Trots op het NBA/NOREA volwassenheidsmodel of …

toch nog een vooroordeel?

Hielkje van Staa-Oldenhuis
Henk Links

4 juni 2026

The Institute of Internal Auditors Netherlands

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

Wie zijn wij – Wie zijn jullie?

Hielkje van Staa-Oldenhuis,
expert integrated auditing, IT en operational auditing,
audit methodology

Henk Links,
Senior IT adviseur ROC Menso Alting en Adviseur
Informatieveiligheid programma Cyberveiligheid mbo

The Institute of Internal Auditors Netherlands

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

Agenda

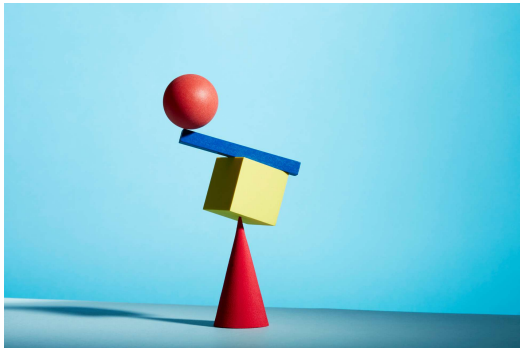
1. Informatiebeveiliging (incl. cyber security)
2. Informatiebeveiliging: een actueel thema
3. NBA/NOREA volwassenheidsmodel
4. NBA/NOREA volwassenheidsmodel in de Onderwijssector

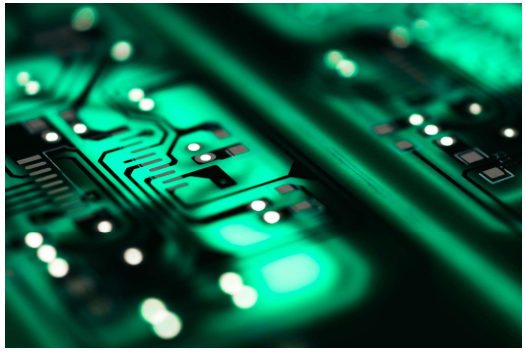
The Institute of Internal Auditors Netherlands

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

1. Informatiebeveiliging

Multidisciplinair vakgebied:



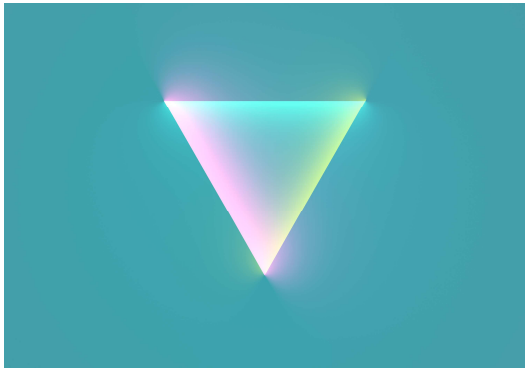


The Institute of Internal Auditors Netherlands

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

1. Kernbegrippen Informatiebeveiliging

Beschikbaarheid, Integriteit en Vertrouwelijkheid



The Institute of Internal Auditors Netherlands

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

1. Recente wetenschappelijke thema’s

1 Quantumveiligheid
2 Privacy protecting technologies
3 AI-veiligheid
4 Supply-chain-risico’s
5 Security governance & cultuur

The Institute of Internal Auditors Netherlands

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

2. Dreigingen volgens wetenschap en veiligheidsdiensten

1 State-sponsored hacking
2 Ransomeware-ecosystemen
3 AI-gestuurde aanvallen
4 Kwetsbaarheden in cloud- en IoT-systemen
5 Toenemende complexiteit van netwerken

2. Voorbeelden van cyberproblemen

National Defense Corp

CHANGE HEALTHCARE

snowflake
THE AI DATA CLOUD

Ascension

Ransomware Attack Compromised
5.6 Million Patients Data

2. Enkele Nederlandse hacks en datalekken (2024-2026)

Gemeente Hof van Twente

2. Oorzaken

- Geen multifactor authenticatie
- Ongepatchte systemen
- Slechte wachtwoordhygiene
- Afhankelijkheid van één kritieke leverancier
- Social engineering

2. Modellen en raamwerken: AFM

1 april 2026

AFM: Accountantsorganisaties, zorg voor een passend raamwerk voor informatiebeveiliging

Op basis van inzichten uit de sector benadrukt de AFM dat accountantsorganisaties hun IT-risicobeheersing verder moeten versterken, onder andere door actuele risicoregisters, goed getest continuïteitsmanagement, inzicht in systeemafhankelijkheden, zorgvuldig...

Nieuws | Digitalisering

Digitale incidenten, zoals datalekken, laten zien hoe kwetsbaar organisaties zijn en onderstrepen het belang van sterke informatiebeveiliging, zeker voor accountantsorganisaties die met gevoelige data werken. Een passend en toekomstbestendig raamwerk voor informatiebeveiliging helpt niet alleen om risico's te beheersen en incidenten te voorkomen, maar ook om de impact ervan te beperken. Daarbij spelen factoren zoals menselijk handelen, monitoring en duidelijke verantwoordelijkheden een grote rol. Bestaande richtlijnen, zoals de Good Practice Informatiebeveiliging, bieden praktische handvatten om risicomanagement structureel en proportioneel in te richten.

Lees meer

Artikel AFM: Accountantsorganisaties: zorg voor een passend raamwerk voor informatiebeveiliging

2. Modellen en raamwerken

1 ISO-27000-familie
2 NIST Cybersecurity Framework
3 SURF-audit-kader (gebaseerd op NBA volwassenheidsmodel)
4 Zero Trust-architecturen

The Institute of Internal Auditors Netherlands

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

3. NBA/NOREA Volwassenheidsmodel

XLSX-document (410,18 kB)
NBA NOREA Volwassenheidsmodel Informatiebeveiliging 3.0 (werkdocument)

3. Doelstelling NBA/NOREA Volwassenheidsmodel

Auditors alsmede directies van organisatie een leidraad en handvatten geven waarmee zij doelgericht en op pragmatische wijze hun organisaties kunnen ondersteunen bij het **meten**, **bepalen** en **verbeteren** van het volwassenheidsniveau van informatiebeveiliging (inclusief cyber security)

Maar…. *geen assurance product*

3. Handreiking voor:

- Het **toetsen** van de geïmplementeerde beheersmaatregelen tegen het vereiste volwassenheidsniveau voor informatiebeveiliging
- Het **adviseren** over een gericht implementatietraject van beheersmaatregelen om een bepaald volwassenheidsniveau voor informatiebeveiliging te bewerkstelligen.

3. Ontwerp (1)

- Model is gebaseerd op ‘good practices’
- Referenties naar CobIT, ISO27K, BIO, NIST (en voorheen ook DNB)
- Aanvullende handreiking opgesteld

3. Ontwerp (2)

15 Domeinen	
Governance	System Development
Organisation	Data Management
Risk Management	Identity & Access Management
Human Resources	Security Management
Configuration Management	Physical Security
Incident & Problem Management	Computer Operations
Change Magement	Business Continuity Management
	Supply Chain Management

3. Ontwerp (3)

5 volwassenheidsniveaus conceptueel uitgewerkt.

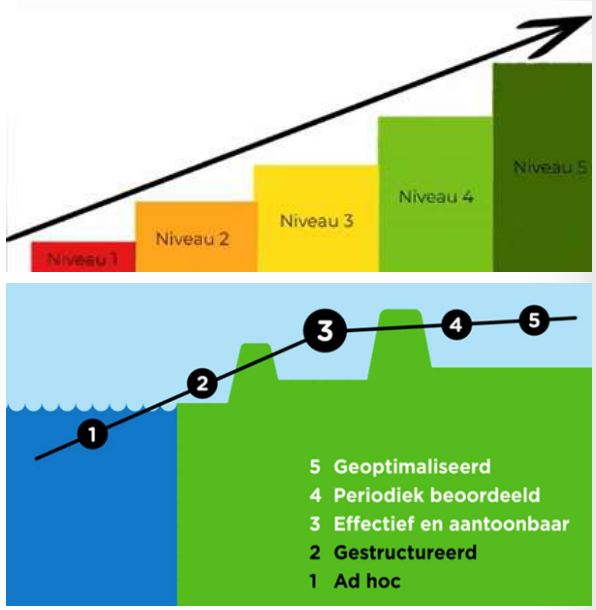
1: **Initial** (geen of beperkte controls geïmplementeerd, niet of ad hoc uitgevoerd, niet of deels gedocumenteerd, wijze van uitvoering afhankelijk van individu)

2: **Repeatable** (control is geïmplementeerd, uitvoering is consistent en standaard, informeel en grotendeels gedocumenteerd)

3: **Defined** (control gedefinieerd o.b.v. risico assessment, gedocumenteerd en geformaliseerd, opzet bestaan`en effectieve werking aantoonbaar)

4: **Managed & Measurable** (periodieke evaluatie en opvolging vindt plaats, rapportage management vindt plaats)

5: **Continuous Improvement** (self-assessment, gap en root cause analyses, real time monitoring, inzet automated tooling)



3. Toepassing van het model

Context zelf meewegen: maak risico-indicatie organisatiespecifiek

- aard van business en informatievoorziening
- IT-landschap
- afhankelijkheid van informatievoorziening en derden in ‘waardeketen
- wet- en regelgeving
- risicobereidheid

Rapportages: toegevoegde waarde door periodieke dialoog met stakeholders

- kwetsbaarheden, impact en risico’s
- prioritering en opvolging mitigerende acites
- ‘challenge’ sessie met verantwoordelijke directie

3 Hoe ziet het er dan uit?

NOREA | Volwassenheidsmodel voor informatiebeveiliging 3.0

- Volwassenheidsmodel informatiebeveiliging 3.0 (pdf)
- Volwassenheidsmodel informatiebeveiliging 3.0 (excel)
- Uitleg van het Volwassenheidsmodel

NBA Webinar - Volwassenheidsmodel

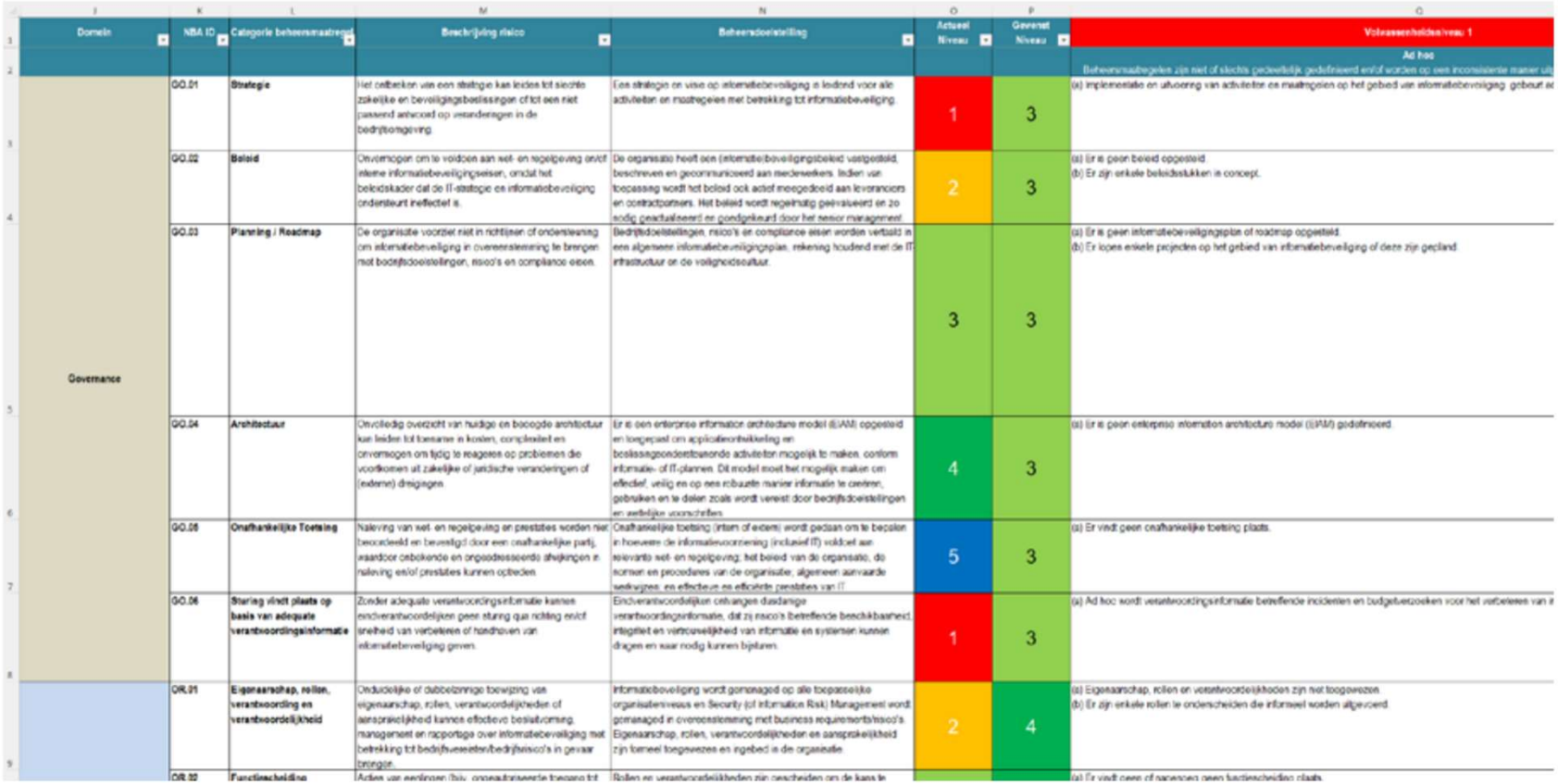
3 Vervolg

15 (SC) Ketenbeheer
15.69 (SC.01) Contract Manage
15.70 (SC.02) Service Level Ma
15.71 (SC.03) Interne beheersi

(SC) Ketenbeheer	
15.70 (SC.02)	**Service Level Management**
Risico	Gebrek aan controle op de levering van diensten waardoor afwijkingen in de prestaties van leveranciers niet of niet op tijd worden gedetecteerd, wat kan leiden tot een afname van de algemene bedrijfsprestaties.
Doel	De geleverde dienstenservicelevels worden periodiek gecontroleerd, en eventuele bevindingen worden opgevolgd.
Volwassenheidsniveau 1	(a) Er zijn geen afspraken over periodieke rapportages of overleg over diensten en dienstenservicelevels.
Volwassenheidsniveau 2	(a) Er zijn enkele afspraken over periodiek op te leveren rapportages, maar die worden ad hoc gecontroleerd.
Volwassenheidsniveau 3	(a) Periodieke rapportages worden ook mondeling besproken en geëvalueerd. Waar nodig worden verbeteracties gedefinieerd en opgevolgd. (b) Periodiek wordt de kwaliteit van de IT-dienstverlener onderzocht, gerapporteerd en geëvalueerd, bijvoorbeeld: • Certificeringen en assurancerapportages opgevraagd en geëvalueerd (bijv. ISAE3402 of ISO27001). • Een intern audit rapport van de serviceprovider (nadat de bekwaamheid en scope van interne audit gevalideerd is). • Door, waar nodig, gebruikmaking van de "recht op audit of recht of pentest" clausule.
Volwassenheidsniveau 4	(a) De bedrijfsmatige vereisten voor service-onderdelen worden periodiek vergeleken met de daadwerkelijke prestaties van de geleverde onderdelen en wanneer deze niet voldoen aan de formele SLA levels/requirements worden mitigerende acties ondernomen om deze binnen redelijke tijd te herstellen.
Volwassenheidsniveau 5	(a) Organisatie kan actuele service level real time inzien bij service provider.

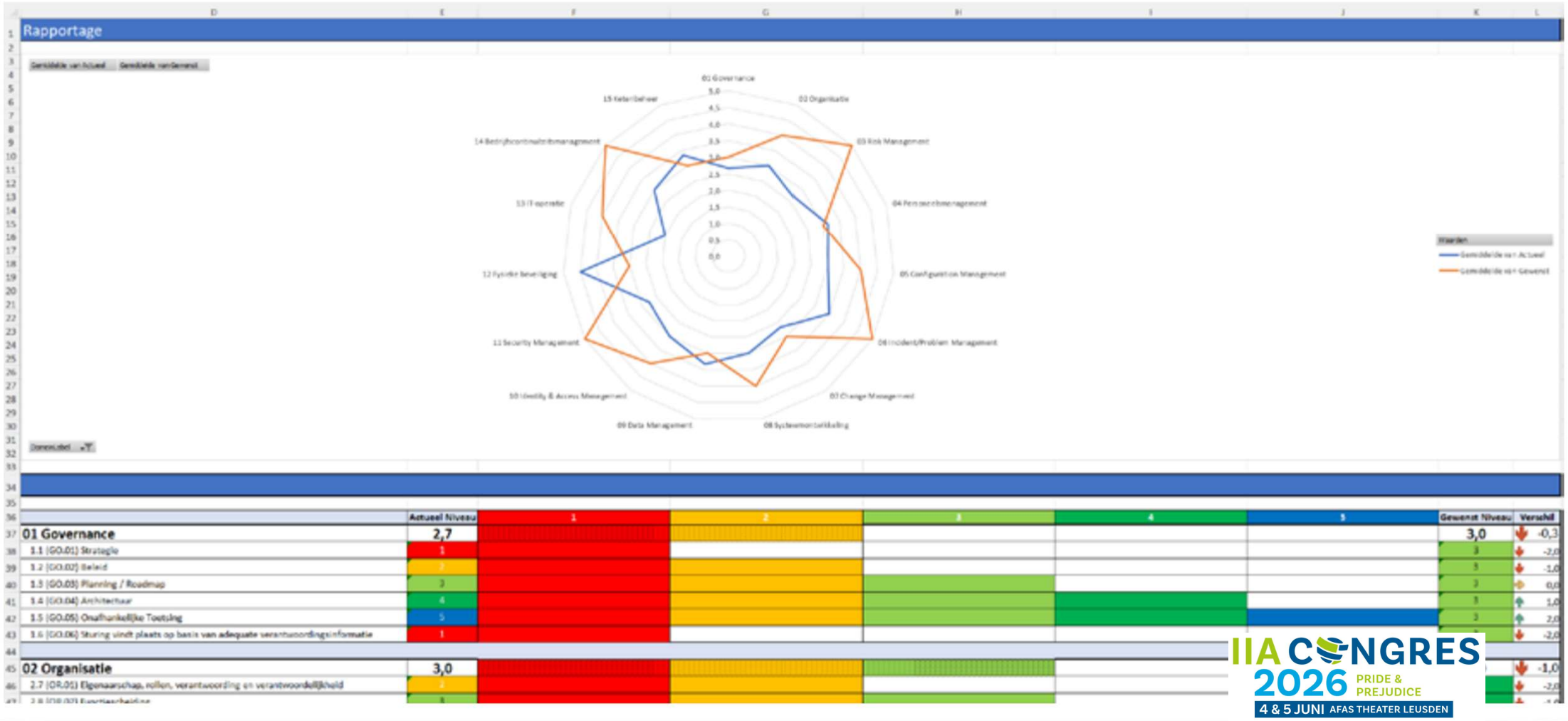
COBIT 5	ISO 27001:2013 27002:2013	ISO 27001:2022 27002:2022	BIO 2019	NIST Cybersecurity Framework
APO09.05, APO09.06	8.1 A.12.2.1 A.14.2.7 A.15.1.1, A.15.1.2, A.15.1.3 A.15.2.1, A.15.2.2	8.1 A5.19, A5.20, A5.21, A5.22 A8.30	12.2.1, 12.2.1.1, 12.2.1.2, 12.2.1.3, 12.2.1.4, 12.2.1.5 14.2.7, 14.2.7.1 15.1.1, 15.1.1.1, 15.1.1.2, 15.1.1.3 15.1.2, 15.1.2.1, 15.1.2.2, 15.1.2.3, 15.1.2.4, 15.1.2.5, 15.1.2.6 15.1.3, 15.1.3.1 15.2.1, 15.2.1.1 15.2.2	ID.SC-1, ID.SC-2, ID.SC-3, ID.SC-4, ID.SC-5 ID-GV.3 PR.AC-3 PR.MA-1, PR.MA-2 DE.CM-6 DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5

3 Ingevuld voorbeeld domein Governance



Domein	NBA ID	Categorie beheersmaatregel	Beschrijving risico	Beheersdoelstelling	Actueel Niveau	Gewenst Niveau	Volwassenheidsniveau 1
							Ad hoc
							Beheersmaatregelen zijn niet of slechts gedeeltelijk gedefinieerd en/of worden op een inconsistente manier uit
Governance	GO.01	**Strategie**	Het ontbreken van een strategie kan leiden tot slechte zakelijke en beveiligingsbeslissingen of tot een niet passend antwoord op veranderingen in de bedrijfsomgeving.	Een strategie en visie op informatiebeveiliging is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging.	1	3	(a) Implementatie en uitvoering van activiteiten en maatregelen op het gebied van informatiebeveiliging gebeurt ad
	GO.02	**Beleid**	Onvermogen om te voldoen aan wet- en regelgeving en/of interne informatiebeveiligingseisen, omdat het beleidskader dat de IT-strategie en informatiebeveiliging ondersteunt ineffectief is.	De organisatie heeft een (informatiebeveiligings)beleid vastgesteld, beschreven en gecommuniceerd aan medewerkers. Indien van toepassing wordt het beleid ook actief meegedeeld aan leveranciers en contractpartners. Het beleid wordt regelmatig geëvalueerd en zo nodig geactualiseerd en goedgekeurd door het senior management.	2	3	(a) Er is geen beleid opgesteld. (b) Er zijn enkele beleidsstukken in concept.
	GO.03	**Planning / Roadmap**	De organisatie voorziet niet in richtlijnen of ondersteuning om informatiebeveiliging in overeenstemming te brengen met bedrijfsdoelstellingen, risico's en compliance eisen.	Bedrijfsdoelstellingen, risico's en compliance eisen worden vertaald in een algemeen informatiebeveiligingsplan, rekening houdend met de IT infrastructuur en de veiligheidscultuur.	3	3	(a) Er is geen informatiebeveiligingsplan of roadmap opgesteld. (b) Er lopen enkele projecten op het gebied van informatiebeveiliging of deze zijn gepland.
	GO.04	**Architectuur**	Onvolledig overzicht van huidige en beoogde architectuur kan leiden tot tijdsverlies en kosten, complexiteit en onvermogen om tijdig te reageren op problemen die voortkomen uit zakelijke of juridische veranderingen of (externe) dreigingen.	Er is een enterprise information architecture model (EIAM) opgesteld en toegepast om applicatieontwikkeling en besluitvormingsondersteunende activiteiten mogelijk te maken, conform informatie- of IT-plannen. Dit model moet het mogelijk maken om effectief, veilig en op een robuuste manier informatie te centreren, gebruiken en te delen zoals wordt vereist door bedrijfsdoelstellingen en wettelijke voorschriften.	4	3	(a) Er is geen enterprise information architecture model (EIAM) gedefinieerd.
	GO.05	**Onafhankelijke Toetsing**	Naleving van wet- en regelgeving en prestaties worden niet beoordeeld en bevestigd door een onafhankelijke partij, waardoor onbekende en ongeadresseerde afwijkingen in naleving en/of prestaties kunnen optreden.	Onafhankelijke toetsing (intern of extern) wordt gedaan om te bepalen in hoeverre de informatievoorziening (inclusief IT) voldoet aan relevante wet- en regelgeving, het beleid van de organisatie, de normen en procedures van de organisatie, algemeen aanvaarde werkwijzen, en effectieve en efficiënte prestaties van IT.	5	3	(a) Er vindt geen onafhankelijke toetsing plaats.
	GO.06	**Sturing vindt plaats op basis van adequate verantwoordingsinformatie**	Zonder adequate verantwoordingsinformatie kunnen eindverantwoordelijken geen sturing qua richting en/of snelheid van verbeteren of handhaven van informatiebeveiliging geven.	Eindverantwoordelijken ontvangen duidelijke verantwoordingsinformatie, dat zij risico's betreffende beschikbaarheid, integriteit en vertrouwelijkheid van informatie en systemen kunnen dragen en waar nodig kunnen bijsturen.	1	3	(a) Ad hoc wordt verantwoordingsinformatie betreffende incidenten en budgetverzoeken voor het verbeteren van i
	OR.01	**Eigenaarschap, rollen, verantwoording en verantwoordelijkheid**	Onduidelijke of dubbelzinnige toewijzing van eigenaarschap, rollen, verantwoordelijkheden of aansprakelijkheid kunnen effectieve besluitvorming, management en rapportage over informatiebeveiliging met betrekking tot bedrijfseigenaren/bedrijfsrisico's in gevaar brengen.	Informatiebeveiliging wordt gemanaged op alle toepasselijke organisatieniveaus en Security (of Information Risk) Management wordt gemanaged in overeenstemming met business requirements/risico's. Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid zijn formeel toegewezen en ingebed in de organisatie.	2	4	(a) Eigenaarschap, rollen en verantwoordelijkheden zijn niet toegewezen. (b) Er zijn enkele rollen te onderscheiden die informeel worden uitgevoerd.
	OR.02	**Functiescheidings**	Acties van werknemers (bijv. ongeautoriseerde toegang tot	Rollen en verantwoordelijkheden zijn gescheiden om de kans te			(a) Er vindt geen of nagenoeg geen functiescheiding plaats.

3 Rapportage in grafiekvorm



4. NBA/NOREA Volwassenheidsmodel in de Onderwijssector

Henk Links | Information Security Officer

Houdt zich binnen het programma Cyberveiligheid voornamelijk bezig met het NBA-volwassenheidsmodel informatiebeveiliging om de onderwijsinstellingen aantoonbaar te laten groeien naar het gewenste volwassenheidsniveau

Was als hoofd ICT op een middelgrote scholengemeenschap in het voortgezet onderwijs een verbindende schakel tussen de mogelijkheden van IT en de uitdagingen binnen het onderwijs en stapte in 2015 de wereld van het mbo binnen

Sterk in het leggen van verbanden, scherp in zijn analyse, en vindt begrip erg belangrijk

Drijfveer Samenwerken, ook tussen onderwijssectoren, om bij te dragen aan betrouwbare en veilige onderwijsomgeving.

4. Context Onderwijs

- Funderend Onderwijs
  - Primair Onderwijs (PO)
  - Voorgezet Onderwijs (VO)
- Middelbaar Beroepsonderwijs (mbo)
- Hoger BeroepsOnderwijs
- Universitair Onderwijs

4. Context IBP in het Onderwijs

Ministerie van Onderwijs, Cultuur en Wetenschap

- Funderend Onderwijs

PO RAAD VO RAAD Kennisnet SIVON

- Middelbaar Beroepsonderwijs (mbo)
- Hoger BeroepsOnderwijs
- Universitair Onderwijs

MBO Raad mbo digitaal SURF Vereniging Hogescholen Universiteiten van Nederland

4. NBA-model in het Onderwijs

Universiteit / HO en mbo

- SURFaudit Toetsingskader Informatiebeveiliging
  (Voorheen op ISO gebaseerd)
- NBA Volwassenheidsmodel Informatiebeveiliging 
- SURFaudit Toetsingskader Privacy
  (Dezelfde methodiek: 25 statements)

Funderend Onderwijs

- Normenkader Informatiebeveiliging en Privacy voor het onderwijs

4. Argumenten NBA-model

1. Het model is met 69 maatregelen een stuk compacter dan het huidige toetsingskader.
2. Het is minder gericht op technische beheersmaatregelen, in plaats daarvan is er meer aandacht voor governance, leveranciersmanagement en risicomanagement.
3. Het model nodigt uit om per statement een risico-afweging te maken en het vereiste volwassenheidsniveau daarop af te stemmen.
4. Voor elk statement zijn de volwassenheidsniveaus 1-5 gedetailleerd beschreven, wat het model praktisch toepasbaar en objectief toetsbaar maakt.
5. Het model wordt door de beroepsgroep breed geaccepteerd, waardoor interne- en externe

4. Aandachtsgebieden/Thema's

GOVERNANCE		PROCESSEN		TECHNISCHE WEERBAARHEID	
G01	Strategie 1.1	P08	Human Resources 4.1/4.2/4.3/4.4/4.5/4.6	T15	MFA - Thuiswerken 11.2/11.3
G02	Beleid 1.2	P09	ITIL 5.1/5.2/6.1/6.2/6.3/6.4 7.1/7.2/7.3/7.4/7.5/7.6 12.1/12.2	T16	SOC SIEM 11.4
G03	Architectuur 1.4	P10	Datamanagement 8.1/8.2/8.3/9.1/9.2/9.3/9.4/9.5/9.6	T17	Pentesten 11.5
G04	Eigenaarschap 2.1/2.2	P11	IAM 10.1/10.2/10.3/10.4/10.5	T18	Patchbeheer 11.6/11.7
G05	Risk Management 3.1/3.2/3.3	P12	Security Baselines 11.1	T19	Infrastructuur 11.8/11.9
G06	Roadmap 1.3	P13	Business Continuïteit 14.1/14.2/14.3/14.4/14.5	T20	Security Policy 11.10/11.11/11.12/11.13
G07	Toetsing 1.5	P14	Cloud Leveranciers 15.1/15.2/15.3/15.4	T21	Computer Operations 13.1/13.2/13.3

4. Ondersteuning vanuit Kennisnet

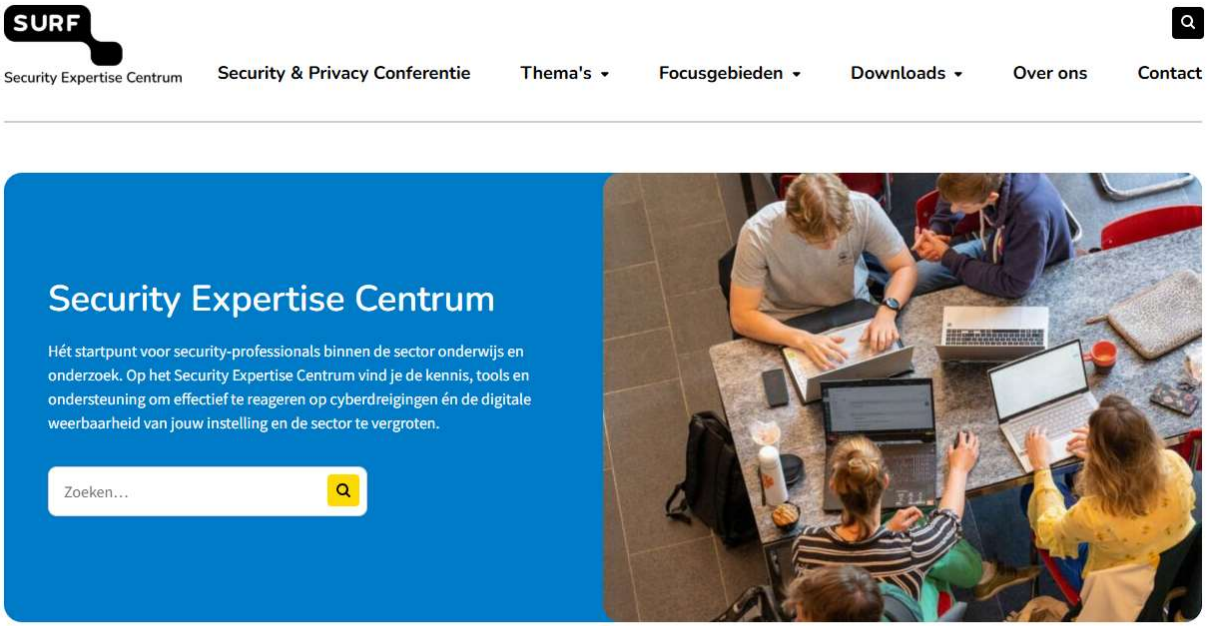
[Normenkader IBP voor het onderwijs - Normenkader informatiebeveiliging en privacy voor het onderwijs]

Bit by Bit: stap voor stap naar digitaal veilig onderwijs

Elke leerling moet kunnen leren in een digitaal veilige schoolomgeving. Ook jouw schoolorganisatie werkt met persoonlijke informatie van minderjarigen én medewerkers. Tegelijkertijd nemen sectorbreed de privacy- en beveiligingsrisico's toe. Steeds vaker gaat het (bijna) mis, waardoor gegevens op straat komen te liggen of lessen niet kunnen doorgaan. Schoolbestuurders hebben de verantwoordelijkheid om samen met (de) schoolleider(s) en IBP'er(s) een digitaal veilige schoolomgeving te realiseren.

[Digitaal Veilig Onderwijs]

4. Ondersteuning vanuit SURF



4. Ondersteuning vanuit MBO Digitaal

PROGRAMMA
Cyberveiligheid

Met het programma Cyberveiligheid mbo verhogen we de cyberweerbaarheid van de sector. Mbo-instellingen, cyberexperts, juristen en IT-specialisten delen binnen het programma kennis en ervaringen, identificeren kwetsbaarheden en werken samen aan best practices voor informatiebeveiliging en privacy. Samen staan we sterker tegen cybercriminaliteit.

Aanleiding voor het programma Cyberveiligheid mbo

De ransomware-aanval bij ROC Mondriaan in 2021 is de aanleiding voor het programma Cyberveiligheid mbo. Het incident maakt veel los. Niet alleen binnen de mbo-sector, maar ook in de politiek. De minister van Onderwijs, Cultuur en Wetenschap verzoekt de MBO Raad daarom om de digitale weerbaarheid van mbo-instellingen te verhogen. Met dit doel gaat het programma Cyberveiligheid mbo in september 2022 van start.

Intensieve samenwerkingen

MBO Digitaal, het digitaliseringsplatform van de MBO Raad, voert het programma Cyberveiligheid mbo uit. Het programma werkt nauw samen met mbo-instellingen en de netwerken van MBO Digitaal, zoals het netwerk IBP, de regiegroep IBP en het CSC-netwerk van SURF-contactpersonen. Ook ontwikkelt het programma veel activiteiten met SURF en overlegt het met branchevereniging VH en UNL. Op deze pagina lees je meer over samenwerkingen vanuit het programma.

Financiële ondersteuning

Programma Cyberveiligheid mbo

zoeken in programma ZOEKEN

- Praatplaat cyberveiligheid
- Samenwerken in de sector
- Ons team

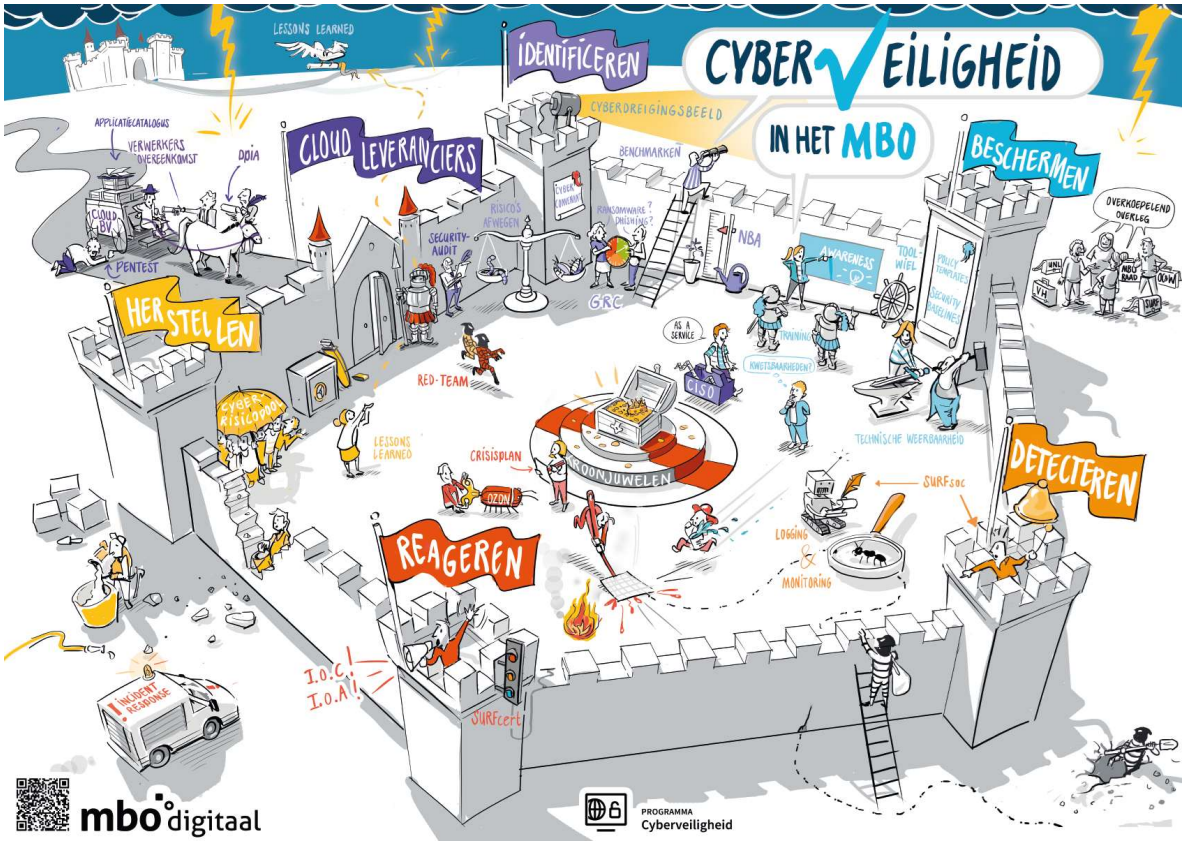
De 6 thema's van het programma

- Identificeren van dreigingen en risico's
- Beschermen tegen cyberrisico's
- Detecteren van onregelmatigheden
- Reageren op incidenten
- Herstellen van incidenten
- Samenwerken met cloudleveranciers

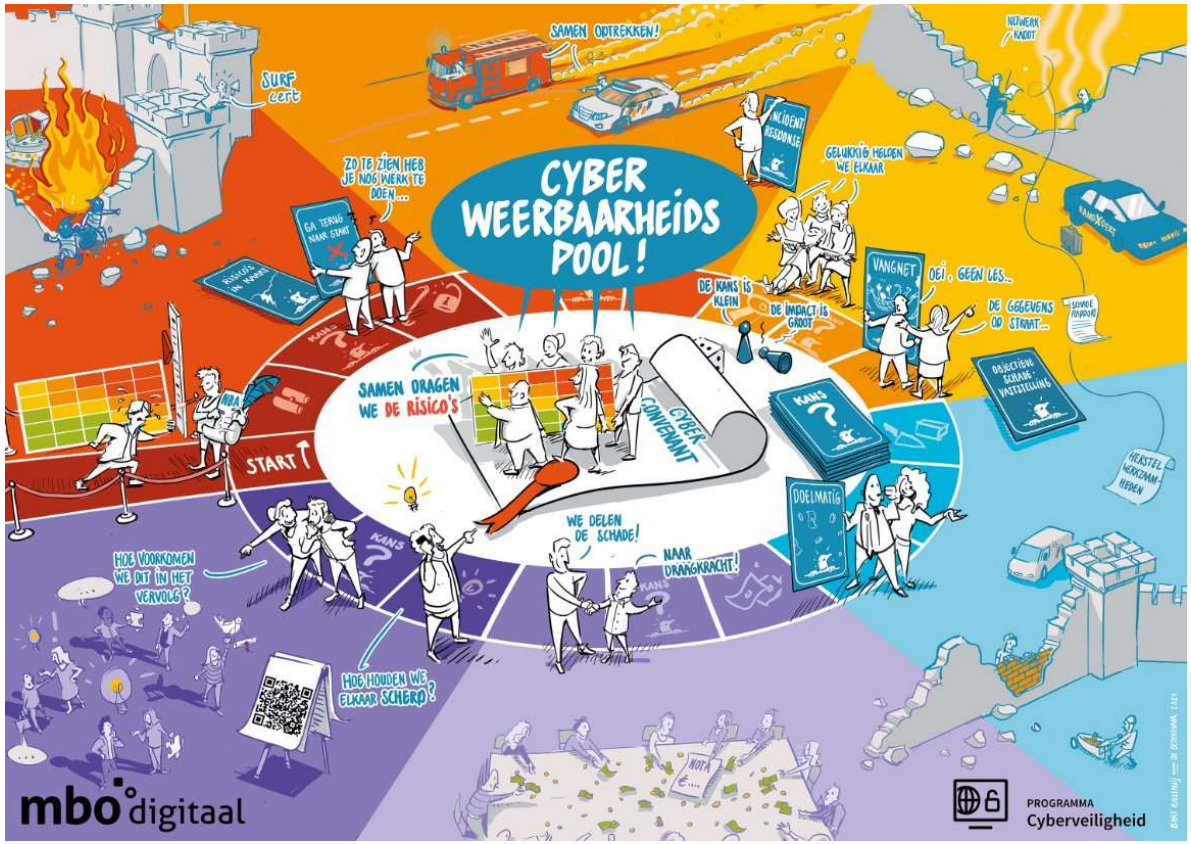
Gerelateerde berichten

Workshops gezamenlijke netwerkdag: AI &

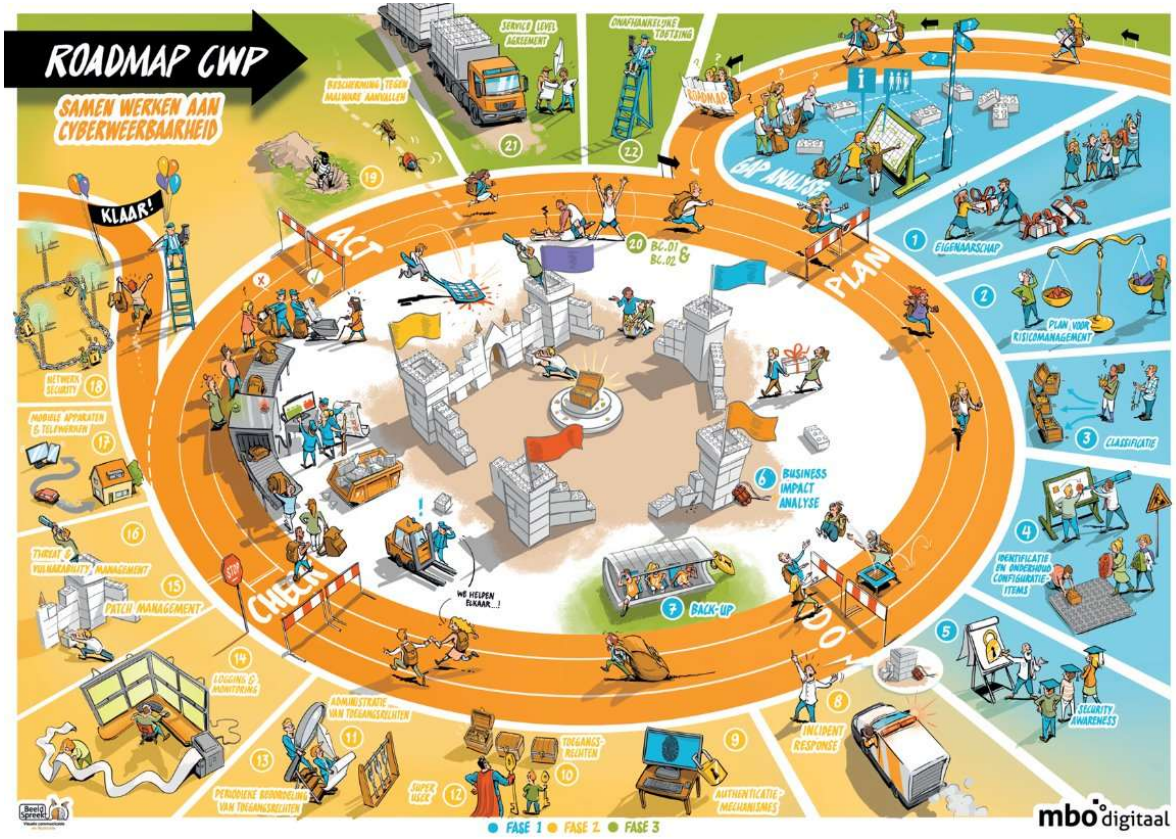
4. Programma Cyberveiligheid mbo



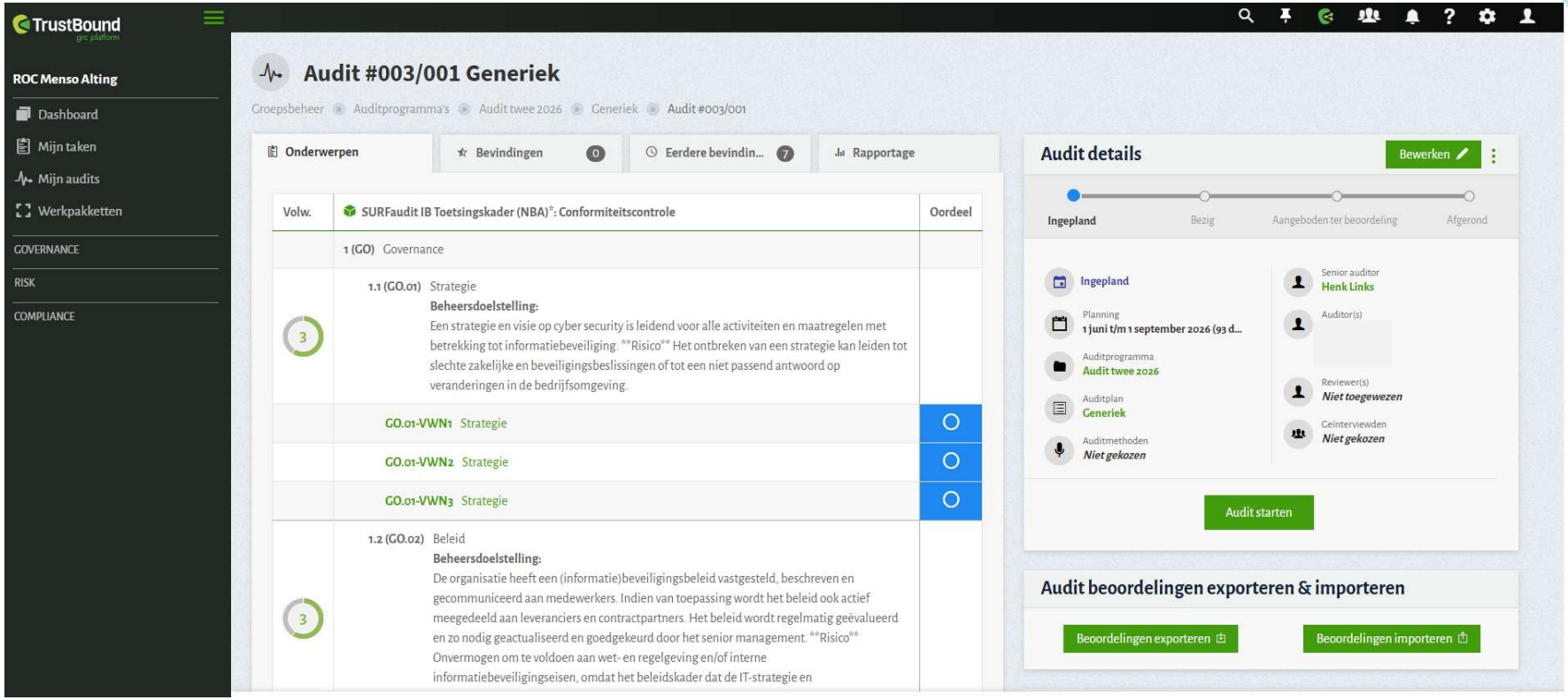
4. Cyberweerbaarheidspool mbo



4. Roadmap Cyberweerbaarheidspool mbo



4. De Audit


TrustBound
ROC Menso Alting
Dashboard
Mijn taken
Mijn audits
Werkpakketten
GOVERNANCE
RISK
COMPLIANCE
Audit #003/001 Generiek
Groepsbeheer » Auditprogramma's » Audit twee 2026 » Generiek » Audit #003/001
Onderwerpen
Bevindingen 0
Eerdere bevindin... 7
Rapportage
Volw.
SURFaudit IB Toetsingskader (NBA)*: Conformiteitscontrole
Oordeel
1 (GO) Governance
1.1 (GO.01) Strategie
Beheersdoelstelling:
Een strategie en visie op cyber security is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging. **Risico** Het ontbreken van een strategie kan leiden tot slechte zakelijke en beveiligingsbeslissingen of tot een niet passend antwoord op veranderingen in de bedrijfsomgeving.
GO.01-VWN1 Strategie
GO.01-VWN2 Strategie
GO.01-VWN3 Strategie
1.2 (GO.02) Beleid
Beheersdoelstelling:
De organisatie heeft een (informatie)beveiligingsbeleid vastgesteld, beschreven en gecommuniceerd aan medewerkers. Indien van toepassing wordt het beleid ook actief meegedeeld aan leveranciers en contractpartners. Het beleid wordt regelmatig geëvalueerd en zo nodig geactualiseerd en goedgekeurd door het senior management. **Risico** Onvermogen om te voldoen aan wet- en regelgeving en/of interne informatiebeveiligingseisen, omdat het beleidskader dat de IT-strategie en
Audit details
Bewerken
Ingepland
Bezig
Aangeboden ter beoordeling
Afgerond
Ingepland
Planning
1 juni t/m 1 september 2026 (93 d...
Auditprogramma
Audit twee 2026
Auditplan
Generiek
Auditmethoden
Niet gekozen
Senior auditor
Henk Links
Auditor(s)
Reviewer(s)
Niet toegewezen
Geïnterviewden
Niet gekozen
Audit starten
Audit beoordelingen exporteren & importeren
Beoordelingen exporteren
Beoordelingen importeren

4. Benchmark (sectorrapportage)

Eindresultaat Benchmark

	Mbo-sector	Hbo-sector	Wo-sector
Type audit	Zelf-evaluatie	(Deels) externe audit*	Externe audit
Aantal deelnemers	55 van de 55	34 van de 36	14 van de 14
Eindscore informatiebeveiliging	2,3	2,1	2,5
Eindscore privacy**	2,3	2,1	2,1

*: De meerderheid van de hogescholen deed mee op basis van een externe audit, een minderheid deed mee op basis van zelfevaluatie.

**: Voor privacy is de deelname lager bij hogescholen en universiteiten

4. Benchmark (instellingsrapportage)

Domein	Instelling 2022	Instelling 2024	Sector 2024	Groei Instelling	Verschil Sector
01 Governance	2,6	2,6	2,4	0,0	0,2
02 Organisatie	2,5	2,5	2,4	0,0	0,1
03 Risk Management	2,0	2,0	1,9	0,0	0,1
04 Personeelsmanagement	2,7	2,8	2,4	0,1	0,4
05 Configuration Management	3,5	3,0	2,5	-0,5	0,5
06 Incident/Problem Management	2,5	2,5	2,5	0,0	0,0
07 Change Management	2,5	2,7	2,1	0,2	0,6
08 Systeemontwikkeling	3,3	2,7	2,0	-0,6	0,7
09 Datamanagement	2,3	2,5	2,2	0,2	0,3
10 Identity & Access Management	1,6	2,0	2,3	0,4	-0,3
11 Security Management	2,8	2,8	2,5	0,0	0,3
12 Fysieke beveiliging	2,5	2,5	2,3	0,0	0,2
13 IT-Operatie	2,0	2,0	2,3	0,0	-0,3
14 Bedrijfscontinuiteitsmanagement	2,0	2,2	2,2	0,2	0,0
15 Ketenbeheer	2,5	2,5	2,3	0,0	0,2
Eindtotaal	**2,5**	**2,5**	**2,3**	**0,0**	**0,2**
		Hoogste Stijging / Grootste Positieve Verschil		0,4	0,7
		Hoogste Daling / Grootste Negatieve Verschil		-0,6	-0,3

Thema	Instelling 2022	Instelling 2024	Sector 2024	Groei Instelling	Verschil Sector
(G) Governance	2,4	2,4	2,2	0,0	0,2
G01 Strategie	3,0	3,0	2,4	0,0	2,4
G02 Beleid	3,0	3,0	3,0	0,0	0,0
G03 Architectuur	2,0	2,0	2,0	0,0	0,0
G04 Eigenaarschap	2,5	2,5	2,4	0,0	0,1
G05 Risk Management	2,0	2,0	1,9	0,0	0,1
G06 Roadmap	3,0	3,0	2,4	0,0	0,6
G07 Toetsing	2,0	2,0	2,3	0,0	-0,3
(P) Processen	2,4	2,5	2,3	0,1	0,2
P08 Human Resources	2,7	2,8	2,4	0,1	0,4
P09 ITIL	2,6	2,6	2,3	0,0	0,3
P10 Datamanagement	2,7	2,6	2,2	-0,1	0,4
P11 IAM	1,6	2,0	2,3	0,4	-0,3
P12 Security Baselines	2,0	2,0	2,4	0,0	-0,4
P13 Business Continuïteit	2,0	2,2	2,2	0,2	0,0
P14 Cloud Leveranciers	2,5	2,5	2,3	0,0	0,2
(T) Technische Weerbaarheid	2,7	2,7	2,5	0,0	0,2
T15 MFA - Thuiswerken	2,5	2,5	2,5	0,0	0,0
T16 SOC SIEM	5,0	5,0	2,4	0,0	2,6
T17 Pentesten	2,0	2,0	2,3	0,0	-0,3
T18 Patchbeheer	3,0	3,0	2,6	0,0	0,4
T19 Infrastructuur	2,5	2,5	2,5	0,0	0,0
T20 Security Policy	3,0	3,0	2,7	0,0	0,3
T21 Computer Operations	2,0	2,0	2,3	0,0	-0,3
Eindtotaal	**2,5**	**2,5**	**2,3**	**0,0**	**0,2**
		Hoogste Stijging / Grootste Positieve Verschil		0,4	2,6
		Hoogste Daling / Grootste Negatieve Verschil		-0,1	-0,4

4. Checklist of Groeimodel

4. Checklist of Groeimodel

4. Toekomst NBA-model (in het onderwijs)

- HO en Universiteiten vallen onder de Cyberbeveiligingswet (Cbw)
  - ➔ Willen over naar ISO

    - Internationaal erkend
    - Wordt onderhouden
    - Risicogebaseerd
    - Bekend bij IT-Auditors

    - PO VO en mbo gaan voorlopig in ieder geval door met het NBA-model

4 Toekomst NBA-model…