Roadmap Cyberweerbaarheidspool MBO

Samen werken aan de randvoorwaarden

Doelstelling: *Deelnemende onderwijsinstellingen voldoen aantoonbaar aan de vastgestelde weerbaarheidseisen uit het NBA-normenkader, die als voorwaarde gelden om aanspraak te kunnen maken op de dekking vanuit de cyberweerbaarheidspool.*

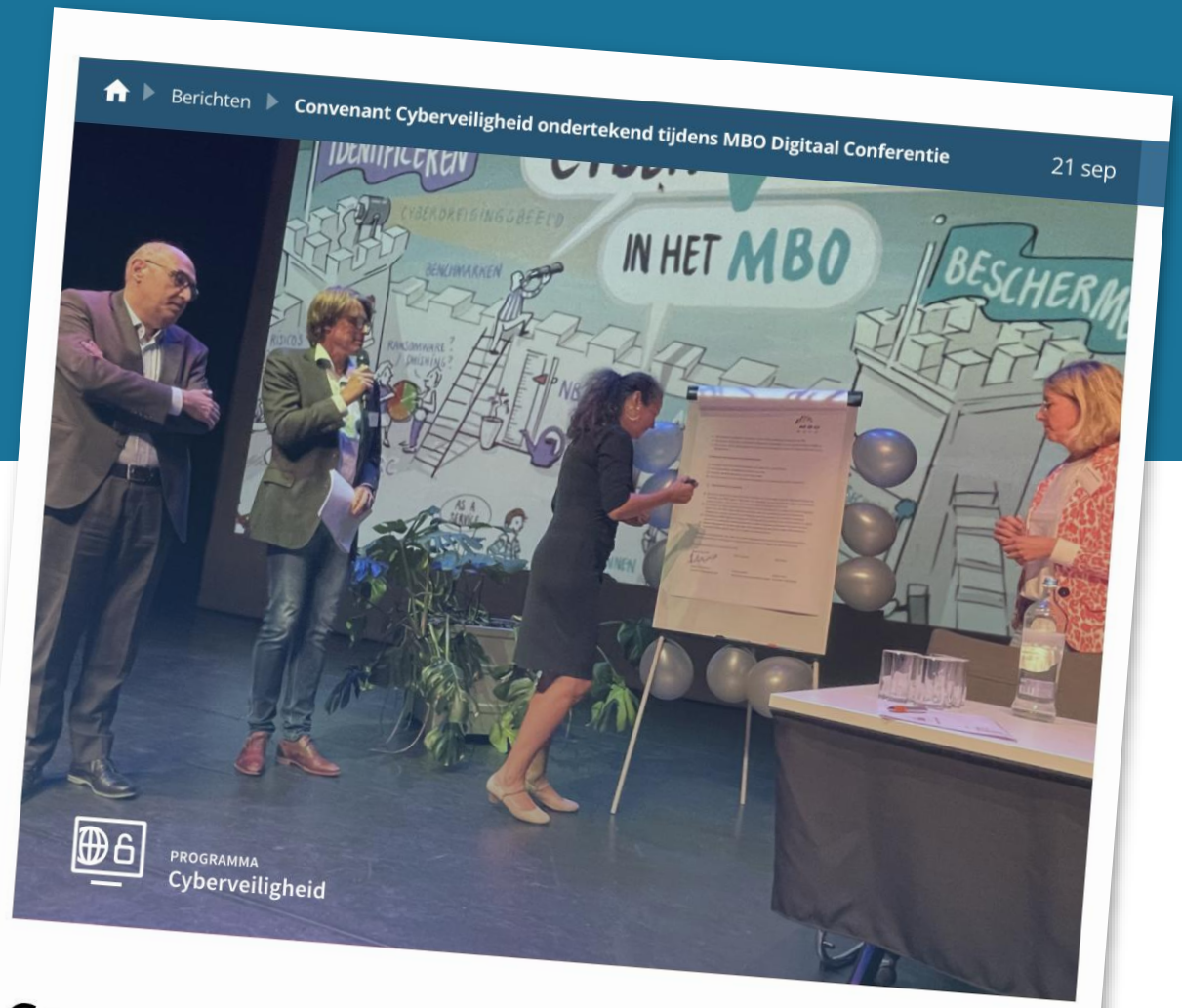
Doelstelling roadmap: Het gefaseerd ondersteunen van de onderwijsinstellingen vanuit het programma Cyberveiligheid om op de meest efficiënte wijze te voldoen aan de randvoorwaarden. Dit door het aanbieden van best practices, workshops, sjablonen, trainingen en – waar nodig – gerichte coaching.

Programma Cyberveiligheid
6 maart 2026
Versie 1.0

Agenda

1. Waarom de Cyberweerbaarheidspool
2. Aanleiding van de roadmap
3. Rol van de roadmap
4. Uitgangspunten van de roadmap
5. De roadmap
6. Roadmap ritme en rapportage
7. Vragen aan het publiek

mbo digitaal

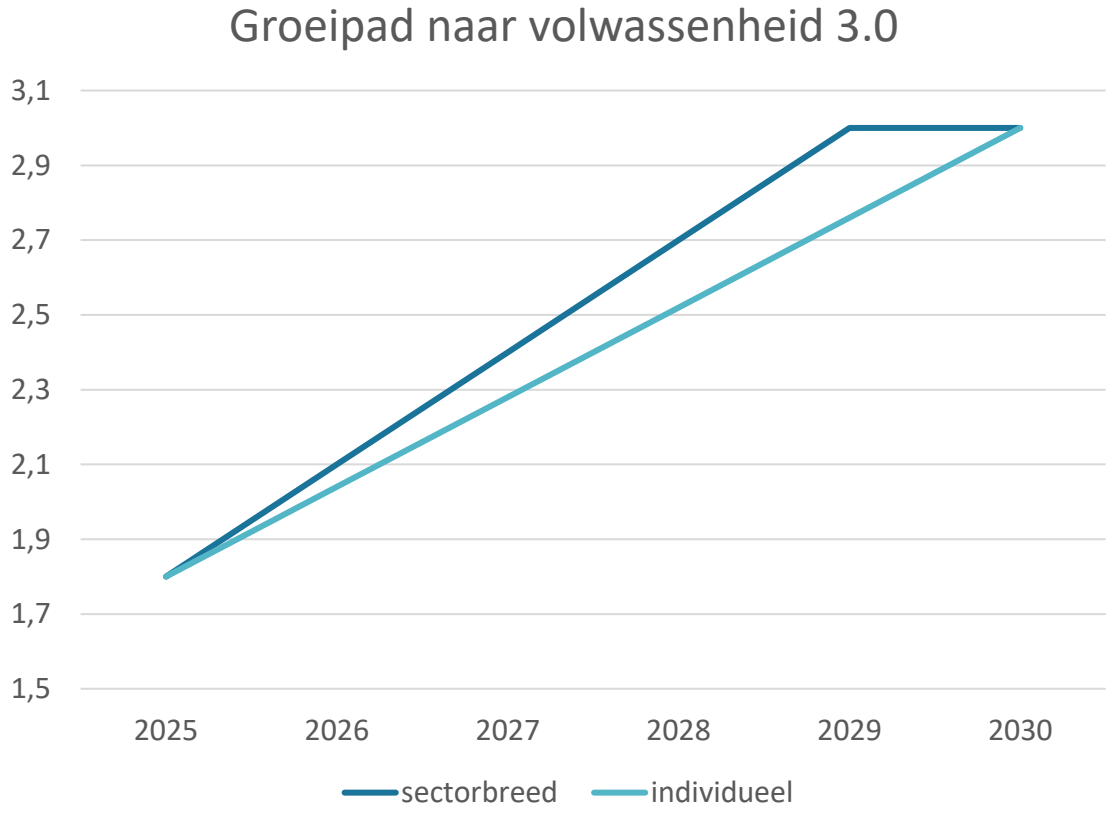


Convenant Cyberveiligheid ondertekend tijdens MBO Digitaal Conferentie

Vandaag is het Convenant Cyberveiligheid officieel ondertekend. Tijdens de MBO Digitaal Conferentie hebben Jozien Winterman (voorzitter Regiegroep IBP), Pauline Satter (voorzitter MBO Digitaal) en Adnan Tekin (voorzitter van de MBO Raad) het convenant met hun handtekeningen bekrachtigd. Hiermee onderstrepen zij dat de mbo-scholen samenwerken op het gebied van cyberveiligheid.

In het Convenant C

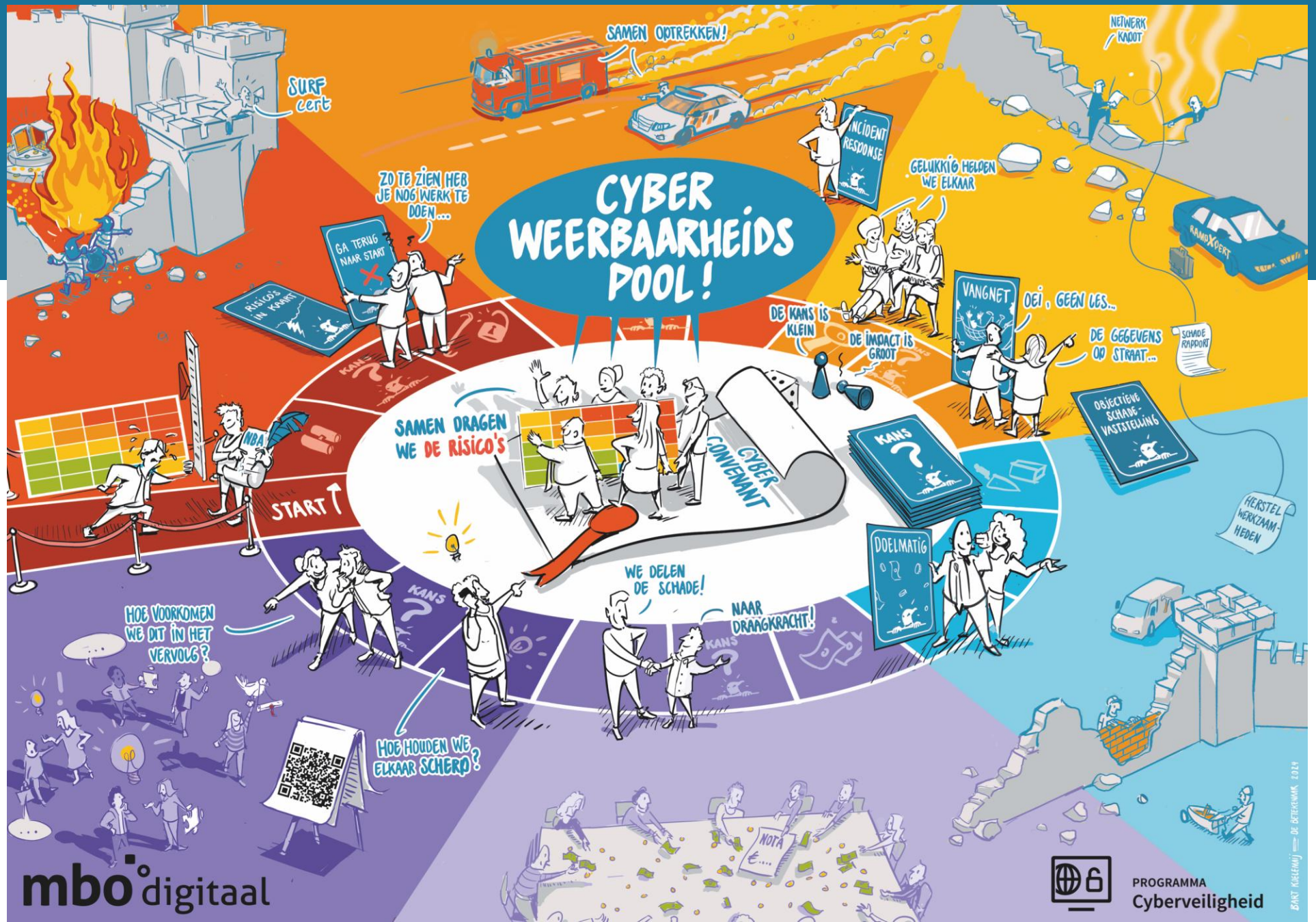
1. Waarom de cyberweerbaarheidspool



- Huidige gemiddelde volwassenheid na externe audits: 1.8
- Forse ambitie richting 3.0
- Na 2027 is er nog veel werk te doen, ook op het gebied van technische weerbaarheid
- Het programma Cyberveiligheid stopt echter per 30 september 2027 en de scholen kunnen en willen dat niet alleen

- **De cyberweerbaarheidspool borgt de verdere samenwerking na 2027**

mbo digitaal



1. Waarom de cyberweerbaarheidspool

Garantstelling als aanjager voor samenwerking en groei

- Voorwaarden volwassenheid en technische weerbaarheid
- Heldere doelstellingen
- Betekenis, duiding en prioritering van maatregelen
- Gemeenschappelijke planning richting 2030

We houden zicht en toezicht op elkaar

En organiseren de ondersteuning gezamenlijk

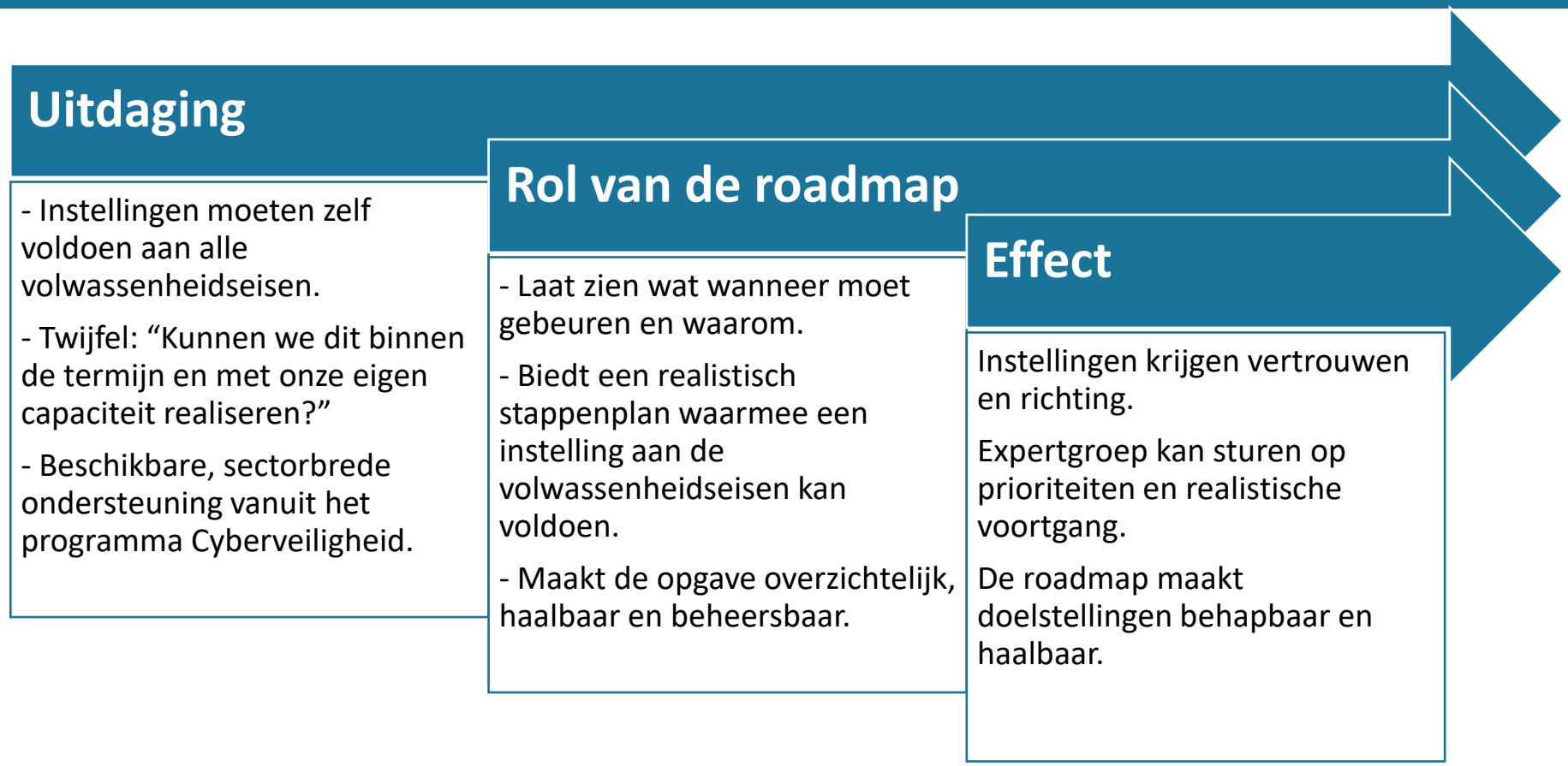
2. Aanleiding van de roadmap

Volwassenheidseisen cyberweerbaarheidspool
Om aanspraak te kunnen maken op de dekking vanuit de cyberweerbaarheidspool gelden er volwassenheidseisen voor 22 statements uit het NBA-toetsingskader IB. Hierbij is sprake van een ingroeimodel tot 1 oktober 2028.

	VWN 2	VWN 3	Totaal
Per 1 oktober 2027*	6	16	22
Per 1 oktober 2028*	1	21	22

Waarom een roadmap
Doel is om de mbo-instellingen comfort, perspectief en het vertrouwen te geven dat de gestelde volwassenheidseisen haalbaar zijn. De roadmap biedt de ondersteuning die de scholen nodig hebben om het vereiste niveau op efficiënte wijze te halen.

3. Rol van de roadmap



4. Uitgangspunten van de roadmap

1. **Geprioriteerde uitvoering in fasen**
   De roadmap is opgebouwd uit logisch opeenvolgende en geprioriteerde fasen. Instellingen kunnen – afhankelijk van hun eigen startsituatie en volwassenheidsniveau – bepalen welke fasen zij direct volgen en waar versnelling of verdieping nodig is. De fasering borgt dat alle instellingen op een efficiënte en gestructureerde manier kunnen groeien richting het vereiste volwassenheidsniveau.

2. **Inhoudelijke en sectorbrede expertise**
   Het Programma Cyberveiligheid ondersteunt de instellingen door het aanbieden van best practices, workshops, sjablonen, trainingen en – waar nodig – gerichte coaching. Deze ondersteuning is gericht op het versnellen van de implementatie van beleid, processen en technische maatregelen, waarbij onderwijsinstellingen ook van elkaars expertise gebruik kunnen maken op basis van de planning van de roadmap.

3. **Maximale benutting van SURF- en MBO-Digitaal-materialen**
   Er wordt, waar mogelijk, gebruik gemaakt van beschikbare templates, handreikingen, formats en best practices van SURF en MBO Digitaal. Dit versnelt het opstellen van beleid, procedures en technische documentatie, en bevordert harmonisatie binnen de sector.

4. **Uniformiteit waar mogelijk, maatwerk waar noodzakelijk**
   De roadmap biedt uniforme kaders voor alle instellingen, maar laat ruimte voor instellingsspecifieke verschillen in technische architectuur, procesinrichting en volwassenheidsniveaus.

5. **Informeren en rapporteren**
   Het programmateam krijgt periodiek inzicht in de voortgang, risico's en afwijkingen. Wanneer deadlines of volwassenheidsniveaus in het geding komen wordt dit door de betreffende instelling tijdig gerapporteerd aan het programmateam. Zo kunnen we tijdig bijsturen en voorkomen dat problemen pas zichtbaar worden bij de start van de Cyberweerbaarheidspool.

6. **Aantoonbaarheid en volwassenheid[illegible]atie in TrustBound**
   De instellingen leggen de volwassenheid[illegible]trols vast in TrustBound en onderhouden deze administra[illegible]MS-proces (PDCA-cyclus) en de evidence voor opzet, bestaan [illegible] daarmee inzichtelijk binnen TrustBound.

7. **Opzet, Bestaan èn Werking**
   Voor de volwassenheidseisen wordt doorgaans alleen op opzet en bestaan van de maatregelen getoetst. Hoewel dit voor de veiligheidswaarborgen voor de pool geen vereiste is, ligt de focus van de ondersteuning op opzet, bestaan èn werking. Iedere fase levert concrete, toetsbare output op.

8. **Verandermanagement en bewustwording**
   Onderwijsinstellingen worden ondersteund vanuit het programma via gerichte communicatie, trainingen en bewustwordingsprogramma's en de duiding van de impact van volwassenheidseisen op rollen en verantwoordelijkheden.

5. De roadmap 2026-2028

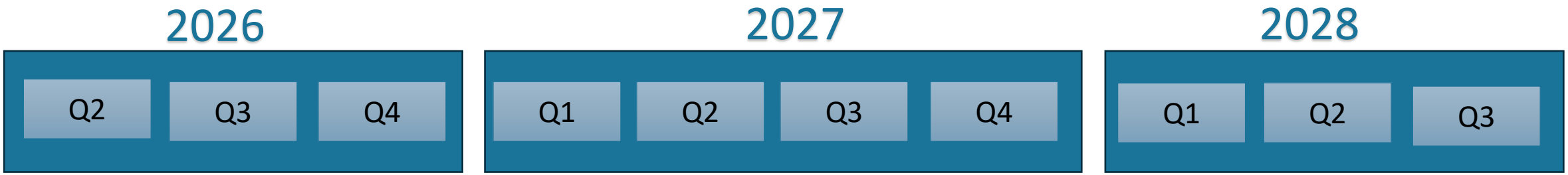
Fase 1: De basis op orde

Fase 2: Kernmaatregelen en operatie

Fase 3: Integratie en borging

mbo digitaal

Roadmap – 3 fasen



Fase 1

sterk fundament voor governance, risico inzicht en inventarisaties.

Fase 2

Directe weerbaarheid verhogen & basis IAM & technische maatregelen actief.

Fase 3

Aantonen dat maatregelen werken; integratie in reguliere processen.

Fase 4

De vijf dispensatie eisen (ingroeimodel) naar niveau 3 + permanente borging.

In ontwikkeling

mbo digitaal

Fase 1: De basis op orde

"In fase 1 zorgen we ervoor dat we weten wie verantwoordelijk is, wat we beschermen en waarom"

Doel

Een sterk fundament voor governance, risico-inzicht en overzicht over kritieke processen, systemen en data.

Kernacties, indien nog niet (volledig) gerealiseerd:

- **Governance inrichten**: eigenaarschap, rollen, verantwoording en verantwoordelijkheid.
- **Risicomanagement organiseren:** Vaststellen en inrichten van het risicomanagementproces.
- **Asset-inventarisatie uitvoeren**: Het IT-landschap in kaart brengen.
- **Data-classificatie inrichten**: Het informatie-landschap in kaart brengen.
- **BIA uitvoeren**: Bedrijfsdoelstellingen koppelen aan IT-recovery eisen.
- **Back-up en herstel inrichten**
- **Awareness**: Opstellen van een (jaar)programma voor security-awareness voor medewerkers.

Waarom in deze fase?

- Zonder Governance en Risicomanagement geen gerichte beveiligingsmaatregelen.
- Configuratiebasis en Dataclassificatie zijn essentieel voor inrichting van technische maatregelen.
- Bewustwording zorgt dat medewerkers vanaf het begin betrokken zijn bij veilig gedrag.
- Back-up en Continuïteitsplanning leveren directe risicoreductie op en vergroten de weerbaarheid.

- **OR.01**
- **RM.03**
- **CO.01**
- **DM.02**
- **OP.02**
- **BC.01**

mbo digitaal

Fase 2: Kernmaatregelen & Operatie

"In fase 2 bewijzen we dat onze afspraken ook écht werken."

Doel

Beveiligingsmaatregelen daadwerkelijk laten functioneren in de dagelijkse praktijk, zodat de belangrijkste cyberrisico's actief en aantoonbaar worden beheerst..

Kernacties, indien nog niet (volledig) gerealiseerd:

- **IAM inrichten**: Toegangsrechten inrichten, beheren en controleren, ook privileged accounts.
- **Incidentrespons organiseren**: Procedures vaststellen, rollen beleggen (en oefenen).
- **Authenticatie en autorisatie inrichten**: Sterke authenticatie en consistente toegangscontrole.
- **Technische basismaatregelen inrichten**: Patchmanagement, netwerkbeveiliging en malwarebescherming.
- **Logging en monitoring inrichten**: Inzicht krijgen in / opvolgen van beveiligingsgebeurtenissen.
- **Kwetsbaarheden beheren**: Structureel inzicht in dreigingen en kwetsbaarheden en opvolging daarvan.

Waarom deze fase

- Operationele maatregelen zijn snel te realiseren en verlagen onmiddellijk de kans op incidenten.
- Voorbereiding op borging: IAM en andere kernprocessen starten hier zodat beleid, processen en tooling tijdig gereed zijn voor toetsing in fase 3
- Van papier naar praktijk: de focus verschuift naar operationele werking van beveiligingsmaatregelen.

- IM.03
- ID.01
- ID.02
- ID.03
- ID.05
- SM.02
- SM.03
- SM.04
- SM.06
- SM.07
- SM.11
- SM.12

mbo digitaal

Fase 3: Integratie en borging

"In fase 3 tonen we aan dat onze maatregelen structureel werken en geborgd zijn."

Doel

Cyberweerbaarheid duurzaam borgen, aantoonbaar maken en gereed zijn voor onafhankelijke toetsing en verantwoording.

Kernacties, indien nog niet (volledig) gerealiseerd:

- **Borging van IAM**: periodieke herbeoordeling van toegangsrechten en structurele controle op privileges.
- **Continuïteit testen**: uitvoeren en evalueren van disaster-recovery-tests en continuïteitsoefeningen.
- **Monitoring en opvolging bestendigen**: structurele opvolging van meldingen, kwetsbaarheden en verbeterpunten.
- **Leveranciersafspraken vastleggen**: service levels en security-afspraken expliciet maken en naleven.
- **Onafhankelijke toetsing voorbereiden en uitvoeren**: verzamelen van bewijs, uitvoeren van audit en opvolgen van bevindingen.

Waarom deze fase

- Van werking naar zekerheid: deze fase laat zien dat maatregelen niet alleen werken, maar ook blijvend werken.
- Aantoonbare 'in control'-status: testen, reviews en audits maken cyberweerbaarheid toetsbaar en betrouwbaar.
- Vertrouwen en verantwoording: essentieel voor bestuur, toezichthouders en deelname aan de cyberweerbaarheidspool.
- Continu verbeteren: bevindingen worden structureel benut om het niveau verder te verhogen en vast te houden.

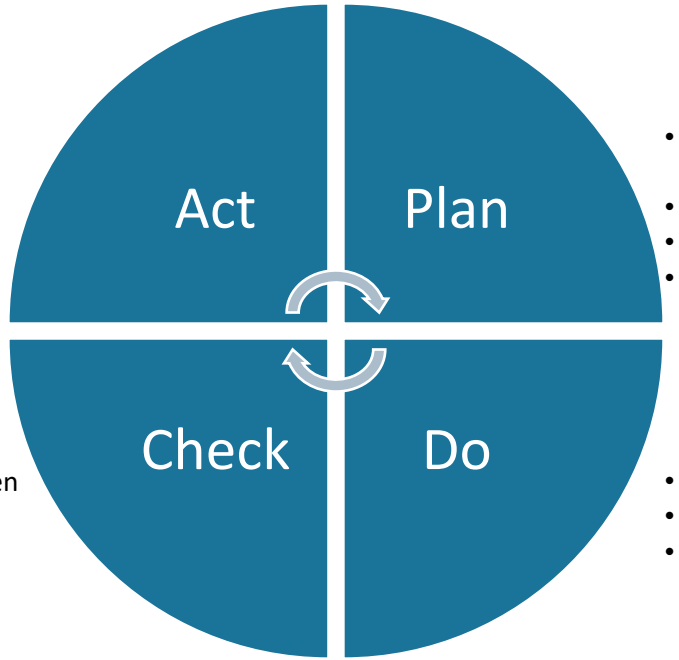
- **GO.05**
- **ID.05**
- **OP.02**
- **BC.01**
- **BC.02**
- **SC.01**

Statement:	OR.01 Eigenaarschap, rollen, verantwoording en verantwoordelijkheid		Doelstelling: VWN3
Accountable:	*<Naam uit RACI>*	Responsible:	*<Naam uit RACI>*
Complexiteit implementatie:	Organisatorisch: ●●●	Procesmatig: ●●	Technisch: ●
Startdatum:	*<Datum>*	Einddatum:	*<Datum>*	Goedkeuring Senior Mgmt vereist: ☑

Normtekst:

a) Alle rollen op het gebied van Information Risk en Security Management zijn vastgesteld en toegewezen.
b) De verantwoordelijkheid (en aansprakelijkheid) voor Information Risk en Security Management is op organisatieniveau vastgesteld en behandelt organisatiebrede kwesties.
c) Er is een intentieverklaring van het senior management, die de doelen en uitgangspunten van informatiebeveiliging en Information Risk Management ondersteunen en deze is in overeenstemming met de strategie en de organisatiedoelstellingen.

- Bijsturen (indien nodig) door onderwijsinstelling:
- Bijsturen (indien nodig) door programma:
- Escalatie naar bestuurlijk niveau door onderwijsinstelling en programma



- Achtergrond, interpretatie en volwassenheidscriteria door programma
- Voorbeelden / Templates vanuit programma
- Baseline assessment door onderwijsinstelling
- Planning door onderwijsinstelling

- Bewaken van voortgang door onderwijsinstelling en programma:
- Controle op aantoonbaarheid door onderwijsinstelling en programma
- Risico's per onderwijsinstelling:

- Implementatie door onderwijsinstelling
- Op te leveren door onderwijsinstelling
- Ondersteuning door programma

Statement:	OR.01 Eigenaarschap, rollen, verantwoording en verantwoordelijkheid		Doelstelling: VWN3
Accountable:	*<Naam uit RACI>*	Responsible:	*<Naam uit RACI>*
Complexiteit implementatie:	Organisatorisch: ●●●	Procesmatig: ●●	Technisch: ●
Startdatum:	*<Datum>*	Einddatum:	*<Datum>*	Goedkeuring Senior Mgmt vereist: ☑

Normtekst:

a) Alle rollen op het gebied van Information Risk en Security Management zijn vastgesteld en toegewezen.
b) De verantwoordelijkheid (en aansprakelijkheid) voor Information Risk en Security Management is op organisatieniveau vastgesteld en behandelt organisatiebrede kwesties.
c) Er is een intentieverklaring van het senior management, die de doelen en uitgangspunten van informatiebeveiliging en Information Risk Management ondersteunen en deze is in overeenstemming met de strategie en de organisatiedoelstellingen.

Plan

- **Achtergrond, interpretatie en volwassenheidscriteria door programma**:
  - Wie is eigenaar van het statement en wie stelt (beschikbare resources) vast
  - Wat wordt verwacht op niveau 3 voor OR.01
  - Welke bewijsstukken moeten overlegd
  - Welke valkuilen zijn er (bijv. “rollen zijn wel benoemd, maar niet formeel vastgesteld”).
- **Voorbeelden / Templates vanuit programma:**
  - Template RACI-tabel
  - Template Governance en Organisatie
  - Management Intentieverklaring
- **Baseline assessment:**
  - Wat is het huidig volwassenheidsniveau en waar zitten de hiaten?
- **Planning door onderwijsinstelling:**
  - Voorbeeld

Do

- **Implementatie door onderwijsinstelling**:
  - Definiëren van rollen en verantwoordelijkheden
  - Toewijzen van rollen en verantwoordelijkheden
  - Vaststelling van definitie/toewijzing door senior management
  - Integreren van management intentieverklaring in IBP-beleid
  - Vaststelling van IBP-beleid door senior management
- **Op te leveren door onderwijsinstelling:**
  - Vastgesteld beleidstuk governance en organisatie IBP
  - Vastgestelde RACI
  - Vastgesteld IBP-beleid met Management intentieverklaringl
- **Ondersteuning door programma:**
  - Centrale coaching (wekelijks)
  - Individuele coaching (op aanvraag)

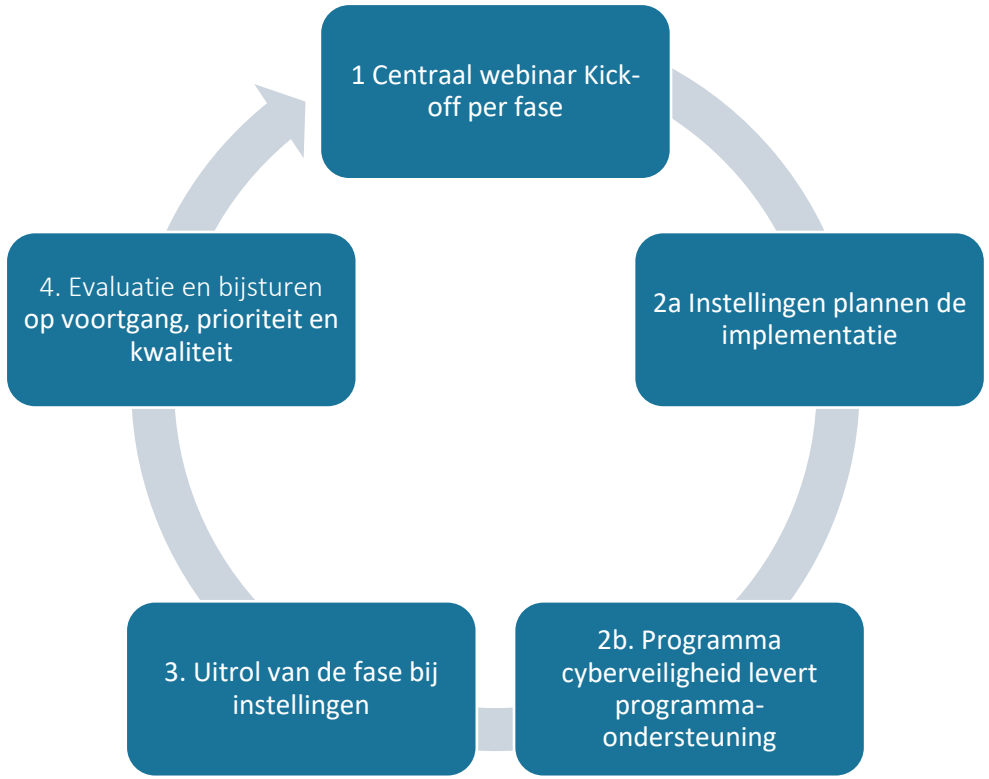
Check

- **Bewaken van voortgang door onderwijsinstelling en programma:**
  - Status implementatie:
    - Niet begonnen
    - In concept
    - Grotendeels geïmplementeerd
    - Volledig vastgesteld en aantoonbaar
- **Controle op aantoonbaarheid door onderwijsinstelling en programma**
- **Risico’s per onderwijsinstelling:**
  - (bijv. “geen bestuurlijke betrokkenheid”)
  - (Template test of controls?)
  - Integratie in Trustbound?

Act

- **Bijsturen (indien nodig) door onderwijsinstelling:**
  - bijv. Verbeterplan per instelling (deadlines, benodigde capaciteit, escalatieroutes)
- **Bijsturen (indien nodig) door programma:**
  - bijv. Sectorbrede aanscherping van templates (complexiteit, normuitleg)
- **Escalatie naar bestuurlijk niveau door onderwijsinstelling en programma**
  - bijv. Gesprek met bestuur of directie
  - bijv. Rapportage op sectorniveau
  - Hoe stuur je bij op afwijkingen / hoe rapporteer je bevindingen: risicoregister

6. Roadmap ritme



1. Centraal Webinar – Kick-off per fase

Het Programma Cyberveiligheid verzorgt een centrale toelichting op de nieuwe fase, inclusief uitleg van de doelen, deliverables en prioriteiten, sectorbrede lessons learned van de vorige fase, praktische handreikingen en templates, standaardtaken in Trustbound en Q&A voor alle instellingen. Dit zorgt voor een eenduidige start en gelijke uitgangspunten.

2a. Instellingen plannen de implementatie

Elke instelling stelt zelf een stappenplan op voor de komende fase gebaseerd op de standaardtaken afgestemd op de reeds behaalde scores voor de individuele instelling. De regie over (en daarmee verantwoordelijkheid voor) de implementatie ligt bij de instelling. Eventuele behoefte aan ondersteuning wordt bij het programma aangevraagd.

2b. Programma cyberveiligheid identificeert en beoordeeld benodigde programma-ondersteuning

Het Programma Cyberveiligheid identificeert en beoordeeld sectorbrede en instellingspecifieke ondersteuning op basis van:

- aanvragen van de instellingen;
- voortgangsrapportages van volwassenheid uit Trustbound;
- analyse van trends en risico’s sectorbreed;
- programmamiddelen versus behoefte.

3. Uitrol van de fase bij instellingen

Instellingen voeren de werkzaamheden van de fase uit op basis van het eigen goedgekeurde stappenplan en de ondersteuning vanuit het programma Cyberveiligheid. Hierover wordt maandelijks gerapporteerd.

4. Evaluatie van de roadmapfase

Het programmateam en de instellingen evalueren de effectiviteit van implementatie van de roadmap en sturen bij.

7. Vragen aan het publiek

- Wat vind je van het principe van de roadmap (uitgangspunten, opzet, tijdslijnen)?
- Wat vind je van de 22 gekozen statements?
- Wat vind je van de mogelijkheid om gebruik te maken van Trustbound?
- Over welke statements maak jij je ‘zorgen’ en waarom?
- Waar moet specifiek aandacht voor zijn bij de doorontwikkeling van de roadmap?
- Wat vind je van de planning in fasen?
- Wat vind je inhoudelijk van fase 1 en waar zie je uitdagingen?
- Waar en hoe verwacht je welke ondersteuning vanuit het programma?

mbo digitaal

NBA-ID	Omschrijving	Vereist niveau per 1 oktober 2027*	Vereist niveau per 1 oktober 2028*	Opzet vereist?	Bestaan vereist?	Werking vereist?	Type	Fase 1	Fase 2	Fase 3
GO.05	Onafhankelijke toetsing	2	3	Ja	Ja	Nee	Governance			X
OR.01	Eigenaarschap, rollen, verantwoording en verantwoordelijkheid	2	3	Ja	Ja	Nee	Governance	X		
RM.03	Plan voor behandeling en beperking van risico's (inclusief risicoacceptatie)	3	3	Ja	Ja	Nee	Processen	X		
HR.06	Veiligheidsbewustzijn	3	3	Ja	Ja	Nee	Processen	X		
CO.01	Identificatie en onderhoud van configuratie-items	3	3	Ja	Ja	Nee	Processen	X		
IM.03	Incidentrespons op (cyber) beveiligingsincidenten	3	3	Ja	Ja	Ja	Processen		X	
DM.02	Classificatie	3	3	Ja	Ja	Nee	Processen	X		
ID.01	Toegangsrechten	3	3	Ja	Ja	Ja	Processen		X	
ID.02	Administratie van toegangsrechten	2	3	Ja	Ja	Ja	Processen		X	
ID.03	Super users	3	3	Ja	Ja	Ja	Processen		X	
ID.05	Periodieke beoordeling van toegangsrechten	3	3	Ja	Ja	Ja	Processen		X	X
OP.02	Procedures voor backup en herstel	3	3	Ja	Ja	Nee	Processen	X		X
BC.01	Bedrijfscontinuïteitsplanning	3	3	Ja	Ja	Nee	Processen	X (BIA)		X
BC.02	Testen van disaster recovery	2	2	Ja	Ja	Nee	Processen			X
SC.01	Service level overeenkomst	3	3	Ja	Ja	Nee	Processen			X
SM.02	Authenticatiemechanismes	3	3	Ja	Ja	Nee	Techniek		X	
SM.03	Mobiele apparaten en telewerken	2	2	Ja	Ja	Nee	Techniek		X	
SM.04	Logging, monitoring en opvolging	2	3	Ja	Ja	Nee	Techniek		X (SOC)	
SM.06	Patchmanagement	3	3	Ja	Ja	Nee	Techniek		X	
SM.07	Threat en vulnerability management	3	3	Ja	Ja	Nee	Techniek		X	
SM.11	Network security	3	3	Ja	Ja	Nee	Techniek		X	
SM.12	Beheersing van malware-aanvallen	3	3	Ja	Ja	Nee	Techniek		X	
*Nog niet formeel vastgesteld										

mbo digitaal

Samen werken we aan één doel: een sector die aantoonbaar cyberweerbaar is.