Brightlyn
SOLVING COMPLEXITY

Getting in control of NIS2

Sandeep Gangaram Panday, MSc

Co-founder & security advisor

The Institute of Internal Auditors Netherlands

05-06-2026

IIA CONGRES 2026 PRIDE & PREJUDICE
4 & 5 JUNI AFAS THEATER LEUSDEN

Nice to meet you!

Sandeep Gangaram Panday, MSc RE CISA

Co-founder & security advisor @ **Brightlyn**
Chair Regulatory Taskforce NOREA
Chair DevOps Working Group NOREA

- DevOps in Control
- Ransomware in Control
- DORA in Control
- NIS2/Cbw in Control

sandeep@brightlyn.nl

Overview of EU Legislations in the Digital Sector

Network and Information Security Directive 2 (NIS2)

16/01/2023

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition & Single Market	Media	Finance
Digital Europe Programme Regulation (EU) 2021/694	Recovery and Resilience Facility Regulation (EU) 2021/241	Frequency Bands Directive (EEC) 1987/372	ePrivacy Directive (EC) 2002/58	Database Directive (EC) 1996/9	Regulation for a Cybersecurity Act (EU) 2019/881	Law Enforcement Directive (EU) 2016/680	Toys Regulation (EC) 2009/48, 2023/0290(COD)	Unfair Contract Terms Directive (UCTD) (EEC) 1993/13	EC Merger regulation (EC) 2004/139	Satellite and Cable Directive (EEC) 1993/83	Common VAT system (EC) 2008/112, 2022/0407(CNS), 2022/0409(CNS)
Horizon Europe Regulation (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation (EU) 2021/523	Radio Spectrum Decision (EC) 2002/676	European Statistics (EC) 2009/223	Community Design Directive (EC) 2002/6	Regulation to establish a European Cybersecurity Competence Centre (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment (EU) 2019/713	European Standardization Regulation (EU) 2012/1025	Price Indication Directive (EC) 1998/6	Technology Transfer Block Exemption (EC) 2014/316	Information Society Directive (EC) 2001/29	Administrative cooperation in the field of taxation (EU) 2011/16
Regulation on a pilot regime distributed ledger technology (EU) 2022/858	Connecting Europe Facility Regulation (EU) 2021/1153	Electromagnetic compatibility Directive (EMC) (EU) 2014/30	General Data Protection Regulation (GDPR) (EU) 2016/679	Enforcement Directive (IPR) (EC) 2004/48	NIS 2 Directive (EU) 2022/2555	Regulation on interoperability between EU information systems in the field of borders and visa (EU) 2019/817	Radio Equipment Directive (RED) (EU) 2014/53	E-commerce Directive (EC) 2000/31	Company Law Directive (EU) 2017/1132	Audio-visual Media Services Directive (AVMSD) (EU) 2010/13	Payment Service Directive 2 (PSD2) (EU) 2015/2366, 2023/0209(COD)
European Innovation Act	Regulation on High Performance Computing Joint Undertaking (EU) 2021/1173	Open Internet Access Regulation (EU) 2015/2120	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies (EU) 2018/1725	Protection of trade secrets (Directive) (EU) 2016/943	Cybersecurity Regulation (EU) 2023/2841	Regulation on terrorist content online (EU) 2021/784	eIDAS Regulation (European Digital Identity Framework) (EU) 2014/910	Unfair Commercial Practices Directive (UCPD) (EC) 2005/29	Screening of foreign direct investments Regulation (EU) 2019/452	Portability Regulation (EU) 2017/1128	Digital Operational Resilience Act (DORA Regulation) (EU) 2022/2554
	Regulation on Joint	European Electronic	Free flow of non-personal	Design Directive (EU) 2024/2823	Cyber Resilience Act (EU) 2024/2847	Temporary CSAM Regulation (EU) 2021/1232, 2022/0155(COD)	Regulation for a Single Digital Gateway (EU) 2018/1724	Directive on Consumer Rights (CRD) (EU) 2011/83	Market Surveillance Regulation (EU) 2019/1020	Satellite and Cable II Directive (EU) 2019/789	Crypto-assets Regulation (MiCA) (EU) 2023/1114
				...sory licensing of ...ts ...2129(COD)	Cyber Solidarity Act (Regulation) (EU) 2025/38	E-evidence Regulation (EU) 2023/1543	General Product Safety Regulation (EU) 2023/988	e-invoicing Directive (EU) 2014/55	P2B Regulation (EU) 2019/1150	Copyright Directive (EU) 2019/790	Anti-money laundering Regulation (AML) (EU) 2024/1624
					Information Security Regulation 2022/0084(COD)	Digitalisation of cross-border judicial cooperation (EU) 2023/2844	Machinery Regulation (EU) 2023/1230	Consumer Protection Cooperation Regulation (EU) 2017/2394	Single Market Programme (EU) 2021/690	European Media Freedom Act (EU) 2024/1083	Financial Data Access Regulation 2023/0205(COD)
					Digital package	Directive on combating violence against women (EU) 2024/1385	AI Act (Regulation) (EU) 2024/1689	Geo-Blocking Regulation (EU) 2018/302	Vertical Block Exemption Regulation (VBER) (EU) 2022/720		Payment Services Regulation 2023/0210(COD)
						Directive for combating sexual abuse and child sexual abuse material 2024/0035(COD)	Eco-design Regulation (EU) 2024/1781	Digital content Directive (EU) 2019/770	Digital Market Act (DMA Regulation) (EU) 2022/1925		Digital Euro 2023/0212(COD)
	Net Zero Industry Act (EU) 2024/1735	Digital Networks Act	collection for short-term rental (EU) 2024/1028			EU Digital Travel application, 2024/0670(COD)	Product Liability Directive (PLD) (EU) 2024/2853	Digital Contracts for Goods Directive (EU) 2019/771	Regulation on distortive foreign subsidies (EU) 2022/2560		Regulation on combating late payment 2023/0323(COD)
	EU Space Act	EU Cloud and AI Development Act	European Health Data Space (Regulation) (EU) 2025/327					Digital Services Act (DSA Regulation) (EU) 2022/2065	Horizontal Block Exemption Regulations (HBER) (EU) 2023/1066, (EU) 2023/1067		
	Quantum Act		Harmonization of GDPR enforcement procedures 2023/0202(COD)					Political Advertising Regulation (EU) 2024/900	Internal Market Emergency and Resilience Act (EU) 2024/2747		
	European Biotech Act		GreenData4all					Right to repair Directive (EU) 2024/1799	Platform Work Directive (PWD) (EU) 2024/2831		
	Advanced Materials Act		European Data Union Strategy					Digital Fairness Act	28th regime		
	Circular Economy Act								Revision of directives on Public Procurement		

= Applicable law

= In negotiation

= Planned initiative

Source: https://cdn.ceps.eu/wp-content/uploads/2025/07/CEPS-Zenner-Dataset-July-2025-1.pdf

The gap between attackers and defenders is widening

Brightlyn
SOLVING COMPLEXITY

Attackers are accelerating

+11%
Exploitation of vulnerabilities
Up from last year, now the leading initial-access vector

48%
of breaches involve ransomware
Up from prior year; impact is operational, not just data

+60%
Breaches via third parties
Supply chain is now a primary attack path

Defenders are falling behind

26%
of critical vulnerabilities fully remediated in 2025
A drop from last year

43 days
Median time to resolve
Up from 32 days last year

+50%
More critical vulnerabilities to patch in 2025
Backlog grows faster than capacity

NIS2 closes this gap with mandatory baseline controls and accountability.

Source: Verizon DBIR 2026

Small and public-sector organizations under pressure

5% → 35%

Small organizations
report insufficient cyber resilience
Up from 5% in 2022 to 35% in 2025 — a seven-fold jump.

38%

Public-sector organizations
say their resilience is insufficient
Up from 36%; the gap is widening, not closing.

71%

Cyber leaders agree
small organizations have hit a tipping point
Where they can no longer secure themselves against the growing complexity.

NIS2 closes this gap by raising the floor across critical and important entities.

Source: WEF Global Cybersecurity Outlook 2025

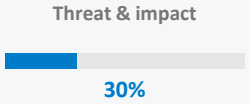
The more critical IT becomes, the bigger the target

Brightlyn
SOLVING COMPLEXITY

Supporting

Internal tools, reporting

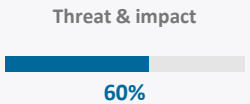
Useful, but the business runs without it.
Downtime is inconvenient but limited operational impact.



Mission critical

Core banking, ERP, claims

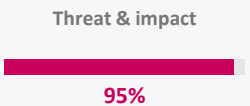
The business cannot operate without it.
An outage halts operations and revenue immediately.



Society critical

Energy, payments, telecom, healthcare

Society cannot function without it.
Disruption hits citizens, safety, and the economy.



Purpose of the law*

The law strengthens the cybersecurity of critical functions through rules on:

01

Manage risks

For network and information systems

02

Prevent incidents

Proactive security measures

03

Limit impact

Minimise consequences when incidents occur

04

Share information

On incidents, threats and vulnerabilities

* Cyberbeveiligingswet

Or simply..

Source: Adapted by the World Economic Forum and the University of Oxford from Linkov, I., & Trump, B.D. (2019). *The science and practice of resilience: Risk, systems and decisions*, Chapter 6. Springer. https://doi.org/10.1007/978-3-030-04565-4_6

Making our focus bigger..

COMMON PERSPECTIVE

Focus on cybersecurity

"Preserving confidentiality, integrity, and availability of information."

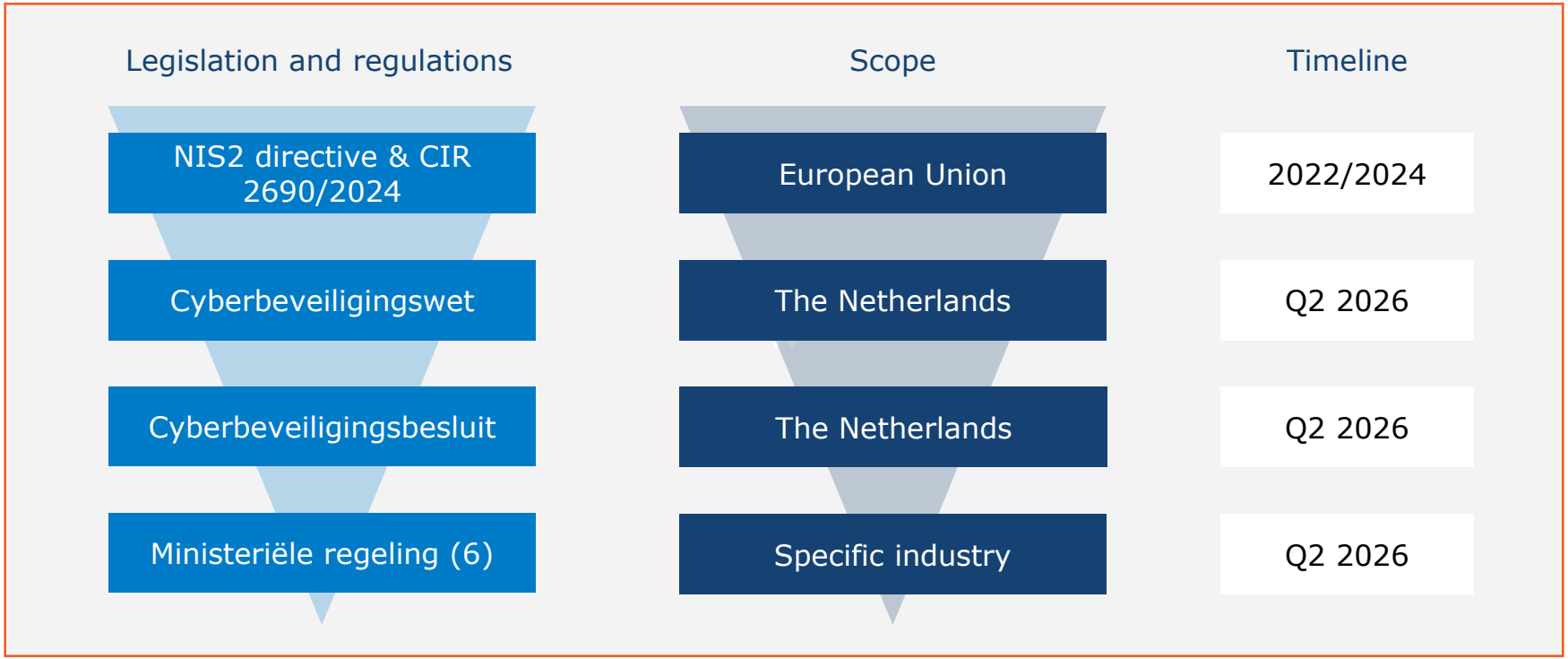
'NEW' PERSPECTIVE

Focus on resilience

"Anticipating, withstanding, recovering from, and adapting to adverse conditions, stresses, attacks, or compromises."

FOCUS NEEDS TO BE ON BOTH

NIS2 cascade



Brightlyn
SOLVING COMPLEXITY

Governance and Risk Management

1. Management responsibilities
2. Risk management framework
3. Risk assessments
4. (Internal) ICT audit

Operational Management

5. Asset management
6. Change management
7. ICT operations

Continuity Management

8. Backup management
9. Response & recovery

Incident Management

10. Incident classification
11. Incident management

Software and Systems Development

12. Acquisition, development, and maintenance
13. Project management

Third-party Risk Management

14. Third-party due diligence and selection
15. Third-party (standard) contract management
16. Third-party (critical) contract management
17. Third-party risk management
18. Subcontracting management

Resilience Testing

19. Digital operation resilience testing
20. Threat-led penetration testing

Security Management

21. Architectural and network security
22. Security monitoring & log management
23. Data and (legacy) system security
24. Encryption and cryptography
25. Identity and access management
26. Physical and environmental security
27. Security awareness
28. Vulnerability and patch management

Compared to DORA

Brightlyn
SOLVING COMPLEXITY

Same subjects, different depth and scope

NIS2

SCOPE
18 sectors, including financial institutions
DEPTH
Mostly the What
GUIDANCE
Additional frameworks needed for the How

DORA

SCOPE
Financial institutions only
DEPTH
Both the What and the How
STATUS
Lex specialis for financial institutions

FINANCIAL INSTITUTIONS IN SCOPE OF NIS2

Kredietinstellingen · Exploitanten voor handelsplatformen · Centrale tegenpartijen

What NIS2 adds on top of DORA*

Brightlyn
SOLVING COMPLEXITY

Governance & accountability

Board training
Mandatory training for board members within 2 years, with certificates as proof.

Personal liability
More concretely defined, with a clearer definition of “management body” and personal fines.

National measures
National authority to restrict or ban technology from specific suppliers.

Enforcement sanctions
Appoint monitoring officer, public disclosure of breach, suspension of board members, administrative fine etc.

* Non exhaustive overview

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Auditdienst Rijk
Ministerie van Financiën

Brightlyn
SOLVING COMPLEXITY

Studierapport Cbw (NIS2) Control Framework

Een praktisch framework bij de implementatie van de Cyberbeveiligingswet (NIS2-richtlijn), voor het versterken van de digitale operationele weerbaarheid.

Auteurs
L.M. Molewijk, ADR
S. Gangaram Panday, Brightlyn
E. Hummel, ADR
T. Meeuws, ADR

Auditdienst Rijk
Postbus 20201, 2500 EE Den Haag
Telefoon: 088 – 442 80 00
E-mail: adrcommunicatie@minfin.nl

NOREA
Postbus 242, 2130 AE Hoofddorp
Telefoon: 088 – 496 03 80
E-mail: norea@norea.nl

Cbw (NIS2) Control Framework is endorsed by

Statement from the NCSC and the Dutch supervisory authorities

"Het NCSC en de Cbw-toezichthouders hebben kennisgenomen van het kader ontwikkeld door ADR en NOREA, dat erop gericht is de sector een framework te bieden voor de praktische implementatie van de Cbw, Cbb en sectorspecifieke eisen. Hoewel NCSC en de Cbw-toezichthouders niet hebben bijgedragen aan de ontwikkeling ervan of een diepgaande beoordeling hebben uitgevoerd, zien ze de creatie van dergelijke kaders als een goede invulling op hun eerdere oproepen tot sectorbrede samenwerking. Deze samenwerking is cruciaal voor het verbeteren van de algehele cyberweerbaarheid van de sector en, waar gewenst, gezamenlijk ontwikkelen en bijwerken van standaarden die aan dit doel kunnen bijdragen. NCSC en de Cbw-toezichthouders benadrukken dat naleving van de toepasselijke wetten en voorschriften de verantwoordelijkheid blijft van elke organisatie. Het kader kan organisaties helpen hun aanpak te structureren en te versterken, maar het blijft altijd de verantwoordelijkheid van de organisatie zelf om te beoordelen of zij volledig voldoen aan de toepasselijke wet- en regelgeving."

Key features of the framework

NOREA

Auditdienst Rijk
Ministerie van Financiën

Studierapport Cbw (NIS2)
Control Framework

Een praktisch framework bij de implementatie van de Cyberbeveiligingswet (NIS2-richtlijn), voor het versterken van de digitale operationele weerbaarheid.

Auteurs
L.M. Molewijk, ADR
S. Gangaram Panday, Brightlyn
E. Hummel, ADR
T. Meeuws, ADR

Auditdienst Rijk
Postbus 20201, 2500 EE Den Haag
Telefoon: 088 – 442 80 00
E-mail:

NOREA
Postbus 242, 2130 AE Hoofddorp
Telefoon: 088 – 496 03 80
E-mail:

Actionable controls

Modular

Management system

Maturity model

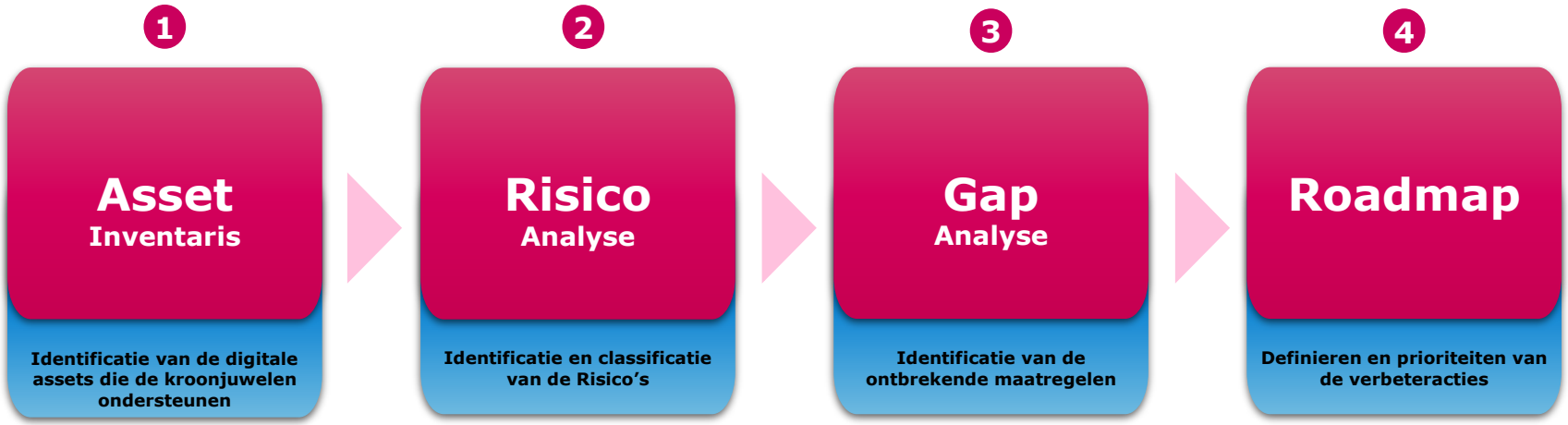
Management dashboard

Mappings

Recommended approach

Brightlyn
SOLVING COMPLEXITY

Risk perspective



Scope definition

Scope

In tabel 1. leggen organisaties vast op welke organisatie(onderdelen), systemen of processen de evaluatie is toegepast. De opsomming in de tabel is slechts een voorbeeld en kan naar wens worden aangepast. Het is belangrijk deze informatie vast te leggen, omdat het zicht geeft op het bereik van de evaluatie, helpt bij het interpreteren van de resultaten en ondersteunt bij verantwoording richting bestuur en toezichthouders. Met name voor organisaties met een divers landschap is dit van belang.

1	
(Kritieke) bedrijfsprocessen	
Betrokken afdeling(en)	
Gerelateerde kritieke applicaties	
Onderliggende support systemen	
Funtioneel management uitgevoerd door	
Infrastructuur management uitgevoerd door	
Betrokken derde partijen	

Gewenst volwassenheidsniveau

In tabel 2 geeft de organisatie per domein aan welk volwassenheidsniveau zij willen bereiken. Het is belangrijk dat de organisatie van tevoren nadenkt over het gewenste niveau, zodat duidelijk is wat het doel is van de evaluatie en welke verbeteracties passend zijn.

Het volwassenheidsmodel in het Cbw (NIS2) Control Framework is gebasseerd op het NBA-LIO/NOREA Volwassenheidsmodel voor informatiebeveiliging 3.0. Beide kennen vijf niveaus. **Organisaties zullen op basis van risicomanagement moeten bepalen welk volwassenheidsniveau gewenst is.** Daarbij is het waarschijnlijk dat dit zal verschillen per organisatieonderdeel, systeem, proces en/of onderwerp.

Bij twijfel over het gewenste volwassenheidsniveau, overweeg hetvolgende;
Als men uitgaat van het kunnen aantonen van opzet, bestaan en werking, komt dit vereenkomt met volwassenheidsniveau 3.
De Cyberbeveiligingswet geeft, naast het expliciet verplichten van aantoonbaarheid, ook aanknopingspunten die beter aansluiten bij volwassenheidsniveau 4, zoals periodieke evaluaties.

2.1	
Beleid over netwerk en informatiesystemen	
Beleid over risicomanagement	
Evaluatie	
Incidentenbehandeling	
Bedrijfscontinuïteit en crisisbeheer	
Beveiliging van de toeleveringsketen	
Verwerven, ontwikkelen en onderhouden van informatiesystemen	
Cyberhygiëne en opleidingen	
Beleid over cryptografie	
Beveiligingsaspecten t.a.v. personeel	
Beveiligingsaspecten t.a.v. toegangsbeleid	

Actionable controls

Thema	Domein	Cbw mapping	Control ID	Beheersmaatregel	Toelichting
Governance (art. 24)	Eisen aan de training, de trainer en het certificaat en doel van de training	Cbw art. 24.2 Cbb art. 21, 22, 23	14.1	informatiesystemen te kunnen identificeren en de gevolgen daarvan voor de diensten die door de entiteit worden verleend te kunnen beoordelen. Daarnaast zorgt de training dat ieder bestuurslid in staat is om risicobeheersmaatregelen op het gebied van cyberbeveiliging en de gevolgen daarvan voor de diensten die door de entiteit worden verleend te kunnen beoordelen.	a. de soorten risico's voor netwerk- en informatiesystemen; b. risicomanagementprocessen; c. risicobeoordelingsmethodiek; d. risicobeheersingsmaatregelen op het gebied van cyberbeveiliging (zoals ook vastgelegd in beveiligingsbeleid). Het certificaat van de training, bevat in ieder geval: a. de naam van het lid van het bestuur van de essentiële entiteit of belangrijke entiteit; b. de datum of data waarop de training is gevolgd; c. de behandelde onderwerpen in de training; en d. de naam van de aanbieder van de training. Het certificaat van de training is opgesteld in de Nederlandse taal of de Engelse taal.
		Cbw art. 24.3, 24.4	14.2	Ieder lid van het bestuur van een entiteit voldoet binnen twee jaar aan de trainingseisen. Daarnaast houdt ieder bestuurslid de kennis aantoonbaar actueel.	
	Meldplicht significante incidenten	Cbw art. 25.1, 25.2, 26.1, 33	15.1	De entiteit meldt ieder significant incident aan haar CSIRT en de bevoegde autoriteit.	Een incident is significant als het: a. een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of b. andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Vrijwillige meldplicht: elke entiteit heeft de mogelijke om vrijwillig een melding van een incident, bijna-incident of cyberdreiging te doen bij haar CSIRT of bevoegde autoriteit.

Modular

Brightlyn
SOLVING COMPLEXITY

	Toelichting	Mapping per Cbw-sector		
		Beheer van ICT-diensten, digitale infrastructuur en digitale aanbieders	Overheid	Bankwezen en infrastructuur voor de financiële markt
		Uitvoeringsverordening (EU) 2024/2690	BIO2	DORA Control Framework
e entiteit worden diensten die door de	a. de soorten risico's voor netwerk- en informatiesystemen; b. risicomanagementprocessen; c. risicobeoordelingsmethodiek; d. risicobeheersingsmaatregelen op het gebied van cyberbeveiliging (zoals ook vastgelegd in beveiligingsbeleid). Het certificaat van de training, bevat in ieder geval: a. de naam van het lid van het bestuur van de essentiële entiteit of belangrijke entiteit; b. de datum of data waarop de training is gevolgd; c. de behandelde onderwerpen in de training; en d. de naam van de aanbieder van de training. Het certificaat van de training is opgesteld in de Nederlandse taal of de Engelse taal.			
ast houdt ieder		Dit onderwerp valt buiten de scope van de Uitvoeringsverordening, hier dient de Cbb gevolgd te worden.	n.v.t.	1.2
	Een incident is significant als het: a. een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of b. andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Vrijwillige meldplicht: elke entiteit heeft de mogelijke om vrijwillig een melding van een incident, bijna-incident of cyberdreiging te doen bij haar CSIRT of bevoegde autoriteit.	Art. 3.1 Een incident wordt voor de toepassing van artikel 23, lid 3, van Richtlijn (EU) 2022/2555 met betrekking tot de relevante entiteiten als significant beschouwd indien aan een of meer van de volgende criteria is voldaan: a) het incident heeft voor de relevante entiteit direct financieel verlies veroorzaakt of kan verlies veroorzaken dat hoger is dan 500 000 EUR of meer dan 5 % van de totale jaaromzet van de relevante entiteit in het voorgaande boekjaar, indien dat lager is; b) het incident heeft het uitlekken van bedrijfsgeheimen als bedoeld in artikel 2, punt 1, van Richtlijn (EU) 2016/943 van de relevante entiteit veroorzaakt of kan dit veroorzaken; c) het incident heeft de dood van een natuurlijke persoon veroorzaakt of kan dit veroorzaken; d) het incident heeft aanzienlijke schade aan de gezondheid van een natuurlijke persoon veroorzaakt of kan dit veroorzaken; e) er heeft een succesvolle, vermoedelijk kwaadwillige en ongeoorloofde toegang tot netwerk- en informatiesystemen plaatsgevonden, die ernstige operationele verstoringen kan veroorzaken; f) het incident voldoet aan de criteria van artikel 4; g) het incident voldoet aan een of meer van de criteria van de artikelen 5 tot en met 14. Art 4. Incidenten die afzonderlijk niet als een significant incident in de zin van artikel 3 worden beschouwd, worden gezamenlijk als één significant incident beschouwd indien zij aan alle volgende criteria voldoen: a) zij hebben zich ten minste tweemaal binnen zes maanden voorgedaan; b) zij hebben dezelfde kennelijk onderliggende oorzaak; c) zij voldoen gezamenlijk aan de criteria van artikel 3, lid 1, punt a).	n.v.t.	11.3

Toelichting | Keuzes | Cbw (NIS2) Control Framework | ISMS evaluatie | Resultaten | Volwassenheid beheersmaatregel | Template | Mapping Uitvoeringsverordening | Mapping BIO2 | Mapping DORA

Management system

Thema	Domein	Control ID	Beheersmaatregel	VNG IBD vragen ISMS	Score zelf-evaluatie
Plan	Context	P.1	De entiteit heeft inzicht in de eigen organisatie en weet binnen welke context zij hun processen en diensten hebben ingericht. Daarnaast is de entiteit zich bewust van de toepasbaarheid van de wetgeving en de grenzen van de wetgeving binnen de eigen organisatie.	Is er documentatie aanwezig die interne en externe factoren geïdentificeerd? Is er een stakeholderanalyse die de belanghebbenden goed in kaart brengt? Zijn de behoeften van belanghebbenden goed in kaart gebracht? Is de reikwijdte van het ISMS bekend, is dit in een apart document of in de contextanalyse opgenomen? Heeft de organisatie bepaald wat zij wil vastleggen en monitoren in het ISMS? Let op: dit kan zo klein zijn als een spreadsheet en ze groot als een GRC-tool.	
	Leiderschap	P.2	Het bestuur van de entiteit toont leiderschap en betrokkenheid met betrekking tot het Informatiebeveiligingsbeleid.	Zijn verantwoordelijkheden voor informatiebeveiliging beschreven en staat hierin opgenomen dat de directie de uiteindelijke verantwoordelijkheid draagt? Is het beleid voor informatiebeveiliging door de directie goedgekeurd? Heeft de directie op enige wijze het informatiebeveiligingsbeleid kenbaar gemaakt naar de medewerkers en daarbij het belang van informatiebeveiliging uitgesproken? Zijn voor het ISMS en voor informatiebeveiliging benodigde middelen beschikbaar? D.w.z. zijn er budget en personen beschikbaar om uitvoer te geven aan de acties die nodig zijn i.h.k.v. het ISMS en informatiebeveiliging? Worden planningen, acties en bevindingen via de reguliere P&C cyclus gemonitord en bestuurd? Is er een door het (top)management (directie) goedgekeurd informatiebeveiligingsbeleid? Zijn er informatiebeveiligingsdoelstelllingen opgesteld? Stuurt het beleid aan op continue verbetering van het ISMS voor informatiebeveiliging? Is het beleid beschikbaar voor iedereen en wordt hierover gecommuniceerd?	
	Planning	P.3	De entiteit vertaalt strategische-organisatiedoelen, risico's en compliance eisen in een algemeen informatiebeveiligingsplan dat rekening houdt met de IT-infrastructuur en de veiligheidscultuur.	Is er een risicoprocedure welke omschrijft wanneer een risicoanalyse moet plaatsvinden, welke definities voor kans en impact gelden, en hoe en onder welke voorwaarden een risico geaccepteerd mag worden? Zijn de risico's m.b.t. het in stand houden van het ISMS in kaart gebracht en zijn de er maatregelen benoemd en getroffen om deze risico's te beheersen? Zijn de risico's m.b.t. informatie binnen de scope van het ISMS in kaart gebracht en zijn de er maatregelen benoemd en getroffen om deze risico's te beheersen? Hebben alle risico's een eigenaar? Is er een risico behandelplan/ risicoregister? Beschikt de organisatie over een verklaring van toepasselijkheid (VVT)? Wordt in deze VVT minimaal van alle BIO2 maatregelen aangegeven of deze wel of niet in scope zijn met daarbij een onderbouwing van de reden? NB: afhankelijk van het aandachtsgebied kunnen additionele beveiligingsmaatregelen vereist zijn (bijvoorbeeld OT) Zijn er doelstellingen voor informatiebeveiliging opgesteld en geaccordeerd door de directie? Zijn de	
			De entiteit heeft vastgesteld welke middelen nodig zijn en stelt ze dienovereenkomstig beschikbaar voor het inrichten, implementeren, onderhouden en continu verbeteren van informatiebeveiliging.	Zijn er voldoende middelen beschikbaar voor het ISMS en blijkt dit uit budgetten en jaarplannen? Zijn de noodzakelijke competenties vastgesteld van de perso(o)n(en) die onder haar gezag werkzaamheden verricht(en) die de prestaties van de organisatie op het gebied van informatiebeveiliging beïnvloeden? Is vastgesteld dat deze personen competent zijn op basis van de juiste scholing, opleiding of ervaring en worden waar nodig maatregelen genomen om de benodigde competentie te verwerven en worden de doeltreffendheid van de genomen maatregelen geëvalueerd? Zijn de medewerkers binnen de organisatie zich bewust van het informatiebeveiligingsbeleid? Is er bewustzijn bij management en medewerkers voor het naleven van de basis beveiligingsmaatregelen?	

Maturity model

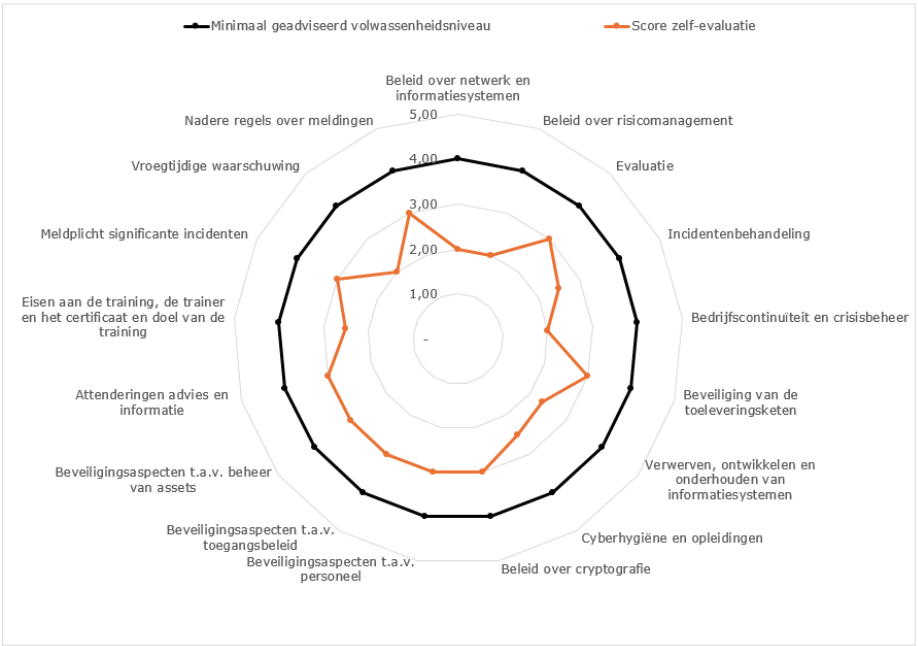
Domein	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
Beleid over de toeleveringsketen	Er is geen vastgesteld beleid met betrekking tot de beveiliging van de toeleveringsketen. Afhankelijkheden van leveranciers worden ad hoc benaderd.	Er is een conceptbeleid opgesteld over toeleveringsketenbeveiliging, maar dit is nog niet vastgesteld of organisatiebreed toegepast.	Er is vastgesteld beleid over de toeleveringsketen en afhankelijkheden worden geïnventariseerd. Toepassing vindt aantoonbaar plaats, maar zonder structurele borging of aantoonbaarheid	Het beleid is vastgesteld, breed gecommuniceerd en wordt toegepast binnen relevante processen. Afhankelijkheden worden periodiek geëvalueerd.	Het beleid is volledig geïntegreerd in governance en risicomanagement. Evaluatie en bijstelling vinden cyclisch plaats op basis van risico's en leveranciersontwikkeling. Er is continue monitoring van naleving.
Cyberbeveiligingseisen toeleveringsketen	Er worden geen of slechts incidenteel afspraken gemaakt over cyberbeveiliging met leveranciers.	Er zijn enkele schriftelijke afspraken gemaakt met leveranciers, maar deze zijn niet gebaseerd op uniform beleid. Naleving wordt niet actief bewaakt.	Schriftelijke afspraken over beveiliging worden systematisch gemaakt voor nieuwe contracten, gebaseerd op het beleid. Naleving wordt aantoonbaar reactief gemonitord.	Er is een standaard raamwerk voor beveiligingseisen in contracten. Naleving wordt actief en regelmatig gecontroleerd.	Cyberbeveiligingseisen zijn onderdeel van alle leveranciersrelaties. Er vindt gestructureerde toetsing en auditing plaats. Er is een escalatiemechanisme bij niet-naleving.
Overzicht van de toeleveringsketen	Er is geen centraal of actueel overzicht van leveranciers en bijbehorende afspraken.	Een overzicht wordt handmatig en beperkt bijgehouden, maar is incompleet of verouderd.	Er is een actueel overzicht van leveranciers, producten/diensten en afspraken. Dit wordt periodiek handmatig bijgewerkt.	Het leveranciersoverzicht is volledig, digitaal toegankelijk en geïntegreerd in de beheersprocessen. Wijzigingen worden systematisch verwerkt.	Het overzicht is realtime, gekoppeld aan contractbeheer en risicobeoordeling. Er is inzicht in ketenafhankelijkheden, risico's en beveiligingsafspraken per leverancier.
Ontwikkelen en onderhouden van informatiesystemen	Er zijn geen maatregelen of beleid voor veilige ontwikkeling en onderhoud van informatiesystemen. Kwetsbaarheden worden niet systematisch beheerd.	Er zijn enkele ontwikkel- en onderhoudsactiviteiten, maar zonder formeel beleid of vastgelegde procedures. Beveiligingsmaatregelen worden incidenteel toegepast.	Er is vastgesteld beleid waarin maatregelen zijn opgenomen voor veilige ontwikkeling en onderhoud van informatiesystemen, inclusief rollen, verantwoordelijkheden en basismaatregelen voor het omgaan met kwetsbaarheden. De maatregelen uit het beleid worden aantoonbaar toegepast tijdens ontwikkeling en onderhoud.	Er is structurele aandacht voor kwetsbaarheden, en updates en patches worden volgens vaste processen uitgevoerd.	Beveiliging is geïntegreerd in de gehele levenscyclus van informatiesystemen. Beleid wordt periodiek aangepast op basis van nieuwe kwetsbaarheden, dreigingen en technologische ontwikkelingen. Verbeteringen worden systematisch doorgevoerd.
Cyberhygiene en opleidingen (algemeen)	Er is geen structurele aandacht voor bewustwording of cyberhygiëne.	Er zijn incidentele communicatie- of bewustwordingsacties, zoals een	Er is een basisbewustwordingsprogramma actief.	Cyberbewustwording is geïntegreerd in het onboardingproces, periodieke	Er is een doorlopend en aangepast bewustwordingsprogramma, gebaseerd

Management dashboard

Brightlyn
SOLVING COMPLEXITY

Resultaten Cbw (NIS2) Control Framework

Thema	Domein	Gewenst volwassenheids-niveau*	GAP	Score zelf-evaluatie	Score reviewer
Zorgplicht	Beleid over netwerk en informatiesystemen	4,00	-2,00	2,00	-
	Beleid over risicomanagement	4,00	-2,00	2,00	-
	Evaluatie	4,00	-1,00	3,00	-
	Incidentenbehandeling	4,00	-1,50	2,50	-
	Bedrijfscontinuïteit en crisisbeheer	4,00	-2,00	2,00	-
	Beveiliging van de toeleveringsketen	4,00	-1,00	3,00	-
	Verwerven, ontwikkelen en onderhouden van informatiesystemen	4,00	-1,67	2,33	-
	Cyberhygiëne en opleidingen	4,00	-1,50	2,50	-
	Beleid over cryptografie	4,00	-1,00	3,00	-
	Beveiligingsaspecten t.a.v. personeel	4,00	-1,00	3,00	-
	Beveiligingsaspecten t.a.v. toegangsbeleid	4,00	-1,00	3,00	-
	Beveiligingsaspecten t.a.v. beheer van assets	4,00	-1,00	3,00	-
	Attenderingen advies en informatie	4,00	-1,00	3,00	-
Goverance	Eisen aan de training, de trainer en het certificaat en doel van de training	4,00	-1,50	2,50	-
Meldplicht	Meldplicht significante incidenten	4,00	-1,00	3,00	-
	Vroegtijdige waarschuwing	4,00	-2,00	2,00	-
	Nadere regels over meldingen	4,00	-1,00	3,00	-

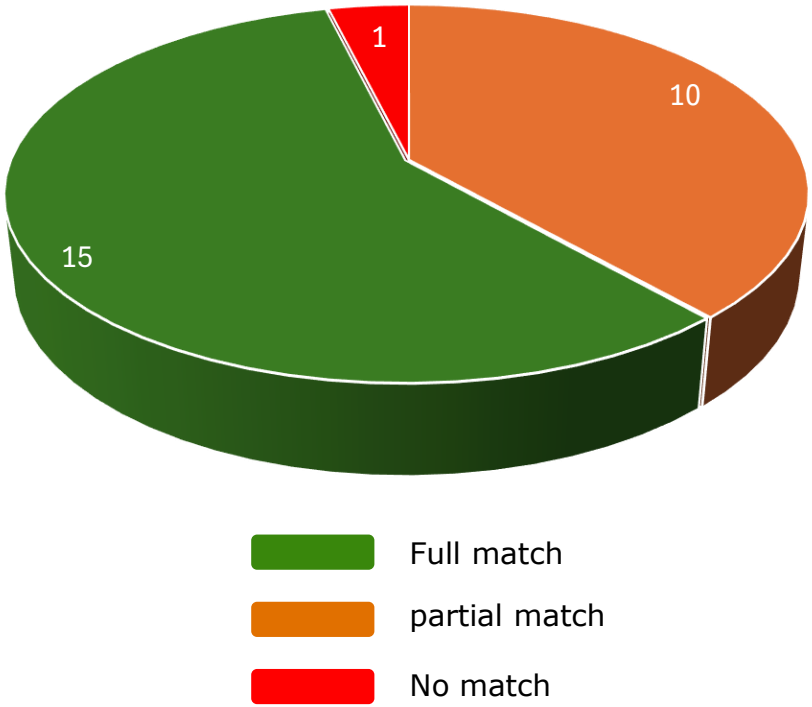


Toelichting | Keuzes | Cbw (NIS2) Control Framework | ISMS evaluatie | Resultaten | Volwassenheid beheersmaatregel | Template | Mapping Uitvoeringsverordening | Mapping BIO2 | Mapping DORA

ENISA GUIDANCE – Including ISO27001 mapping

- Specifically for digital infrastructures
- Recommended by ENISA for all NIS2 sectors
- Contains control guidance and example evidence
- Mapping based on the CIR 2024/2690
- Actually, not mappings but relationships
  - ISO27001
  - NIST CSF
  - CyFun etc.
- Contains relationships to 75% of the ISO27001 controls

ISO27001 mapping



Partial match:
- Logging specific incident information
- Specific BCP items
- Crisis management plan
- Periodic assessment of supplier
- Specific software lifecycle controls
- Training of boardroom members < 2 years
- Reporting of significant incidents

No match:
- Significant incident reporting timelines

Refinement, not revolution.

We need more focus and more agility

Auditdienst Rijk
Ministerie van Financiën

Presenting:
Boardroom training guideline

Boardroom training

Control 14.1 | Cbw art. 24.2 & Cbb art. 21, 22, 23:
"Het bestuur van de entiteit is, naar aanleiding van een training, in staat om risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren en de gevolgen daarvan voor de diensten die door de entiteit worden verleend te kunnen beoordelen. Daarnaast zorgt de training dat ieder bestuurslid in staat is om risicobeheersmaatregelen op het gebied van cyberbeveiliging en de gevolgen daarvan voor de diensten die door de entiteit worden verleend te kunnen beoordelen."

Control 14.2 | Cbw art. 24.3, 24.4:
"Ieder lid van het bestuur van een entiteit voldoet binnen twee jaar aan de trainingseisen. Daarnaast houdt ieder bestuurslid de kennis aantoonbaar actueel."

"In organizations that are best in class, you can ask business leaders, 'What are the most pressing cybersecurity issues?' And they will be able to name the top three because they are working on those issues"

Natalia Oropeza, Global Chief Cybersecurity Officer, Siemens

Key features

Brightlyn
SOLVING COMPLEXITY

Focus on DORA & NIS2

8 actionable objectives

NCSC & CSR guidelines integrated

Statement from DNB, AFM, RDI, CIO Rijk

Domain	Knowledge objectives	Responsibility objectives	Mapping to practical questions for improved boardroom dialogue based on the factsheet from the NCSC[4] and CSR[5]
1.Governance & Risk Management	• Understand the roles, responsibilities and accountability of the Management Body members, including the 3LoD. • Understanding the organisation's ICT risk management framework and the risk cycle (plan, do, check and act) • Being able to contribute to the definition of the organization's risk appetite and risk tolerance level • Understanding the organisation's critical functions and their degree of dependency on ICT services • Understand the expectations of the Digital Operational Resilience Strategy (DORA specific) or IT security strategy • Being able to understand and approve the most important security policies • Understand the need for transparent cyber reporting to and active oversight by the Management Body	• Carry out the management body responsibility for digital resilience and updating the ICT risk framework taking into account the organization's environment (e.g. increased threats or geopolitical developments) • Oversee the resilience of most critical ICT and the mitigation of the cyber security risks of the organization within the risk appetite • Understand and approve the Internal Audit year plan and specifically, the prioritization and added value of the audits in relation to the key IT risks • Oversee compliance with regulatory cyber requirements (DORA and NIS2 specific) or IT security strategy.	NCSC: • What are the most pressing issues I need to focus on? • What do you need to ensure that management allocates sufficient people and resources to achieve the objectives? • What mechanism is in place within the organization to secure the cybersecurity strategy and approval of policies around risk management by management? • With what frequency is cybersecurity on the agenda to ensure that there is sufficient progress on this topic? • What is the role and task of the CISO when it joins board meetings? • As a board member, what do I need to know to gain sufficient insight into this organization's cybersecurity risks? • Are risk assessments carried out, if so, what are the main issues and outcomes of the risk assessments carried out? • What are our biggest risks and threats and do we have sufficient control over them? • Which of these risks are incidental and/or structural? • How do we identify and calculate the probability and impact and distinguish between the different types of risks and what role do I play in them? • What residual risks are there? Are these acceptable?

Statement from authorities

"These knowledge objectives have been prepared by NOREA to provide guidance to the industry on practical implementation of boardroom training. DNB, AFM and the Cbw-supervisory authorities did not contribute to its development. The development of these knowledge objectives is in accordance with previous initiatives from DNB, AFM, the Cbw-supervisory authorities and CIO Rijk to work together within the sector to increase the overall cyber resilience. DNB, AFM, the Cbw-supervisory authorities and CIO Rijk appreciate these sectoral initiatives which support overall awareness of cyber resilience.
DNB, AFM, the Cbw-supervisory authorities and CIO Rijk stress that complying with applicable laws and regulations is at all times a responsibility of the institution. No confidence can be derived from the use of this guidance that parties thereby act in accordance with laws and regulations.
"

Take aways

Brightlyn
SOLVING COMPLEXITY

1 Continuous, AI-assisted testing
Annual sample-based testing is no longer sufficient. AI agents review contracts and SOC 2 reports, test key controls continuously and quantify sovereignty and concentration risk.

2 Security as a functional requirement
Treat security as a product feature, not a compliance overlay. Accept planned downtime so patches ship faster,

3 Assume breach, build to break
Adopt zero trust and chaos engineering. Architect for fast, frequent rebuild of critical components. Recovery time is the metric, not prevention alone.

4 Continuous, scenario-driven risk
Risk assessment moves from annual checklist to continuous and scenario-led. Controls adjust with the threat, not the calendar.

RETHINK CIA
Plan for secrets leaking (C), make identity attributes changeable (I) and design for fast recovery (A)

Thank you

Sandeep Panday

Sandeep@brightlyn.nl

https://www.linkedin.com/in/sandeep-panday/