mbo digitaal

ONDERZOEK NAAR GOVERNANCE VAN INFORMATIEBEVEILIGING IN HET MBO 2023

Leren van de sector

Datum	*Versie*	*Auteur*
21 februari 2024	1.0	Victor Meerloo

Dit is een uitgave van: MBO Digitaal
Houttuinlaan 6, 3447 GM Woerden

Auteur: Victor Meerloo

Publicatienummer: 1.0

Contactgegevens: m.bijleveld@mbodigitaal.nl

mbo digitaal

SAMENVATTING

44 van de 55 aangeschreven mbo-instellingen hebben eind 2023 deelgenomen aan een landelijk onderzoek naar governance van informatiebeveiliging binnen het mbo. Een onderzoek met als doel vast te stellen hoe mbo-instellingen omgaan met het aansturen van informatiebeveiliging. Zowel een bestuurder als de IBP-functionaris van elk van de deelnemende instellingen heeft in het kader van het onderzoek enkele tientallen vragen beantwoord. Waarbij een deel van de vragen aan beide groepen is gesteld. Dit om te achterhalen of er ten aanzien van bepaalde onderwerpen een verschil in inzicht bestaat tussen bestuurder en IBP-functionaris. En hoewel er in grote lijnen overeenstemming bestaat tussen beide groepen, zijn er uit het onderzoek ook zeker verschillen naar voren gekomen.

Verschil van inzicht bijvoorbeeld als het gaat over de vraag wie er eindverantwoordelijk is voor het vaststellen van instellingsbrede trends, knelpunten en verbeterpunten op het vlak van informatiebeveiliging. De IBP-er legt opvallend vaker de verantwoordelijkheid hiervoor bij de IB&P-stuurgroep, terwijl de bestuurder deze verantwoordelijkheid eerder bij zichzelf of bij de manager ICT legt. Het informatiebeveiligingsbeleid is de aangewezen plek om verantwoordelijkheden te verankeren. Dit onder het kopje Taken, Bevoegdheden en Verantwoordelijkheden. Dit is daarom een van de urgente ‘bespreektips’ voor bestuurders en IBP-functionarissen die in deze rapportage is opgenomen.

Onderwerpen die in het onderzoek uitgebreid aan bod komen, zijn uiteraard de rol van de bestuurder ten aanzien van informatiebeveiliging en de positionering van de IBP-functionaris binnen de organisatie. Wat die laatste positie betreft zien we een trend van de IBP-functionaris die zich steeds meer beweegt richting de traditionele CISO-rol. Een rol van waaruit het gehele speelveld van informatiebeveiliging meer en meer met een tactisch/strategische blik wordt bekeken en minder vanuit tactisch/operationeel oogpunt, zoals voorheen. Een belangrijke aanbeveling uit het onderzoek is, gezien deze verschuiving, de positionering van de IBP-functionaris regelmatig te evalueren om zo te bekijken of deze nog aansluit bij de behoeften en de volwassenheid van de organisatie. Een goede positionering draagt immers bij aan een vergroting van de effectiviteit van informatiebeveiligingsmaatregelen.
Ten aanzien van de rol van de bestuurder blijkt uit het onderzoek duidelijk dat bestuurders zich in behoorlijke mate betrokken voelen bij het onderwerp informatieveiligheid. IBP-functionarissen zien deze betrokkenheid echter iets minder. Ook op dit vlak is het daarom raadzaam samen het gesprek aan te gaan en verwachtingen en behoeften naar elkaar uit te spreken. Denk hierbij ook aan de vragen als hoe en wanneer een bestuurder wordt geïnformeerd over de voortgang van informatiebeveiliging en maak hierover duidelijke afspraken. Belangrijk in het kader van de controlerende rol van de bestuurder.

Ten aanzien van de rol van de bestuurder lijkt een hoge betrokkenheid van de bestuurder te leiden tot een hogere score op volwassenheid van de informatiebeveiliging. Dit hadden de 3 succesvolle instellingen op het gebied van informatiebeveiliging in ieder geval gemeen.

Als rode draad door de rapportage loopt het belang van een risicogerichte aanpak van informatiebeveiliging of informatieveiligheid. Binnen de context van dit onderzoek behelst informatiebeveiliging namelijk het controleren van risico's ten aanzien van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen mbo-instellingen: hoe groter het risico, hoe groter de urgentie om te komen tot een oplossing. Een aanpak die helpt bij het stellen van prioriteiten. Wanneer je hierbij gebruikmaakt van risico-overzichten als basis voor risico-overleg met verschillende stakeholders, stel je deze prioriteiten binnen een organisatie gezamenlijk. Belangrijk voor het creëren van draagvlak voor beheersmaatregelen. Uit het onderzoek blijkt dat 30 van de 44 deelnemende instellingen in de ogen van de IBP-functionarissen enigszins of volledig risicogericht werken. Een bemoedigend signaal om op verder te bouwen.

mbo digitaal

INHOUD

1 INLEIDING

In het mbo is in 2023 landelijk onderzoek gedaan naar governance rond informatiebeveiliging binnen onderwijsinstellingen. Met als doel te achterhalen hoe mbo-instellingen omgaan met het aansturen van informatiebeveiliging. In totaal hebben 44 van de 55 aangeschreven mbo-instellingen deelgenomen aan het onderzoek.
Het is geweldig dat van zoveel instellingen zowel de bestuurder als de IBP-functionaris (functionaris informatiebeveiliging en privacy) de tijd heeft genomen om de enquête in te vullen. Een compliment daarvoor is op zijn plaats. Dankzij deze respons is een goed beeld verkregen van het onderwerp.
Belangrijk, want het ontbreken van een duidelijke governance met betrekking tot informatiebeveiliging kan leiden tot verkeerde keuzes ten aanzien van beveiligingsrisico's die optreden bij het verwerken van (geautomatiseerde) informatie. Risico's die de veiligheid en integriteit van vertrouwelijke gegevens binnen een instelling in gevaar kunnen brengen.

Betrokken onderzoekers gaan ervan uit dat een goede governance een belangrijke bijdrage levert aan de mate waarin de bestuurder en zijn organisatie in control zijn wat betreft het onderwerp informatieveiligheid. Zonder sturing immers geen controle. Daarbij kan een betrokken bestuurder sneller ingrijpen wanneer een organisatie de verkeerde koers vaart.
Deze rapportage begint met een verkenning van een aantal basisonderwerpen rond informatiebeveiliging. Wat is de essentie van informatiebeveiliging, wat zijn kenmerken van governance en hoe kun je risicomanagement goed organiseren? Deze basis wordt vooral gebruikt als gedeeld referentiekader. Wanneer een organisatie anders is ingericht, maar wel goed functioneert, is dit natuurlijk ook prima.
Bij de bestudering van de resultaten van het onderzoek is het interessant te zien welke rol de bestuurder zichzelf toekent op het gebied van informatieveiligheid. Deze vraag is met name relevant in het licht van de toegenomen aandacht voor de rol van de bestuurder als integraal risico-eigenaar. Je kunt ergens verantwoordelijk voor zijn, maar als bestuurder daadwerkelijk actief participeren op een lastig onderwerp als informatieveiligheid is daarmee nog niet vanzelfsprekend.
Voor deze rapportage is een analyse gemaakt van de onderzoeksresultaten. Waarbij vooral de opvallende resultaten zijn uitgelicht. Voor belangstellenden die geïnteresseerd zijn in de individuele vragen zijn de gemiddelde scores in de bijlage opgenomen.

1.1 GOVERNANCE VOLGENS HET NBA-VOLWASSENHEIDSMODEL

Vanuit het NBA-volwassenheidsmodel voor informatiebeveiliging zijn al de nodige best practices, in de vorm van statements, beschreven voor het inrichten van governance binnen een organisatie. Deze statements zijn binnen MBO Digitaal gegroepeerd naar centrale thema's om de veelheid aan eisen overzichtelijker te maken. Onder het onderwerp 'governance' zijn de volgende statements opgenomen.

Id	Statement	NBA-id	NBA-thema
G01	Strategie	GO.01	Strategie
G02	Beleid	GO.02	Beleid
G06	Planning/ Roadmap	GO.03	Roadmap
G03	Architectuur	GO.04	Architectuur
G07	Onafhankelijke toetsing	GO.05	Assurance
G04	Eigenaarschap, rollen, verantwoording en verantwoordelijkheid	OR.01	Eigenaarschap
G04	Functiescheiding	OR.02	Eigenaarschap
G05	Informatie risicomanagement framework	RM.01	Risk Management
G05	Risicobeoordeling	RM.02	Risk Management
G05	Plan voor behandeling en beperking van risico's	RM.03	Risk Management

Figuur 1 Governance gerelateerde statements uit het NBA-model

1.2 VAN HET WAT NAAR HET HOE

Aan ieder statement is een set van beheersmaatregelen gekoppeld om te kunnen groeien in volwassenheid waarmee de vraag is beantwoord **WAT** er moet worden ingericht. De vraag binnen dit onderzoek over governance is vervolgens: **HOE** hebben de instellingen dit ingericht? Waarbij het onderzoek zich concentreert op de volgende hoofdvragen.

1. Hoe groot is de zorg rond het thema informatieveiligheid en wordt de mate van bezorgdheid gedeeld door de bestuurder en de IBP-er?
2. Wat is de rol van de bestuurder binnen het onderwerp informatieveiligheid en in hoeverre komt dit onderwerp aan bod aan de bestuurstafel?
3. Hoe duidelijk zijn verantwoordelijkheid en eigenaarschap binnen de organisatie belegd en wie pakt welke taak op zich rond het onderwerp risicomanagement?
4. Wat is de rol en positie van de IBP-functionaris, welke takenpakket heeft hij en op welke besturingsniveaus (strategisch, tactisch, operationeel) wordt zijn bemoeienis gevraagd?
5. Hoe ziet het proces van kwaliteitsmanagement (Plan-Do-Check-Act) eruit binnen de organisatie en hoe is dit vastgelegd in een geformaliseerd Information Security Management Systeem (ISMS)?
6. Hoe komen budgetten voor informatiebeveiliging tot stand?
7. Hoe hebben succesvolle instellingen informatiebeveiliging georganiseerd?

1.3 PERSPECTIEF VAN HET ONDERZOEK

Om het onderwerp governance van informatiebeveiliging behapbaar te houden, is ervoor gekozen dit specifieke onderwerp in dit onderzoek geïsoleerd te behandelen. In de praktijk is het nuttig om informatiebeveiliging te integreren in het bredere domein van informatiemanagement binnen een organisatie. Met een heldere visie op informatiemanagement, kan een goed doordachte benadering van informatiebeveiliging worden uitgewerkt. De best practice voor risicomanagement die in dit document wordt beschreven, blijft een waardevol startpunt, ook wanneer we informatiebeveiliging in samenhang met informatiemanagement benaderen.

2 EEN GEMEENSCHAPPELIJKE BASIS

Een nulmeting met betrekking tot governance op het gebied van informatiebeveiliging vraagt om een gedeeld referentiekader met betrekking tot het onderwerp. Daarom volgt eerst een beschrijving van een aantal uitgangspunten die voor het opstellen van deze rapportage zijn gehanteerd. Te beginnen met de vraag wat binnen deze rapportage wordt verstaan onder informatiebeveiliging, gevolgd door een toelichting op het 3-lines model voor risicomanagement.

2.1 ESSENTIE VAN INFORMATIEBEVEILIGING

Wanneer we het onderwerp informatiebeveiliging bespreken, hebben we het binnen de context van deze rapportage over het controleren van risico's ten aanzien van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Binnen de mbo-sector is afgesproken dat hiervoor het NBA-volwassenheidsmodel voor informatiebeveiliging wordt gebruikt. Dit is feitelijk een best practice op het gebied van risicomanagement. Door risico's volgens het NBA-volwassenheidsmodel overzichtelijk in kaart te brengen ontstaat een beeld van de belangrijkste risico's en kan de aanpak hiervan eenvoudiger worden geprioriteerd. Uitganspunt binnen governance-onderzoek is daarmee altijd: *informatiebeveiliging = risicomanagement.* De hele sturing (=governance) draait om het inzicht krijgen in en het onder controle houden van de belangrijkste risico's rond informatieveiligheid, het garanderen van de bedrijfscontinuïteit en de garantie dat alle gegevens die vertrouwelijk blijven en de integriteit van de gegevens gewaarborgd is.
De meeste risico's die het NBA-model benoemt, worden beleidsmatig aangepakt. Voorbeelden zijn:

- Informatiebeveiligingsbeleid - voor de globale beschrijving van onder meer de inrichting van governance, risicomanagement, het managementsysteem (PDCA-cyclus) en de beschrijving van taken, bevoegdheden en verantwoordelijkheden.
- Encryptiebeleid met betrekking tot de manier waarop vertrouwelijke informatie wordt versleuteld, denk aan websites en mail.
- Autorisatiebeleid en de autorisatiematrix die bepalen wie welke toepassing mag gebruiken en welke rechten een bepaalde rol met zich meebrengt.
- Et cetera

2.2 OPERATIONEEL RISICOMANAGEMENT

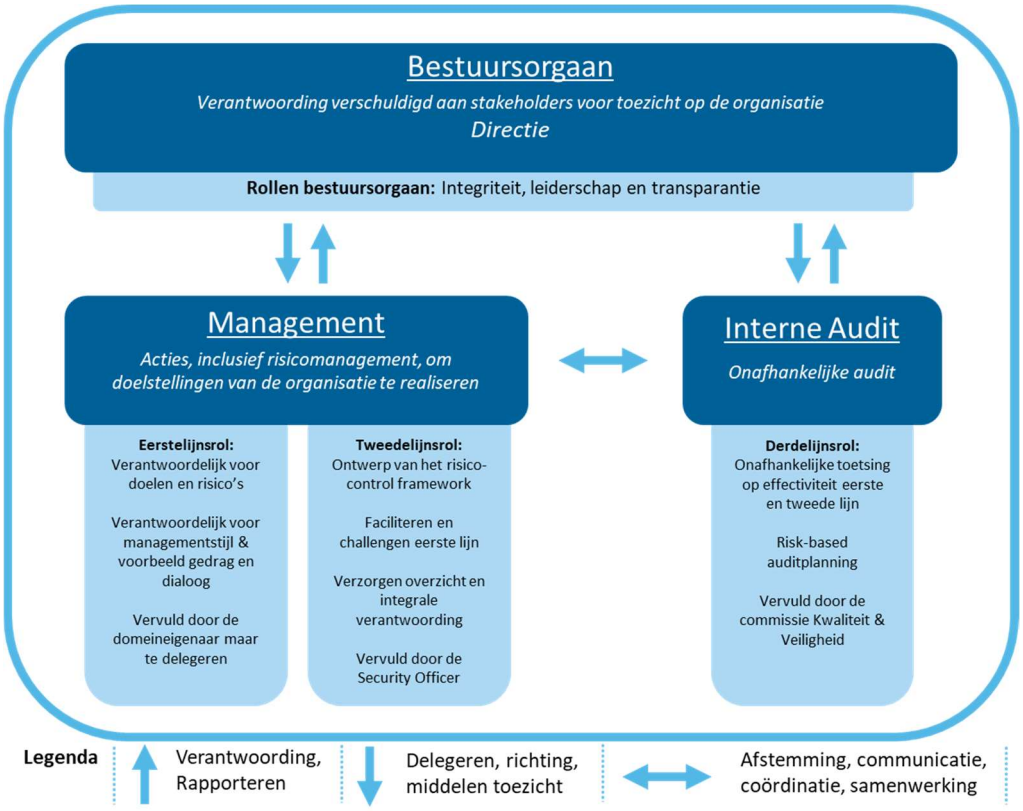
Meer ad hoc risico's kunnen ontstaan wanneer zich onverwachte incidenten voordoen. Deze risico's worden mogelijk niet gedekt door beleid, waardoor er operationeel moet worden ingegrepen om de kans op - of de effecten van - de dreiging afdoende te verminderen. Deze tak van risicomanagement noemen we *operationeel risicomanagement*[1]. Daar waar beleid dus is gericht op het uitbannen van te voorziene risico's houdt operationeel risicomanagement zich

[1] Operationeel risico betreft het risico dat ontstaat als gevolg van het falen of tekortschieten van interne processen, menselijke en technische tekortkomingen en onverwachte externe gebeurtenissen. Bron: dnb.nl

meer bezig met onvoorziene risico's. Deze vorm van risicomanagement blijft noodzakelijk om tijdelijke maatregelen voor nieuwe, niet voorziene risico's om te zetten naar meer structurele beheersmaatregelen.

2.3 HET 3-LINES MODEL VOOR RISICOMANAGEMENT

Er bestaat een algemeen geaccepteerd raamwerk om risicomanagement in te richten: het 3-lines model. In dit raamwerk is niet de IBP-functionaris de eigenaar van het risicomanagementproces, maar de bestuurder. De bestuurder wordt door de IBP-functionaris voorzien van het integrale risicobeeld van de organisatie op het gebied van informatieveiligheid.
In de eerste lijn, vertegenwoordigd door de domeineigenaar, identificeren medewerkers dagelijkse risico's en passen ze beheersmaatregelen toe om de risico's te verminderen[2]. De domeineigenaar draagt verantwoordelijkheid voor het beheer van risico's die uniek zijn voor zijn specifieke domein.



Figuur 2 Organisatie overzicht risicomanagement

De tweede lijn, vertegenwoordigd door de IBP-functionaris, ondersteunt en bewaakt de implementatie van beheersmaatregelen. De IBP-functionaris is verantwoordelijk voor het coördineren van de algehele informatiebeveiliging binnen de organisatie en zorgt ervoor dat de

[2] Risico = kans x impact. Een risico kan worden verkleind door de kans dat een ongewenste gebeurtenis zich voordoet te verkleinen of door de impact van de ongewenste gebeurtenis te verkleinen. Een valhelm verkleint de kans op hersenletsel. Een verzekering verkleint de (financiële) impact van een ongeval.

toegepaste maatregelen effectief zijn en voldoen aan normen zoals beschreven in het informatiebeveiligingsbeleid.
De derde lijn voert de interne audits uit en evalueert onafhankelijk of de eerste twee lijnen adequaat functioneren. De toevoeging van de derde lijn biedt een extra laag van controle en verificatie om ervoor te zorgen dat het risicomanagementproces effectief is en risico's op een acceptabel niveau worden gehouden.
In dit onderzoek is de organisatieaanpak gespiegeld aan de 3-lines aanpak en de standaard governance uitgangspunten zoals hierboven beschreven. Het kan zijn dat je als instelling governance anders hebt ingericht. Dat betekent niet dat die aanpak onjuist is. Mogelijk is een andere bestuursvisie gehanteerd. Zeker wanneer de volwassenheid van de risicomanagementorganisatie een goede ontwikkeling doormaakt, is er wellicht geen aanleiding om processen bij te stellen. Overwegen kan natuurlijk altijd.

2.4 RISICOGERICHTE AANPAK

Aan het begin van dit hoofdstuk is het uitgangspunt beschreven voor informatiebeveiliging: ***informatiebeveiliging = risicomanagement*.** In het verlengde hiervan is het logisch om het proces rond informatiebeveiliging risicogericht in de richten. Hoe groter het risico hoe groter de urgentie om te komen tot een oplossing. Een praktische aanpak omdat deze manier van organiseren helpt te prioriteren. Daarbij kunnen risico-overzichten in de praktijk als basis worden gebruikt voor een risico-overleg. Dit betekent dat risico's letterlijk in een risicoregister worden vastgelegd en hieruit risico-overzichten worden gegenereerd. Risico-overzichten dienen in dat geval als communicatiemiddel tussen verschillende stakeholders. Door het risico-overzicht te bespreken met verschillende stakeholders kan er een gedeeld beeld ontstaan over de inschatting van bepaalde risico's en kunnen maatregelen in gezamenlijkheid worden geprioriteerd. Een manier van werken die helpt het draagvlak voor beheersmaatregelen te vergroten.
Voor deze aanpak is het uiteraard nodig dat een instelling een risicogerichte aanpak hanteert. Uit de antwoorden van de IBP-functionarissen in het onderzoek blijkt dat in ieder geval 30 (21+9) instellingen enigszins of volledig risicogericht werken. Een bemoedigend signaal (F21).

Instelling hanteert risicogerichte aanpak	Aantal	Relatief
01 - volledig mee eens	9	20%
02 - enigszins mee eens	21	48%
03 - niet eens - niet mee oneens	7	16%
04 - grotendeels mee oneens	6	14%
05 - volledig mee oneens	1	2%
Totaal	**44**	**100%**

GRC-applicatie voor risicogericht werken

Begin dit jaar (2024) is de mbo-brede GRC-applicatie van Trustbound kosteloos vier jaar ter beschikking gesteld aan alle instellingen binnen het mbo in Nederland. GRC staat voor Governance, Risk Management en Compliance. De GRC-applicatie is een geavanceerde toepassing die helpt beveiligingsrisico's in kaart te brengen in een risico-register en passende maatregelen te beschrijven op het gebied van informatieveiligheid en privacy. De GRC-applicatie is ingericht volgens drie gebruiksscenario's: basis, uitgebreid en volledig risicogebaseerd. Daardoor is de

software geschikt voor zowel ervaren risk-managers als startende IBP-functionarissen én voor compliance-officers van grote instellingen, maar ook voor IBP-functionarissen van kleinere mbo-scholen.

De GRC-applicatie zorgt ervoor dat je grip krijgt op je volwassenheid, je risico's en je maatregelen. Ook helpt de applicatie je bij het bewaken van je prioriteiten en je planning. Als de GRC-applicatie op de juiste manier wordt bijgehouden, kan op elk gewenst moment de actuele stand van zaken rond risico's, beheersmaatregelen en openstaande taken worden weergegeven. Ideaal om ook de bestuurder op ieder gewenst moment inzicht te geven in de actuele stand van zaken.

Dankzij de GRC-applicatie zijn mbo-instellingen veel eenvoudiger in staat grip te krijgen op hun informatieveiligheid en privacy. Lees hierover meer op de site van MBO Digitaal.
https://mbodigitaal.nl/programmas/programma-cyberveiligheid-mbo/dreigingen-en-risicos-identificeren/grc-applicatie/

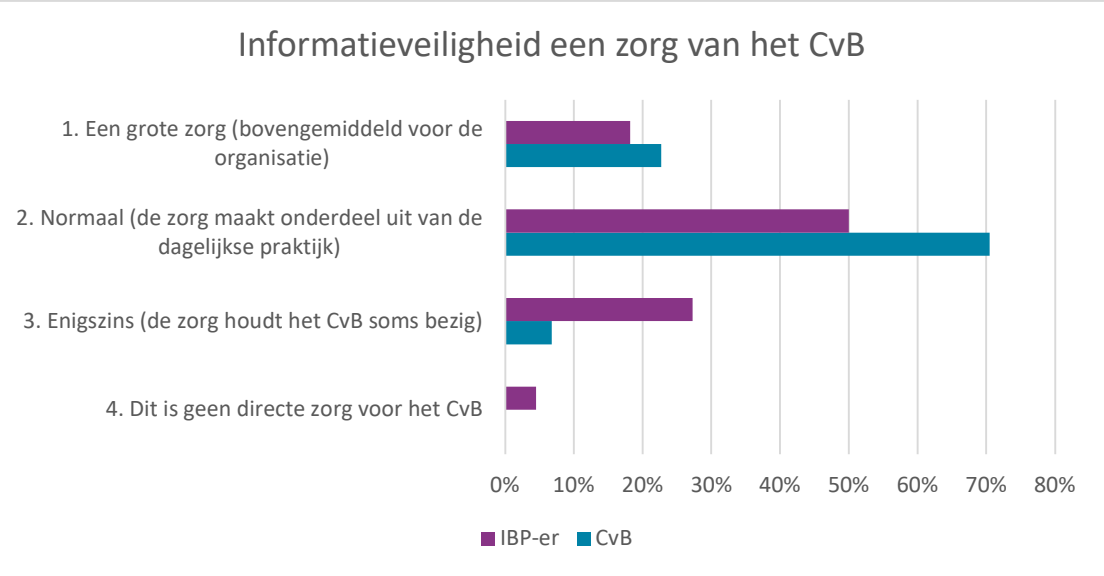
3 NULMETING GOVERNANCE

In dit hoofdstuk wordt de 0-meting met betrekking tot governance uitgewerkt. De uitwerking is gebaseerd op de ingevulde vragenlijsten door de bestuurders en IBP-functionarissen van de 44 deelnemende mbo-instellingen. Te beginnen met de vraag in hoeverre onderwerpen als cyberveiligheid, kwetsbaarheden en het verbeteren van awareness bij studenten en medewerkers een zorg zijn voor het CvB. Vervolgens worden vragen over de rol van de IBP-functionaris en zijn positie in de organisatie besproken en tot slot de manier waarop risico-eigenaarschap binnen de deelnemende instellingen is belegd.

3.1 DE ZORG ROND HET THEMA INFORMATIEVEILIGHEID

In de uitvraag zijn sommige vragen zowel aan de bestuurder als aan de IBP-functionaris gesteld. Met als doel te kijken of de bestuurder en de IBP-functionaris hetzelfde over een onderwerp denken. In grote lijnen is er best veel overeenstemming, maar er zijn ook enkele verschillen.

Een van de eerste vragen in het onderzoek was (B4F4): In hoeverre zijn onderwerpen als cyberveiligheid, kwetsbaarheden, verbeteren van awareness bij studenten en medewerkers een zorg voor het CvB? De vraag is zowel gesteld aan de bestuurder zelf als aan de IBP-functionaris.



Figuur 3 *Informatieveiligheid een zorg*

Informatieveiligheid een zorg	CvB	IBP-functionaris
Een grote zorg (bovengemiddeld voor de organisatie)	23%	18%
Normaal (de zorg maakt onderdeel uit van de dagelijkse praktijk)	71%	50%
Enigszins (de zorg houdt het CvB soms bezig)	7%	27%
Dit is geen directe zorg voor het CvB	0%	5%
Totaal	100%	100%

Het beeld dat de IBP-functionaris heeft over de mate van zorg bij het CvB is duidelijk lager dan hetgeen de bestuurders zelf aangeven. In de meeste gevallen vindt de bestuurder het een normale zorg die onderdeel uitmaakt van de dagelijkse praktijk. Opvallend is dat 32 procent (27 +5 procent) van de IBP-functionarissen denkt dat het onderwerp nauwelijks tot geen zorg is voor het CvB. Dat is vanuit governance perspectief opvallend. Zeker gelet op de verantwoordelijkheid van de bestuurder met betrekking tot het onderwerp risicomanagement. Slechts 6,8 procent van de bestuurders geeft aan dat het voor het CvB enigszins een zorg is, terwijl geen enkele bestuurder fluitend door het leven gaat zonder zich over dit thema zorgen te maken.

Ga als IBP-functionaris het gesprek aan met de bestuurder om de zorg over en het belang van het onderwerp informatieveiligheid met elkaar te bespreken.

3.2 DE ROL VAN DE BESTUURDER

3.2.1 Formele rol van de bestuurder

In het eerste hoofdstuk van deze rapportage is vastgesteld dat informatieveiligheid volledig gaat over het beheersen van risico's. Risico's die de strategische doelstellingen van de organisatie rechtstreeks en ernstig kunnen schaden. In de CODE GOED BESTUUR MBO 2020 wordt beschreven dat het college van bestuur verantwoordelijk is voor het bereiken van de strategische doelstellingen. Ontwikkelingen (risico's) die het behalen van de strategische doelstellingen direct of indirect bedreigen, vallen daarmee automatisch onder de verantwoordelijkheid van de bestuurder. Dit uitgangspunt wordt gehanteerd in deze rapportage: de bestuurder is eindverantwoordelijk voor risicomanagement binnen de organisatie.

3.2.2 De visie op zijn eigen rol

Governance betekent letterlijk sturing. Het is interessant om te zien hoe de bestuurder zélf tegen zijn rol in deze met betrekking tot informatieveiligheid aankijkt en hoe de IBP-functionaris de rol van de bestuurder ten aanzien van informatieveiligheid ziet (B5F5). Dit vooral in het licht van het eerdergenoemde uitgangspunt dat informatiebeveiliging gaat over risicomanagement. Wil de bestuurder hierin een toeschouwende rol vervullen of wil hij actief ingrijpen? De uitvraag over dit onderwerp is gedaan in stellingen waarbij de bestuurder en de IBP-functionaris moesten aangeven in welke mate ze het eens zijn met de stelling. De keuze liep van 'volledig oneens' (1) naar 'volledig eens' (5).

1	Volledig mee oneens
2	Grotendeels mee oneens
3	Niet eens - niet mee oneens
4	Enigszins mee eens
5	Volledig mee eens

De resultaten geven het volgende beeld:

Rol van de bestuurder	Bestuurder	IBP-er	verschil
a) Zich informeren	5,00	4,56	0,44
b) Richtinggevend (strategisch)	4,80	4,19	0,61
c) Kaderstellend (beleid en bevoegdheden)	4,86	4,37	0,49
d) Sturend / bijsturend (tactisch)	3,89	3,30	0,59
e) Evaluerend / kritische reflectie	4,45	4,12	0,33
f) Controlerend	3,68	3,44	0,24
g) Stimulerend	4,45	3,91	0,54
h) Voorbeeld functie	4,86	4,35	0,51
i) Vertegenwoordigende functie (stakeholders	4,09	3,77	0,32

Figuur 4 *Rol van de bestuurder*

In 7 van de 9 gevallen (a tot en met i) zien we bij de bestuurder een gemiddelde score van 4 of hoger. Dat betekent dat de bestuurder zich enigszins tot volledig kan vinden in de beschreven rol. We zien dus dat bestuurders zelf hun rol ten aanzien van het onderwerp informatieveiligheid als behoorlijk betrokken beschouwen. De IBP-functionaris ziet deze betrokken rol van bestuurders iets minder, maar ook hier zien we in 5 van de 9 gevallen nog een gemiddelde score van betrokkenheid die boven de 4 ligt. Op een aantal onderwerpen vallen de verschillen (in geel gearceerd) op, waarbij gelijk de vraag kan worden gesteld wat een goede inzet zou zijn van de bestuurder op deze onderwerpen.

Een gesprek tussen de bestuurder en de IBP-functionaris zou het beeld over de betrokkenheid van de bestuurder meer in balans kunnen brengen. Vooral op een onderwerp als de kaderstellende taak waarbij wordt bepaald welke taken, bevoegdheden en verantwoordelijkheden gelden ten aanzien van informatieveiligheid is dit essentieel.

Op het vlak van informatiebeveiliging is het belangrijk goed te beschrijven wie welke taak uitvoert en wie verantwoordelijk is voor risicomanagement en het nemen van beheersmaatregelen (eigenaarschap). Taken, bevoegdheden en verantwoordelijkheden ten aanzien van informatiebeveiliging worden meestal beschreven in het informatiebeveiligingsbeleid van een instelling. Dat de bestuurder dit beleid bekrachtigt, kan de legitimiteit van de toegewezen taken, bevoegdheden en verantwoordelijkheden alleen maar versterken. Een onderdeel van de controlerende functie van de bestuurder.
Uit het onderzoek (F20) blijkt dat volgens de IBP-functionaris in 52 procent van de instellingen de bestuurder meerdere keren per jaar informeert naar de voortgang van informatiebeveiliging. Dit geeft aan dat bestuurders betrokkenheid tonen vanuit een controlerende rol. De bestuurders zelf zijn hierover nog positiever. Ze geven in 96 procent van de gevallen aan dat ze een of meerdere keren per jaar naar de voortgang op het vlak van informatiebeveiliging informeren.

Spreek met elkaar af hoe en wanneer of in welke gevallen de bestuurder wordt geïnformeerd. Kijk hierbij ook duidelijk naar wat de behoefte is van de bestuurder en waarover de bestuurder geïnformeerd wenst te worden.

Belangen rond informatiebeveiliging kunnen verschillen (B21F34). Denk aan een medewerker die een apparaat wil aanschaffen dat wordt gekoppeld aan het internet en de IBP-functionaris die dit een risico vindt voor de informatieveiligheid en privacy. Hier treedt een belangenconflict op. Uit de enquête blijkt dat, volgens de IBP-functionaris, in het overgrote deel van de instellingen de bestuurder (39 procent) of de manager ICT (23 procent) een beslissing neemt in deze belangenweging[3]. De bestuurder heeft hierover een ander beeld. Hij denkt dat hij vaker de knoop doorhakt, in 57 procent van de gevallen, zo blijkt uit het onderzoek. Dat de bestuurder niet altijd wordt betrokken en dat geschillen buiten zijn beeld blijven, zou een logische verklaring kunnen zijn voor dit verschil. Het is in dit soort gevallen hoe dan ook belangrijk dat de IBP-functionaris de besluitvormers goed informeert over de risico's zodat in een conflict een weloverwogen besluit kan worden genomen.

3.3 RISICO-EIGENAARSCHAP

Zoals uitgelegd onder het kopje 3-lines model wordt de verantwoordelijkheid voor risicomanagement belegd bij de domein- of proceseigenaar. De IBP-functionaris kan nooit eigenaar zijn van een risico omdat hij normaal gesproken niet is gerechtigd in te grijpen in bedrijfsprocessen. Dat recht is voorbehouden aan de domein- of proceseigenaar.
Voorbeelden van proceseigenaren zijn:

- Human Resources — in- door- en uitstroom van personeel, aanstellingsbeleid
- ICT-afdeling — beheer van IT-middelen zoals laptops, netwerk(beveiliging) en kantoorapplicaties
- Opleidingsmanager — opleidingen
- Examencommissie — examineringsproces

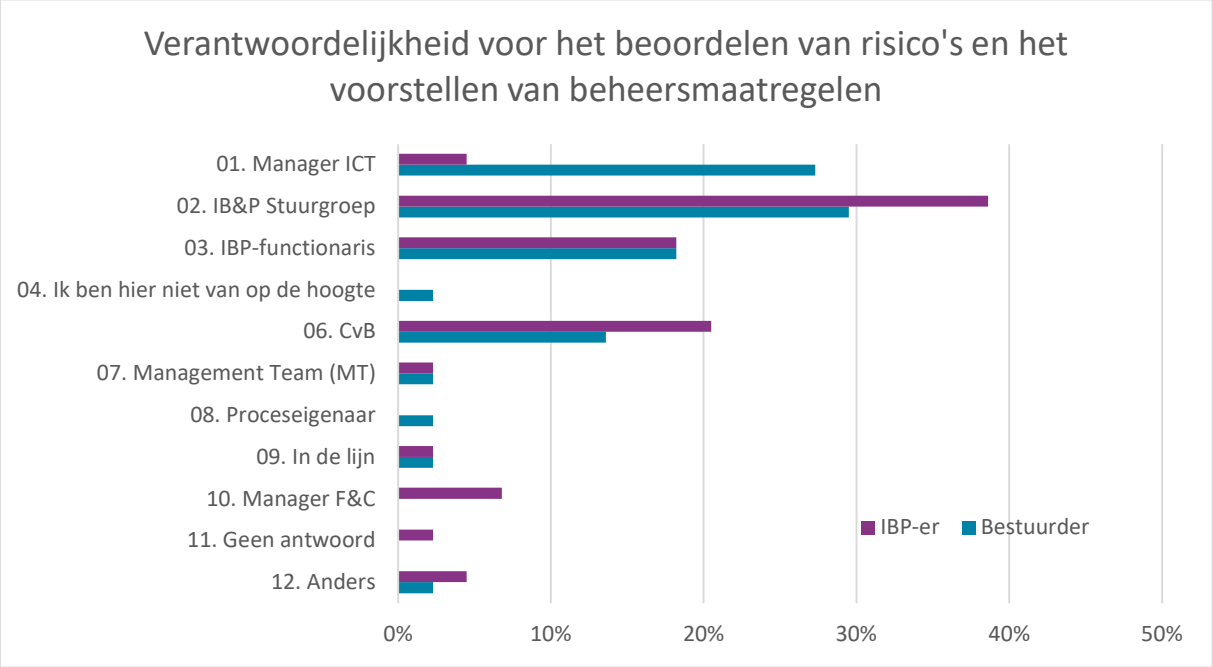
Wanneer zich in een van de domeinen een (operationeel) risico voordoet, kan dat risico via een taak worden toegekend aan de proceseigenaar. De proceseigenaar is er vervolgens voor verantwoordelijk dat het risico verder wordt geanalyseerd en opgelost.
De nieuwe GRC-applicatie, die eerder in de rapportage al werd belicht, biedt de mogelijkheden om taken uit te zetten en de voortgang te rapporteren.

3.3.1 Eindverantwoordelijk voor beoordeling van risico's en adviseren

In het 3-lines model wordt, zoals eerder toegelicht, beschreven hoe eigenaarschap rond risicomanagement kan worden belegd. Voor de invulling hiervan binnen mbo-instellingen werd in het onderzoek de vraag gesteld (B23F38): Welk(e) orgaan/functionaris is eindverantwoordelijk voor het beoordelen van informatiebeveiligingsrisico's en het voorstellen van beheersmaatregelen om risico's te mitigeren?
Toelichting: van alle risico's die bekend worden, moet worden vastgesteld wat de kans is dat het risico zich openbaart en wat vervolgens de impact is voor de organisatie wanneer het risico zich

[3] Hier kan goed beargumenteerd worden dat met een goed ingericht wijzigingsproces deze discussie niet gevoerd hoeft te worden. In de praktijk komt het voor dat aanpassingen niet via een wijzigingsproces lopen en discussies ontstaan en geëscaleerd worden. Dat is dan ook de reden dat de vraag wordt gesteld.

openbaart. De vraag is wie of welk orgaan verantwoordelijk is voor het vaststellen van deze beoordeling?
Uit het onderzoek blijkt dat ook hier bestuurder en IBP-functionaris het niet altijd eens zijn. Volgens de bestuurder ligt deze verantwoordelijkheid opvallend vaak bij ICT (27 procent) terwijl volgens de IBP-functionaris deze slechts in 5 procent van de gevallen bij ICT ligt. De IBP-functionaris denkt daarentegen dat de verantwoordelijk veel vaker bij de IBP-stuurgroep (39 procent) ligt of bij het CvB (30 procent).

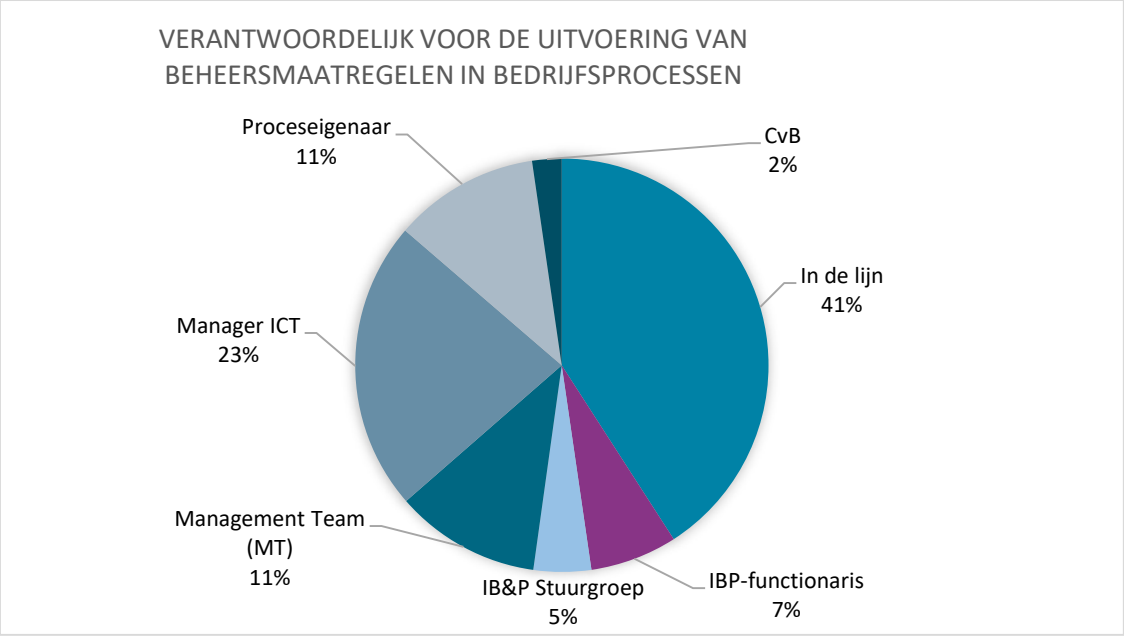


Figuur 5 *Verantwoordelijkheid voor risicobeoordeling*

Deelnemende instellingen aan het onderzoek kunnen vergelijken wat de verschillen zijn in inzicht tussen de bestuurder en de IBP-functionaris. De vergelijking biedt een goede kans om de verschillende inzichten met elkaar te bespreken en te toetsen hoe verantwoordelijkheden zijn beschreven in het informatiebeveiligingsbeleid.

3.4 BEHEERSMAATREGELEN

Als risico's zijn vastgesteld en tegenmaatregelen zijn benoemd, worden beheersmaatregelen gepland en uitgevoerd. De vraag is hoe dit is geregeld met betrekking tot maatregelen in operationele processen. In het onderzoek werd daarom aan de IBP-functionaris de volgende vraag gesteld (F24): Waar is de verantwoordelijkheid belegd voor de uitvoering van beheersmaatregelen in de operationele bedrijfsprocessen?

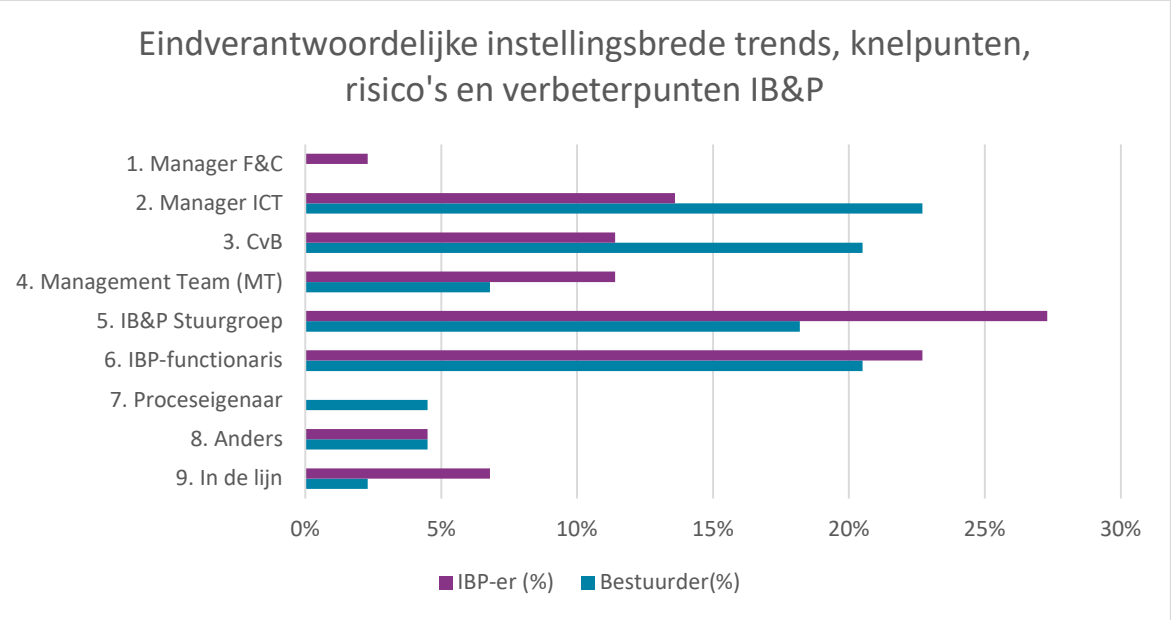


Figuur 6 *Verantwoordelijkheid voor beheersmaatregelen*

Vanuit het 3-lines model is de domeineigenaar verantwoordelijk voor het uitvoeren van beheersmaatregelen. Hij wordt daarbij met adviezen ondersteund door de IBP-functionaris. Wanneer de IBP-functionaris of de IBP-stuurgroep zelf de maatregelen moeten uitvoeren (in respectievelijk 7 en 5 procent van de instellingen) komt de IBP-functie in de eerste lijn terecht in plaats van in de tweede lijn van het 3-lines model. Daarbij is het de vraag hoe de IBP-functionaris eigenaarschap kan pakken als het gaat om onderwerpen die onderdeel zijn van organisatieprocessen waarvan de IBP-functionaris niet de eigenaar is?

3.5 INSTELLINGSBREDE TRENDS VASTSTELLEN

Om IBP-beleidsplannen te formuleren is het nodig om instellingsbrede trends, knelpunten en verbeterpunten met betrekking tot informatiebeveiliging vast te stellen. Ook hierbij is het belangrijk te bepalen wie uiteindelijk de eindverantwoordelijkheid heeft om hieruit voortvloeiende organisatierisico's te analyseren en te prioriteren. Hier gaat het dus meer om de globale ontwikkeling van risico's, ook gelet op het landelijke cyberdreigingsbeeld, en risico's binnen de organisatie. Bij een complex onderwerp als informatiebeveiliging is het waarschijnlijk dat de IBP-functionaris wat dit betreft beschikt over de meeste kennis en het beste inzicht, maar dat de bestuurder hierin wordt meegenomen. Op die manier kan de bestuurder vanuit het oogpunt van integraal risicomanagement eigenaarschap pakken op het onderwerp. Domeineigenaren kunnen op hun beurt risico's voor hun eigen domein bepalen en beheersmaatregelen nemen, maar het overall overzicht ligt bij de bestuurder.
Vraag (B12F17): Welk(e) orgaan/functionaris is eindverantwoordelijke voor het vaststellen van instellingsbrede trends, knelpunten en verbeterpunten m.b.t. informatiebeveiliging inbrengen, analyseren op risico's en prioriteren?



Figuur 7: *Eindverantwoordelijkheid voor vaststellen trend en ontwikkelingen*

Uit de onderzoeksresultaten, weergegeven in de grafiek, blijkt dat het inzicht van de bestuurder en de IBP-functionaris over wie er eindverantwoordelijk is opvallend uiteenloopt.

Eindverantwoordelijk	Bestuurder (%)	IBP-er (%)	Verschil
1. Manager F&C	0%	2%	2%
2. Manager ICT	23%	14%	-9%
3. CvB	21%	11%	-9%
4. Management Team (MT)	7%	11%	5%
5. IB&P Stuurgroep	18%	27%	9%
6. IBP-functionaris	21%	23%	2%
7. Proceseigenaar	5%	0%	-5%
8. Anders	5%	5%	0%
9. In de lijn	2%	7%	5%
Totaal	**100%**	**100%**	**0%**

De verwachting zou kunnen zijn dat de eindverantwoordelijkheid ligt bij degene die verantwoordelijk is op het gebied van informatiebeveiliging. Hier denk je in de lijn van de Proceseigenaar, IBP-functionaris, ICT-manager (afhankelijk van zijn takenpakket) of MT (ook weer afhankelijk van het takenpakket). Opvallend is dat de bestuurders en de IBP-functionaris wat dit betreft in ieder geval niet altijd op een lijn zitten.
In 21 procent van de gevallen trekt de bestuurder deze verantwoordelijkheid naar zich toe. Of hij dan ook de bron van de informatie is waarop hij conclusies in deze baseert, is in het onderzoek niet helder geworden. Het kan zijn dat hij zich hiervoor gewoonweg eindverantwoordelijk voelt.

Maak helder wie verantwoordelijk is voor welke taken binnen het werkgebied van informatiebeveiliging. Leg dit helder vast in het informatiebeveiligingsbeleid onder het kopje Taken, Bevoegdheden en Verantwoordelijkheden.

3.5.1 Mogelijke positionering van de IBP-functionaris

Basis voor de inrichting van de organisatie rond informatiebeveiliging is de vraag hoe de IBP-functionaris door de bestuurder wordt gepositioneerd. Dit werd toegelicht in de enquête aan de hand van de volgende figuur:

Positionerig IBP-Functionaris	kolom 1: Veiligheid van de IB-functie (Information risk management)	kolom 2: Veiligheid van de ICT-functie (ICT beveiliging / cyber security)
rij 1: Strategisch en/of tactisch	traditionele CISO-rol	ICT-beveiligingsmanager
rij 2: Tactische en/of operationeel	traditionele ISO-rol + optioneel Privacy Officer Rol.	ICT-beveiligingsspecialist/beheerder

Figuur 8: *Positie van de IBP-functionaris in de organisatie*

Bij de positionering van deze functionaris in de organisatie speelt enerzijds de vraag of de IBP-functionaris een procesmatige risicomanagement insteek heeft (kolom 1) of een meer technische insteek (kolom 2). Anderzijds speelt de vraag of de IBP-functionaris actief is op strategisch/tactisch niveau (rij 1) of op tactisch/operationeel niveau (rij 2).
De IBP-functionaris kan verschillende rollen hebben die binnen het werkveld van de informatiebeveiliging namen hebben gekregen als:

CISO: (Concern Information Security Officer) traditioneel controlerende en adviserende rol met betrekking tot informatiebeveiligingsmaatregelen op strategisch en tactisch niveau (directieniveau).
ISO/SO: (Information Security Officer/Security Officer) werkzaam op tactisch/ operationeel niveau met als taak de organisatorische implementatie van informatiebeveiliging. Bijvoorbeeld het ontwikkelen van een informatiebeveiligingsbeleid, het uitvoeren van risicoanalyses en het verzorgen van trainingen.
ICT-Beveiligingsmanager: Vanuit de ICT-operatie verantwoordelijk voor het onderwerp informatiebeveiliging. Zal deze taak veelal vanuit een meer technisch perspectief invullen.
ICT-beveiligingsspecialist: Is zelf verantwoordelijk voor de uitvoering van ICT-gedreven beveiligingsmaatregelen.

3.5.2 Positionering van de IBP-functionaris binnen het mbo

Bij de positionering van de IBP-functionaris in de organisatie speelt enerzijds dus de vraag of de IBP-functionaris een procesmatige insteek (kolom 1) of een meer technische, ICT-gerichte insteek (kolom 2) heeft. Anderzijds speelt de vraag of de IBP-functionaris actief is op strategisch/tactisch niveau (rij 1) of op tactisch/operationeel niveau (rij 2).

In het onderzoek is zowel aan de bestuurder als aan de IBP-functionaris de vraag gesteld hoe de IBP-rol binnen de organisatie wordt gepositioneerd. In 5 procent van de gevallen had de bestuurder geen goed beeld van waar de IBP-functionaris geplaatst moet worden. De resultaten zijn vertaald in een tabel die in eerste instantie best ingewikkeld lijkt (B24F39)[4].

Postionering IBP-functionaris (B24F39)		Kolom 1: Veiligheid van de IBP-functie		Kolom 2: Veiligheid van de ICT-functie		Totalen rijen	
positie		bestuurder	IBP-functionaris	bestuurder	IBP-functionaris	bestuurder	IBP-functionaris
Rij 1: Strategisch en/of tactisch	bestuurder	30%		16%		**46%**	
	IBP-functionaris		31%		13%		**44%**
Rij 2: Tactisch en/of operationeel	bestuurder	36%		13%		**49%**	
	IBP-functionaris		40%		16%		**56%**
Totalen kolommen	bestuurder	**66%**		**29%**		**95%**	
	IBP-functionaris		**71%**		**29%**		**100%**

Allereerst is de conclusie te trekken dat '*Kolom 1*' zwaarder is vertegenwoordigd dan '*Kolom 2*'. Dit geldt zowel voor de bestuurder (66 procent) als voor de IBP-functionaris (71 procent). Het overgrote deel van de deelnemers beziet de rol van de IBP-functionaris dus vanuit een integrale organisatie-aanpak (kolom 1).
De verdeling over de 'strategisch/tactische laag' of de 'tactisch/operationele laag' loopt niet ver uiteen. In zijn algemeenheid zien we binnen het werkveld van informatiebeveiliging een beweging van informatiebeveiliging naar de meer 'strategische laag' (rij 1) in de 'veiligheid van de IBP-functie' (kolom 1). Dit komt doordat het onderwerp risicomanagement rond informatieveiligheid een steeds strategischer karakter krijgt[5].

Wat opvalt is dat op dit moment in 13 procent van de gevallen de bestuurder de positie van de IBP-functionaris beoordeelt als meer technisch en operationeel/tactisch. Voor de IBP-functionaris zelf geldt dit in 16 procent van de gevallen. In die gevallen wordt de IBP-functionaris dus minder gezien als strategisch/tactisch gesprekspartner met een organisatiebrede informatiebeveiligingsvisie.
Oorzaak hiervoor zou kunnen zijn dat het gesprek/de informatie-uitwisseling tussen de IBP-functionaris en de bestuurder vaak gaat over technisch operationele/tactische zaken. Dit is voorstelbaar wanneer een IBP-functionaris is doorgegroeid vanuit een netwerkbeheerfunctie. Een situatie die binnen het mbo geregeld voorkomt. Uit de resultaten van het onderzoek is dit echter niet vast te stellen.
Wanneer een technisch beheerder doorgroeit naar een IBP-functie kan de barrière om de bestuurder aan te spreken wellicht hoger zijn. Een minder ontwikkelde routine in het organisatiedenken zou de IBP-functionaris kunnen belemmeren om meer brede, organisatiegerelateerde onderwerpen te bespreken met de bestuurder voor wie dit dagelijkse kost is. Het kost tijd om deze vaardigheid te ontwikkelen.

[4] In de kolom 'totalen rijen' van de tabel telt de kolom van de bestuurder op tot 95%. Dit omdat 5 procent van de bestuurders geen goed beeld heeft van waar de IBP-functionaris gepositioneerd moet worden.

[5] Voorbeeld I-strategie Rijk 2021 – 2025, Doorpakken op digitale transformatie

Ga eens het gesprek aan over de positie van de IBP-functionaris binnen jullie instelling. Welke positie wordt gekozen en hoe wordt deze onderbouwd. Als een meer tactisch/operationele insteek wordt gekozen, kijk dan hoe de strategisch/tactische positie wordt ingevuld.

3.6 IBP-FUNCTIONARIS OP DRIE STURINGSNIVEAUS

Een vraag die bij de positionering van de IBP-functionaris gesteld moet worden, is in hoeverre hij een rol heeft in het behalen van strategische doelen. Bij een grootschalige verstoring van de informatievoorzieningen is het zeker dat primaire bedrijfsfuncties gaan uitvallen. Hierdoor komt het bieden van onderwijs rechtstreeks in gevaar. Daarmee kun je concluderen dat de uitgangspunten met betrekking tot informatiebeveiligingsbeleid op strategisch niveau gedefinieerd moeten worden. Maar ook op tactisch en operationeel niveau heeft de IBP-functionaris taken.

1. Strategisch niveau:

- *Beleidsontwikkeling*

  Op strategisch niveau is de IBP-functionaris betrokken bij het ontwikkelen en implementeren van beleid met betrekking tot informatieveiligheid. Dit omvat het formuleren van algemene doelstellingen, normen en richtlijnen om de informatiebeveiliging op lange termijn te waarborgen.
- *Risicobeheer*

  Het identificeren en evalueren van risico's met betrekking tot informatieveiligheid op strategisch niveau is van essentieel belang. Op dit niveau helpt de IBP-functionaris bij het vaststellen van prioriteiten en het bepalen van de juiste strategieën om deze risico's te minimaliseren.

2. Tactisch niveau:

- *Samenwerking met belanghebbenden*

  Op tactisch niveau werkt de IBP-functionaris samen met verschillende belanghebbenden, zoals onderwijsmanagers, lijnmanagers, IT-personeel en schoolbestuurders. Door deze samenwerking kan hij ervoor zorgen dat informatiebeveiliging geïntegreerd wordt in de dagelijkse activiteiten en besluitvorming.
- *Training en bewustwording*

  Het organiseren van trainingen en het bevorderen van bewustwording over informatieveiligheid behoren tot de tactische verantwoordelijkheden. Dit helpt medewerkers en studenten om op een veilige manier met informatie en technologie om te gaan.

3. Operationeel niveau:

- *Implementatie van beveiligingsmaatregelen*

  De rol van IBP-functionaris kan bestaan uit het coördineren van de implementatie en handhaving van beveiligingsmaatregelen, het monitoren van systemen en het reageren op beveiligingsincidenten binnen een organisatie.
- *Incidentrespons*

In geval van beveiligingsincidenten speelt de IBP-functionaris mogelijk een belangrijke rol bij het coördineren van de respons. Dit omvat het onderzoeken van incidenten, het nemen van corrigerende maatregelen en het documenteren van lessen die kunnen worden toegepast voor toekomstige verbeteringen.

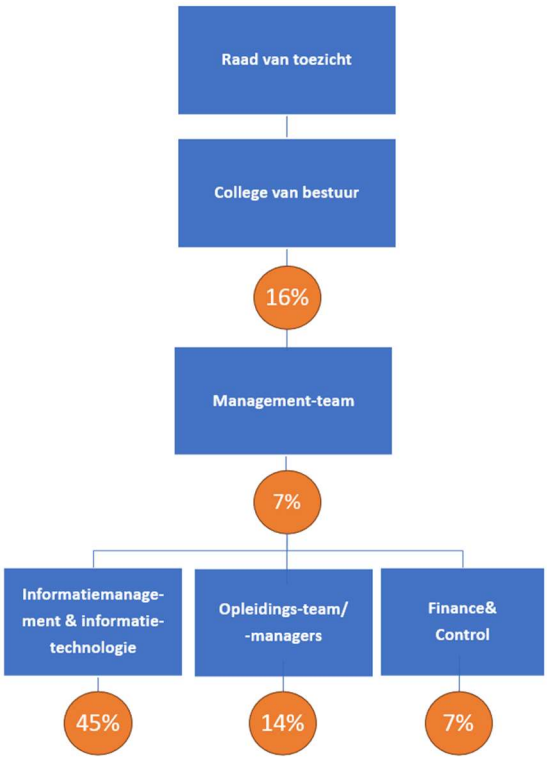
Door zowel op strategisch, tactisch als operationeel niveau actief te zijn, kan de IBP-functionaris een meer allesomvattende benadering hanteren om de informatieveiligheid van het middelbaar onderwijs te waarborgen. Deze aanpak maakt informatiebeveiliging niet alleen een technische kwestie, maar een integraal onderdeel van de algehele strategie en werking van de onderwijsinstelling.
Hoe ieder van de kwadranten in bovenstaande figuur over de mogelijke positionering van de IBP-functionaris wordt ingevuld, is natuurlijk aan de instelling zelf. Dat hierin een afweging wordt gemaakt naar de aard van de werkzaamheden en de kwaliteiten van een medewerker spreekt voor zich. Het lijkt wel belangrijk om oog te hebben voor het onderwerp informatiebeveiliging op alle drie de organisatieniveaus (strategisch, tactisch en operationeel).

3.6.1 De IBP-functionaris in de organisatiestructuur

De vraag waar volgens de bestuurder de IBP-functionaris in de hiërarchie van de organisatie is geplaatst (B25F41), levert een wisselend beeld op. In 45 procent van de gevallen valt deze onder de ICT-manager. Terwijl 34 procent van de bestuurders aangeeft dat de IBP-functionaris onder een bestuurlijke laag valt, te weten het MT (9,1 procent) of het CvB (25 procent).
Het meest opvallende verschil tussen de bestuurder en de IBP-functionaris in deze is dat de IBP-functionaris vaker denkt dat hij in de lijn valt. Terwijl de bestuurder aangeeft dat de IBP-functionaris vaker direct onder het CvB valt.

72 procent van de bestuurders geeft aan dat er binnen de organisatie een IB&P Stuurgroep (informatiebeveiliging & privacy) is (B19). Deze stuurgroep kan helpen bij het beoordelen van risico's en beleidsnotities. Als de stuurgroep is samengesteld uit verschillende geledingen binnen de organisatie helpt dit draagvlak te creëren en nieuw beleid breder uit te dragen.
In het hieronder weergegeven organogram is de positie van de IBP-functionaris in een gemiddelde mbo-instelling weergegeven. Dit op basis van de antwoorden van de IBP-functionarissen die deelnamen aan het onderzoek. Overige bedrijfsfuncties zijn buiten beschouwing gelaten in het model. De rode bollen geven de positie aan van de IBP-functionaris *(inclusief eventuele stuurgroep)* met daarin het percentage van de gevallen dat de IBP-functionaris zich op deze positie bevindt.

In de meeste gevallen (45 procent) valt de IBP-functionaris onder de afdelingsmanager ICT, zo blijkt uit het onderzoek. Dit heeft voor de bestuurlijke functie mogelijk het voordeel dat hij één loket heeft waarmee hij complexe zaken met een ICT-aspect kan opnemen. Zeker als informatieveiligheid ook onder het budget van ICT valt, is dit wel zo handig voor de bestuurder. Ook is de afstemming met de ICT-functie directer. Deze aanpak kan werken als de ICT-manager een organisatiebrede blik heeft op het onderwerp informatiebeveiliging.
Dat de eerste zorg van de organisatie rond informatiebeveiliging van technische aard is, is begrijpelijk. Voor open organisaties als scholen is het niet wenselijk dat de digitale deur naar buiten wagenwijd open staat voor hackers of andere ongewenste geïnteresseerden.
ICT kan met technische maatregelen sowieso een stevig, zij het rudimentair, slot leveren voor ICT-voorzieningen. Zonder verdere inrichting van de informatiebeveiligingsorganisatie loopt een organisatie wel in toenemende mate risico's op beveiligingslekken rond vertrouwelijke informatie.



Figuur 9: Meest voorkomende posities IBP-functionaris. (Overige ongedefinieerd = 11%).

Een puur technische insteek is doorgaans meer gericht op specifieke bedreigingen en kwetsbaarheden. Wanneer de technologische omgeving verandert, kunnen deze maatregelen minder effectief worden. Een meer holistische benadering, inclusief beleid en procedures, kan helpen om een flexibeler beveiligingsraamwerk te creëren.

Het plaatsen van de IBP-functionaris onder de ICT-manager wijst mogelijk op een meer traditionele benadering van informatiebeveiliging als een technisch probleem. In de praktijk zien we, zoals eerder gezegd, steeds meer een verschuiving van de IBP-functie naar een meer tactisch/strategische laag over de organisatie-as. Wanneer de IBP-functie onder ICT valt, heeft dat namelijk een aantal nadelen voor de organisatie waarmee rekening gehouden moet worden:

- Er kan een conflict of interest ontstaan, omdat de ICT-afdeling vaak gericht is op het optimaliseren van technologische processen en prestaties. Een IBP-functionaris moet echter ook kunnen ingrijpen en beperkingen kunnen opleggen in gevallen waarin veiligheidsmaatregelen conflicteren met de optimale prestaties van systemen.
- Er kunnen communicatieproblemen ontstaan tussen de IBP-functionaris en andere afdelingen. Informatiebeveiliging vereist samenwerking met diverse belanghebbenden, zoals HR, juridische zaken en het hoger management. Wanneer de IBP-functionaris te sterk is geïntegreerd in de ICT-afdeling, kan dit de communicatie met andere afdelingen bemoeilijken.

- Informatiebeveiliging omvat niet alleen technische maatregelen, maar ook aandacht voor menselijke factoren, zoals bewustwording, gedrag en training. Als de IBP-functionaris alleen onder de ICT-afdeling valt, kan de aandacht voor deze menselijke aspecten mogelijk worden verwaarloosd.

3.7 RECHTSTREEKSE RAPPORTAGELIJN NAAR RVB

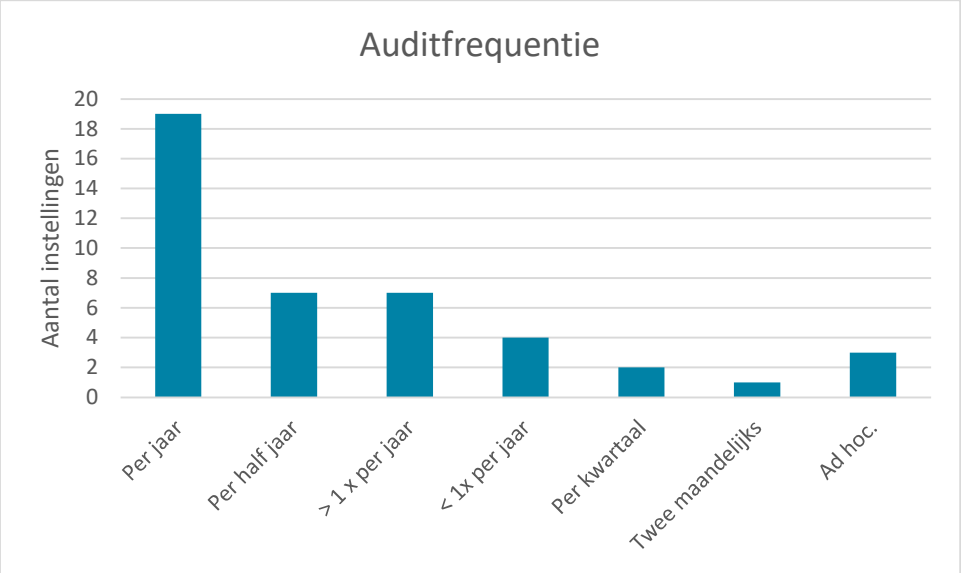
Interessant is te zien hoeveel IBP-functionarissen een rechtstreekse rapportagelijn naar de RvB hebben. Dit zou een onafhankelijke positie van de IBP-functionaris ondersteunen. In situaties die dat vragen kan de IBP-functionaris dan naar de RvB stappen om deze te informeren over bijvoorbeeld grote acute risico's of belangrijke risico's waarin mogelijke belangenconflicten spelen.
Uit het onderzoek blijkt dat volgens de IBP-functionaris in 52 procent van de instellingen een rechtstreekse rapportagelijn bestaat van de IBP-functionaris naar de bestuurder (F42). In 48 procent van de instellingen is dit niet het geval. Het zou interessant zijn om te achterhalen waarom dat zo is. Dit kan een bewuste keuze zijn wanneer de IBP-functionaris bijvoorbeeld onder een andere functionaris is geplaatst die wél een rechtstreekse lijn heeft met de RvB. Dat zou bijvoorbeeld kunnen spelen wanneer een IBP-functie puur technisch over de tactisch/operationele kant is ingevuld. Op de (on)wenselijkheid van die positionering zijn we eerder in dit hoofdstuk dieper ingegaan.
Als in 52 procent van de instellingen een rechtstreekse rapportagelijn bestaat van de IBP-functionaris naar de RvB roept dat de vraag op in hoeverre de positie van de IBP-functionaris in de organisatiehiërarchie van belang is. Het lijkt vooral belangrijk dat de onafhankelijkheid van de IBP-functionaris is gegarandeerd. De positie onder de afdeling ICT riep wat dit betreft eerder al vragen op.

3.8 MANAGEMENTSYSTEEM (ISMS)

Een Information Security Management System (ISMS) is een gestructureerd raamwerk voor het systematisch beheren van informatieveiligheid binnen een organisatie. Het omvat beleid, processen, procedures en technologieën om risico's te identificeren, te beoordelen en te beheersen, met als doel de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen en te verbeteren.
Het ISMS gaat over de instandhouding van kwaliteitsmanagement rond informatieveiligheid wat velen zullen herkennen als de Plan-Do-Check-Act cyclus of Deming circle. Bij de beheersing van de werking van het ISMS zijn opzet, bestaan en werking van beheersmaatregelen belangrijk. Opzet betekent dat maatregelen (zoals beleid) zijn beschreven. Bij bestaan wordt aangetoond dat de maatregelen daadwerkelijk worden uitgevoerd. Bij de werking wordt gekeken of de maatregelen het beoogde effect hebben, dus of het doel van de maatregelen wordt bereikt. Zo zou het gebruik van multifactor authenticatie een effectieve maatregel zijn om aan te tonen dat een leerling die inlogt ook daadwerkelijk de leerling is die hij zegt dat hij is.
Uit de toets kan blijken dat processen niet werken of moeten worden bijgesteld. Aanleiding om verbeteringen uit te voeren met betrekking tot de informatiebeveiligingsorganisatie. Externe auditors zijn altijd zeer geïnteresseerd in de interne audits omdat deze een belangrijk onderdeel vormen van de plan-do-check-act cyclus van informatiebeveiliging. Doet de organisatie wat ze

zegt dat ze doet en hoe wordt continu gesleuteld aan de kwaliteit van de informatiebeveiligingsprocessen?

Uit het onderzoek komt volgens de IBP-functionaris de volgende auditfrequentie naar voren (F44). De bestuurder gaf een vergelijkbaar antwoord.

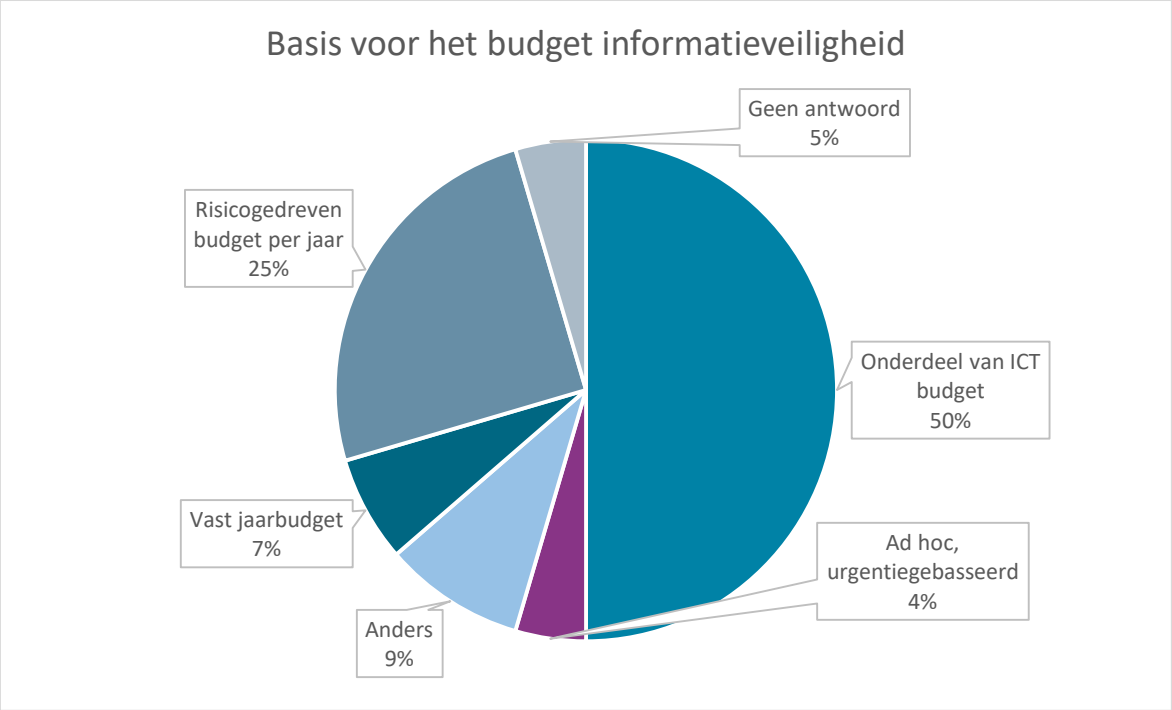


Figuur 10 *Auditfrequentie volgens de IBP-functionaris*

Het belangrijkste is dat er periodiek wordt gecontroleerd of processen nog goed werken: leveren de processen dat waarvoor ze bedoeld zijn? Een externe auditor zal controleren of ieder jaar interne audits worden uitgevoerd.

3.9 BUDGETTEN VOOR INFORMATIEBEVEILIGING

Waar we ook nieuwsgierig naar zijn, is de vraag hoe budgetten voor informatiebeveiliging worden vastgesteld. Het onderzoek bood de volgende uitkomsten volgens het inzicht van de bestuurder (B30).



Figuur 11: *Wijze van vaststelling budget informatiebeveiliging*

In de meeste gevallen is het dus onderdeel van het ICT-budget. Een risicogedreven budget lijkt goed aan te sluiten bij een meer risicogedreven aanpak. Deze aanpak wordt in een kwart van de instellingen gehanteerd.
Onderstaand overzicht geeft een beeld van het gemiddeld aantal formatieplekken binnen mbo-instellingen met betrekking tot informatiebeveiliging (F51).

- Coördinatie IB (inclusief inhuur) op strategisch/tactisch niveau op het onderwerp information risk management (vergelijkbaar met CISO- rol). 0,55 FTE
- Coördinatie IB (inclusief inhuur) op tactisch/operationeel niveau op het onderwerp information risk management (vergelijkbaar met ISO- rol). 0,53 FTE
- Technisch beheer IB (inclusief inhuur) op strategisch/tactisch niveau op het technisch uitvoerend vlak (vergelijkbaar met ICT-beveiligingsmanager). 0,44 FTE
- Technisch beheer IB (inclusief inhuur) op tactisch/operationeel niveau op het technisch uit te voeren vlak (vergelijkbaar met ICT-beveiligingsbeheerder). 0,90 FTE
- Privacy op strategisch/tactisch niveau op het onderwerp information risk management (rol Functionaris Gegevensbescherming). 0,45 FTE
- Privacy op tactisch/operationeel niveau op het onderwerp information risk management (Privacy Officer-rol). 0,41 FTE

Wat betreft de inzet voor technisch beheer geeft ongeveer de helft van de instellingen aan hiervoor 0,5 FTE of minder in te zetten, waarbij negen instellingen aangeven hiervoor geen FTE te hebben. Verder onderzoek zou moeten uitwijzen hoe dit geïnterpreteerd moet worden. Dit vraagt om een vervolgonderzoek.

4 VEELBELOVENDE INSTELLINGEN

4.1 VOLWASSENHEID VOLGENS HET NBA-KADER

Eerder in 2022 is onder mbo-instellingen de nulmeting informatiebeveiliging uitgevoerd op basis van het NBA-toetsingskader. Het moet worden opgemerkt dat dit een self assessment betrof en dus geen formele audit. Gemiddeld werd in het onderzoek een score van 2,1 behaald op een schaal van 5. Wat duidt op een beperkte volwassenheid. Hier was dus ruimte voor ontwikkeling. De hoogste score binnen de nulmeting informatiebeveiliging kwam uit rond de 3 op een schaal van 5. Niveau 3 houdt in dat beheersmaatregelen zijn gedocumenteerd en op gestructureerde en geformaliseerde wijze worden uitgevoerd. Daarbij is de uitvoering aantoonbaar en wordt deze getoetst. Bij het behalen van niveau 3 is dus sprake van een aantoonbare opzet en het bestaan van beheersmaatregelen. Bij een niveau hoger (niveau 4) wordt ook de effectiviteit van de beheersmaatregelen getoetst (bron: NBA, zie bijlage 1)
Kijkend naar de scores van alle deelnemers aan het onderzoek naar de NBA-volwassenheid van de informatiebeveiliging uit 2022 zien we de volgende geaggregeerde cijfers:

				Gemiddelden	
Statement	**Thema code**	**Thema**	**NBA-ID**	**Nederland**	**Top 3**
Strategie	G01	Strategie	GO.01	2,4	3,3
Beleid	G02	Beleid	GO.02	2,9	3,3
Planning/ Roadmap	G06	Roadmap	GO.03	2,4	3,0
Architectuur	G03	Architectuur	GO.04	2,0	3,0
Onafhankelijke toetsing	G07	Assurance	GO.05	2,1	2,7
Eigenaarschap, rollen, verantwoording en verantwoordelijkheid	G04	Eigenaarschap	OR.01	2,1	2,7
Functiescheiding	G04	Eigenaarschap	OR.02	2,3	3,0
Informatie risico- management framework	G05	Risk Management	RM.01	1,6	2,3
Risicobeoordeling	G05	Risk Management	RM.02	1,7	2,3
Plan voor behandeling en beperking van risico's (inclusief risicoacceptatie)	G05	Risk Management	RM.03	1,9	2,3
Gemiddelde				**2,2**	**2,9**

Tabel 12: *Volwassenheid informatiebeveiliging mbo-instellingen 2022*

4.2 TOP 3-INSTELLINGEN

De omzet van twee van de top 3-instellingen zit tussen de 90 en 230 miljoen euro per jaar. Grote instellingen dus. De derde instelling zit qua omzet tussen de 31 en 60 miljoen euro. Een relatief kleinere instelling dus. De top 3 omvat dus niet alleen grote organisaties. Daarbij blijkt dus ook een kleinere instelling in staat om een goede volwassenheid te realiseren.
De drie beter scorende mbo-instellingen op het gebied van informatiebeveiliging hebben op de volgende manier invulling gegeven aan governance:

- De drie geanonimiseerde instellingen scoorden bij de NBA 0-meting een gemiddelde volwassenheidsscore van 2,9 op het onderwerp governance. Dit volgens de alternatieve indeling van het NBA-kader. In deze indeling zijn taken, bevoegdheden en verantwoordelijkheden, functiescheiding en risicomanagement inbegrepen.
- Bij alle drie de instellingen zien we een hoge betrokkenheid van de bestuurder op alle onderwerpen. In alle gevallen neemt de bestuurder de eindverantwoordelijkheid voor risicomanagement op zich. Ambities ten aanzien van informatiebeveiliging zijn volledig helder. Plannen worden jaarlijks opgesteld/bijgesteld. Er wordt één keer per kwartaal overlegd. De bestuurder is in hoge mate betrokken bij alle uitgevraagde taken:
  a) Richting geven
  b) Rapporteren
  c) Evalueren (risico)
  d) (Eind)Controle
  e) Stimuleren
  f) Voorbeeldfunctie
  g) Besluitvorming, ook bij conflicterende belangen

- Taken, bevoegdheden en verantwoordelijkheden zijn duidelijk gedefinieerd en bekend bij het CvB.
- Opvallend is dat in deze drie voorbeelden de manager ICT duidelijk een omvangrijke taak heeft op het gebied van informatiebeveiliging, meedenkt in plannen en rapporteert over het onderwerp. Dit gaat in tegen de visie, die aan populariteit wint, waarbij de IBP-functionaris direct verantwoordelijkheid aflegt aan de besturende laag als het gaat om governance van informatiebeveiliging.
- In de drie voorbeeldorganisaties zijn proceseigenaren beperkt tot volledig verantwoordelijk voor het risicomanagement binnen hun proces. Hier is geen eenduidige lijn te trekken.
- Er vinden één tot meerdere keren per jaar audits plaats om opzet, bestaan en werking van beheersmaatregelen aan te tonen. Resultaten worden tijdens de normale evaluatie-afstemming met het CvB besproken, tenzij er aanleiding is dit eerder te doen. Dit gebeurt normaal twee keer per jaar.
- De IBP-functionaris wordt ingezet over de informatie risicomanagement-as (kolom 1) en niet primair over de cybersecurity/technische as (kolom 2). Hieruit is af te leiden dat de IBP-functionaris zich duidelijk bezighoudt met het sturen en bewaken van organisatiebrede risicomanagementprocessen.

Positionerig IBP-Functionaris	kolom 1: Veiligheid van de IB-functie (Information risk management)	kolom 2: Veiligheid van de ICT-functie (ICT beveiliging / cyber security)
rij 1: Strategisch en/of tactisch	traditionele CISO-rol	ICT-beveiligingsmanager
rij 2: Tactische en/of operationeel	traditionele ISO-rol + optioneel Privacy Officer Rol.	ICT-beveiligingsspecialist/beheerder

Figuur 13: Positionering IBP-functionaris

- Draagvlak is binnen de drie voorbeeldorganisaties in het merendeel van de organisatielagen aanwezig.
- De samenstelling van het budget is niet eenduidig over de instellingen vast te stellen. Dat kan een vast budget zijn of afhankelijk van de risico's die zich voordoen.
- Het aantal formatieplekken voor de IBP-functionaris ligt tussen de 1,0 FTE en 1,5 FTE. Voor technisch beheer op het gebied van informatiebeveiliging/netwerkbeheer ligt dit bij de drie instellingen tussen de 1 en 2 FTE. Voor de invulling van de rol van privacy coördinator is dit 0,2 tot 1,0 FTE.

4.3 CONCLUSIE TOP 3-INSTELLINGEN

Bij de drie meer succesvolle instellingen zien we dus een aantal belangrijke overeenkomsten die andere instellingen ook aan het denken zouden kunnen zetten over hun aanpak:

- Grote betrokkenheid van de bestuurder.
- De NBA-score voor governance (alternatieve indeling) ligt rond de 3.
- Er is sprake van een planmatige aanpak van informatiebeveiliging met een jaarlijkse cyclus.
- Verantwoordelijkheden worden belegd bij proces-/domeineigenaren.
- Verantwoording afleggen door de IBP-functionaris aan de manager ICT blijkt *-tegen de verwachting in-* te werken als besturingsmodel.
- Er is sprake van een duidelijke beschrijving van taken, bevoegdheden en verantwoordelijkheden ten aanzien van informatiebeveiligingsbeleid.
- Minimaal 1 FTE inzet op het onderwerp informatiebeveiliging.

5 AANBEVELINGEN

In dit documenten is governance rond informatiebeveiliging vanuit diverse perspectieven bekeken. Vanuit de onderzoeksresultaten zijn een aantal aanbevelingen op te stellen die instellingen mogelijk helpen bij het verbeteren van de governance. Deels komen deze voort uit best practices. De aanbevelingen zijn:

GEDEELD REFERENTIEKADER

Zorg voor een gemeenschappelijke basis door het vaststellen van een gedeeld referentiekader voor informatieveiligheid. Gebruik het NBA-volwassenheidsmodel als een best practice voor risicomanagement om een overzicht van de belangrijkste risico's op te stellen en de aanpak te prioriteren.

VERHELDER DE ROL VAN DE BESTUURDER EN VERGROOT DIENS BETROKKENHEID

Ondanks een algemene betrokkenheid van bestuurders, kunnen er verschillen zijn in de interpretatie van hun rol. Het is raadzaam dat bestuurders en IBP-functionarissen de dialoog aangaan om te begrijpen hoe de bestuurder zijn rol ziet. Duidelijke afspraken over informatiebeveiligingstaken, bevoegdheden en verantwoordelijkheden kunnen bijdragen aan een effectiever risicomanagement. Bedenk dat een hogere betrokkenheid van de bestuurder bijdraagt aan een hogere volwassenheid van informatieveiligheid.

EVALUEER DE POSITIONERING VAN DE IBP-FUNCTIONARIS

Het onderzoek geeft inzicht in de verschillende manieren waarop de IBP-functionaris binnen een organisatie kan worden gepositioneerd. Het is belangrijk om regelmatig de positie van de IBP-functionaris te evalueren en ervoor te zorgen dat deze aansluit bij de behoeften van de organisatie. Een goede positionering kan de effectiviteit van informatiebeveiligingsmaatregelen vergroten.

RISICOGERICHTE AANPAK

Richt het proces rond informatiebeveiliging risicogericht in. Gebruik risico-overzichten als basis voor risico-overleg met verschillende stakeholders om een gedeeld beeld te creëren over de inschatting van risico's en om gezamenlijk prioriteiten te stellen. Overweeg het gebruik van een GRC-applicatie voor risicogericht werken.

3-LINES MODEL VOOR RISICOMANAGEMENT

Volg het 3-lines model voor risicomanagement, waarbij de bestuurder de eigenaar is van het risicomanagementproces. De eerste lijn (domeineigenaar) dagelijkse risico's identificeert, de tweede lijn (IBP-functionaris) de implementatie van beheersmaatregelen ondersteunt en bewaakt en de derde lijn interne audits uitvoert ter controle en verificatie.

OPERATIONEEL RISICOMANAGEMENT

Implementeer operationeel risicomanagement om ad hoc risico's aan te pakken die mogelijk niet gedekt zijn door beleid. Zorg ervoor dat er procedures zijn om onvoorziene risico's te verminderen en om te zetten naar meer structurele beheersmaatregelen.

Versterk risico-eigenaarschap binnen de organisatie

Het is belangrijk dat risico-eigenaarschap op een heldere manier aan domein- of proceseigenaren wordt toegewezen. Organisaties moeten ervoor zorgen dat dit principe duidelijk wordt gedefinieerd en toegepast. Het vastleggen van taken, bevoegdheden en verantwoordelijkheden in het informatiebeveiligingsbeleid kan bijdragen aan een effectiever risicomanagement.

GRC-applicatie

Overweeg het gebruik van een GRC-applicatie, zoals Trustbound, om beveiligingsrisico's in kaart te brengen, maatregelen te beschrijven en grip te krijgen op volwassenheid, risico's en planning. Houd de applicatie bij om op elk gewenst moment inzicht te hebben en te kunnen geven in de actuele stand van zaken rond risico's, beheersmaatregelen en openstaande taken.

Verbeter de afstemming tussen bestuurders en IBP-functionarissen

De 0-meting laat zien dat er verschillen zijn in de perceptie van bestuurders en IBP-functionarissen over de mate van zorg met betrekking tot informatieveiligheid. Het is essentieel om de communicatie te verbeteren en een gemeenschappelijk begrip te creëren. IBP-functionarissen kunnen het gesprek aangaan met bestuurders om zorgen over en het belang van informatieveiligheid te bespreken.

Optimaliseer de samenwerking tussen IBP-functionarissen en besluitvormers

Er spelen conflicterende belangen bij besluitvorming over informatiebeveiliging. Het is van cruciaal belang dat IBP-functionarissen besluitvormers goed informeren over risico's, vooral in gevallen waarin belangen conflicteren. Een effectieve communicatie kan helpen bij het nemen van weloverwogen beslissingen.

Best Practice Organisaties

De drie in hoofdstuk 3 uitgelichte veelbelovende instellingen vertonen belangrijke overeenkomsten in hun aanpak op het vlak van informatiebeveiliging, waaronder grote betrokkenheid van de bestuurder, een score van rond de 3 op het onderdeel governance volgens de alternatieve indeling van het NBA-kader, een planmatige aanpak, duidelijke verantwoordelijkheden en voldoende formatie-inzet. Wellicht kan de aanpak van deze organisaties voor de eigen organisatie als leidraad worden gebruikt.

6 CONCLUSIES

In 2023 is in het mbo landelijk onderzoek gedaan naar governance rond informatiebeveiliging binnen onderwijsinstellingen. Met als doel te achterhalen hoe mbo-instellingen omgaan met het aansturen van informatiebeveiliging.
In totaal hebben 44 van de 55 aangeschreven instellingen deelgenomen aan het onderzoek. Dankzij deze respons is een goed beeld verkregen van het onderwerp.

Informatiebeveiliging = Risicomanagement. Dit uitgangspunt wordt gehanteerd om governance van informatiebeveiliging te boordelen.

Vanuit governance perspectief is de bestuurder eindverantwoordelijk voor het risicomanagement binnen de organisatie. In dat verband zien we dat veel bestuurders zich steeds bewuster zijn van het feit dat:

- Een gebrek aan informatiebeveiliging grote en directe risico's met zich meebrengt voor het bereiken van de organisatiedoelstellingen.
- Ze als bestuurder eindverantwoordelijkheid moeten nemen voor risicomanagement op het gebied van informatieveiligheid.

In 2022 is een nulmeting informatiebeveiliging uitgevoerd op basis van het NBA-volwassenheidsmodel. Het resultaat op het onderwerp governance was een 2,1 gemiddeld (op een schaal van 5). Dit duidde destijds, in 2022 dus, op een beperkte volwassenheid.
Daar waar het NBA-kader vertelt WAT er moet gebeuren, zijn we binnen de nulmeting governance geïnteresseerd in HOE binnen het mbo wordt gestuurd op informatiebeveiliging. Hiervoor is ook gekeken naar een best practice op het gebied van risicomanagement. Dit is het zogenaamde 3-lines model waarbij risico-eigenaarschap wordt belegd bij domeineigenaren en waarbij de IBP-functionaris een ondersteunende rol heeft. 63 procent van de instellingen legt de operationele verantwoordelijkheid voor risicomanagement in de lijn, inclusief het MT. Dat sluit aan bij een 3-lines benadering.
Ten aanzien van de visie op informatieveiligheid van de bestuurder en de IBP-functionaris zijn er verschillen waar te nemen. Dit bijvoorbeeld als het gaat om de positionering van de IBP-functionaris in de organisatie. Op dat vlak zien we steeds vaker dat de IBP-functionaris een beweging maakt van tactisch/operationeel vlak naar een meer tactisch/strategische blik (rij 1) op het gehele speelveld van informatiebeveiliging (kolom 1). De traditionele CISO-rol.

Positionering IB functie	kolom 1: Veiligheid van de IB-functie (Information risk management)	kolom 2: Veiligheid van de ICT-functie (ICT beveiliging / cyber security)
rij 1: Strategisch en/of tactisch	traditionele CISO-rol	ICT-beveiligingsmanager
rij 2: Tactische en/of operationeel	traditionele ISO-rol + optioneel Privacy Officer Rol.	ICT-beveiligingsspecialist/beheerder

Figuur 14 Positionering IBP-functionaris

Vanuit deze positie werkt de IBP-functionaris meer vanuit een ondersteunende overzichtspositie en wordt hij een geschiktere gesprekspartner voor de bestuurder en domeineigenaren. Vanuit de gedachte van het 3-lines model zou daarbij het eigenaarschap voor risicomanagement nog meer bij domeineigenaren komen te liggen. Voorbeelden hiervan zijn HR, opleidingsteams/eigenaren, Finance & Control en natuurlijk ICT zelf.

Wanneer wordt gesproken over de plek in de organisatiestructuur zou je verwachten dat de IBP-functionaris een onafhankelijke verantwoordingsfunctie heeft ten opzichte van de bestuurder. Bij een drietal goed scorende instellingen is de IBP-functionaris echter direct geplaatst onder de IT-manager. Deze positie is normaal gesproken niet gelukkig omdat de focus dan meer technisch georiënteerd is. Ook wordt de IBP-functionaris in dit geval gezien als onderdeel van IT waardoor zijn onafhankelijkheid in het geding is. Speculerend over het succes van deze positionering onder de IT-manager moet het in deze succesvolle voorbeelden wel zo zijn dat de IT-manager de IBP-functionaris de ruimte geeft om onafhankelijk zijn werk te doen. Zodat ook informatieveiligheids- of privacybevindingen op het gebied van het IT-domein niet leiden tot belangenconflicten.
Ook bleek dat de bestuurder binnen succesvol opererende instellingen volledig zijn betrokkenheid toont ten aanzien van informatieveiligheid wat er aan zal bijdragen dat het onderwerp informatiebeveiliging volledig tot zijn recht komt.

In hoofdstuk 4 zijn een aantal aanbevelingen geformuleerd die kunnen bijdragen aan de verbetering van de governance rond informatiebeveiliging binnen organisaties. Deze zijn gebaseerd op de resultaten uit het onderzoek gecombineerd met de gezamenlijke kernpunten uit de aanpak van drie succesvolle mbo-instellingen op het gebied van informatiebeveiliging en governance. Dit zijn de aanbevelingen nog even in het kort:

1. Zorg voor een gedeeld referentiekader tussen de bestuurder en de IBP-functionaris
2. Verhelder de rol van de bestuurder en vergroot diens betrokkenheid.
3. Evalueer de positie van de IBP-functionaris
4. Hanteer een risicogerichte aanpak voor informatiebeveiliging
5. Hanteer het 3-Lines model voor risicomanagement
6. Hanteer Operationeel Risicomanagement voor niet voorziene risico’s
7. Versterk risico-eigenaarschap in de organisatie
8. Zet de GRC-applicatie in om risicomanagement onder controle te krijgen
9. Optimaliseer samenwerking met besluitvormers
10. Verbeter de afstemming tussen bestuurders en IBP-functionarissen
11. Leer van Best Practice Organisaties.

BIJLAGE 1: NBA VOLWASSENHEID

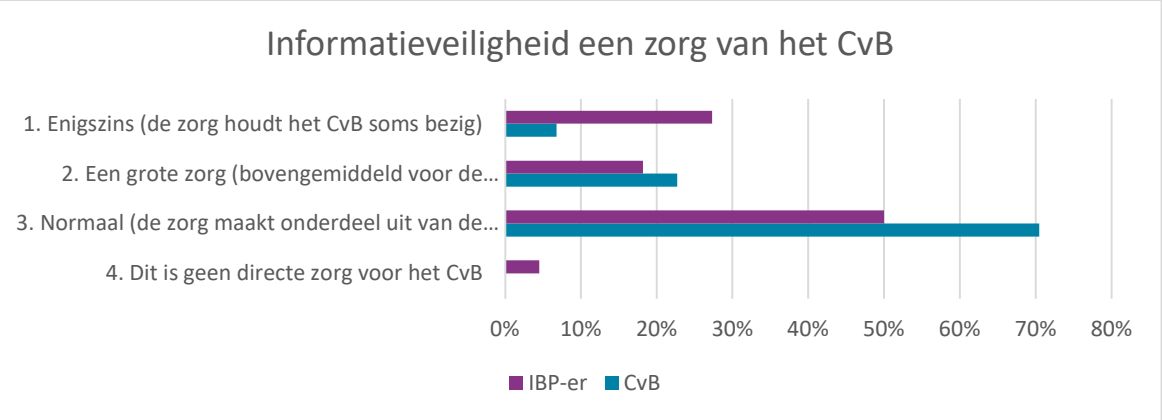
Niveau	Naam	Omschrijving	Indicatieve criteria
1	Initieel	Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte controls geïmplementeerd. • Niet of ad-hoc uitgevoerd. • Niet /deels gedocumenteerd. • 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.

Bron: Handreiking bij Volwassenheidsmodel Informatiebeveiliging, NBA 2019

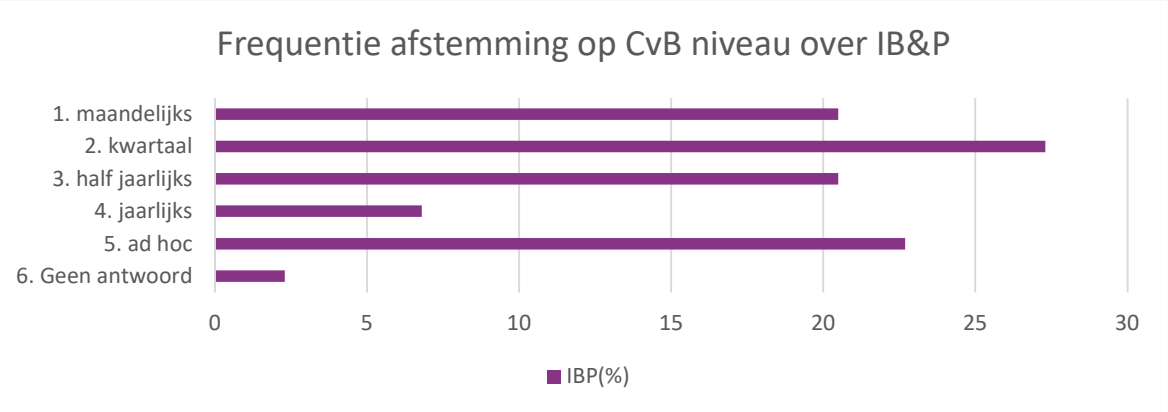
BIJLAGE 2: SCORE OVERZICHT

In deze bijlage zijn de resultaten van het landelijk onderzoek naar de inrichting van de governance binnen het mbo weergegeven. In totaal hebben 44 van de in totaal 55 instellingen (80%) meegedaan aan het onderzoek. In iedere grafiek staat vermeld wie het antwoord heeft gegeven. Dit is de IBP-functionaris of de bestuurder (CvB) die informatiebeveiliging in zijn portefeuille heeft. De meeste resultaten zijn weergegeven in percentages. Deze percentages hebben altijd betrekking op het deel van de 44 instellingen dat een bepaald antwoord heeft gegeven. Totalen van percentages komen dus altijd uit op 100%per vraag. Voor de overzichtelijkheid is gewerkt met grafieken in plaats van tabellen met cijfers.

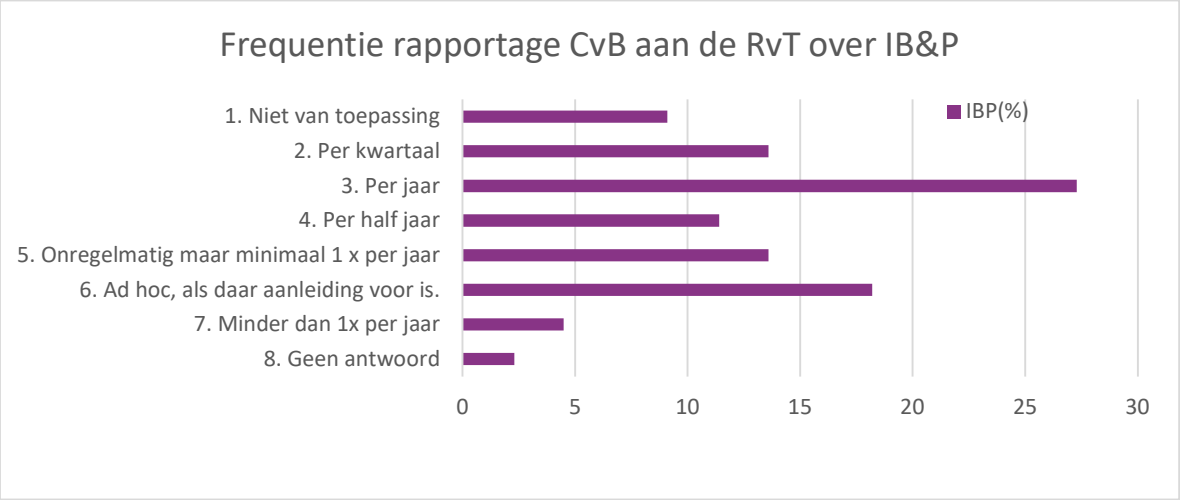
In hoeverre zijn onderwerpen als cyberveiligheid, kwetsbaarheden, verbeteren van awareness bij studenten en medewerkers een zorg voor het CvB? *Bron:* Bestuurder v.s. IBP-functionaris. (B4F4)



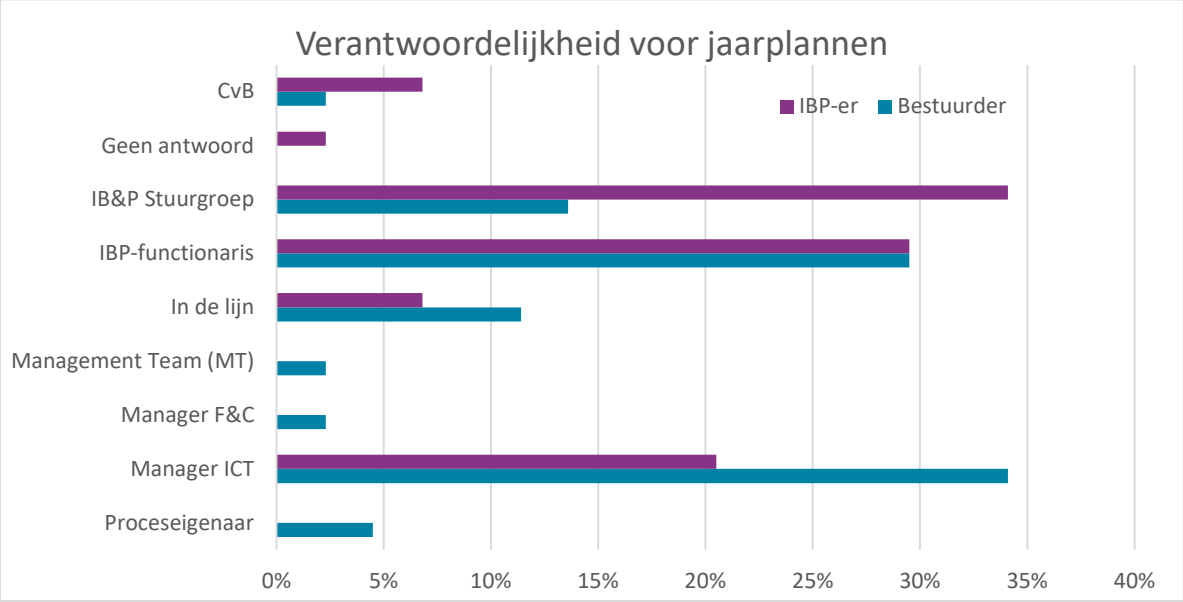
Hoe vaak wordt er op CvB niveau afgestemd over het onderwerp informatieveiligheid en privacy? *Bron*: IBP-functionaris. (F8)



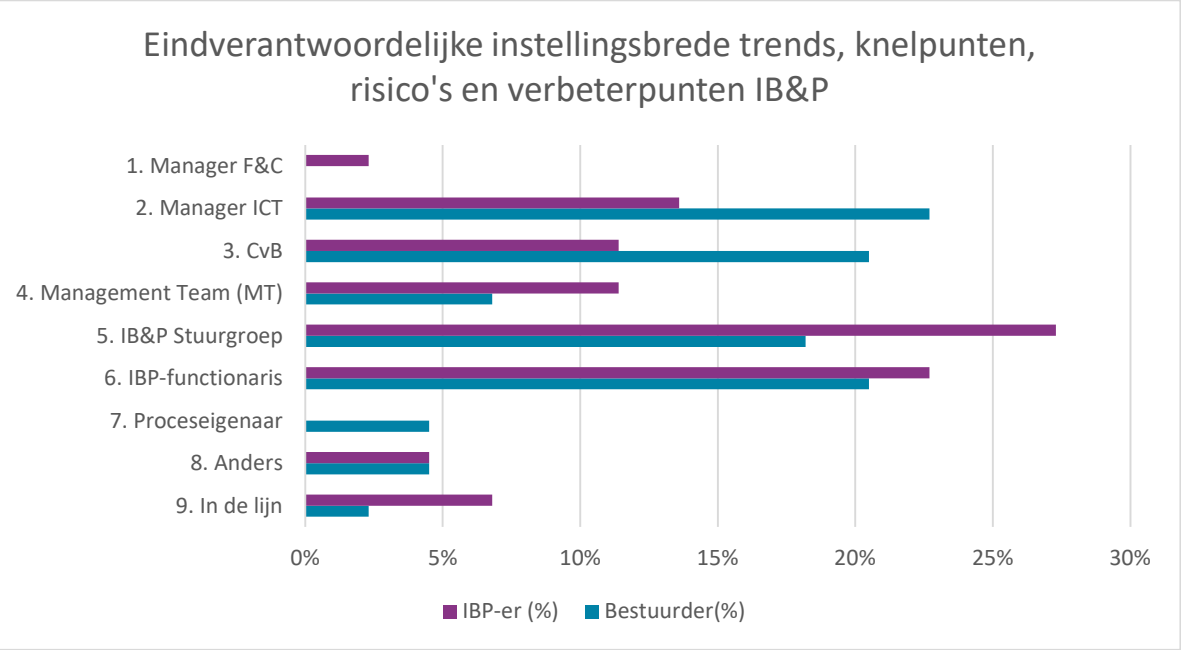
Hoe vaak rapporteert het CvB aan de RvT over de status van informatiebeveiliging? *Bron:* IBP-functionaris. (F9)



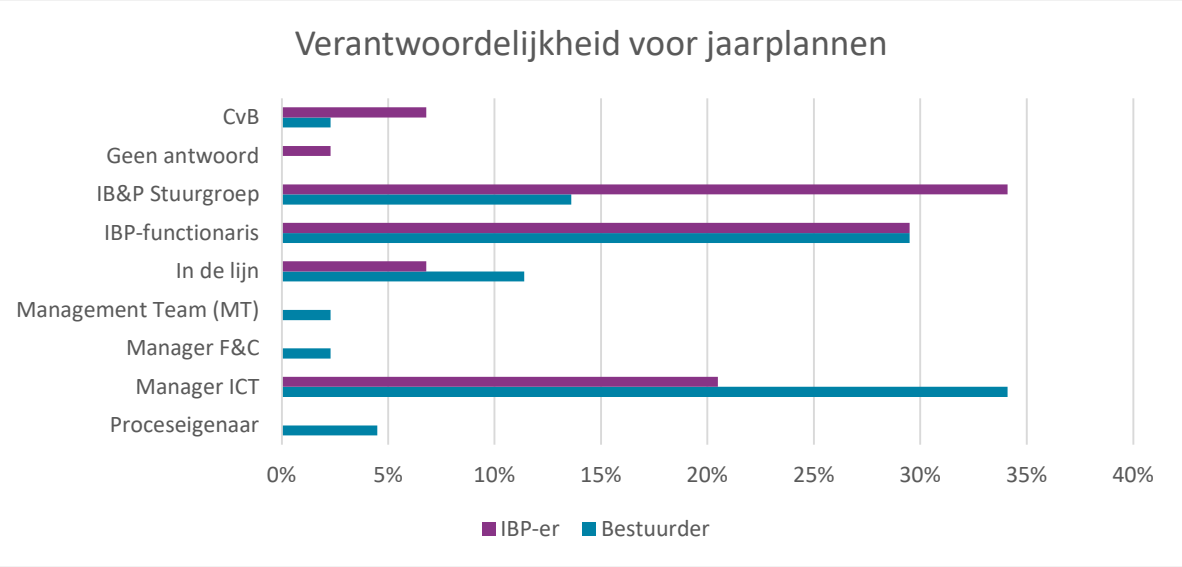
Welke orgaan/functionaris is eindverantwoordelijke voor het opstellen van jaarplannen ten aanzien van informatiebeveiliging? *Bron:* Bestuurder v.s. IBP-functionaris. (F18B13)



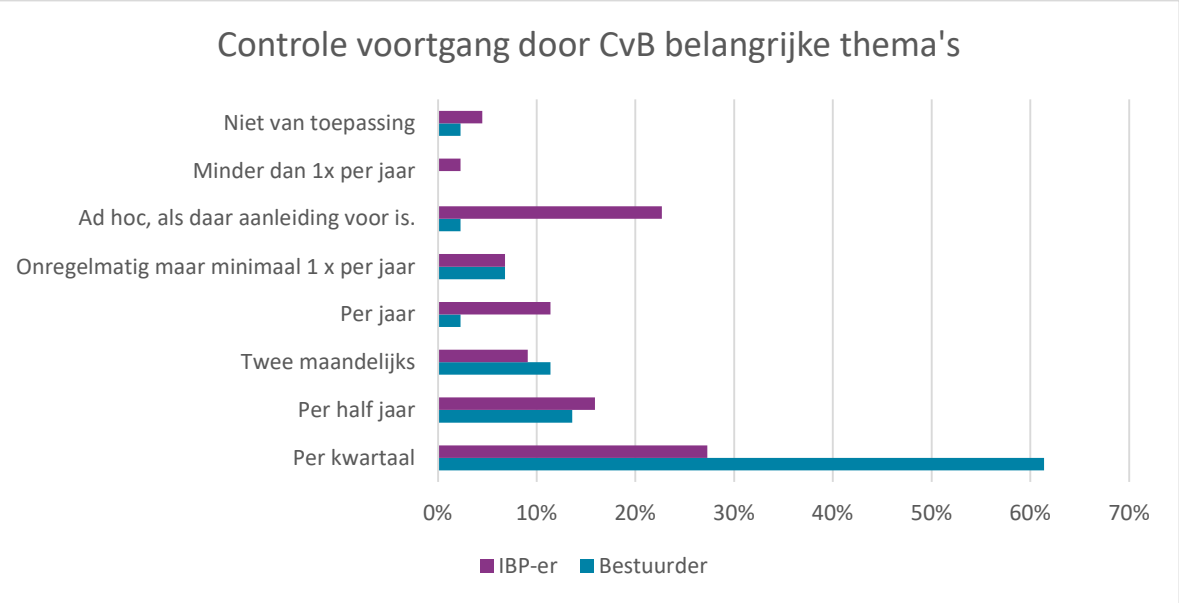
Welke orgaan/functionaris is eindverantwoordelijke voor het vaststellen van instellingsbrede trends, knelpunten en verbeterpunten m.b.t. informatiebeveiliging inbrengen, analyseren op risico's en prioriteren? *Bron:* Bestuurder v.s. IBP-functionaris. (B12F17)



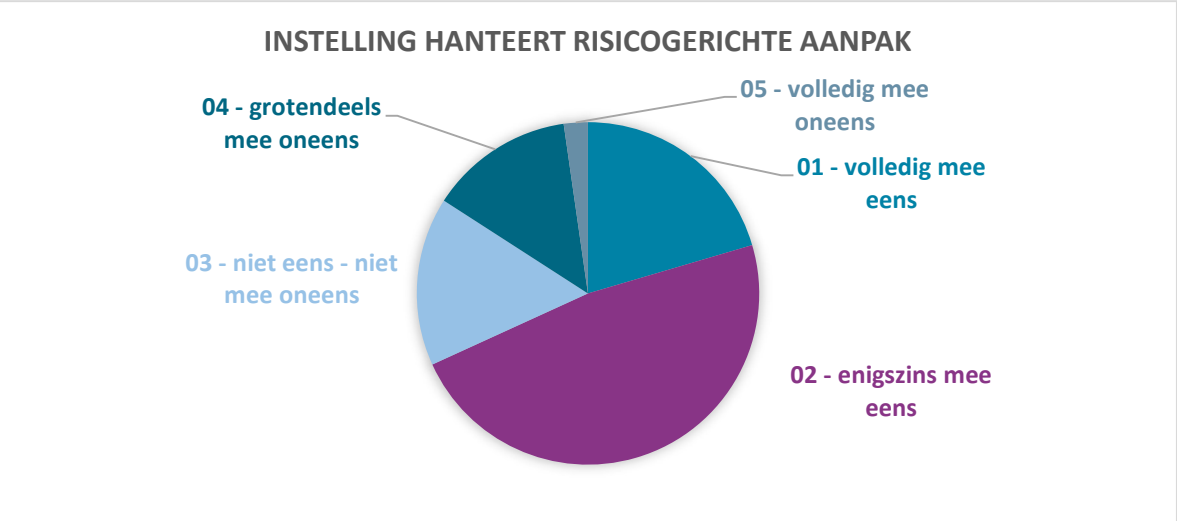
Welke orgaan/functionaris is eindverantwoordelijke voor het opstellen van jaarplannen ten aanzien van informatiebeveiliging? *Bron:* Bestuurder v.s. IBP-functionaris. (F18B13)



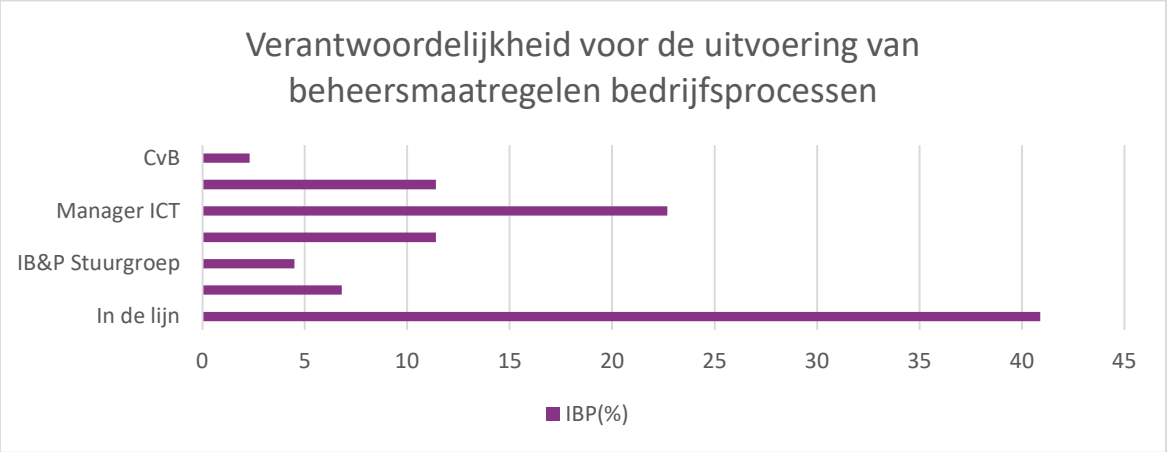
Hoe vaak wordt vanuit het CvB de voortgang van belangrijke thema's gecontroleerd? *Bron:* Bestuurder v.s. IBP-functionaris. (F20B15)



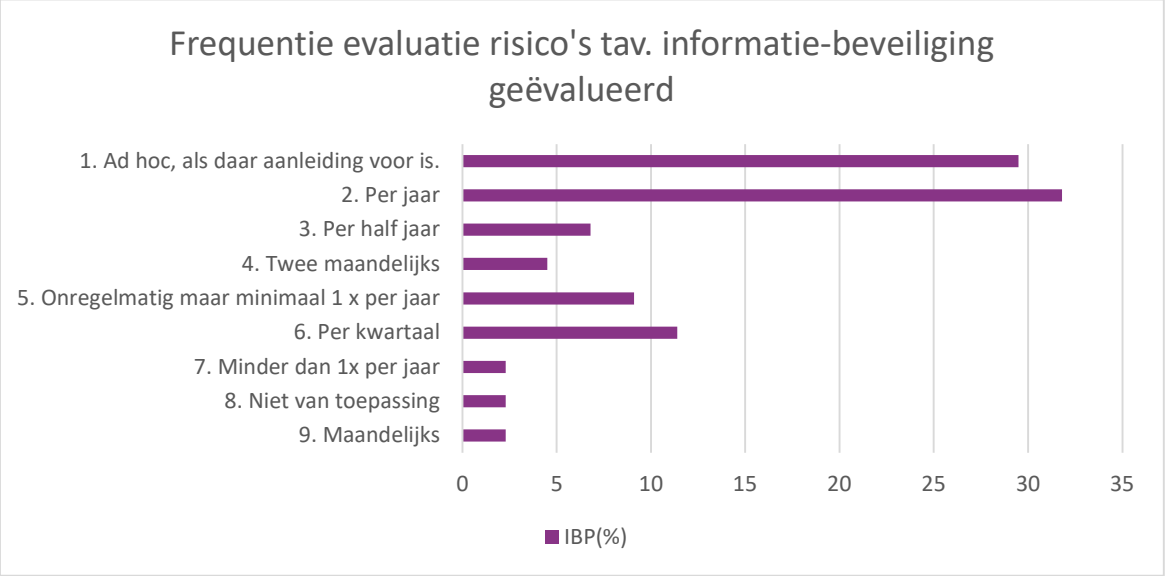
De instelling hanteert een risicogerichte aanpak ten aanzien van informatiebeveiliging. *Bron:* IBP-functionaris. (F21)



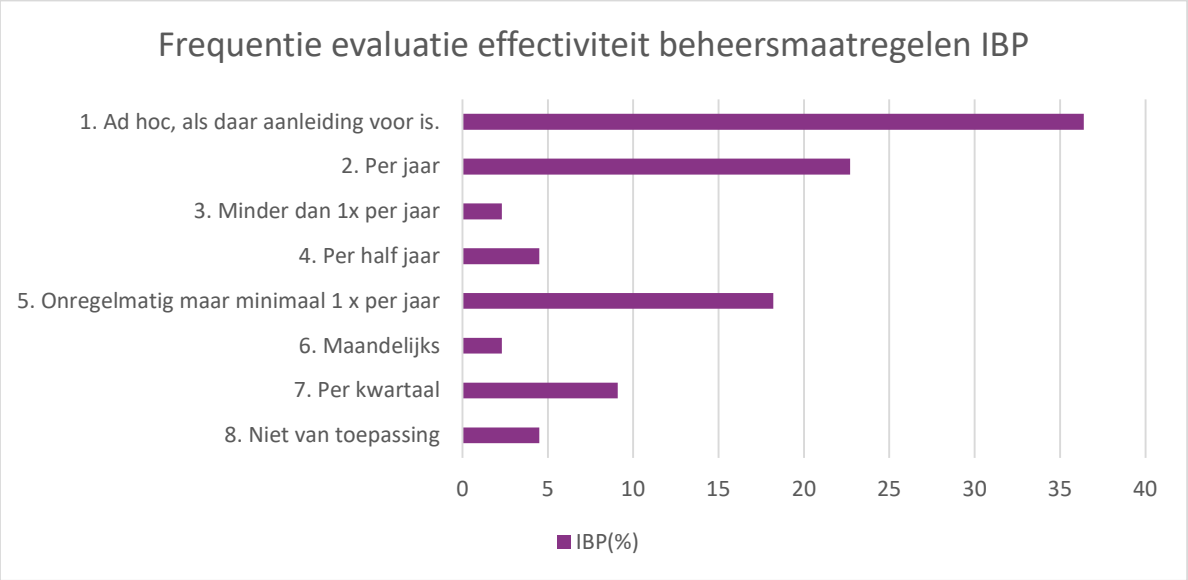
Waar is de verantwoordelijkheid belegd voor de uitvoering van beheersmaatregelen in de operationele bedrijfsprocessen? *Bron:* IBP-functionaris (F24)



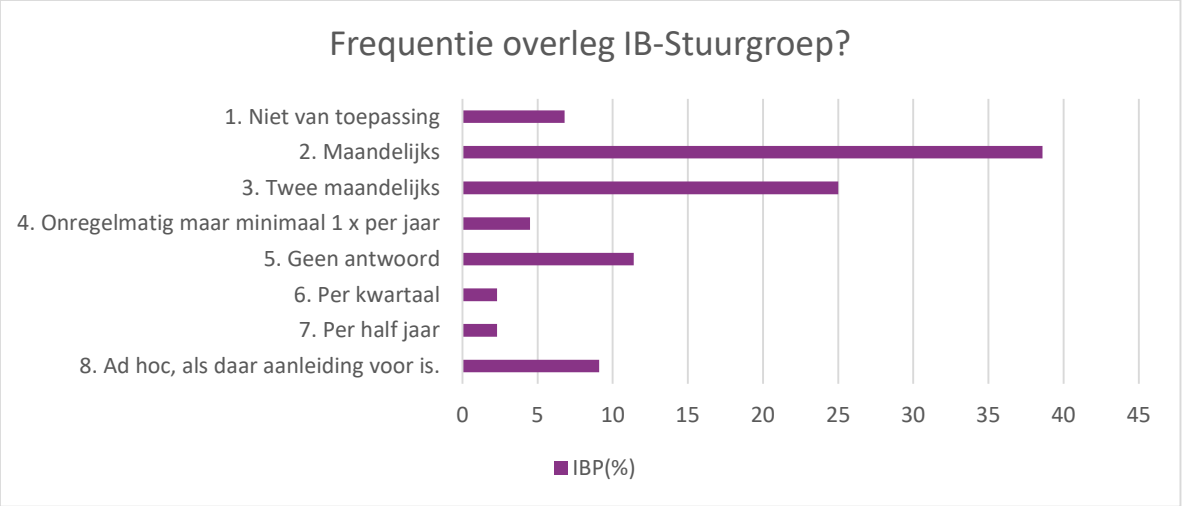
Hoe vaak worden risico's ten aanzien van informatiebeveiliging geëvalueerd als input voor te nemen beheersmaatregelen? *Bron:* IBP-functionaris. (F25)



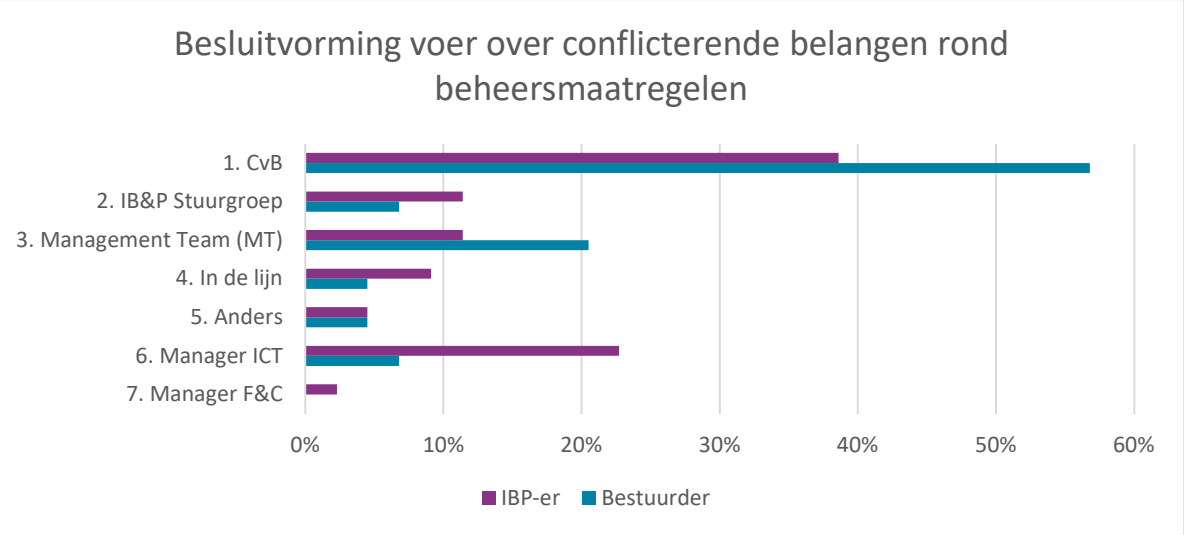
Hoe vaak wordt de realisatie en effectiviteit van beheersmaatregelen ten aanzien van informatiebeveiliging geëvalueerd? *Bron:* IBP-functionaris. (F26)



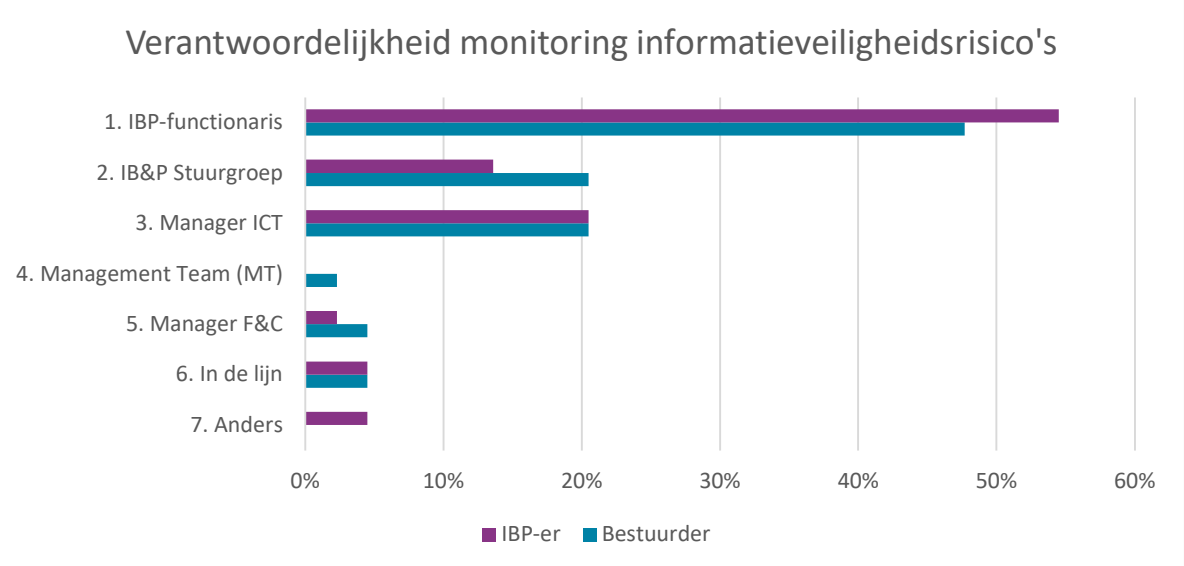
Indien IB-Stuurgroep: hoe vaak vindt er overleg plaats van de IB-Stuurgroep? *Bron:* IBP-functionaris. (F33)



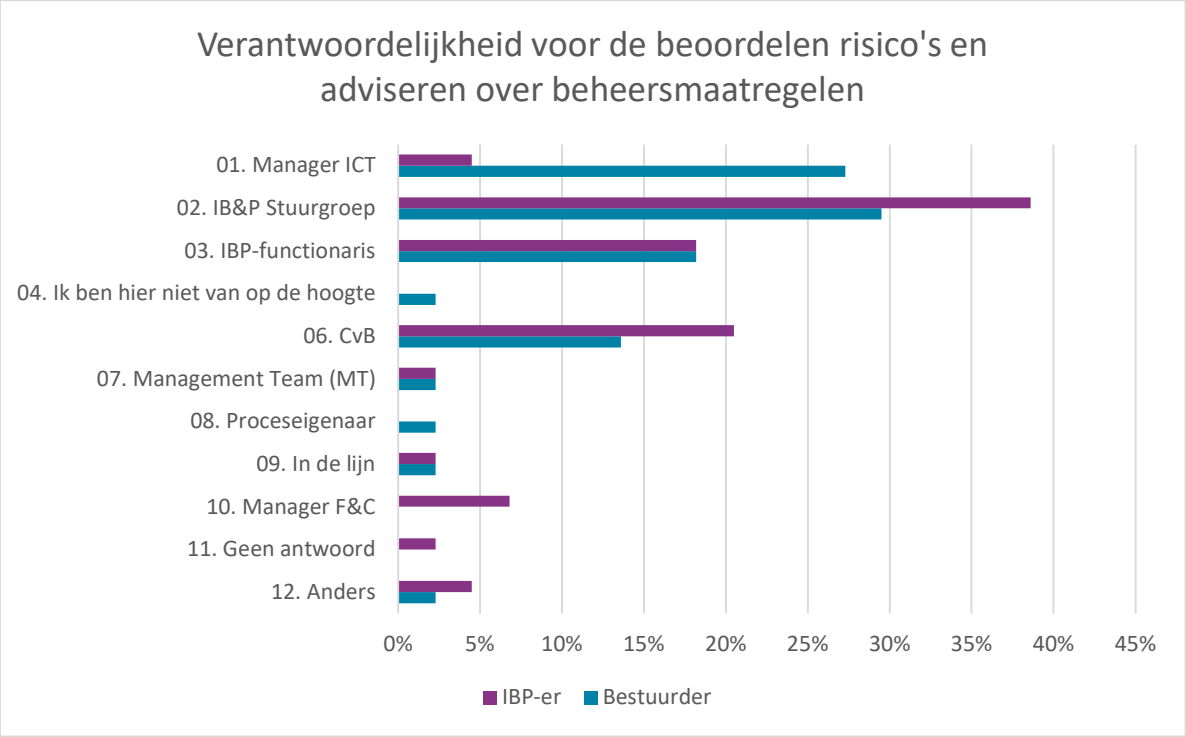
Welk functie of welke gremium maakt doorgaans beslissingen over conflicterende belangen rond de aanpak van grotere risico's voor de informatieveiligheid? *Bron:* Bestuurder v.s. IBP-functionaris.
Toelichting: Bij het maken van beslissingen in de organisatie moet soms een afweging worden gemaakt tussen het realiseren van bedrijfsdoelen en het verminderen van risico's voor de informatieveiligheid. Wanneer de belangen toenemen moet er soms een doorslaggevend besluit worden genomen. (B21F34)



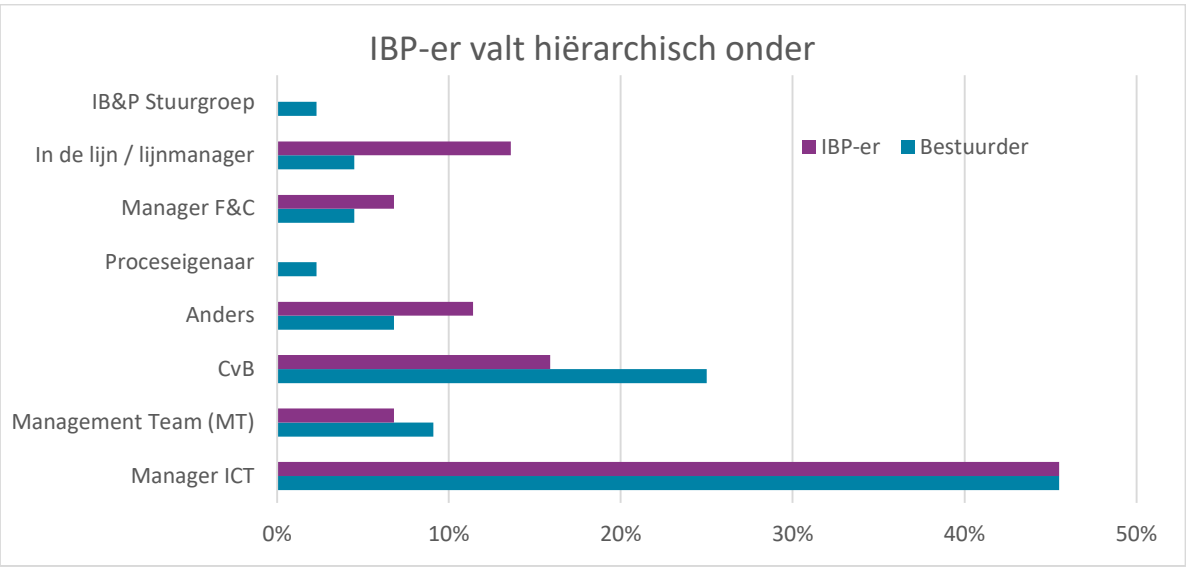
Waar is verantwoordelijkheid primair belegd voor het monitoring en rapporteren op het gebied van informatiebeveiligingsrisico's? *Bron:* Bestuurder v.s. IBP-functionaris. (B22F37)



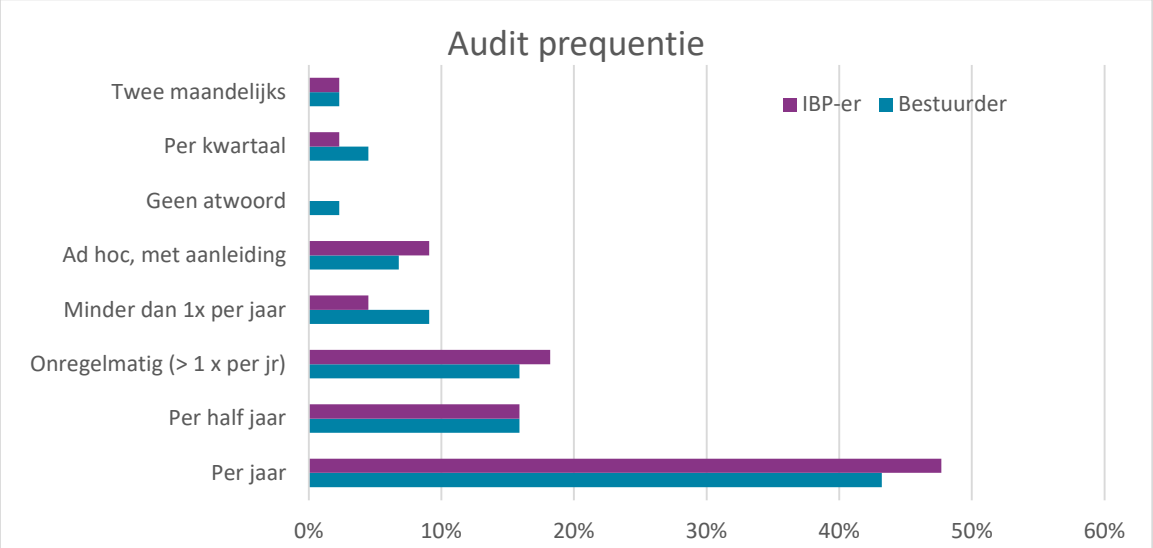
Welke orgaan/functionaris is eindverantwoordelijk voor het beoordelen van informatiebeveiligingsrisico's en het voorstellen voor beheersmaatregelen om risico's te mitigeren? *Bron:* Bestuurder v.s. IBP-functionaris. (B23F38)
Toelichting: Van alle risico's die bekend worden moet wordt vastgesteld wat de kans is dat het risico zich openbaard en de impact is voor de organisatie wanneer het risico zich openbaard. De vraag is wie of welk orgaan verantwoordelijk is voor het vaststellen van deze beoordeling?



Waar in de organisatiestructuur is IBP-functionaris formeel geplaatst? Het orgaan of functionaris waar de IB-Functionaris verantwoording aan aflegt. *Bron:* Bestuurder v.s. IBP-functionaris. *Bron:* Bestuurder v.s. IBP-functionaris. (B25F41)



Hoe vaak wordt de werking van beheersmaatregelen t.a.v. informatiebeveiligingsrisico's geaudit (intern of peer review)? *Bron:* Bestuurder v.s. IBP-functionaris. (B27F44)



Op welke niveau is de eindverantwoordelijkheid voor de controle op de werking van het managementsysteem rond informatiebeveiliging belegd? *Bron:* Bestuurder v.s. IBP-functionaris. Toelichting: Het managementsysteem rond informatiebeveiliging is gericht op het behalen van de doelstellingen die de organisatie over het onderwerp informatieveiligheid heeft geformuleerd. Uitgangspunt daarbij is het voldoen aan wet- en regelgeving en het bewerkstelligen van continue verbetering met het Plan-Do-Check-Act principe (PDCA). (B29F46)