VAN OERS



Whitepaper
Cyberbeveiligingswet (NIS2) implementeren

VANOERS.NL

Cyberbeveiligingswet (NIS2) implementeren

Drie routes en hoe u de juiste kiest

Whitepaper voor bestuurders, IT-verantwoordelijken en organisaties die een duidelijk stappenplan willen in hun Cbw-aanpak.

De Cyberbeveiligingswet (Cbw), de Nederlandse implementatie van de Europese NIS2-richtlijn, zorgt ervoor dat cybersecurity niet langer uitsluitend een technisch vraagstuk is. Voor organisaties wordt digitale weerbaarheid een kwestie van bestuurlijke verantwoordelijkheid, risicobeheersing en aantoonbaarheid. Wie met de Cbw aan de slag gaat, merkt al snel dat de grootste uitdaging niet zit in het implementeren van losse maatregelen, maar in het kiezen van een logische aanpak.

Juist daar gaat het in de praktijk vaak mis. Organisaties starten met het implementeren van maatregelen, zonder eerst te bepalen welke aanpak past bij de organisatie. Dat leidt tot versnippering, dubbel werk en discussies over aantoonbaarheid. Deze whitepaper laat zien welke drie routes in de praktijk het meest voorkomen, wat de verschillen zijn en wanneer welke route het beste aansluit.



Waarom deze whitepaper?
Niet omdat de Cbw nog een extra checklist vraagt, maar omdat organisaties behoefte hebben aan richting. Wie vooraf de juiste route kiest, voorkomt later extra werkzaamheden.

Veel organisaties starten verkeerd met de Cbw

De invoering van de NIS2-richtlijn roept bij veel organisaties dezelfde reflex op: er moet iets gebeuren, maar waar moeten we beginnen? Er worden losse maatregelen geïmplementeerd, maar een integrale aanpak ontbreekt. In deze eerste fase ontstaat juist een risico. De aandacht gaat volledig uit naar wat er moet worden gedaan, terwijl de vraag hoe de organisatie dit wil benaderen nog niet is beantwoord. Hierdoor loopt de organisatie op lange termijn risico doordat maatregelen onvoldoende geborgd zijn binnen de organisatie.

Dat verschil lijkt klein, maar is in de praktijk fundamenteel. De Cbw is geen norm met één vaste implementatiewijze. Het is wetgeving die beschrijft welke verplichtingen gelden, zonder dat er één standaardmethode wordt voorgeschreven om daaraan te voldoen. Daardoor kunnen organisaties kiezen voor verschillende benaderingen. Sommige organisaties bouwen voort op een bestaand managementsysteem. Andere kiezen voor een control-based benadering waarin de wet direct wordt vertaald naar concrete beheersmaatregelen. Weer andere organisaties gebruiken bestaande normenkaders zoals NIS2 Supply Chain of ISO 27001 als praktisch groeimodel.

Wanneer de strategische keuze voor een aanpak uitblijft, ontstaan bijna altijd dezelfde problemen. Losse maatregelen sluiten onvoldoende op elkaar aan, documentatie is niet consistent en bij audits of toezicht blijkt dat het geheel niet goed aantoonbaar is. In zulke situaties moet een organisatie niet alleen aanvullen, maar vaak ook herstructureren. Daarmee wordt de Cbw duurder en tijds-intensiever dan nodig.



De kernvraag
De belangrijkste vraag is niet welke maatregel als eerste moet worden opgepakt, maar vanuit welk omkaderd uitgangspunt de organisatie de Cbw wil implementeren.

De Cbw vraagt om keuzes, geen checklist

De Nederlandse Cyberbeveiligingswet geeft invulling aan de Europese NIS2-richtlijn en vertaalt die naar nationale wetgeving met onder meer een registratieplicht, zorgplicht, meldplicht en toezicht. Deze wet wordt uitgewerkt via de Cyberbeveiligingswet, het Cyberbeveiligingsbesluit en sectorale invulling, bijvoorbeeld voor de overheid via BIO2. Daarmee ontstaat voor organisaties een gelaagd compliance-landschap waarin juridische verplichtingen, sectorspecifieke normen en praktische implementatiekeuzes samenkomen.

Dat maakt de Cbw wezenlijk anders dan een klassieke certificeringsvraag. Waar een norm als ISO 27001 of NEN 7510 organisaties een managementsysteem biedt met een vaste systematiek van context, risico's, maatregelen en continue verbetering, vertrekt de Cbw vanuit maatschappelijke weerbaarheid en wettelijke zorgplichten. De bedoeling is helder: organisaties moeten cyberrisico's beheersen, significante incidenten kunnen melden en bestuurlijk verantwoordelijkheid nemen. De concrete inrichting daarvan is echter afhankelijk van omvang, sector en volwassenheid. Om deze reden kunnen organisaties de wetgeving op verschillende manieren implementeren.

In de praktijk zien wij daardoor drie dominante routes ontstaan. De eerste route is de management-systeemroute via ISO 27001 of, in de zorg, NEN 7510. De tweede route is een controlgerichte route via het Cbw (NIS2) Control Framework van Auditdienst Rijk en NOREA. De derde route is een pragmatisch groeimodel via het NIS2 Supply Chain. Die drie benaderingen vullen verschillende behoeften in. De keuze voor een route bepaalt niet alleen de implementatie, maar ook de manier waarop bewijs, governance en volwassenheid in de organisatie worden opgebouwd.

Wat deze whitepaper doet?
Deze whitepaper helpt niet alleen bij het begrijpen van de drie routes, maar vooral bij het maken van een bewuste keuze. Dat voorkomt dat de Cbw een verzameling losse maatregelen wordt zonder samenhang.

Route 1: ISO 27001 of NEN 7510 als managementsysteemroute

Voor organisaties die Cbw-compliance willen opbouwen vanuit structuur is een managementsysteem vaak de meest logische route. ISO 27001 is daarbij het bekendste kader. De norm richt zich op het opzetten, invoeren, onderhouden en continu verbeteren van een Information Security Management System (ISMS). In de zorg vervult NEN 7510 die rol, waarbij de herziene NEN 7510:2024 expliciet aansluit op de recente ISO-ontwikkelingen en ook beter ondersteunt bij het invullen van NIS2-vereisten.

De kracht van deze route zit in de samenhang. Een organisatie begint niet bij een losse control, maar bij contextbepaling, risicoanalyse, scope, rollen en verantwoordelijkheden. Van daaruit worden maatregelen gekozen, beheerd en geëvalueerd. Dat maakt een ISO- of NEN-route geschikt voor organisaties die een blijvende borging zoeken. De Cbw vraagt immers niet alleen om het bestaan van maatregelen, maar ook om bestuurlijke betrokkenheid, periodieke evaluatie en aantoonbaarheid over tijd. Een managementsysteem ondersteunt precies die behoefte.

Daar staat tegenover dat dit ook de meest intensieve route is. Een goede implementatie vraagt discipline, eigenaarschap en voldoende volwassenheid in de organisatie. Zeker waar nog weinig formele governance is ingericht, kan een volledige ISO 27001- of NEN 7510-implementatie als zwaar of langzaam worden ervaren. Dat maakt deze route niet minder geschikt, maar wel minder vanzelfsprekend voor organisaties die vooral snel eerste stappen willen zetten, een lagere volwassenheid hebben of nog in de verkenningsfase zitten.

Een tweede nuance is dat ISO 27001 of NEN 7510 veel NIS2-thema's dekt, maar de Cbw niet volledig dekt. Om te voldoen aan de Cbw moeten organisaties voldoen aan aanvullende vereisten zoals de registratieplicht, meldplicht, bestuurlijke verantwoordelijkheid en ketenverantwoordelijkheid. In de praktijk is dit dus een sterke route, mits organisaties accepteren dat aanvullingen nodig blijven om volledig aan de wet te voldoen.

Wanneer deze route past

ISO 27001 of NEN 7510 past vooral bij organisaties die de Cbw niet als los project willen benaderen, maar als structureel onderdeel van governance, risicobeheersing en continue verbetering. Tevens kan dit met een certificering aantoonbaar gemaakt worden.

Route 2: het Cbw (NIS2) Control Framework als controlgerichte route

De tweede route ontstaat vanuit de behoefte om de wet direct hanteerbaar te maken. Het Cbw (NIS2) Control Framework van Auditdienst Rijk en IT audit beroepsorganisatie NOREA is precies daarvoor ontwikkeld. Dit framework ondersteunt organisaties bij het verkrijgen van inzicht in de mate waarin zij invulling geven aan de Cyberbeveiligingswet. Het doel is niet het introduceren van nog een extra norm, maar het structureren en evalueren van wettelijke verplichtingen, inclusief aanvullende sectornormen zoals BIO2, DORA en voor de zorg ook NEN 7510.

Het voordeel van deze route is dat zij voor veel organisaties direct begrijpelijk is. In plaats van een volledig managementsysteem op te bouwen, wordt concreet aangegeven welke maatregelen dienen te worden geïmplementeerd om te kunnen voldoen aan de Cyberbeveiligingswet. Daarnaast is er een koppeling toegevoegd met bekende normenkaders zoals BIO2, DORA en ISO 27001, zodat snel overzichtelijk is welke maatregelen eventueel al zijn genomen. Dat maakt het framework geschikt voor fit-gap analyses, nulmetingen, audits en bestuurlijke stuurinformatie. Het framework biedt bestuurders, IT-verantwoordelijken en auditors overzicht en helpt verbeter-punten te identificeren.

Deze controlgerichte benadering is sterk voor organisaties die snel inzicht willen creëren en prioriteiten willen stellen. Zeker wanneer de vraag speelt waar de grootste compliance-risico's zitten of welke onderdelen al voldoende zijn ingericht, kan een framework als dit veel sneller houvast geven dan een volledig managementsysteem. Het is ook geschikt voor organisaties die meerdere normenkaders naast elkaar moeten beheren en behoefte hebben aan één geïntegreerd referentiekader voor interne beheersing.

Tegelijkertijd vraagt deze route om een belangrijke nuance. Een control framework maakt compliance inzichtelijker, maar organiseert niet automatisch de onderliggende governance. Het risico bestaat dat een organisatie vooral stuurt op de concrete maatregelen en minder aandacht heeft voor de managementcyclus daarachter. Daarom werkt deze route het beste wanneer zij wordt gebruikt als tussenlaag: enerzijds om de wet concreet te maken, anderzijds om uitkomsten te vertalen naar processen, eigenaarschap en verbetering.



Sterke toepassing
Het Cbw (NIS2) Control Framework is vooral sterk wanneer de organisatie behoefte heeft aan inzicht, prioritering, toetsbaarheid en een brug tussen wetgeving en uitvoering.

Route 3: NIS2 Supply Chain als pragmatisch groeimodel

De derde route is in veel opzichten de meest praktische en tegelijk de meest verkeerd begrepen. NIS2 Supply Chain is ontwikkeld als hulpmiddel voor organisaties die zelf vaak niet rechtstreeks onder NIS2 vallen, maar wel onderdeel zijn van de keten van een Cbw-plichtige organisatie. Het NIS2 Supply Chain is een praktisch, schaalbaar en risicogebaseerd model met drie niveaus, afgestemd op het risico dat een leverancier vormt voor zijn afnemer. Daarmee is het nadrukkelijk bedoeld om cybersecurity in de keten aantoonbaar en haalbaar te maken.

Juist om die reden is NIS2 Supply Chain voor veel organisaties een aantrekkelijk startpunt. De benadering is concreet, begrijpelijk en beter behapbaar dan een volledig ISO 27001-traject. Organisaties kunnen ermee beginnen hun belangrijkste belangen te identificeren, leveranciers en afhankelijkheden in kaart te brengen, basismaatregelen te implementeren en aan klanten of ketenpartners te laten zien dat zij werk maken van digitale weerbaarheid. Voor veel mkb-organisaties is dat precies de stap die nodig is om van losse beveiligingsmaatregelen naar een meer gestructureerde aanpak te groeien. In die zin is NIS2 Supply Chain een bruikbaar groeimodel. Voor organisaties die via klanten indirect met de Cbw te maken krijgen, kan dit een zeer verstandige route zijn.

Voor direct Cbw-plichtige organisaties ligt dat anders. Voor deze organisaties moet nadrukkelijk onderscheid worden gemaakt tussen een bruikbaar hulpmiddel en een volledige invulling van de wet. Het NIS2 Supply Chain ondersteunt bij te nemen stappen en een stapsgewijze implementatie van ISO 27001 of NEN 7510, maar is geen certificering om aan te tonen dat een Cbw-plichtige organisatie volledig voldoet aan de wet. Er bestaat geen officiële Cbw-certificering; compliance draait om aantoonbaarheid van de juiste maatregelen, bestuurlijke betrokkenheid en de inrichting van processen. NIS2 Supply Chain kan daar wel aan bijdragen, maar dekt die bredere verplichting niet zelfstandig af.

Concreet betekent dit dat NIS2 Supply Chain voor een Cbw-plichtige organisatie vooral waardevol is als onderdeel van een bredere aanpak. Het kan helpen als een trapsgewijze aanpak waarbij de Cyberbeveiligingswet in stappen kan worden geïmplementeerd. Het is wel belangrijk om scherp te houden dat er aanvullende verplichtingen zijn voor Cbw-plichtige organisaties zoals de zorgplicht, meldplicht en bestuurlijke verantwoordelijkheid.

De juiste positionering

NIS2 Supply Chain is sterk als groeimodel. Voor Cbw-plichtige organisaties is het echter geen eindstation, maar een bouwsteen binnen een bredere route naar compliance.

De routes naast elkaar gezet

Hoewel de drie routes hetzelfde vraagstuk raken, namelijk het aantoonbaar beheersen van cyberrisico's onder de Cbw, vertrekken zij vanuit een ander basisprincipe. ISO 27001 of NEN 7510 vertrekt vanuit management en continue verbetering.

Het Cbw (NIS2) Control Framework vertrekt vanuit wet en specifieke controls. NIS2 Supply Chain is een vertrekpunt voor een concreet groeimodel. Daardoor is er geen universeel beste route. De juiste keuze hangt af van de vraag wat de organisatie wil oplossen: structurele borging, snelle toetsbaarheid of pragmatische implementatie.

Daarmee is ook verklaard waarom organisaties in de praktijk vaak elementen combineren. Een organisatie kan bijvoorbeeld een nulmeting en prioritering doen met een control framework, haar structurele borging inrichten via ISO 27001 of NEN 7510 en hiervoor het NIS2 Supply Chain als groeimodel hanteren.

Aspect	ISO 27001 / NEN 7510	Cbw (NIS2) Control Framework	NIS2 Supply Chain
Primair vertrekpunt	Managementsysteem en continue verbetering	Wetgeving, controls en volwassenheid	Groeimodel voor Cbw-compliance
Sterk in	Structurele borging, toetsbaarheid, governance	Nulmeting, prioritering, toetsbaarheid	Laagdrempelige start, groeipad
Minder sterk bij	Snelle start zonder bestaande governance of volwassen basis	Het automatisch inrichten van governance en een managementcyclus	Volledige invulling van Cbw voor direct Cbw-plichtige organisaties
Geschikt voor	Organisaties die structurele borging willen en dit eventueel aantoonbaar willen maken middels certificering.	Organisaties die snel inzicht en bestuurlijke sturing willen	Organisaties die pragmatisch willen starten en dit eventueel aantoonbaar willen maken middels certificering.
Rol voor Cbw-plichtige entiteit	Sterke hoofdroute	Sterke hoofd- of tussenroute	Ondersteunend groeimodel



Praktisch lezen van deze vergelijking

Wie zoekt naar een volledig en duurzaam stelsel, komt meestal uit bij een management-systeem. Wie eerst overzicht en bestuurlijke sturing wil, heeft veel aan het control framework. Wie een praktisch groeimodel wil, heeft veel aan het NIS2 Supply Chain.

Welke route past bij welk type organisatie?

Voor organisaties die al werken met formele governance, duidelijke eigenaarschappen en een bestaande audit- of compliancecyclus, ligt de route van ISO 27001 het meest voor de hand. Daar is vaak al genoeg structuur aanwezig om de Cbw op te nemen in een bredere cyclus van risico-analyse, beleid, evaluatie en verbetering. In de zorg kan NEN 7510 daarbij een logische keuze zijn, juist omdat de norm sectorspecifiek is en in de meest recente versie sterker aansluit op zowel ISO 27001 als de Cbw.

Voor organisaties die nog niet zover zijn, maar wel snel bestuurlijke duidelijkheid nodig hebben, is een controlgerichte benadering vaak effectiever. Dat geldt bijvoorbeeld voor organisaties die weten dat zij onder de Cyberbeveiligingswet vallen, maar waar nog onvoldoende scherp hebben wat de grootste gaps zijn. In dat scenario levert een de aanpak van het Cbw (NIS2) Control Framework vaak sneller bruikbare sturingsinformatie op.

Voor organisaties die stapsgewijs aan de slag willen met de Cyberbeveiligingswet en een lager volwassenheidsniveau hebben, is het NIS2 Supply Chain een passende aanpak. Deze aanpak is een praktische werkwijze om toe te groeien naar Cbw-compliance.

Vuistregel
Hoe groter de behoefte aan structurele borging, hoe logischer de route via een managementsysteem. Hoe groter de behoefte aan snelle duiding en toetsbaarheid, hoe logischer het control framework. Hoe groter de behoefte voor een praktische en laagdrempelige aanpak, hoe relevanter NIS2 Supply Chain wordt.

Waar het in de praktijk vaak misgaat

Een van de meest voorkomende knelpunten is dat organisaties de implementatieroute verwarren met het einddoel. Een certificaat, nulmeting of framework lijkt dan het antwoord op zichzelf, terwijl de echte opgave ligt in het aantoonbaar beheersen van risico's. Dat verschil is cruciaal. Wie te vroeg focust op het middel, loopt het risico dat de gekozen route onvoldoende past bij de aard van de organisatie of de wettelijke positie van de entiteit.

Een tweede fout is dat ketenbeveiliging te smal wordt geïnterpreteerd. De Cbw benadrukt leveranciersrisico's, maar ketenbeveiliging is meer dan het opvragen van een vragenlijst of het eisen van een keurmerk. Het vraagt om inzicht in afhankelijkheden, risico's en het maken van contractuele en operationele afspraken die passen bij hoe kritiek de leverancier is.

Een derde fout is bestuurlijke onderwaardering. De Cbw maakt cybersecurity expliciet tot een bestuursverantwoordelijkheid. Daarmee is het niet voldoende dat IT of de securityfunctie de maatregelen kent; het bestuur moet kunnen sturen, toezicht houden en ook scholing aantoonbaar hebben gevolgd.

Tot slot gaat het regelmatig mis in de volgorde. Organisaties willen snel voldoen en slaan daardoor informatie over die eerst nodig is om tot de juiste prioriteiten te komen. Denk aan een goede scope, een reële risicoanalyse, inzicht in de keten en helder eigenaarschap. Een gefaseerde aanpak is daarom geen teken van traagheid, maar van volwassenheid.

Praktisch gevolg
De kans op dubbel werk neemt sterk af wanneer organisaties eerst hun route bepalen, vervolgens hun scope en risico's scherpstellen en pas daarna maatregelen en bewijs inrichten.

Conclusie:
De Cbw begint met het kiezen van een route

De kern van Cbw-compliance is niet dat iedere organisatie dezelfde maatregelen op exact dezelfde manier invoert. De kern is dat organisaties passend en aantoonbaar omgaan met cyberrisico's, incidenten en bestuurlijke verantwoordelijkheid. Juist daarom is de keuze voor een implementatie-route zo belangrijk. Die route bepaalt of maatregelen samenhang krijgen, of de organisatie effectief prioriteert en of bewijs later overtuigend genoeg is voor klanten, auditors of toezicht-houders.

ISO 27001 en NEN 7510 bieden de sterkste basis voor organisaties die structurele borging willen. Het Cbw (NIS2) Control Framework is bijzonder sterk voor organisaties die bestuurlijke grip, specifieke controls en toetsbaarheid nodig hebben. NIS2 Supply Chain is een waardevol groei-model, maar voor direct NIS2-plichtige organisaties doorgaans niet voldoende als enige route. Wie dat onderscheid scherp houdt, maakt betere keuzes en voorkomt dat de Cbw wordt benaderd als verzameling losse acties.



Slotgedachte

De Cbw is geen excuus voor meer beleid zonder richting. Het is juist een aanleiding om governance, risico's, ketenafhankelijkheden en aantoonbaarheid in één samenhangende aanpak bijeen te brengen.

Disclaimer:
Deze whitepaper is bedoeld als richtinggevend document en niet als juridisch advies. De uiteindelijke toepasbaarheid van een route hangt altijd af van sector, omvang, ketenpositie en de specifieke context van de organisatie.

Contactpersonen | Marjon van de Lindeloof & Wesley Riool

Onderneem met voorsprong
VANOERS.NL