleefd. Maak een procedure voor het beoordelen van het effect van de beheersmaatregelen. Zorg voor regelmatige rapportage aan het management.	5.36

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

NIS2-Quality Mark High: NIS2-QM30		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**
1.27	Informatiebeveiliging en bewijsverzameling tijdens een incident: Om ervoor te zorgen dat de organisatie operationeel blijft en er adequaat gereageerd wordt op een beveiligingsincident, is het noodzakelijk om vast te leggen hoe en wanneer bewijsmateriaal verzameld wordt, en hoe een passend niveau van informatiebeveiliging gehandhaafd blijft, zelfs in geval van een incident.	5.28/ 5.29
2. Mensgerichte beheersmaatregelen		
2.1	Overeenkomst werkzaamheden en verantwoordelijkheden (arbeidsovereenkomst): In arbeidscontracten dient expliciet te worden vermeld welke verplichtingen medewerkers hebben met betrekking tot informatiebeveiliging.	6.2
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
2.4	Blijvende verantwoordelijkheden na vertrek of wijziging in de arbeidsrelatie: Het is van cruciaal belang om te waarborgen dat gevoelige informatie veilig blijft, zelfs bij veranderingen in functies of vertrek van medewerkers. Dit dient te worden gedocumenteerd en gecommuniceerd met alle betrokken medewerkers.	6.5
2.5	Overeenkomsten voor gegevensbescherming: Formuleer overeenkomsten betreffende de bescherming van informatie en vereis dat deze door zowel medewerkers als andere betrokken partijen worden ondertekend.	6.6
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

*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 High: NIS2-QM30		Mapping* met ISO27001
2. Mensgerichte beheersmaatregelen		
2.7	Registratie en rapportage van gebeurtenissen met betrekking tot informatiebeveiliging en melding cyberincidenten: Zorg voor een gestroomlijnde procedure voor het melden van kwetsbaarheden in de informatieveiligheid gedurende het aankoop-, ontwikkelings- en onderhoudsproces, met specifieke aandacht voor netwerk- en informatiesystemen. Maak concrete afspraken voor een snelle rapportage van bedreigingen voor de informatiebeveiliging. Maak gebruik van interne communicatiekanalen zoals e-mail, WhatsApp en bij voorkeur telefonie voor een directe respons. Overweeg daarnaast de implementatie van een digitaal meldsysteem of een app voor uitgebreidere rapportage. Neem direct actie bij het ontdekken van kwetsbaarheden om de veiligheid van de informatie te waarborgen.	6.8
2.8	Beveiligingsaspecten voor medewerkers vastleggen in een beveiligingsbeleid: Om bedrijfsrisico's te minimaliseren, is het van belang dat een grondige achtergrondcontrole wordt uitgevoerd voordat nieuwe medewerkers worden aangenomen of bestaande medewerkers worden belast met vertrouwelijke taken. Formuleer regels en procedures met betrekking tot het uitvoeren van achtergrondcontroles, waarbij duidelijk wordt vastgesteld welke controles geschikt zijn voor welke functies of verantwoordelijkheden. Leg screeningsvereisten bij gevoelige functies vast in het beveiligingsbeleid. Benoem één of twee personen die gemachtigd zijn en de capaciteit hebben om deze achtergrondcontroles uit te voeren.	6.1
3. Fysieke beheersmaatregelen		
3.1	Zorg voor beleid voor toegangsbeveiliging (logische en fysieke aspecten) en bescherming tegen binnentreden: Logische toegangsbeveiliging: richtlijnen en processen voor toegang tot informatiesystemen en netwerken. Fysieke toegangsbeveiliging: processen en middelen voor gecontroleerde toegang tot terreinen en gebouwen. Zorg ervoor dat bekend is waar gevoelige informatie en apparaten zich bevinden in de organisatie, zodat deze beveiligd kunnen worden. Verleen slechts personen met de juiste bevoegdheden toegang tot de bepaalde zones.	7.1/ 7.2
3.5	Regelgeving voor vertrouwelijke informatie achterlaten op bureau en scherm: Om te voorkomen dat vertrouwelijke informatie op een bureau of op een scherm in verkeerde handen valt, zijn duidelijke en eenduidige regels noodzakelijk waar werknemers zich aan dienen te houden. Er worden regels opgesteld voor een "Clear Desk" en "Clear Screen", zodat gevoelige of vertrouwelijke informatie niet in handen komt van onbevoegden.	7.7
3.8	Gevoelige informatie en software op de juiste manier (veilig) verwijderen of overschrijven: Indien apparatuur wordt vervangen of hergebruikt, is het cruciaal om datalekken te voorkomen door ervoor te zorgen dat gevoelige/informatie en software veilig worden verwijderd of overschreven. Een checklist voor (onderdelen van) apparatuur met opslagmedia kan hierbij van dienst zijn. Deze checklist geeft aan hoe gecontroleerd kan worden of alle gevoelige/informatie correct is verwijderd.	7.14

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

NIS2-Quality Mark High: NIS2-QM30		Mapping* met ISO27001
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
4.2	Bijzondere toegangsbevoegdheden: Het is van belang dat duidelijk is gedocumenteerd welke personen of groepen in de organisatie welke toegangsrechten hebben.	8.2
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
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
4.6	Meervoudige uitvoering van systemen, diensten of infrastructuur (informatieverwerkende faciliteiten): Informatieverwerkende faciliteiten zoals een systeem, dienst of infrastructuur moeten indien nodig meervoudig (redundant) worden uitgevoerd, zodat de faciliteiten te allen tijde operationeel blijven, zelfs in het geval van uitval van een onderdeel. Bepaal de minimaal vereiste beschikbaarheid voor informatieverwerkende systemen en zorg ervoor dat ze voldoende redundantie hebben.	8.14
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
4.8	Netwerken beheren en beveiligen: Indien binnen de organisatie gebruik wordt gemaakt van netwerken tussen computers en andere apparaten, dient ervoor gezorgd te worden dat deze adequaat beveiligd zijn en blijven, zelfs bij eventuele wijzigingen.	8.20
4.9	Indeling van netwerken: Door middel van netwerksegmentatie wordt voorkomen dat één groot netwerk wordt gecreëerd. In plaats daarvan wordt het opgedeeld in specifieke segmenten, waardoor problemen die zich voordoen in één deel niet het hele netwerk treffen.	8.22

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

NIS2-Quality Mark High: NIS2-QM30		Mapping* met ISO27001
4. Technologische beheersmaatregelen		
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
4.11	Logboekregistratie: Door logbestanden te creëren, te beschermen en te analyseren, kunnen onregelmatigheden in netwerken, systemen en applicaties vroegtijdig worden opgespoord.	8.15
4.12	Cryptografie en encryptie: Door het instellen en correct toepassen en controleren van cryptografische en, indien nodig, encryptieprotocollen, wordt een veilige digitale omgeving en communicatie gewaarborgd. Implementeer een beleid omtrent cryptografie en encryptie. Ontwikkel een procedure voor het gebruik van cryptografie en encryptie.	8.24
4.14	Management van technische kwetsbaarheden: Men wenst niet dat kwaadwillenden toegang verkrijgen tot de informatiesystemen via zwakke plekken of gebreken in de beveiliging. Het is daarom van essentieel belang om dergelijke kwetsbaarheden op te sporen, te evalueren en te verhelpen.	8.8
4.15	Beveiliging van netwerk- en informatiesystemen en beheer van wijzigingen: Maak een beveiligingsbeleid voor de levenscyclus van netwerk- en informatiesystemen. Formuleer procedures om de informatiebeveiliging te waarborgen bij het implementeren van wijzigingen in systemen die informatie verwerken, zoals computers.	8.32

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

Hieronder volgen een aantal aanvullende beheersmaatregelen die specifiek gelden voor organisaties die werken in of gebruik maken van Operational Technology (OT) en Information Technology (IT). Vanzelfsprekend hebben de algemene beheersmaatregelen hierboven ook betrekking op deze bedrijven.

NIS2-Quality Mark High: NIS2-QM30		Mapping* met ISO27001
OT- beheersmaatregelen		
5.1	Register van alle OT-bedrijfsmiddelen: Identificeer en documenteer alle hardware- en softwarecomponenten (OT-bedrijfsmiddelen) die binnen de organisatie worden gebruikt. Als er al een gedetailleerd overzicht bestaat, zorg dan dat dit overzicht ook informatie bevat over de specifieke softwareversies en de huidige patch niveaus van elke component.	n/a**
5.2	Bepaal de afhankelijkheid van OT-bedrijfsmiddelen: Breng per OT-bedrijfsmiddel in kaart hoe afhankelijk de organisatie hiervan is en wat de risico's zijn bij uitval.	n/a
5.4	Configuratie en operationele parameter back-up : Deze back-ups zijn van vitaal belang. Ze helpen bij het snel herstellen van systemen na technische problemen of cyberaanvallen, waardoor lange stilstand wordt voorkomen en de bedrijfscontinuïteit gewaarborgd blijft.	n/a
5.5	Recovery plan: Stel een herstelplan op en voer periodieke tests uit. Indien daadwerkelijke testen niet haalbaar zijn, voer dan een zogenaamde droogoefening uit. Simuleer het herstelproces door het plan te volgen en zorg ervoor dat de benodigde middelen (zoals configuraties, documentatie en reserveonderdelen) en betrokken personen (inclusief externe partijen) beschikbaar zijn of zouden zijn geweest.	n/a
5.6	Segmentatie van netwerken: Werk met gescheiden netwerk segmenten binnen het netwerk. Dit betekent het opdelen van het netwerk in afzonderlijke segmenten met in bepaalde gevallen specifieke toegangsrechten om de bescherming van gevoelige informatie te waarborgen.	n/a
5.8	Remote toegang via een Jump Host: Zorg ervoor dat remote toegang altijd plaatsvindt via een gecontroleerd en gemonitord access point, ofwel een zogenaamde Jump Host. Dit is een speciale computer binnen een netwerk die gebruikt wordt als tussenstation voor veilige toegang tot andere systemen.	n/a
5.9	Patch- en scanbeheer: Het bijwerken van systemen en software door middel van patches zorgt ervoor dat ze up-to-date blijven en helpt bij het identificeren van kwetsbaarheden in een vroeg stadium. Het regelmatig scannen van je systemen draagt bij aan het handhaven van een algemene beveiliging van OT-systemen.	n/a
5.11	Versies/revisies van OT-apparatuur en bijbehorende leveranciers: Het accuraat bijhouden van versies/revisies van OT-apparatuur en welke leverancier daarbij hoort draagt bij aan de organisatorische capaciteit om correct te reageren op beveiligingskwetsies, updates efficiënt door te voeren en de onderhoudsplanning te optimaliseren.	n/a

*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 High: NIS2-QM30		Mapping* met ISO27001
IT- beheersmaatregelen		
6.1	Broncode bescherming (versiebeheer en toegang) van software (ontwikkeling): Bescherm de broncode van software door middel van strikt versiebeheer en gedegen toegangscontrolemechanismen. Op deze wijze wordt de integriteit en veiligheid van softwaretoepassingen gehandhaafd en gewaarborgd.	8.4
6.2	Actueel houden van de programmacode (o.a. third party components): Het is van essentieel belang om ervoor te zorgen dat de programmacode up-to-date blijft, vooral wat betreft externe onderdelen, om de veiligheid van informatie te waarborgen. Dit houdt in dat zowel de eigen code als externe componenten regelmatig moeten worden bijgewerkt om gelijke tred te houden met de laatste beveiligingsupdates.	n/a
6.3	Gebruik van recommendations (volgen architectuurrichtlijnen & richtlijnen van OWASP): Om informatieveiligheid te waarborgen is het belangrijk om altijd architectuurrichtlijnen en OWASP te volgen bij het ontwikkelen van software.	8.27
6.4	Security awareness (standaarden toepassen): Het is van belang dat iedereen in de organisatie zich bewust is van beveiligingsaspecten. Security awareness omvat het begrip en de betrokkenheid van medewerkers bij beveiligingspraktijken en -risico's binnen de organisatie.	6.3
6.5	Onafhankelijke kwaliteitstoetsen, externe audits (o.a. PEN-testen): Voer regelmatig onafhankelijke kwaliteitstoetsen en externe audits uit, bijvoorbeeld bij de lancering van een belangrijke software-update. Zo wordt de integriteit en veiligheid van de nieuwe functionaliteiten gewaarborgd en eventuele potentiële kwetsbaarheden worden proactief aangepakt.	8.29
6.6	Uitbestede softwareontwikkeling: Wanneer de ontwikkeling van software wordt uitbesteed, is het belangrijk om de maatregelen te identificeren die op het gebied van informatiebeveiliging worden genomen door de bedrijven waarmee samengewerkt wordt. Zorg voor duidelijke eisen en controleer of deze worden nageleefd door regelmatige controles uit te voeren.	8.3
6.7	Scheiden van ontwikkel, test, acceptatie en productie: Zorg dat er een duidelijke scheiding bestaat tussen ontwikkeling, testen, acceptatie (indien van toepassing) en productieomgevingen. Het is van belang dat elke omgeving zoveel mogelijk geïsoleerd van de overige omgevingen wordt gehouden.	8.31
6.8	Procedures en methodes voor het deployen van software (IAC): Het is noodzakelijk dat de organisatie geschikte procedures en methoden hanteert voor het installeren van software, bijvoorbeeld door het gebruik van Infrastructure as Code (IAC). Dit draagt bij aan het handhaven van informatiebeveiliging en zorgt voor een vlotte installatie van softwareoplossingen.	n/a

*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 High: NIS2-QM30		Mapping* met ISO27001
IT- beheersmaatregelen		
6.9	Alle geleverde programmatuur exact in kaart (welke klant heeft welke software en versies): Verkrijg inzicht in de gebruikte software en versienummers door klanten, om zo het onderhoud en de updates adequaat te kunnen plannen en een effectief licentiebeheer te kunnen handhaven.	n/a
6.10	Alle geleverde apparatuur en programmatuur exact in kaart brengen (welke klanten gebruiken wat, inclusief versies): Het is belangrijk om alle geleverde apparatuur en programmatuur in kaart te brengen om een nauwkeurig overzicht te hebben van het IT-landschap. Dit bevordert effectief beheer, maakt proactief onderhoud mogelijk en waarborgt dat beveiligingsupdates tijdig kunnen worden toegepast bij klanten.	n/a
6.12	Vorbereid zijn om verbeteringen eenvoudig te installeren (plan hoe te gaan releasen en patchen bij klanten): Vereenvoudig de implementatie van nieuwe versies en patches door een gestandaardiseerd stappenplan te volgen, bestaande uit identificatie, communicatie en distributie.	n/a

*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.

Copyright

© 2024 Alle intellectuele eigendomsrechten, waaronder auteursrechten, handelsmerken en ontwerprechten in en op deze cybersecurity norm zijn voorbehouden. Zonder voorafgaande toestemming is het niet toegestaan om enig deel van dit document te kopiëren, wijzigen of anderszins te gebruiken. Dit document is dynamisch van aard. Dit is de versie van 03-04-2024. Raadpleeg de meest recente versie op www.nis2qualitymark.eu.

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

Hoewel de maatregelen opgenomen in het NIS2 Quality Mark en gerelateerde overzicht van maatregelen zijn ontwikkeld door experts en met de grootst mogelijke zorg zijn samengesteld, worden geen garanties gegeven met betrekking tot de correctheid, volledigheid, betrouwbaarheid, geschiktheid, of beschikbaarheid van het NIS2 Quality Mark en de daarin opgenomen informatie, producten, diensten, of gerelateerde grafieken. Het gebruik van het NIS2 Quality Mark en gerelateerde overzicht van maatregelen zijn volledig voor het risico van de gebruiker. Elke aansprakelijkheid voor schade, direct of indirect, voortvloeiend uit of in enig opzicht verband houdend met het gebruik van het NIS2 Quality Mark en gerelateerde overzicht van maatregelen wordt uitgesloten.

In het NIS2 Quality Mark mapping overzicht kunnen verwijzingen zijn opgenomen naar andere standaarden, waaronder ISO 27001 en NEN 7510, uitsluitend voor informatieve doeleinden en om mogelijke samenhang of raakvlakken te identificeren. Deze verwijzingen impliceren geen associatie of goedkeuring van de inhoud van de andere standaarden. Het NIS2 Quality Mark en gerelateerde overzicht van maatregelen en de genoemde andere standaarden zijn afzonderlijke en unieke documenten. Alle rechten met betrekking tot andere standaarden die in het document worden genoemd, behoren toe aan de respectieve rechtmatige eigenaren van die standaarden.

Op NIS2 Quality Mark en gerelateerde overzicht van maatregelen rust auteursrecht. Geen deel van deze standaard mag worden gereproduceerd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorafgaande schriftelijke toestemming.