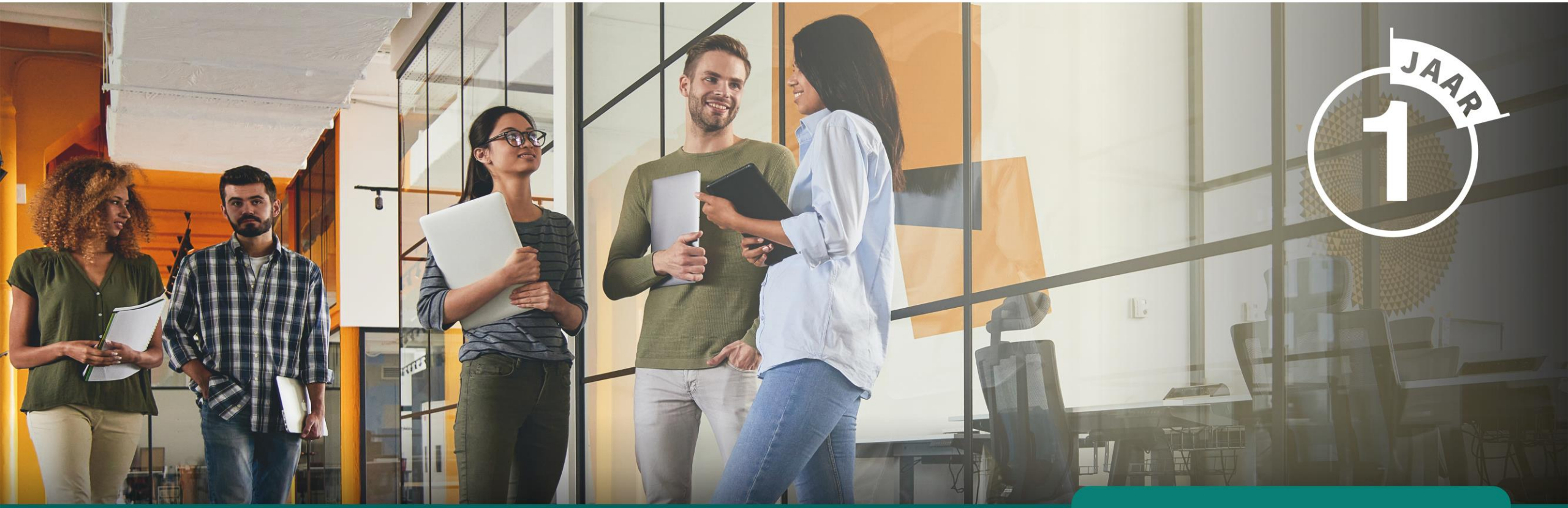
WORKSHOP

Groeien in volwassenheid: hoe dan?

SAMENWERKEN AAN
CYBERVEILIGHEID
IN HET MBO



PROGRAMMA
Cyberveiligheid

NETWERK
Informatiebeveiliging
en Privacy

MBO Raad

mbo digitaal

mbodigitaal.nl/cyberveiligheid

Henk Links | NBA-reisleider

Houdt zich binnen het programma Cyberveiligheid voornamelijk bezig met het NBA volwassenheidsmodel Informatiebeveiliging. Met het aanbieden van een modelaanpak wil hij de onderwijsinstellingen op weg helpen om aantoonbaar te 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 en scherp in zijn analyse. Begrip is voor hem erg belangrijk | **Samenwerken,** ook over de verschillende onderwijssectoren, heeft hij hoog in het vaandel staan en hij wil graag concreet bijdragen aan betrouwbare en veilige onderwijsomgeving.

mbo digitaal

NBA

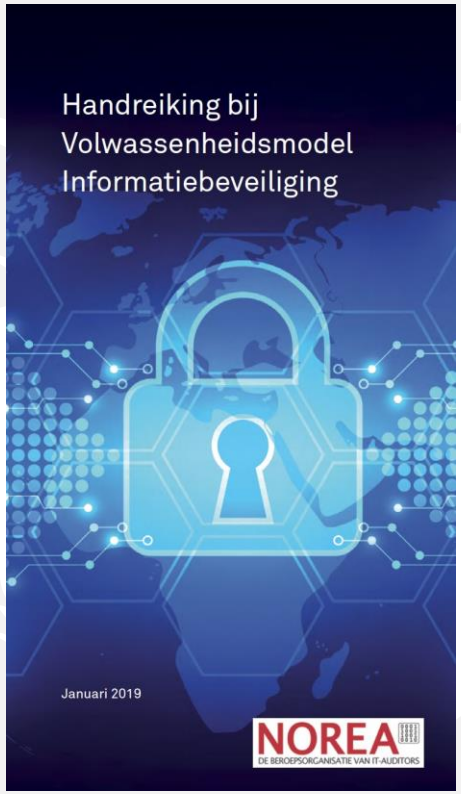
AANPAK

VERVOLG

Het NBA-model

1. Het model is met 69 maatregelen een stuk compacter dan het huidige toetsingskader.
2. Het is minder gericht op alleen de technische beheersmaatregelen: er is 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 auditors en accountants betrokken kunnen worden bij het assessment.

[Volwassenheidsmodel informatiebeveiliging (nba.nl)]



NBA
Koninklijke Nederlandse Beroepsorganisatie van Accountants

mbo digitaal

mbo digitaal

Kennisnet

Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs

SURF

SURFaudit Toetsingskader: beoordeel je informatiebeveiliging

mbo digitaal

NBA Volwassenheidsmodel Informatiebeveiliging

(15 domeinen; 69 statements)

1	Governance	GO.01	Informatiebeveiliging Strategie
		GO.02	Informatiebeveiliging Beleid
		GO.03	Informatiebeveiliging Plan / Roadmap
		GO.04	Enterprise Architectuur
		GO.05	Onafhankelijke Assurance
2	Organisatie	OR.01	Eigenaarschap, Rollen, Aansprakelijkheid en Verantwoordelijkheden
		OR.02	Functiescheiding
3	Risicomanagement	RM.01	Raamwerk voor informatierisicobeheer
		RM.02	Risicobeoordeling
		RM.03	Risicoactie- en mitigatieplan (inclusief risicoacceptatie)
4	Human Resource	HR.01	Werving
		HR.02	Certificering, training en opleiding
		HR.03	Afhankelijkheid van individuen
		HR.04	Functiewijziging en/of beëindiging
		HR.05	Kennisdeling
		HR.06	Veiligheidsbewustzijn (Security Awareness)
5	Configuratie Management	CO.01	Identificatie en onderhoud van configuratie-items
		CO.02	Configuratiedatabase en baseline
6	Incident Management	IM.01	Incident Management
		IM.02	Incident Escalatie
		IM.03	Incidentrespons op (cyber)beveiligingsincidenten
		IM.04	Problem management
7	Change Management	CH.01	Standaarden en procedures voor het wijzigingsproces
		CH.02	Impactanalyse, prioritering en autorisatie
		CH.03	Spoedwijzigingen
		CH.04	Testomgeving
		CH.05	Testen van wijzigingen
		CH.06	Promotie naar productie
8	Systeemontwikkeling	SD.01	Methodologie veilige ontwikkeling en implementatie van software
		SD.02	Ontwikkelaarstoegang tot productie
		SD.03	Gegevensconversie en/of migratie
9	Data Management	DM.01	Eigenaarschap van gegevens (en systeem)
		DM.02	Dataclassificatie
		DM.03	Beveiligingsvereisten voor gegevensbeheer
		DM.04	Opslag- en bewaarregelingen
		DM.05	Uitwisseling van (gevoelige) gegevens
		DM.06	Verwijdering van informatie
10	Identity & Access Management	ID.01	Toegangsregels
		ID.02	Beheer van toegangsrechten
		ID.03	Gebruikers met verhoogde toegangsrechten (Super Users)
		ID.04	Envelop procedure
		ID.05	Periodieke beoordeling van toegangsrechten
11	Security Management	SM.01	Beveiligingsbasisregels
		SM.02	Authenticatiemechanismen
		SM.03	Mobiele apparaten en telewerken
		SM.04	Logging
		SM.05	Testen, bewaking en monitoring van informatiebeveiliging
		SM.06	Patchbeheer
		SM.07	Beheer van bedreigingen en kwetsbaarheden
		SM.08	Bescherming en beschikbaarheid van infrastructuurbronnen
		SM.09	Onderhoud van de infrastructuur
		SM.10	Beheer van cryptografische sleutels
		SM.11	Netwerkbeveiliging
		SM.12	Beheer van malware-aanvallen
		SM.13	Bescherming van beveiligingstechnologie
12	Fysieke Toegangsbeveiliging	PH.01	Fysieke beveiligingsmaatregelen
		PH.02	Beheer van fysieke toegangsrechten
13	Computer Operations	OP.01	Taakverwerking
		OP.02	Backup- en herstelprocedures
		OP.03	Capaciteits- en prestatiebeheer
14	Business Continuity Management	BC.01	Bedrijfscontinuïteitsplanning (Business Continuity Planning)
		BC.02	Testen van noodherstel (disaster recovery)
		BC.03	Externe opslag van backupmedia
		BC.04	Gegevensreplicatie
		BC.05	Crisismanagement
15	Supply Chain Management	SC.01	Service Level Agreement
		SC.02	Service Level Management
		SC.03	Risicobeheer van leveranciers
		SC.04	Interne controle bij externe dienstverleners (service providers)

mbo digitaal

	A	C	E	F	G	H	I	J	
1							Volwassenheidsniveau 1	Volwassenheidsniveau 2	Volw
2	Domein	NBA ID	Categorie beheersmaatregel	Beschrijving risico	Beheersdoelstelling	Benchmark Score	Ad hoc Beheersmaatregelen zijn niet of slechts gedeeltelijk gedefinieerd en/of worden op een inconsistente manier uitgevoerd en zijn sterk afhankelijk van individuen.	Gestructureerd Beheersmaatregelen bestaan en worden op een gestructureerde en consistente, maar informele manier uitgevoerd.	Effe Beheersmaatregelen z gestructureerde en form maatregelen is
3	**Governance**	**GO.01**	**Strategie**	Het ontbreken van een strategie kan leiden tot slechte bedrijfs- en beveiligingsbeslissingen of tot een niet passend antwoord op veranderingen in de bedrijfsomgeving.	Een strategie en visie op informatie- en cyber security is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging.		- Implementatie en uitvoering van activiteiten en maatregelen op het gebied van informatiebeveiliging en/of cybersecurity gebeurt ad hoc.	- Een strategie en visie is geformuleerd, maar is niet formeel vastgesteld.	- Strategie en visie zijn goe - Strategie en missie worde medewerkers, leveranciers
4		**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 (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.		- Er is geen beleid opgesteld. - Er zijn enkele beleidsstukken in concept.	- Er is (informatie)beveiligingsbeleid waarin de meest relevante aspecten van informatiebeveiliging zijn opgenomen	- Informatiebeveiligingsbele management. - Beleid wordt actief gecon leveranciers en contract pa copy beschikbaar. - Het beleid maakt onderde programma. - Het voldoen aan beleid w - Het informatiebeveiligings
		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 naar een algemeen informatiebeveiligingsplan en/of cyber security plan, rekening houdend met de IT-infrastructuur en de veiligheidscultuur.		- Er is geen informatiebeveiligings- of cybersecurity plan of roadmap opgesteld. - Er lopen enkele projecten op het gebied van IT beveiliging of deze zijn gepland.	- Er is een informatiebeveiligings- en/of cybersecurity plan of roadmap opgesteld. Dit plan bestrijkt alle relevante organisatiedoelstellingen, risico's en eisen op het gebied van wet- en regelgeving.	- Het plan of roadmap is go - Het plan is uitgewerkt in (procedures, tezamen met diensten, personeel, softw - Gerelateerd beleid en -pr gebruikers en stakeholders

1-69

Bestuur

1.1 (GO.01) Strategie

Risico:

Het ontbreken van een strategie kan leiden tot slechte zakelijke en beveiligingsbeslissingen of tot een niet passend antwoord op veranderingen in de bedrijfsomgeving.

Doelstelling:

Een strategie en visie op informatie- en cyber security is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging.

Volwassenheidsniveaus:

1	a. Implementatie en uitvoering van activiteiten en maatregelen op het gebied van informatiebeveiliging en/of cyber security gebeurt ad hoc.
2	a. Een strategie en visie is geformuleerd, maar is niet formeel vastgesteld.
3	a. Strategie en visie zijn goedgekeurd door het senior management. b. Strategie en missie worden actief gecommuniceerd naar medewerkers, leveranciers en business partners.
4	a. Strategie en visie is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging en cyber security. b. Indien van toepassing wordt vastgelegd hoe er in lijn met strategie en visie gewerkt wordt. c. De geldigheid en uitvoerbaarheid van de strategie en visie wordt periodiek geverifieerd.
5	a. De strategie geeft aan hoe IT de organisatie helpt haar doelstellingen te behalen. b. Indien noodzakelijk worden strategie en visie bijgesteld om organisatiedoelstellingen en externe ontwikkelingen bij te houden.

Referenties:

Normenkader Informatie-beveiliging mbo2019 *01 Beleid en Organisatie*	1.1
COBIT 4.1	PO1.4 ME4.2
COBIT 5	APO02.01 APO02.02 APO02.03 APO02.04 APO02.05
ISO 27K 2013	5.1 A.5.1.1
DNB 2014/2017	1.2
BIO 2019	5.1.1 5.1.1.1
NIST Cybersecurity Framework	ID.GV-3

mbo digitaal

domeinnaam

statement titel

Bestuur

1.1 (GO.01) Strategie

Risico:

Het ontbreken van een strategie kan leiden tot slechte zakelijke en beveiligingsbeslissingen of tot een niet passend antwoord op veranderingen in de bedrijfsomgeving.

Doelstelling:

Een strategie en visie op informatie- en cyber security is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging.

Volwassenheidsniveaus:

1	a. Implementatie en uitvoering van activiteiten en maatregelen op het gebied van informatiebeveiliging en/of cyber security gebeurt ad hoc.
2	a. Een strategie en visie is geformuleerd, maar is niet formeel vastgesteld.
3	a. Strategie en visie zijn goedgekeurd door het senior management. b. Strategie en missie worden actief gecommuniceerd naar medewerkers, leveranciers en business partners.
4	a. Strategie en visie is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging en cyber security. b. Indien van toepassing wordt vastgelegd hoe er in lijn met strategie en visie gewerkt wordt. c. De geldigheid en uitvoerbaarheid van de strategie en visie wordt periodiek geverifieerd.
5	a. De strategie geeft aan hoe IT de organisatie helpt haar doelstellingen te behalen. b. Indien noodzakelijk worden strategie en visie bijgesteld om organisatiedoelstellingen en externe ontwikkelingen bij te houden.

beheersmaatregelen

mbo digitaal

Deel 1
Normenkader
informatiebeveiliging

1 Bestuur
2 Organisatie
3 Risicomanagement
4 Personeelsbeheer
5 Configuration Management
6 Incident/Problem Management
7 Change Management
8 Systeemontwikkeling
9 Datamanagement
10 Identity & Access Management
11 Security Management
12 Fysieke beveiliging
13 IT-operatie
14 Bedrijfscontinuïteits-management
15 Ketenbeheer

1

Bestuur

Welke onderwerpen staan in dit domein?
In het domein Bestuur zijn vijf normen opgenomen. Deze normen geven richting en ondersteuning om de informatiebeveiliging in te richten in lijn met organisatie-doelstellingen, risicobereidheid en wet- en regelgeving. Ze gaan over de naleving van het normenkader. Met andere woorden: de normen binnen dit domein vormen belangrijke kaders voor de invulling van de normen uit de andere domeinen.

Allereerst is het nodig om je strategie en visie voor informatiebeveiliging te bepalen. Op basis daarvan bepaal je het informatiebeveiligingsbeleid. Als afgeleide van je beleid maak je periodiek informatiebeveiligingsplannen die zorgdragen voor verbetering van je informatiebeveiliging. Vervolgens is er een Enterprise Architectuur die inzicht in en overzicht over de organisatiestructuur en de informatievoorziening geeft en helpt om op verantwoorde wijze veranderingen door te voeren. De laatste norm binnen dit domein gaat over het (laten) toetsen van hoe je er als organisatie voor staat op het gebied van informatiebeveiliging, met als doel inzicht te krijgen in verbetermogelijkheden om risico's te verkleinen.

Wie is verantwoordelijk?

Voor alle onderdelen binnen dit domein geldt dat het bevoegd gezag eindverantwoordelijkheid draagt. Wanneer het gaat over zaken als strategie en beleid, dan zal de voorbereiding meestal gebeuren door een adviseur op het gebied van informatiebeveiliging binnen de organisatie. Deze stemt af met functionarissen als de FG, en de verantwoordelijken voor IBP en IT. Het bevoegd gezag stelt de naleving van informatiebeveiliging vast en is daarvoor ook verantwoordelijk. Medewerkers binnen de organisatie worden geïnformeerd over de zaken die hen aangaan, zoals het informatiebeveiligingsbeleid. In opdracht van het bevoegd gezag voeren interne en/of externe auditors het toezicht op naleving uit. De audit zelf wordt vaak voorbereid door de IBP-coördinator.

Ondersteuningsproducten

Beschikbaar:

- Template *IBP-beleidsplan* (zie Aanpak IBP)
- Toelichting op het template IBP-beleidsplan (zie Aanpak IBP)
- *Funderend Onderwijs Referentie Architectuur* (FORA)

In ontwikkeling/te ontwikkelen:

- Handreiking en format *Strategie en visie*
- Handreiking *Jaarlijkse aandacht voor informatiebeveiliging en privacy*
- Handreiking *Functiebeschrijving informatiemanagement*
- Handreiking *Architectuur*
- Audit-as-a-service

mbo digitaal

Deel 1
Normenkader
informatiebeveiliging

1 Bestuur
2 Organisatie
3 Risicomanagement
4 Personeelsbeheer
5 Configuration Management
6 Incident/Problem Management
7 Change Management
8 Systeemontwikkeling
9 Datamanagement
10 Identity & Access Management
11 Security Management
12 Fysieke beveiliging
13 IT-operatie
14 Bedrijfscontinuïteits-management
15 Ketenbeheer

1.1 Strategie

NORM

GO.01
Een strategie en visie op informatie- en cybersecurity is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging.

Waarom doen we dit?
Het hebben van een strategie leidt tot gepaste zakelijke en beveiligingsbeslissingen, tot samenhang in beveiligingsbeslissingen en tot een passend antwoord op veranderingen in de bedrijfsomgevingen.

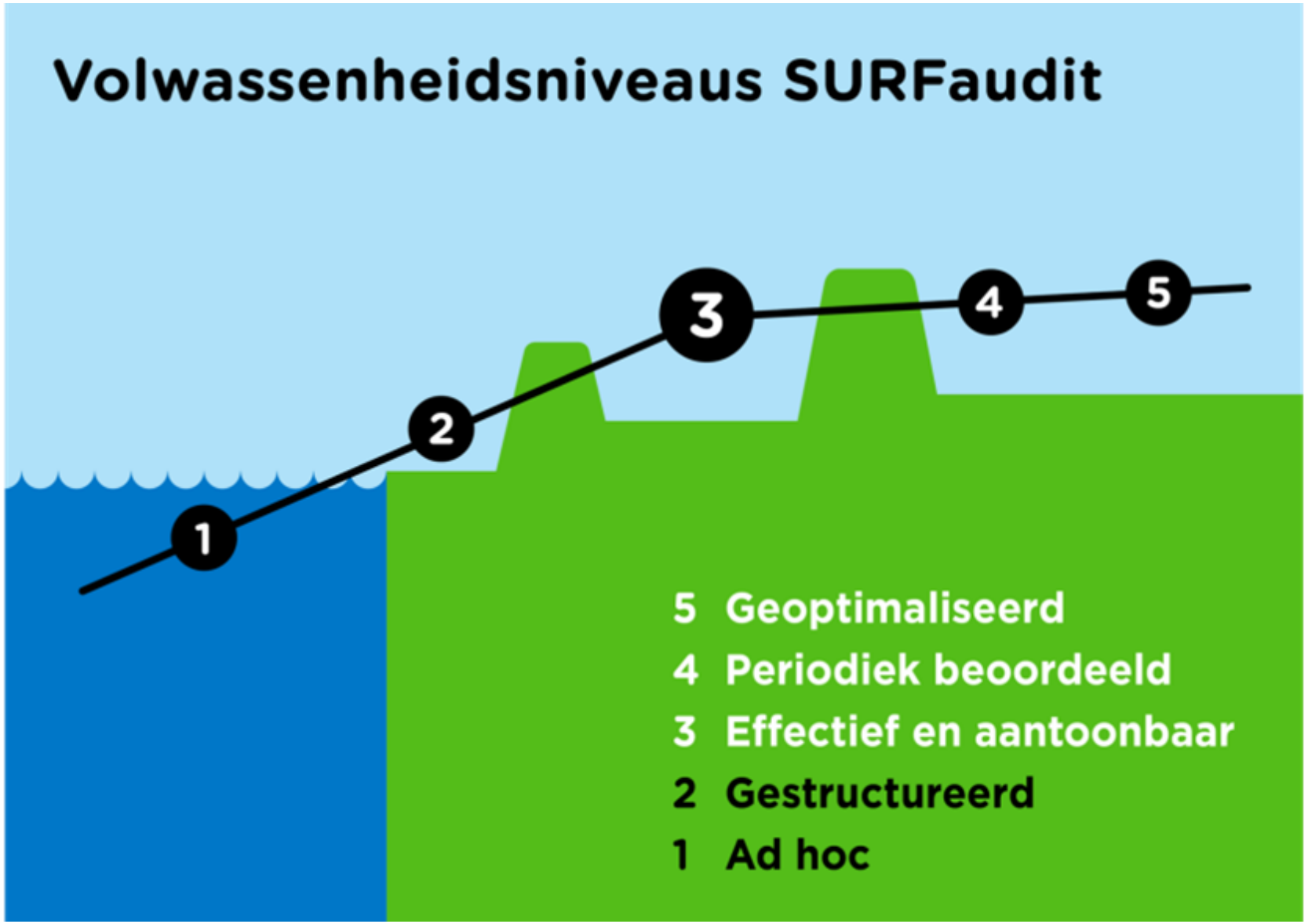
TOETSINGSKADER

- Strategie en visie zijn goedgekeurd door het bevoegd gezag.
- Strategie en missie worden actief gecommuniceerd naar medewerkers, leveranciers en businesspartners.

VOORBEELDMAATREGELEN

1. Het schoolbestuur heeft een strategie en visie geformuleerd op informatie-beveiliging en cybersecurity. De opbouw van deze strategie en visie bevat de elementen die aangereikt worden in de Handreiking *Strategie en Visie* vanuit het ondersteuningsaanbod. Er kan gebruikgemaakt worden van het Format Strategie en Visie.
2. Het bevoegd gezag heeft de strategie en visie vastgesteld.
3. De strategie en visie zijn (digitaal) beschikbaar, bijvoorbeeld via de website en het intranet.

mbo digitaal


Volwassenheidsniveaus SURFaudit
1
2
3
4
5
5 Geoptimaliseerd
4 Periodiek beoordeeld
3 Effectief en aantoonbaar
2 Gestructureerd
1 Ad hoc

Niveau	Naam	Korte omschrijving	Toelichting
1	Initieel	Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte controls geïmplementeerd. • Niet of ad-hoc uitgevoerd. • Niet /deels gedocumenteerd. • Wijze van uitvoering afhankelijk van individu.
2	Herhaalbaar	Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	Control is geïmplementeerd. Uitvoering is consistent en standaard. Informeel en grotendeels gedocumenteerd.
3	Gedefinieerd	Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.	• Control gedefinieerd o.b.v. risico assessment. • Gedocumenteerd en geformaliseerd. • Verantwoordelijkheden en taken eenduidig toegewezen. • Opzet, bestaan en effectieve werking aantoonbaar. • Rapportage van uitvoering van beheersingsmaatregel aan management. • Effectieve werking van controls wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie. • De toetsing toont aan dat de control effectief is.
4	Beheerst en meetbaar	De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd.	• Periodieke (control) evaluatie en opvolging vindt plaats. • Evaluatie is gedocumenteerd en geformaliseerd. • Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks. • Rapportage van de evaluatie aan management.
5	Continu verbeteren	De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.	• Continu evalueren van de beheersingsmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit Self-assessment, gap en root cause analyses. • De getroffen beheersingsmaatregelen worden gebenchmarkt en zijn ‘Best Practice’ in vergelijking met andere organisaties. • Real time monitoring. • Inzet automated tooling.

Niveau	Korte omschrijving	Toelichting
1	Maatregelen zijn ad hoc.	Beheersmaatregelen zijn niet of slechts gedeeltelijk vastgesteld en/of worden op een inconsistente manier uitgevoerd en zijn sterk afhankelijk van individuen.
2	Maatregelen bestaan en worden op consistente wijze uitgevoerd.	Beheersmaatregelen bestaan en worden op een gestructureerde en consistente, maar informele manier uitgevoerd.
3	Maatregelen zijn gedocumenteerd en de uitvoering is aantoonbaar.	Beheersmaatregelen zijn gedocumenteerd en worden op een gestructureerde en formele manier uitgevoerd. Uitvoering van de maatregelen is aantoonbaar, getest en effectief.
4	Er is een verbetercyclus aanwezig en gedocumenteerd.	De effectiviteit van beheersmaatregelen wordt periodiek beoordeeld en indien nodig verbeterd. Deze beoordeling is gedocumenteerd.
5	Er is een bedrijfsbrede aanpak van risico’s.	Een bedrijfsbreed risico- en beheersprogramma voorziet in continue en effectieve beheersing en aanpak van risico's.

Checklist of Groeimodel

Checklist of Groeimodel


NBA

Aanpak

mbo digitaal

IM.01 ↑ Overzicht				
	Beheersmaatregel	**Incident management**	**Procesverantwoordelijke(n)**	• **Incident Manager**
	Inherent Risico	**Incidenten zijn niet correct geclassificeerd en worden onjuist behandeld in het incidentbeheerproces, wat uiteindelijk leidt tot verminderde prestaties en kwaliteit van de informatievoorziening.**	**Referenties** **BIO**	7.2.3. 12.6.1, 12.6.1.1, 16.1.1, 16.1.2, 16.1.2.1, 16.1.2.2, 16.1.2.3, 16.1.2.4, 16.1.2.5, 16.1.2.6, 16.1.2.7, 16.1.3, 16.1.3.1, 16.1.4, 16.1.4.1, 16.1.5, 6.1.6, 16.1.6.1, 16.1.6.2, 16.1.7, 16.1.7.1, Supplement BIG: 13.1.1.5, 13.1.1.6 [A]
	Beheersdoelstelling	**Een formeel incidentmanagementproces wordt gecommuniceerd en geïmplementeerd. Er zijn procedures om ervoor te zorgen dat alle incidenten en storingen worden geregistreerd, geanalyseerd, gecategoriseerd en geprioriteerd op basis van impact. Alle incidenten worden bijgehouden en periodiek beoordeeld om ervoor te zorgen dat ze tijdig worden opgelost.**	**COBIT 5**	DSS02.01, DSS02.02, DSS02.03, DSS02.05, DSS02.06, DSS02.07
			DNB	15.1, 15.2
			ISO27000	A.7.2.3, A.12.6.1, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
			NIST	RS.RP-1, PR.IP-9, PR.IP-10, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2

Bewijsvoering Opzet & Bestaan	**Vraagstelling**
• Procesbeschrijving/werkinstructie voor het melden van incidenten; • Procesbeschrijving incident management proces; • Vastlegging van rollen, verantwoordelijkheden en afspraken (vastlegging, classificatie, terugkoppeling en binnen tijdsbestek incidenten worden afgehandeld) binnen incident afhandelingsproces; • Criteria voor classificatie van incidenten (prioritering) • Voorbeeld van een volledig afgehandelde ticket. • Inzicht in monitoringproces op de (tijdige) incidentafhandeling;	• Hoe verloopt het incident management proces voor incidenten mbt applicaties, procedures, processen, systemen? • Is deze procedure ook geformaliseerd en gecommuniceerd binnen de organisatie? • Wordt in dit beleid ook de rollen en verantwoordelijkheden uiteengezet en zijn deze ook duidelijk gecommuniceerd? • Wordt er gebruik gemaakt van het ticketsysteem om incidenten te registreren, op te pakken, te autoriseren en door te voeren? • Hoe wordt er gewaarborgd dat incidenten goed worden geclassificeerd en geprioriteerd? • Hoe wordt gewaarborgd dat incidenten tijdig en adequaat worden opgevolgd? • Wordt de kwaliteit en effectiviteit van het incident management beleid periodiek geëvalueerd? En zo ja, op welke manier wordt dit gedaan? • Met welke periodiciteit vindt er een herbeoordeling plaats van incident management beleid? • Hoe wordt het management op de hoogte gehouden van relevante incidenten?

Bewijsvoering per volwassenheidsniveau

1	2	3	4	5
a) Er is geen beleid voor incidentmanagement. b) Er zijn geen rollen en verantwoordelijkheden vastgelegd. c) Er zijn geen procedures om te garanderen dat alle incidenten en storingen worden gedocumenteerd en geanalyseerd. d) Incidenten worden bijgehouden en geëvalueerd op individuele basis. e) Reacties op informatiebeveiligingsincidenten zijn ad hoc.	a) Er is een informeel incidentmanagementproces gedefinieerd om kritische incidenten aan te pakken. b) Rollen en verantwoordelijkheden zijn gedeeltelijk vastgelegd. c) De meeste incidenten worden gedocumenteerd en geanalyseerd, maar afwijkingen van de standaarden worden waarschijnlijk niet gedetecteerd. d) Er zijn geen criteria bepaald voor het categoriseren en prioriteren van incidenten op basis van impact. e) Incidenten worden ad hoc toegewezen. Er wordt handmatig en op individuele basis toezicht gehouden. f) Er is geen formele training en communicatie over de standaardprocedures.	a) Het incidentmanagementbeleid is formeel gedocumenteerd en gecommuniceerd. b) Rollen en verantwoordelijkheden van de organisatie en de leveranciers zijn duidelijk gedefinieerd. c) Aspecten rondom juridisch en forensisch onderzoek zijn vastgesteld en toegewezen. d) Het registreren van, de communicatie over, de toewijzing van en de analyse van incidenten zijn formeel belegd in de organisatie. e) Incidenten worden gecategoriseerd en geprioriteerd op basis van impact. f) (Cyber)beveiligingsincidenten worden voorkomen of gedetecteerd en er is een proces om deze tijdig en effectief aan te pakken. g) Informatie wordt op een proactieve en formele manier gedeeld door personeel. h) Er wordt gemonitord of incidenten tijdig worden opgelost. i) Er wordt beperkt gerapporteerd aan management over incident- en oplossingsanalyses.	Aanvullend: a) Incidenten worden proactief geanalyseerd om oorzaken te achterhalen. b) Er is een functie (responsteam) geïmplementeerd om beveiligingscrises te herkennen en beheren. c) Het incidentmanagementproces betrekt belangrijke functies in de organisatie en bij externe service providers. d) Op het tijdig aanpakken van incidenten wordt streng toegezien. Onopgeloste incidenten (bekende foutmeldingen waar omheen gewerkt wordt) worden gedocumenteerd en gerapporteerd als input voor probleembeheer. e) De kwaliteit en operationele effectiviteit van het incidentmanagementproces worden periodiek geëvalueerd. f) Er is een overzicht van het proces van intake tot afsluiting van een incident. g) Er is een procedurebeschrijving en mandatenregeling voor forensische deskundigen (CSIRT-team).	Aanvullend: a) De registratie, rapportage en analyse van incidenten en oplossingen zijn volledig geautomatiseerd en geïntegreerd met configuratie- en probleembeheer. b) De meeste systemen zijn uitgerust met automatische detectie- en waarschuwingssystemen, die voortdurend gemonitord en beoordeeld worden. c) Incidentbeheer wordt voortdurend geanalyseerd voor verbetering.

Hoe ga ik met het Normenkader IBP FO aan de slag?

Je kunt niet alles tegelijk doen, dus hoe stel je als schoolbestuur prioriteiten in de normen die je op orde wil gaan brengen. Onderstaande tabel helpt je met het aanbrengen van prioriteiten. In plaats van jouw organisatie direct op alle onderdelen te gaan scoren kun je beginnen met 'de basis op orde'. Als je dat goed in kaart hebt en de juiste acties in gang hebt gezet, kun je aan de slag met het mitigeren van de hoge en later de medium risico's. In de laatste fase is het dan tijd om de puntjes op die i te zetten. Op deze manier is de grote hoeveelheid aan normen een stuk beter hanteerbaar.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
De basis op orde	1.1 1.2	2.1				6.1 6.2 6.4	7.1 7.2 7.3		9.1 9.2 9.3			12.1		14.1 14.5	
Mitigeren *hoge* risico's			3.1 3.2 3.3	4.6			7.4 7.5 7.6	8.1 8.2	9.5	10.1 10.2 10.3 10.5	11.2 11.4 11.6 11.12 11.13	12.2	13.2	14.2 14.3	15.3
Mitigeren *medium* risico's	1.4 1.5	2.2		4.1 4.4	5.1 5.2	6.3			9.4 9.6		11.1 11.3 11.5 11.7		13.3	14.4	15.1 15.2 15.4
Verdere verfijning	1.3			4.2 4.3 4.5				8.3		10.4	11.8 11.9 11.10 11.11		13.1		

mbo digitaal

Hoe ga ik met het Normenkader IBP FO aan de slag?

Je kunt niet alles tegelijk doen, dus hoe stel je als schoolbestuur prioriteiten in de normen die je op orde wil gaan brengen. Onderstaande tabel helpt je met het aanbrengen van prioriteiten. In plaats van jouw organisatie direct op alle onderdelen te gaan scoren kun je [illegible] basis op orde'. Als je dat goed in kaart hebt en de juiste [illegible] slag met het mitigeren van de [illegible] om de [illegible] te zetten. Op [illegible] bete[illegible]

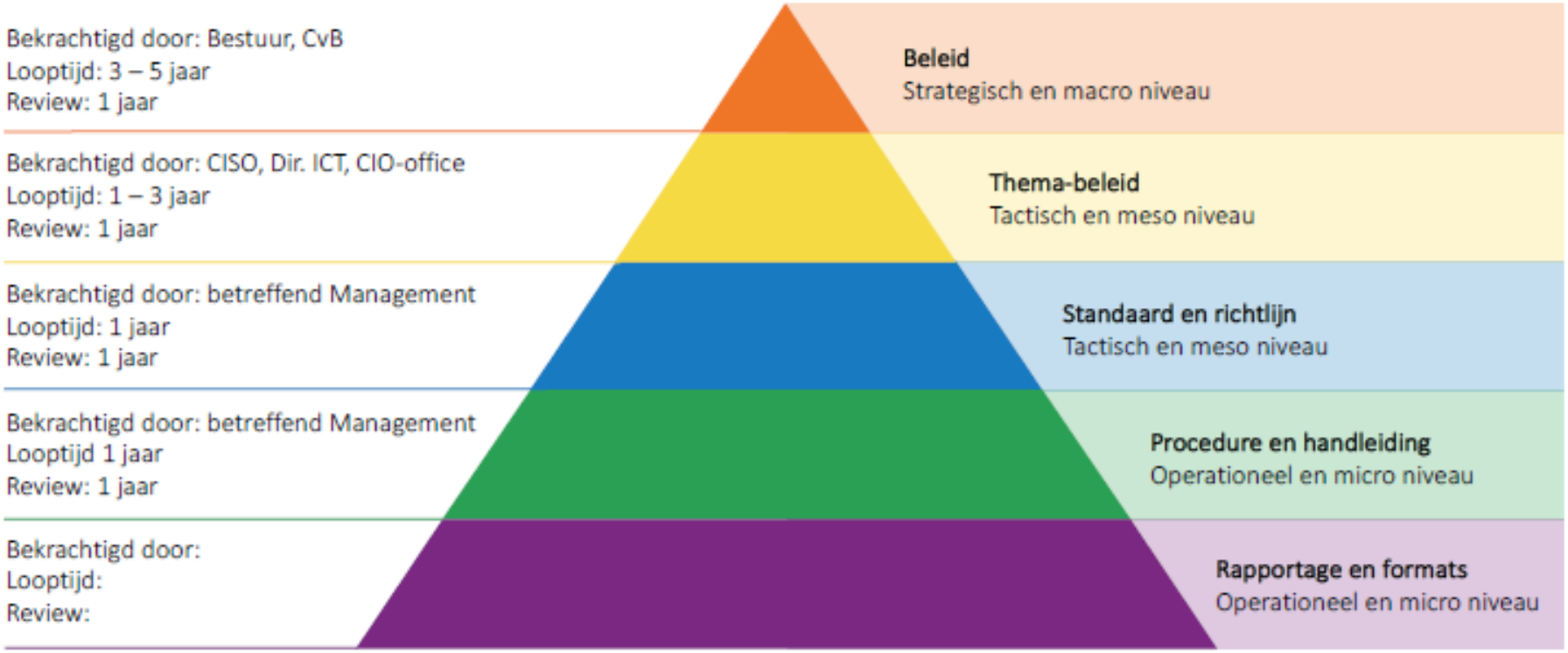
Net als jullie een paar jaar nodig zullen hebben om volledig aan het normenkader te voldoen, zo zullen wij een paar jaar nodig hebben om alle stukken te schrijven. De volgorde waarin we verwachten dat jullie met de normen aan de slag gaan, staat in de 'aan-de-slag-wijzer' bij het normenkader. We zullen de stukken schrijven in de volgorde waarin jullie geacht worden aan de normen te gaan voldoen.

We zullen alle kennisproducten openbaar maken, en onder een vrije licentie herbruikbaar maken. Zo hopen we dat we zoveel mogelijk anderen op weg kunnen helpen.

De ba[illegible]																
Mitige[illegible] risico's																
Mitigere[illegible] risico's												11.5 11.7			14.4	15.1 15.2 15.4
Verdere verfijning				4.5				8.3		10.4	11.8 11.9 11.10 11.11		13.1			

mbo digitaal

Beleidspiramide



NBA Volwassenheidsmodel Informatiebeveiliging

(3 aandachtsgebieden; 21 thema's; 69 statements)

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

GOVERNANCE		
G01	Strategie 1.1	Continuïteit – Kwaliteit – Veiligheid Toetsbaar
G02	Beleid 1.2	3 lines of defences
G03	Architectuur 1.4	MORA
G04	Eigenaarschap 2.1/2.2	RACI functiescheiding
G05	Risk Management 3.1/3.2/3.3	inventarisatie –> analyse -> plan
G06	Roadmap 1.3	actie!
G07	Toetsing 1.5	self assessment – mini assessments – peer review – externe audit

mbo digitaal

PROCESSEN		
P08	**Human Resources** 4.1/4.2/4.3/4.4/4.5/4.6	• Werving (4.1) / Certificering, training en scholing (4.2) • Afhankelijkheid van individuen (4.3) • Verandering of beëindiging van functie (4.4) • Kennisdeling (4.5) • Veiligheidsbewustzijn (4.6)
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	• Configuratie Management • Incident Management • Problem Management • Change Management • Fysieke Beveiliging
P10	**Datamanagement** 8.1/8.2/8.3/9.1/9.2/9.3/9.4/9.5/9.6	• Data Conversie en / of migratie (8.3) • Data (en systeem) eigenaarschap (9.1) • Classificatie (9.2) • Beveiligingseisen voor datamanagement (9.3) • Inrichting van opslag en retentie - bewaartermijnen (9.4 / 9.6) • Uitwisseling van (gevoelige) gegevens (9.5)
P11	**IAM** 10.1/10.2/10.3/10.4/10.5	• Autorisatiebeleid
P12	**Security Baselines** 11.1	• SURF Security Baselines -> Hoe!
P13	**Business Continuïteit** 14.1/14.2/14.3/14.4/14.5	• Business Continuïteitsplan • Disaster recovery • Crisisplan
P14	**Cloud Leveranciers** 15.1/15.2/15.3/15.4	• Service Level Overeenkomst (15.1) • Service Level Management (15.2) • Supplier Risk Management (15.3) • Interne beheersing bij derden (15.4)

mbo digitaal

TECHNISCHE WEERBAARHEID		
T15	MFA - Thuiswerken 11.2/11.3	• Alle studenten en medewerkers maken gebruik van MFA. • Alle managed laptops worden voorzien van MFA en worden op afstand voorzien van updates en eventueel bij diefstal gewist (middels Intune).
T16	SOC SIEM 11.4	• Medewerkers die speciale of admin rechten worden gelogd. • Medewerkers die gegevens met vertrouwelijkheid Hoog verwerken worden gelogd. • Technische devices (Firewalls, etc.) worden gelogd. • Het netwerk wordt middels SOC SIEM 7x24 gecontroleerd op ongewenste activiteiten. Foxit is als partner aangewezen.
T17	Pentesten 11.5	• Tweejaarlijks worden er pentesten uitgevoerd op onzevharde infrastructuur, onze publiek toegankelijke webdiensten en de door ons aangeschafte applicaties. • De pentesten op onze applicaties worden door SURF uitgevoerd. • De kosten van de pentesten zijn op genomen in de meerjarenbegroting (5 jaar).
T18	Patchbeheer 11.6/11.7	• Patches met een CVSS (Common Vulnerability Scoring System) score van 8 of hoger worden meteen opgepakt. • De uitvoer van patches worden gecontroleerd met behulp van Holm Security software en Defender for Cloud. • Maandelijks ontvangt het CvB een rapport betreffende uitgevoerde en niet- uitgevoerde patches met een CVSS score van 8 of hoger.
T19	Infrastructuur 11.8/11.9	• De beschikbaarheid van het netwerk is 99,9%. Reserve devices en metingen dragen zorg voor de beschikbaarheid. • Een meerjarenbegroting (5 jaar) en pro-actief onderhoud zorgen voor de gewenste beschikbaarheid.
T20	Security Policy 11.10/11.11/11.12/11.13	• BitLocker is geïnstalleerd op alle managed werkplekken waardoor gegevens standaard versleuteld worden. • Certificaten van leveranciers worden actief onderhouden. • Het netwerk is gesegmenteerd. • Microsoft Defender is geïnstalleerd op alle managed werkplekken. Servers zijn voorzien van McAfee. • Gevoelige IT documenten zijn versleuteld en voor slechts 3 medewerkers toegankelijk.
T21	Computer Operations 13.1/13.2/13.3	• Job processing bij indiensttreding is beschreven. • Back up en herstel beleid voor on premise vindt regelmatig plaats. • Capacity en performance metingen worden uitgevoerd met behulp van Nagios.

mbo digitaal

SURF Security Baselines

Wat is de SURF security baseline?

Diverse instellingen hebben in SURF-verband samengewerkt aan de SURF security baseline voor onderwijs en onderzoek. Met deze set van informatiebeveiligingsmaatregelen zorg je ervoor dat systemen en toepassingen in je instelling aan een minimum beveiligingsniveau voldoen. Zowel nieuwe als bestaande systemen, en zowel eigen als aangeschafte systemen.

Hoe werkt het?

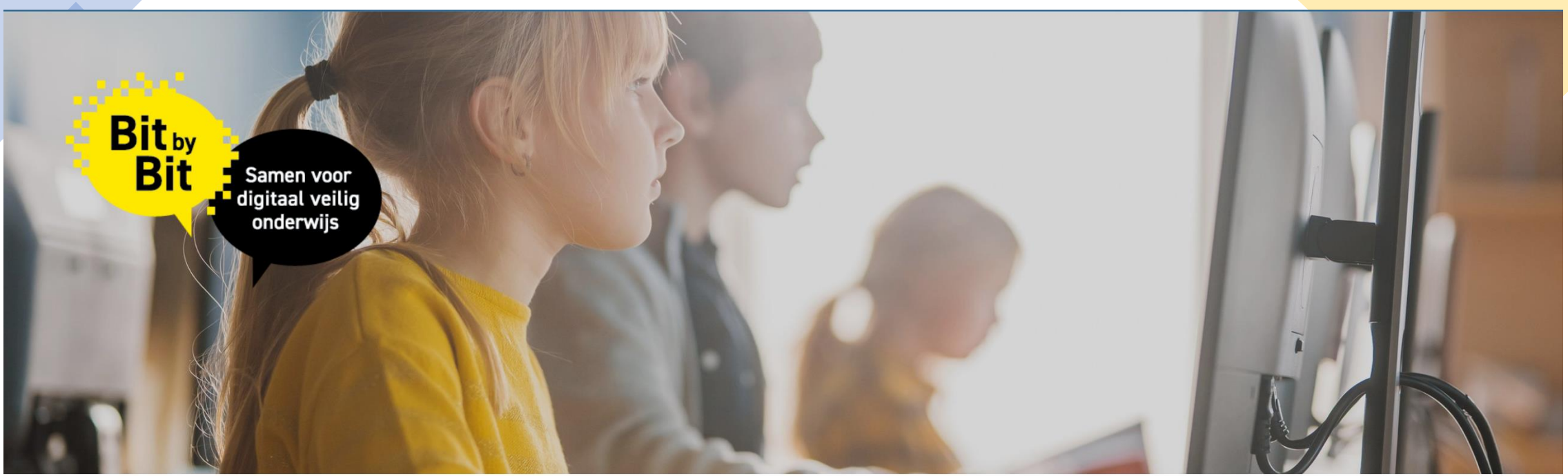
De SURF security baseline helpt je bij het samenstellen van informatiebeveiligingsmaatregelen, voor zowel je interne organisatie als voor je leveranciers. De maatregelen (controls genoemd) zijn onderverdeeld in 15 categorieën, zoals netwerkbeveiliging en logging. Je kunt één of meer categorieën kiezen op basis van je behoeften en vereisten.

SURF Security Baselines

	Governance							Processen							Technische weerbaarheid						
	Strategie	Beleid	Architectuur	Eigenaarschap	Risk Management	Roadmap	Toetsing	HR	ITIL	Datamanagement	IAM	Security Baselines	BCM	Cloudleveranciers	MFA	SOC SIEM	Pentesten	Patchbeheer	Infrastructuur	Security policy	Computer operations
SURF Security Baseline																					
Asset Management		1.2		2.1	3.2				5.1, 5.2, 7.1, 7.2, 7.3			11.1		15.3				11.6, 11.7			
Backup & Restore										9.3, 9.4, 9.6		11.1	14.1, 14.2, 14.3, 14.4								13.2, 13.3
Communications Security									9.3, 9.5			11.1								11.10, 11.11, 11.12, 11.13	
Crisis & Incident Response								4.5	6.1, 6.2, 6.3, 6.4, 7.3				14.5	15.1, 15.2, 15.3, 15.4		11.4					
Cryptography									9.3, 9.5			11.1								11.10	
Data Protection									9.1, 9.2, 9.3, 9.4, 9.5, 9.6			11.1								11.10	13.2, 13.3
Endpoint Security									9.3		10.1, 10.3	11.1			11.2, 11.3	11.4				11.11, 11.12, 11.13	
Human Recourse Security		1.2		2.1				4.1, 4.2, 4.3, 4.4, 4.5, 4.6													13.3
Identity & Access Management															11.2, 11.3				11.8, 11.9	11.11, 11.12, 11.13	
Logging & Monitoring					3.2				6.1, 6.2, 6.3, 6.4				14.5		11.2	11.4				11.11, 11.12, 11.13	13.3
Network Security			1.4									11.1	14.1	15.1, 15.2					11.8, 11.9	11.11, 11.12, 11.13	13.3
Physical & Environmental Security									12.1, 12.2										11.8, 11.9	11.11	
Privileged Access Management											10.3, 10.4, 10.5				11.2, 11.3						
Secure Development										8.1, 8.2, 8.3											
System Hardening									5.1, 5.2			11.1									
Vulnerability Management							1.5										11.5	11.6, 11.7	11.8	11.10, 11.11, 11.12, 11.13	

Vervolg

https://sec.surf.nl/



Ministerie van Onderwijs, Cultuur en Wetenschap

Kennisnet

SIVON

PO RAAD

VO RAAD
Vereniging van scholen in het voortgezet onderwijs

Bit by bit, samen voor digitaal veilig onderwijs

https://www.digitaalveiligonderwijs.nl/

PROGRAMMA
Cyberveiligheid

Het programma Cyberveiligheid heeft als doel om de cyberweerbaarheid van de mbo-sector te vergroten. Binnen dit programma werken de mbo-scholen samen om kennis te delen, kwetsbaarheden te identificeren en best practices uit te werken. Samen staan we sterker tegen cybercriminaliteit.

Aanleiding voor het programma Cyberveiligheid

De aanleiding voor het programma Cyberveiligheid was de ransomware-aanval bij ROC Mondriaan in 2021. Deze aanval heeft veel losgemaakt. Niet alleen binnen de mbo-sector, maar ook in de politiek. De minister van OCW heeft daarom aan de MBO Raad gevraagd om met een plan te komen om de digitale weerbaarheid van de mbo-instellingen te verhogen. Dit heeft geleid tot het programma Cyberveiligheid mbo dat in september 2022 van start is gegaan.

Grote verschillen tussen de instellingen

Op het gebied van informatiebeveiliging zijn er grote verschillen in volwassenheid tussen mbo-scholen. Dat blijkt uit de benchmarks die we sinds 2015 jaarlijks uitvoeren op het gebied van informatiebeveiliging en privacy. Dit biedt kansen, omdat we veel van elkaar kunnen leren.

Gerelateerde berichten


Convenant Cyberveiligheid ondertekend tijdens MBO Digitaal Conferentie


Security- en privacy-awareness: het bewustzijn is er, nu nog ernaar handelen

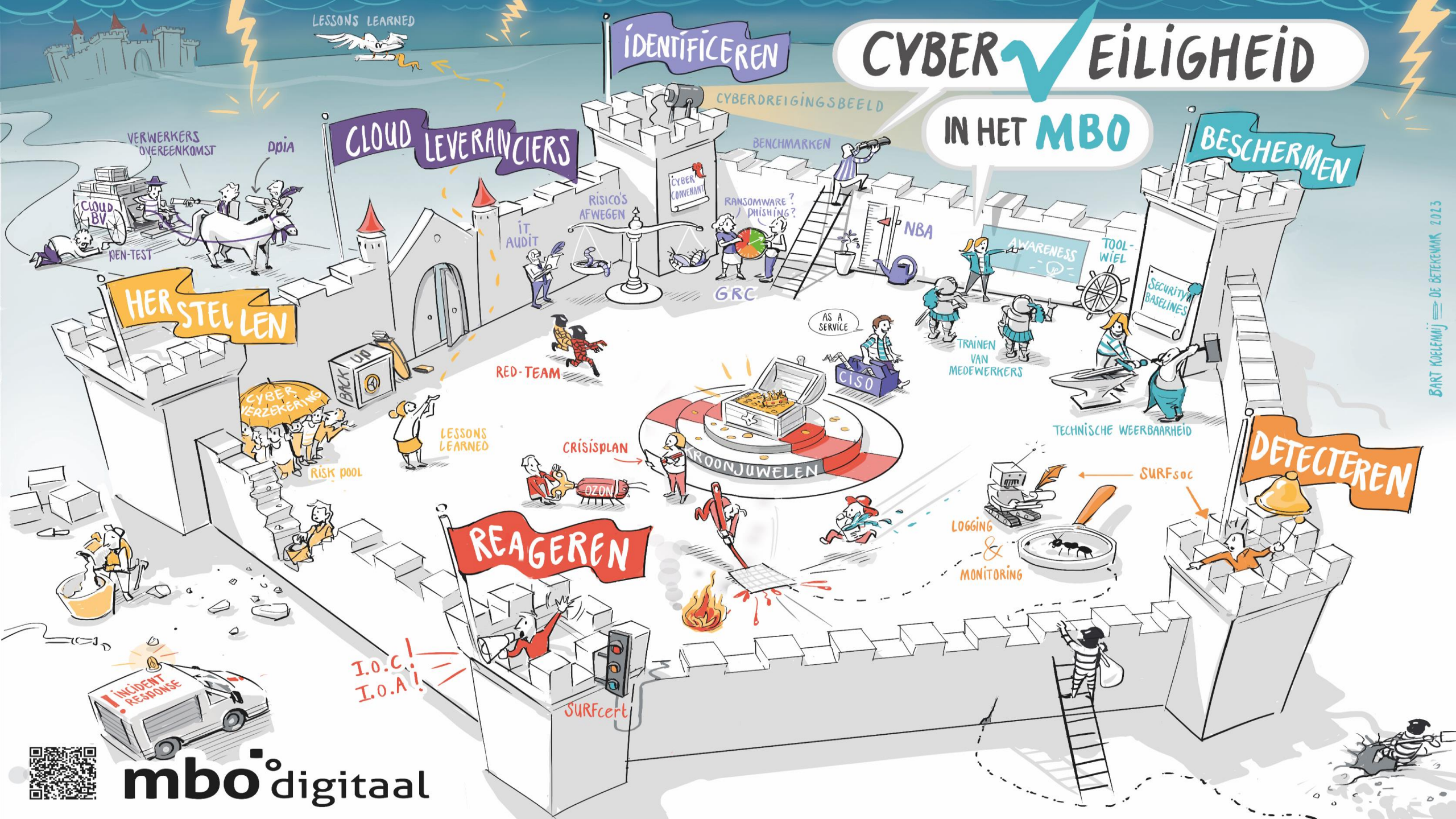

Pauline Satter: 'We moeten samen optrekken in digitale veiligheid'


Aanbesteding IT-auditdiensten start deze zomer


Dienst Verwerkersovereenkomsten Kennisnet

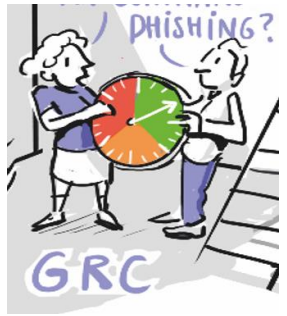

Convenant Cyberveiligheid vastgesteld

https://mbodigitaal.nl/programmas/programma-cyberveiligheid-mbo/


CYBER VEILIGHEID
IN HET MBO
IDENTIFICEREN
CYBERDREIGINGSBEELD
BENCHMARKEN
CLOUD LEVERANCIERS
VERWERKERS OVEREENKOMST
DPIA
CLOUD BV
PEN-TEST
IT AUDIT
RISICO'S AFWEGEN
CYBER CONVENANT
RANSOMWARE? / PHISHING?
GRC
NBA
BESCHERMEN
AWARENESS
TOOL-WIEL
SECURITY BASELINES
TRAINEN VAN MEDEWERKERS
TECHNISCHE WEERBAARHEID
HERSTELLEN
BACK UP
CYBER VERZEKERING
RISK POOL
LESSONS LEARNED
RED-TEAM
AS A SERVICE
CISO
KROONJUWELEN
CRISISPLAN
OZON
REAGEREN
I.O.C.!
I.O.A.!
SURFcert
INCIDENT RESPONSE
SURFsoc
LOGGING & MONITORING
DETECTEREN
BART KUELEMIJ — DE BETEKENAAR 2023
mbo digitaal

AANPAK…

- MASTERCLASSES
- GRC-tool (benchmark en audits)
- AUDITS
- NOZON
- CISO as a SERVICE
- TECHNISCHE WEERBAARHEID



mbo digitaal

Opzet Masterclasses

- Dag 1:
  - Inleiding NBA Toetsingskader
  - Governance

- Dag 2
  - Processen
  - Technische Weerbaarheid

=> Samen aan de slag!