NIS2

Nieuwe regels.

Nieuwe kansen.

Nu handelen.

Casusbespreking Samen Slimmer: "Van compliance naar crisisbeheersing: De rol van de archivaris onder NIS2"

Van compliance-verplichting naar strategische hefboom voor een gezonde informatiehuishouding

Webinar host: Layla Hassan

AGENDA

01

NIS2

Wat is het, wie valt eronder, waarom nu?

02

De impact in beeld

Verplichtingen, risico's en boetes

03

Informatiehuishouding als fundament

Waarom I&A onmisbaar is voor NIS2-compliance

04

Aanknopingspunten & quickwins

Concrete acties voor records & info managers

05

Routekaart & prioritering

Hoe start je morgen? Wat doe je dit jaar?

VAN NIS1 NAAR NIS2 — WAT VERANDERT ER ECHT?

NIS1 2016	NIS2 2024/1 Juli 2026
7 sectoren	18+ sectoren incl. overheid, post, afval
Vrijwillige melding	Melding: 24u alert + 72u rapport
Beperkte handhaving	Boetes tot €10M of 2% omzet
Geen persoonlijke aansprakelijkheid	Bestuurders persoonlijk aansprakelijk

NIS2 is geen upgrade — het is een paradigmashift.

WIE VALT ONDER NIS2?

Essentiële entiteiten *Zwaarste verplichtingen + actief toezicht*	Belangrijke entiteiten *Lichtere eisen, reactief toezicht*
Energie, Transport, Bankwezen	Post, Chemie, Voedselproductie
Gezondheidszorg & farmacie	Maakindustrie (medisch, defensie)
Drinkwater, Digitale infra, Cloud	Digitale aanbieders, Sociale media
Overheid (centraal), Ruimtevaart	Lokale overheden, Onderzoek
Drempel: ≥250 mw of ≥€50M omzet	Drempel: ≥50 mw of ≥€10M omzet

BLOK 02

De impact in beeld

Verplichtingen, risico's, boetes en de harde realiteit van niet-naleving — voor bestuurders én uitvoerders.

24u
Eerste melding na incident

€10M
Max boete essentiele entiteiten

72u
Volledig incidentrapport

DE 10 KERNVERPLICHTINGEN VAN NIS2

Artikel 21 NISD — concrete eisen voor uw organisatie

01	Risicobeheer & beveiligingsbeleid	06	Cryptografie & encryptie
02	Supply chain beveiliging	07	Toegangsbeheer & HR-beveiliging
03	Incidentbeheer & -respons	08	Multi-factor authenticatie (MFA)
04	Bedrijfscontinuïteit & crisis	09	Meldplicht (24u / 72u / 1 maand)
05	Beveiliging bij systeemaanschaf	10	Bestuurlijke verantwoordelijkheid

Elk van deze 10 punten raakt direct aan informatiebeheer.

AANSPRAKELIJKHEID & SANCTIES

NIS2 maakt bestuurders direct verantwoordelijk

- Bestuurders persoonlijk aansprakelijk bij ernstige nalatigheid
- Tijdelijk verbod op uitoefening bestuursfuncties mogelijk
- Toezichthouder kan verplichte audits opleggen
- Publieke verklaring bij non-compliance (reputatieschade)

Boetekader: Essentieel tot €10.000.000 of 2% omzet | Belangrijk tot €7.000.000 of 1,4% omzet

BLOK 03

Informatiehuishouding als fundament

NIS2 compliance is alleen haalbaar als je weet wat je hebt,

waar het staat, wie er toegang toe heeft en hoe lang je het bewaart.

Dat is exact het domein van informatie- en archiefbeheer.

Zonder orde in informatie: geen betrouwbare melding, geen aantoonbare compliance, geen verdediging bij audit.

DE DIRECTE VERBINDING NIS2 ↔ INFORMATIEHUISHOUDING

Elk NIS2-artikel raakt aan informatiebeheer

NIS2-verplichting		Informatiehuishouding-actie
Risicobeheer	→	Informatieanalyse & classificatie
Incidentbeheer/meldplicht	→	Logretentie, audit trails, bewijsvoering
Toegangsbeheer	→	Autorisatiematrix & informatiestromen
Bedrijfscontinuïteit	→	Back-up, versiebeheer, herstelbare archieven
Supply chain beveiliging	→	Verwerkersovereenkomsten & datakwaliteit
Bestuurlijke verantw.	→	Accountabiliteitsrecords & besluitdossiers

WAT GAAT ER MIS ZONDER GOEDE INFORMATIEHUISHOUDING?

Shadow IT/ Schaduwarchief

Kritieke info buiten beheerde systemen — niet traceerbaar, niet veilig

Geen bewijs

Incident melden in 24u? Onmogelijk zonder actuele informatiekaart

Bewaar-chaos

Te lang bewaren vergroot aanvalsoppervlak; te vroeg is rechtsschending

Toegang op gevoel

Autorisatiematrix ontbreekt of al jaren niet bijgehouden

Leveranciers blindheid

Verwerkersovereenkomsten incompleet — supply chain risico ongedekt

Geen verantwoording

Bestuur kan compliance niet aantonen bij audit of RDI-onderzoek

BLOK 04

Aanknopingspunten & quickwins

Hier zit de kracht van informatie- en archiefbeheer:
jij hebt de tools, de kennis en het mandaat om
NIS2 compliance écht te versnellen.

Dit is jullie moment om van kostenpost naar strategische partner te worden.

AANKNOPINGSPUNT 1 — INFORMATIEANALYSE & CLASSIFICATIE

Weet wat je hebt. Echt. Volledig. Nu.

- Maak een actueel informatieregister (data-inventaris) per systeem en proces
- Classificeer op vertrouwelijkheid, integriteit en beschikbaarheid (VIB/CIA)
- Koppel classificatie aan bewaar- en beveiligingseisen
- Identificeer kroonjuwelen: welke info is bedrijfskritiek bij cyberaanval?

NIS2-link: Art. 21(2)a risicobeheer + Art. 21(2)e systeemaanschaf + AVG Art. 30

Quickwin: gebruik bestaand informatieregister als startpunt voor NIS2 data-inventaris

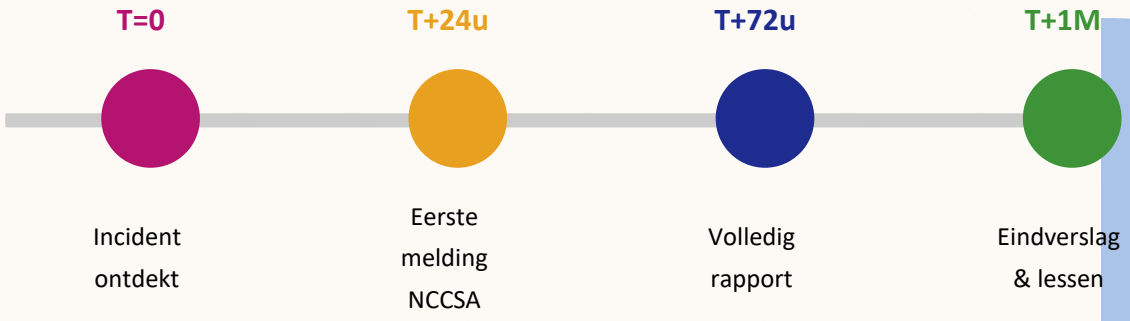
AANKNOPINGSPUNT 2 — RETENTIE, SELECTIE & VERNIETIGING

De juiste informatie, zo lang als nodig — niet langer.

Categorie	Bewaartermijn	IB-actie
Beveiligingslogboeken	Min. 12 maanden (NIS2)	**Borgen in retentieschema**
Incidentrapporten	Min. 5 jaar	**Archiefwaardig verklaren**
Risicoanalyses	Actueel + 3 versies	**Versiebeheer + archivering**
Verwerkersovereenk.	Looptijd + 7 jaar	**Centraal contractbeheer**
Operationele data	Per procesvereiste	**Selectielijst actualiseren**

AANKNOPINGSPUNT 3 — AUDIT TRAILS & BEWIJSVOERING

Geen log = geen bewijs. Geen bewijs = aansprakelijkheid.



Wat moet gelogd zijn:

- Toegangslogboeken systemen (wie, wanneer, wat) — min. 12 maanden
- Wijzigingshistorie kritieke bestanden en configuraties
- Authenticatie-events incl. mislukte pogingen

AANKNOPINGSPUNT 4 — TOEGANGSBEHEER & AUTORISATIEMATRIX

Principle of least privilege — wie heeft wat echt nodig?

De autorisatiematrix is het instrument van informatiebeheer — én een kerneis van NIS2:

Rol	Toegangsniveau
Records Manager	Informatieregister, retentieschema's, archief (schrijf)
Informatiearchitect	Systeem- en gegevensstroomoverzichten (lees + annoteer)
Beveiligingsfunctionaris	Logs, audits, incidentdossiers (lees)
Lijnmanager	Eigen procesinformatie (lees + upload)
Medewerker	Eigen werkomgeving, geen kruistoegang

Quickwin: autorisatiematrix + informatieregister koppelen = directe NIS2-aantoonbaarheid

AANKNOPINGSPUNT 5 — BEDRIJFSCONTINUÏTEIT & CRISISARCHIEF

Wat doe je als alles plat ligt? NIS2 eist een antwoord

- (Business Continuity Pla)BCP vereist kennis van kritieke informatiestromen per proces
- Archiefbeheer definieert (Recovery Time Objective)RTO per informatiecategorie
- Offline back-ups van kritieke records — harde eis bij ransomware
- Crisiscommuncatiedossiers vooraf opgesteld en toegankelijk

RTO & RPO per categorie

Categorie	RTO	RPO
Incidentdossiers	< 1 uur	< 15 min
Klantdata	< 4 uur	< 1 uur
Operationele proc.	< 24 uur	< 4 uur
Historisch archief	< 1 week	< 24 uur

AANKNOPINGSPUNT 6 — LEVERANCIERSBEVEILIGING & CONTRACTBEHEER

Jouw risico reikt verder dan jouw muren — NIS2 weet dat.

1

Inventariseer leveranciers

Welke externe partijen verwerken kritieke informatie? SaaS, cloud, ICT.

2

Verwerkersovereenkomsten

Zijn DPA's NIS2-proof? Beveiliging, meldplicht en auditrecht vastgelegd?

3

Risicoklassificatie

Hoog/midden/laag risico per leverancier op basis van toegang en kritiekheid.

4

Contractbeheer & renewals

Centrale registratie looptijden + herijking bij verlenging op NIS2-vereisten.

BLOK 05

Routekaart & prioriteiten

Hoe zet je de eerste stap? Wat doe je deze maand, dit kwartaal, dit jaar?

Een heldere prioriteitenmatrix voor informatie- en archiefprofessionals.

"Begin niet met techniek. Begin met weten wat je hebt."

ROUTEKAART NIS2 — INFORMATIEHUISHOUDING IN 3 FASEN

Gestructureerd, realistisch en direct toepasbaar

Fase 1
0–3 maanden

Meten & weten

- Informatieregister & datamapping
- Gap-analyse retentieschema's
- Inventariseer leveranciers & contracten
- Quickscan audit trail-capaciteit
- Rapport aan bestuur

Fase 2
3–9 maanden

Inrichten & borgen

- Retentieschema's actualiseren
- Autorisatiematrix opstellen
- VOK's NIS2-proof maken
- BCP-scenario's testen
- Logging-beleid borgen

Fase 3
9–18 maanden

Optimaliseren & aantonen

- Eerste interne NIS2-audit I&A
- Continuous monitoring logs
- Aantoonbaarheid bestuur versterken
- Leveranciersreviews in cyclus
- Lessons learned verwerken

TOP 5 QUICKWINS — START MORGEN

Haalbaar, impactvol, direct aantoonbaar voor NIS2

01	Informatieregister als NIS2 data-inventaris	Laag	↑ Hoog
02	Retentieschema actualiseren met NIS2-termijnen	Laag	↑ Hoog
03	Autorisatiematrix koppelen aan informatieregister	Midden	↑ Hoog
04	VOK-scan op kritieke leveranciers	Midden	↑ Midden
05	Bestuur briefen + mandaat regelen	Laag	↑ Strategisch

INTERNE SAMENWERKING — JIJ BENT DE VERBINDINGSOFFICIER

NIS2 is geen ICT-project. Het is een organisatiestuk.

CISO / Beveiligingsfunctionaris

Classificatie, risicoanalyse, log-eisen afstemmen

Privacy Officer / FG

Verwerkingsregister koppelen, AVG+NIS2 synergie

Juridische zaken

Contracten NIS2-proof, aansprakelijkheid borgen

ICT / IT-afdeling

Logging-capaciteit, back-up, systeemdocumentatie

Bestuur / Directie

Mandaat, beleid, accountabiliteitsrecords

Lijnmanagement

Procesinformatie aanleveren, bewustwording

Informatie- en archiefbeheer is het zenuwstelsel van NIS2-compliance — zorg dat je aan tafel zit.

HULPMIDDELEN & BRONNEN

Niet opnieuw het wiel uitvinden — gebruik wat er al is

Wet- & regelgeving	Standaarden & frameworks	IB-specifiek
NIS2-richtlijn (EU 2022/2555)	ISO 27001 / NEN 7510	NEN-ISO 15489 — Records management
Wbni — Wet beveiliging netwerk- en infosystemen	BIO (Baseline Informatiebeveiliging Overheid)	TMLO / MDTO — metadatastandaarden
NCSC Handreiking Informatiebeveiliging	NIST Cybersecurity Framework	KIDO — Kwaliteitsinstituut Nederlandse Gemeenten
AVG — koppeling verwerkingsregister	SURF NIS2 Handreiking	Nationaal Archief — Selectielijsten

SAMENVATTING — DE KERN IN 6 PUNTEN

Wat je vandaag meeneemt

1. NIS2 is geen ICT-feestje — het raakt de hele organisatie, inclusief I&A
2. Informatiehuishouding is de fundering: zonder orde geen bewijs, geen verdediging
3. Er zijn 6 aanknopingspunten: classificatie, retentie, audit trails, toegang, BCP, leveranciers
4. De 5 quickwins zijn haalbaar en direct aantoonbaar — start met het informatieregister
5. Samenwerking met CISO, FG, ICT en bestuur is essentieel — zet jezelf op de NIS2-agenda
6. Werk in 3 fasen (0–3, 3–9, 9–18 maanden) en rapporteer voortgang aan het bestuur

Informatiehuishouding

is jullie NIS2-superkracht.

Begin met weten wat je hebt.

Regel het mandaat. Lever de compliance.

Vragen? Discussie? Laten we het gesprek aangaan!
Bedankt en tot snel :-)!