mbo digitaal

Handreiking Security Audit

Voorbereiden op en uitvoeren van de externe audit op basis van het SURF audit Toetsingskader

Datum	*Versie*	*Auteur*
18 juni 2024	1.0	Henry Meutstege, MBO Digitaal
3 juli 2024	1.1	Henry Meutstege, MBO Digitaal
20 september 2024	1.2	Henry Meutstege, Louis van Hemmen, MBO Digitaal
29 oktober 2024	1.3	Henk Links, Henry Meutstege nav Maturity Workshops
20 december 2024	1.4	Henk Links, Max Passet, Henry Meutstege

Deze handreiking is opgesteld om de MBO instellingen te helpen bij het voorbereiden op en het daadwerkelijk uitvoeren van de externe security audit.

mbo digitaal

Inhoudsopgave

1 Inleiding

Onderwijsinstellingen in Nederland hebben afgesproken om periodiek de volwassenheid op het gebied van informatiebeveiliging (en eventueel later ook privacy) te laten toetsen door een externe auditor. In deze handreiking, die in eerste instantie is opgesteld om mbo-instellingen te helpen, gaan we uitleggen hoe je als instelling je kunt voorbereiden op de audit en op welke wijze je daar TrustBound als GRC-applicatie bij kunt gebruiken ter ondersteuning.

1.1 Security Audit

Bij de mbo-instellingen worden tussen 2024 en 2027 twee security-audits uitgevoerd door Deloitte. Beide security audits kennen dezelfde opbouw en aanpak. In de eerste audit wordt gefocust op de opzet en het bestaan van maatregelen uit het SURF audit Toetsingskader Informatiebeveiliging (hierna: toetsingskader). In de tweede audit wordt behalve naar opzet en bestaan ook gekeken naar de werking van de maatregelen uit het toetsingskader.

Wat is nu het verschil wanneer je ook naar werking gaat kijken? Bij opzet en bestaan van een maatregel moet de maatregel allereerst ondersteund en beschreven zijn door een formeel of informeel stuk (beleidsdocument, handreiking, procedure of richtlijn). De auditor beoordeelt of de opzet compleet en al dan niet formeel goedgekeurd is. Bij bestaan kijkt de auditor of de maatregel ook daadwerkelijk geïmplementeerd is in de organisatie. Daarvoor doet de auditor documentatieonderzoek. Ook houdt de auditor interviews. Deloitte kan ook een steekproef doen voor bewijslast. Dit alles is erop gericht om aan te tonen dat de maatregel niet alleen beschreven is (opzet), maar ook daadwerkelijk wordt toegepast en uitgevoerd (bestaan). Bij werking gaat de auditor, nadat opzet en bestaan zijn getoetst, met name kijken of de maatregel effectief is. De auditor beoordeelt dan of de maatregel over een langere periode werkt en of de maatregel doet wat deze geacht wordt te doen. We hebben met de auditor afgesproken dat hij een periode van zes maanden hanteert voor de audit om de werking aan te tonen. In die tijd gaat hij dus op zoek naar bewijslast om aan te onderbouwen dat de maatregel werkt en effectief is.

Een security-audit is anders dan de benchmark IB&P die we jaarlijks uitvoeren. We kijken en gebruiken natuurlijk wel dezelfde meetlat: het afgesproken toetsingskader. Maar een audit is een meer formele en vooral onafhankelijke toetsing, terwijl we tot nu toe vooral zelfassessments hebben uitgevoerd. De security audit geeft per maatregel aan wat het geconstateerde niveau van volwassenheid is, waarbij uitgegaan wordt van het resultaat uit het laatste zelfassessment. Afwijkingen worden geregistreerd als bevinding en als instelling kun je de bevinding vertalen in acties en taken. De auditor brengt verslag uit van zijn bevindingen in een rapportage, die gedeeld wordt met MBO Digitaal. MBO Digitaal krijgt echter niet de hele rapportage te zien maar een geanonimiseerde versie waarin de hoofdlijnen staan. De resultaten en adviezen uit de security audit worden door de auditor ook ingevoerd in TrustBound.

1.2 Kroonjuwelen

In deze security audit hebben we afgesproken een 4-tal kroonjuwelen in scope te nemen van de audit. De auditor zal dan specifiek een aantal maatregelen toetsen op de kroonjuwelen. Bij de mbo-instellingen hebben we de volgende kroonjuwelen afgesproken:

- Het HR-proces
- De financiële administratie

- Het studenteninformatiesysteem*
- Het studentenbegeleidingsysteem*

**bij sommige mbo-instellingen is studentenbegeleidingssysteem en het studenteninformatiesysteem één systeem.*

Van de 69 statements uit het toetsingskader zijn er 30 specifiek die per applicatie worden onderzocht. In bijlage 2 is een overzicht van de statements opgenomen die applicatie-specifiek getoetst worden.

Voor deze applicatie specifieke statements geldt dat de laagste score telt als volwassenheid voor de betreffende maatregel. Let op, in de eerder uitgevoerde zelfassessments hebben we niet naar de kroonjuwelen gekeken. Dit vraagt extra voorbereiding in deze security audit, houd daar rekening mee!

1.3 Toetsingskader

Bij deze security audit kijken we naar het toetsingskader voor Informatiebeveiliging. We gebruiken daarvoor het toetsingskader wat afgeleid is van het NBA model voor volwassenheid (van de Nederlandse Beroepsorganisatie van Accountants) en afgestemd is met het SURF audit Toetsingskader Informatiebeveiliging. Bij SURF is de huidige versie die gehanteerd wordt versie 2.3d. Binnen de MBO's gebruiken we een versie die vrijwel gelijk is met de SURF versie, het MBO Toetsingskader IB V2.0. We hebben een aantal statements en beheersmaatregelen tekstueel verbeterd en we hebben een aantal beheersmaatregelen die wij voor MBO minder relevant achten weg gelaten. Deze versie is opgenomen in TrustBound en gebruiken we als MBO's voor de security audits en voor de benchmark.

1.4 TrustBound als GRC-applicatie

Alle instellingen hebben begin maart 2024 hun zelfassessments uitgevoerd en via TrustBound ingeleverd voor de benchmark IBP. Bij het uitvoeren van de security audit maken we opnieuw gebruik van TrustBound en dan specifiek de audit module in TrustBound. De auditor krijgt bij elke instelling toegang tot de TrustBound-omgeving en maakt gebruik van de audit-module om zijn oordeel te vormen en bevindingen terug te geven aan de instelling.

Vanuit de audit-module toetst de auditor elk statement en elke beheersmaatregel. De eerste stap die de auditor zet, is kijken wat de instelling bij elke maatregel zelf heeft geconstateerd en wat er als onderbouwing is opgenomen. Hier ligt een belangrijke taak voor de instelling ter voorbereiding op de audit. Het is niet meer voldoende om alleen de genoteerde volwassenheid te registreren. Dit zal ook onderbouwd moeten worden met een argumentatie op statement niveau, en een toelichting en ondersteunende documentatie of bewijslast op het niveau van de beheersmaatregelen.

In het volgende hoofdstuk wordt uitgelegd hoe je deze onderbouwing kunt creëren.
Als je de basiskennis van Trustbound nog wilt opfrissen zijn er een aantal starterstrainingen te volgen bij Trustbound zelf, check hier. Ook zijn er veel hulp documenten te vinden over Trustbound in de Trustbound Community, zie op deze pagina.

2 Voorbereiding op de security audit

Wil je de security audit succesvol laten zijn, dan is het belangrijk dat je ervoor zorgt dat de auditor toegang heeft tot de juiste documentatie én dat hij de relevante medewerkers van de instelling te spreken krijgt. Voor de instelling is het verstandig om ruim voor de daadwerkelijke audit de te interviewen personen voor te bereiden en te instrueren. Natuurlijk moet iedereen de vrijheid hebben om zijn mening te geven, toch kan het enorm helpen om vooraf de deelnemers mee te nemen en ze te trainen in de wijze van antwoorden op vragen van de auditor.

2.1 Voorbereiding deelnemers

Het is belangrijk om per statement uit het toetsingskader te bepalen wie de persoon is die door de auditor geïnterviewd gaat worden. In bijlage 3 is een voorstel opgenomen om per statement de eindverantwoordelijke aan te geven. Bij een audit wordt gekeken naar de medewerker die eindverantwoordelijk is voor een statement. Er wordt echter ook rekening gehouden met de medewerkers die een uitvoerende verantwoordelijkheid hebben in de taak. Bijvoorbeeld: de ICT-manager is eindverantwoordelijk voor het proces incident management, maar de uitvoering wordt door een servicedesk of een IT-beheerder gedaan. De auditor wil idealiter zowel de eindverantwoordelijke als de uitvoerenden spreken. De IBP-coördinator (of security officer) wordt betrokken bij de interviews, indien gewenst.

Het is verstandig om vóór de daadwerkelijke audit een voorbereiding bijeenkomst te organiseren waarbij alle te interviewen medewerkers zijn uitgenodigd. Maak duidelijk op welke statements ze bevraagd gaan worden. Neem hen kort mee in de statements of vraag om de statements vooraf een keer goed te lezen. Gebruik de voorbereiding sessie vooral om vragen te beantwoorden. Neem de medewerkers mee in de principes van een audit. Geef ze de ruimte om open en transparant te zijn in de beantwoording maar zorg er ook voor dat ze ook reëel en volledig zijn.

Maak een lijst van de te interviewen medewerkers en stem met hen en de auditor af wanneer met ze gesproken wordt. Maak bij voorkeur vooraf afspraken in de agenda's, zodat deze op tijd vastliggen. Medewerkers kunnen hier dan rekening mee houden. Natuurlijk moet dit ook goed worden afgestemd met de auditor. Het is beter een interview af te zeggen omdat de auditor de informatie al heeft gevonden dan op het laatste moment nog een interview in de drukke agenda's te krijgen.

De auditor voert de interviews waarschijnlijk veelal digitaal uit. Zorg dat je bij het interview in een rustige omgeving zit. Denk vooraf na over eventuele bewijslast. Hoe kun je aantonen dat je een maatregel al dan niet uitvoert? Welke ondersteunende documenten heb je daarvoor beschikbaar? Bij voorkeur heb je deze documentatie ook als bewijslast opgenomen in TrustBound.

2.2 Aanmaken audit programma in TrustBound

Om de audit te kunnen uitvoeren moeten er een aantal zaken in TrustBound worden klaargezet. Een audit programma moet door de instelling opgezet en aangemaakt worden. Hierbij wordt de externe auditor opgevoerd. Ook wordt toegang gegeven tot deze omgeving. Volg hiervoor de stappen in bijlage 1, Handleiding audit module in TrustBound.

2.3 Opvoeren kroonjuwelen

Om de kroonjuwelen te kunnen beoordelen in de audit moeten deze vooraf zijn opgevoerd als bedrijfsmiddel in TrustBound. In stap 2 in bijlage 1 leggen we uit hoe je dat doet.

2.4 Activeren beheersmaatregelen

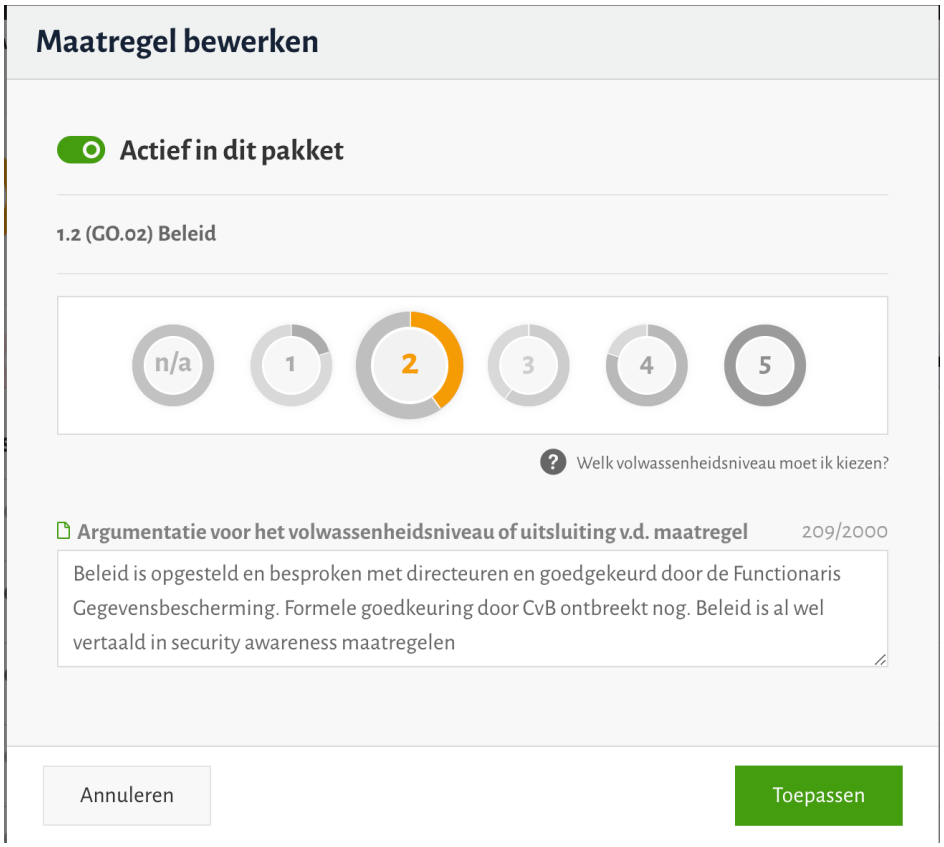
Zorg ervoor dat de maatregelen van het geconstateerde volwassenheidsniveau geactiveerd zijn in het werkpakket. Dan kan de auditor ze beoordelen in de audit. Het is ook goed om de beheersmaatregel met het eerstvolgende volwassenheidsniveau te activeren. Daar kun je dan opschrijven wat je op dit niveau al wel gerealiseerd hebt en je kunt aangeven wat je nog moet realiseren.

2.5 Opvoeren bewijslast per maatregel

Het is niet voldoende om alleen de volwassenheidsscore op te nemen. Per statement en per beheersmaatregel moet eventuele bewijslast (in tekst als toelichting of ondersteund door documenten of schermafbeeldingen) opgenomen zijn. Doe dit in TrustBound. Zorg dat je zowel de argumentatie invult (op statementniveau) als ook de toelichting op de beheersmaatregel van het door jou gekozen volwassenheidsniveau. Het is ook aan te raden om ook het volgende volwassenheidsniveau al te belichten, wat is er al gerealiseerd en wat moet er nog gebeuren om het volgende niveau te halen. De acties die nog uitgevoerd moeten worden om het volgende niveau te halen kun je in TrustBound opvoeren als “Taak” en deze taak kun je toewijzen aan een eigenaar. Als je uiteindelijk alle taken op deze wijze opvoert, heb je eigenlijk je IBP-plan en roadmap gecreëerd en ben je gestructureerd op weg naar het eerstvolgende volwassenheidsniveau.

Maak in een eigen Teams omgeving een kanaal aan met ‘Bewijslast’ en werk met linkjes in TrustBound om de bewijslast aan een maatregel te koppelen. De auditor moet dan ook toegang krijgen tot de Teams omgeving (en dan specifiek het kanaal met Bewijslast). De auditor kan hierdoor op afstand al veel werk doen en heeft dan wellicht minder tijd nodig om mensen uit de instelling te interviewen. Let op! Kijk goed naar de benodigde rechten op de Teams omgeving. Controleer of het mogelijk is om “gasten” of “externen” toegang te geven tot jouw Teams omgeving. Bij sommige instellingen is dit op Office 365 niveau afgeschermd. Ga in dat geval in overleg met de beheerder van Teams om te kijken of voor dit specifieke geval een uitzondering gemaakt kan worden. Mocht dit echt niet lukken is het alternatief om de bewijslast te uploaden in Trustbound zelf.

Voorbeeld: Als je statement “GO.02 Beleid” op volwassenheidsniveau 2 hebt gewaardeerd (omdat het beleid nog niet formeel is goedgekeurd door het College van Bestuur) kun je als argumentatie in TrustBound het volgende plaatsen: “*Beleid is opgesteld en besproken met directeuren en goedgekeurd door de Functionaris Gegevensbescherming. Formele goedkeuring door CvB ontbreekt nog. Beleid is al wel vertaald in security awareness maatregelen*”.

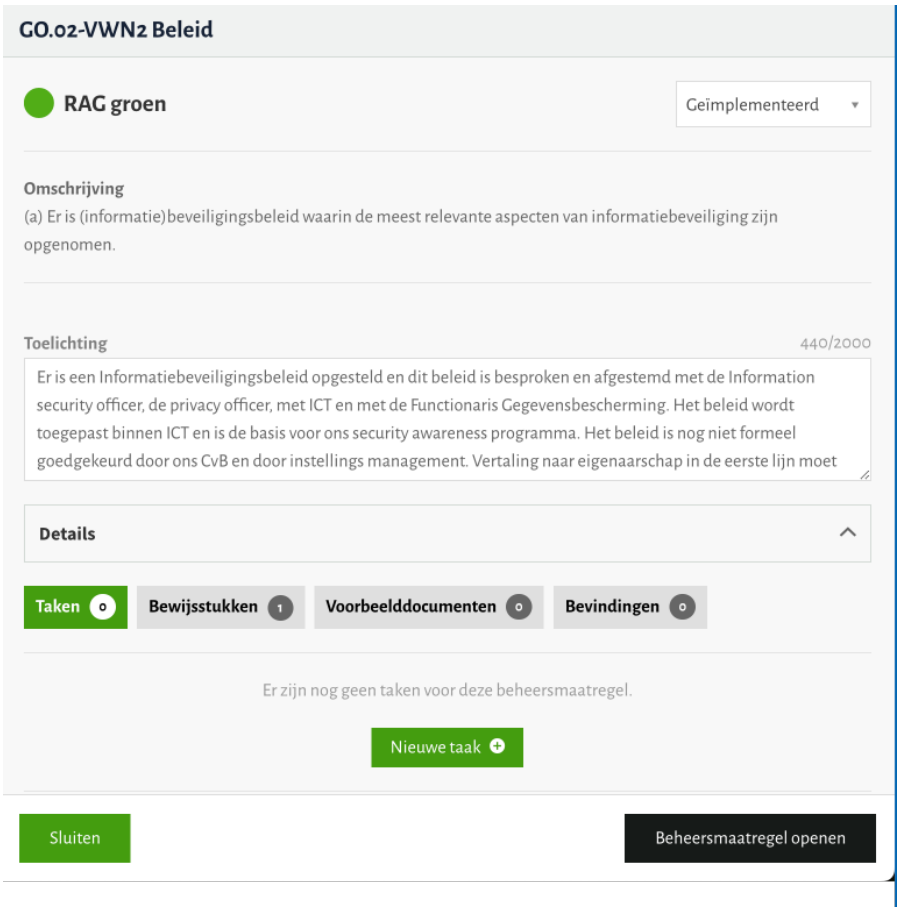


Vervolgens ga je naar de beheersmaatregel van het statement op niveau 2, GO.02-VWN2 Beleid. Hier beschrijf je de toelichting nog iets specifieker. Je probeert hier antwoord te geven op de gestelde voorwaarde in de beheersmaatregel, in dit geval:

"(a) Er is (informatie)beveiligingsbeleid waarin de meest relevante aspecten van informatiebeveiliging zijn opgenomen."

In de toelichting kun je dan opnemen: "Er is een informatiebeveiligingsbeleid opgesteld en dit beleid is besproken en afgestemd met de Information security officer, de privacy officer, met ICT en met de Functionaris Gegevensbescherming. Het beleid wordt toegepast binnen ICT en is de basis voor ons security awareness programma. Het beleid is nog niet formeel goedgekeurd door ons CvB en door instellingsmanagement. Vertaling naar eigenaarschap in de eerste lijn moet nog beter."

Tenslotte zou je in de beheersmaatregel op niveau 3 dan opvoeren: "Beleid moet formeel goedgekeurd worden door het CvB en het management. Tevens moet de borging in de eerste lijn beter om volledig eigenaarschap te krijgen bij het instellingsmanagement".



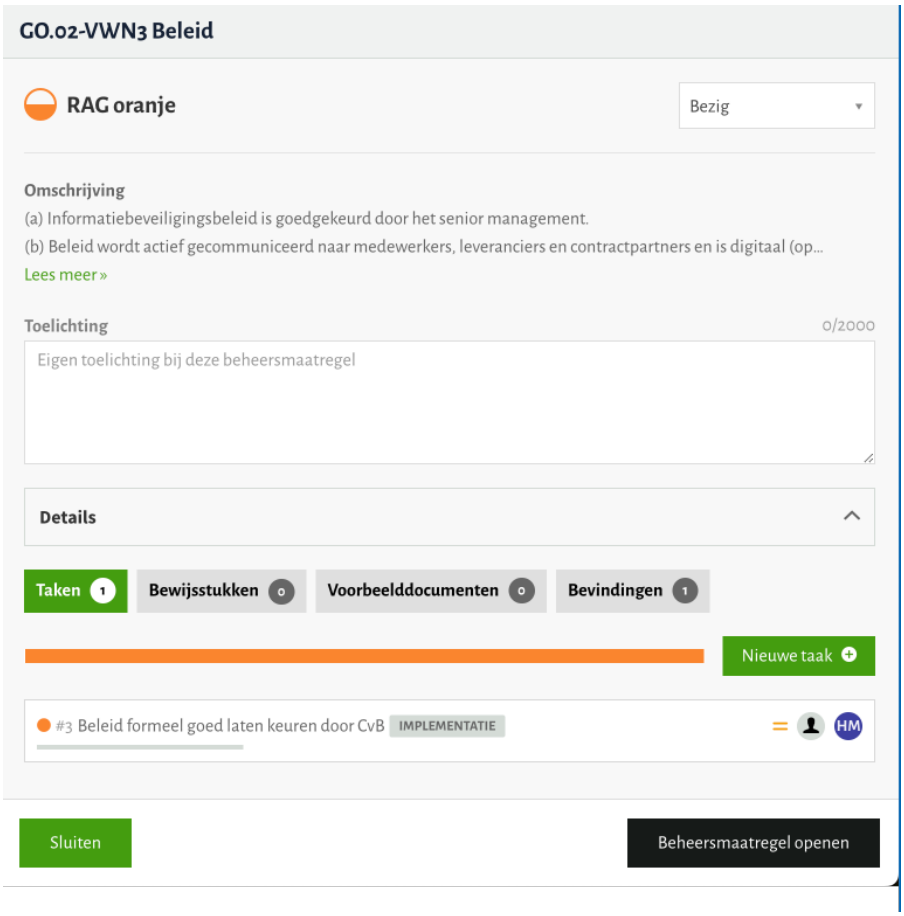
Tenslotte voeg je in de tab ‘Bewijsstukken’ een linkje toe naar het genoemde Informatiebeveiligingsbeleid en zet je de betreffende beheersmaatregel op “Geïmplementeerd”. Zo heb je voor de auditor toegelicht waarom jij denkt dat het genoemde volwassenheidsniveau terecht is gekozen. De auditor controleert en beoordeelt dit. Let op: Dit moet voor elk statement gedaan worden!

Dit is best veel werk. Maar door dit zo te doen gaat TrustBound je echt helpen om ‘in control’ te komen daar waar het gaat om je cyber-volwassenheid en kun je eenvoudiger verantwoording afleggen aan management en bestuur.

2.6 Taken toevoegen aan beheersmaatregelen

Tenslotte kun je in TrustBound taken opvoeren, die beschrijven wat er nog nodig is om het gewenste volwassenheidsniveau te behalen. Op deze wijze vormen alle taken samen het plan of de roadmap die nodig is om het geambieerde volwassenheidsniveau te behalen.

In het geval van statement GO.02 Beleid uit het voorbeeld, voeg je een taak toe aan de beheersmaatregel op volwassenheidsniveau 3; GO.02-VWN3 Beleid. Bijvoorbeeld een taak om het beleid formeel goed te laten keuren door het College van Bestuur van de instelling.

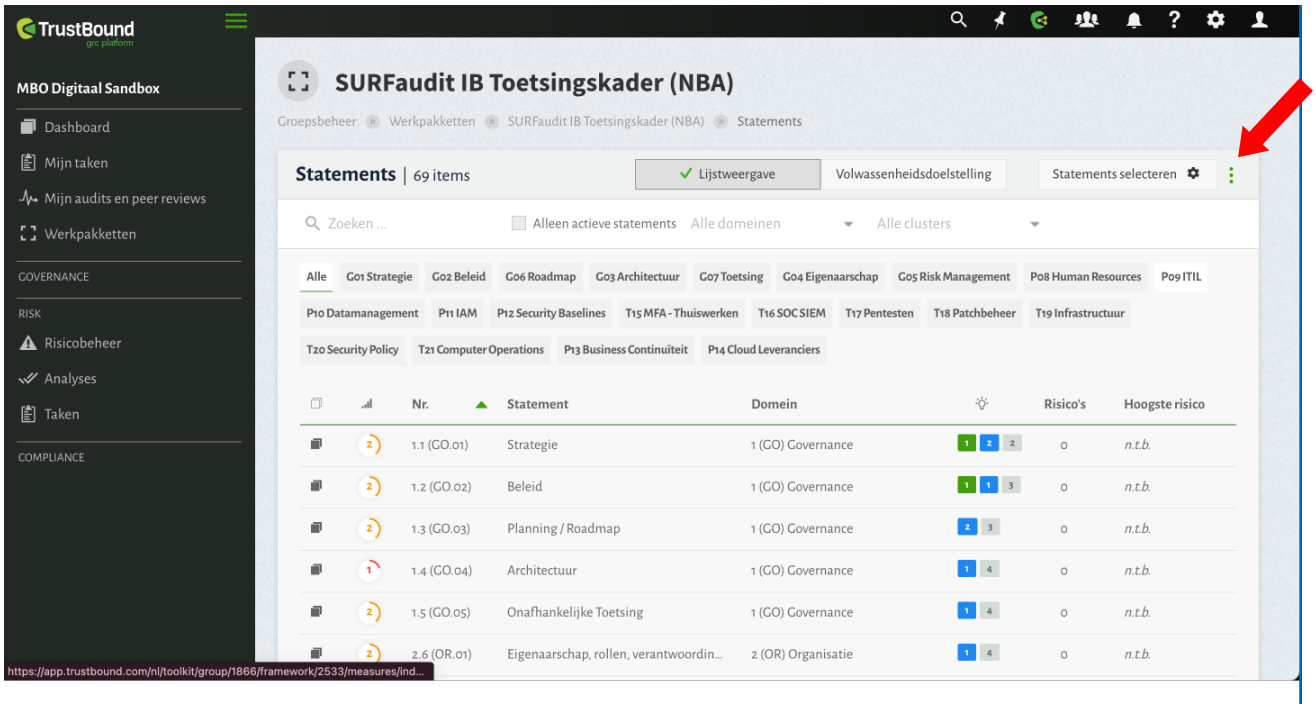


Hier staat de beheersmaatregel nog op “Bezig”, om aan te geven dat we dit niveau nog niet halen.

2.7 Statements exporteren voor de auditor

Om het voor de auditor makkelijk te maken is het mogelijk om alle statements, inclusief de bijbehorende geschreven argumentatie te exporteren in een Excelbestand. De auditor zal daar ook om vragen. Dit helpt de auditor om overzicht te krijgen en minder rond te hoeven klikken in TrustBound.

Je maakt de export op het overzicht scherm van alle statements. Onder de 3 puntjes aan de rechterbovenkant zit de optie om te exporteren. Vink de optie om beheersmaatregelen mee te exporteren aan. Deel deze export met de auditor op het moment dat je als instelling klaar bent met het beschrijven van de argumentatie en het opvoeren van de bewijslast.



3 Onderbouwen van het Toetsingskader

In dit hoofdstuk gaan we de belangrijkste statements uit het toetsingskader langs en delen we de ervaring van de diverse instellingen bij het juist onderbouwen en beargumenteren van een statement. We hanteren de nummering en benaming van de domeinen uit het SURF audit Toetsingskader informatiebeveiliging. Bij het kopje 'te leveren bewijs' worden handreikingen gegeven over hetgeen aan documenten in TrustBound moet worden vastgelegd. Ons credo is we willen "Aantoonbaar in Control" zijn, maar het moet wel werkbaar en uitlegbaar zijn! Dit hoofdstuk zal dan ook groeien en regelmatig aangepast worden.

3.1 Governance

In het aandachtsgebied governance zitten de NBA domeinen "governance", "organisatie" en "risicomanagement".

3.1.1 Strategie

Bij het statement over strategie (GO.01) gaat het vooral om het kunnen leggen van een link tussen de instellingsstrategie en de strategie van de instelling op het gebied van informatiebeveiliging en privacy (IB&P). Bijvoorbeeld in de instellingsstrategie wordt gesproken over een "veilige leeromgeving", daar kun je dan in je IBP beleid naar verwijzen en vertalen in de juiste informatiebeveiliging en privacy beleidsmaatregelen.

Het is niet nodig om een apart document voor je strategie op te stellen, maar zorg dat je het duidelijk in je IBP beleid opneemt.

Te leveren bewijs:

- Beschreven instellingsstrategie met adressering van, of link naar, informatiebeveiliging en privacy
- Goedkeuring strategie van senior management (als onderdeel van het IBP-beleid en/of vastlegging in MT stukken)
- Strategie is beschikbaar op website van de instelling
- IBP-strategie is beschikbaar voor medewerkers, studenten en leveranciers.

3.1.2 Beleid

Het doel van het IBP beleid (GO.02) is om kaders te geven hoe je vormgeeft aan informatieveiligheid. Hierbij wordt meestal gerefereerd naar het NBA toetsingskader met de genoemde domeinen.

Zorg ervoor dat je IBP beleid actueel is en niet ouder is dan 3 jaar. Zorg ervoor dat het verantwoordelijk management jaarlijks een eventuele herijking van het beleid bespreekt. Neem in het beleid een duidelijke verwijzing op naar de goedkeuring en ondersteuning vanuit het bestuur. Dit kun je bijvoorbeeld doen door in het begin als voorwoord een verklaring op te nemen en die ook te laten ondertekenen door je bestuurder.

Veel wordt in het NBA model gesproken over senior management. Wat ons betreft is senior management niet standaard het CvB. Zorg dat je goed definieert en afspreekt op welk niveau een bepaald (beleids-) stuk goedgekeurd mag en kan worden. Dit is veelal afhankelijk van het mandaat wat de manager heeft. Bijvoorbeeld, het lijkt ons prima dat een IT manager de beleidsstukken over technische weerbaarheid goed keurt, daarvoor hoef je niet perse naar het CvB. Ga daar dus slim mee om in je instelling.

Voor communicatie naar medewerkers en studenten kun je vooral gebruik maken van de intranet omgevingen van de instelling. Zorg verder voor een goede uitwerking naar specifiek beleid en gedragscodes van de instelling. Ook moet er een duidelijke link zijn met een security en privacy bewustwordingscampagne. De principes en uitgangspunten uit het beleid kun je opnemen in je awareness programma.

Tot slot is het ook belangrijk dat het beleid wordt meegenomen in de wijzigingen binnen je instelling. Dus bij aanschaf van nieuwe software zitten de beleidsprincipes opgenomen in de uitgangspunten van een eventuele aanbesteding. Zorg er ook voor dat in de standaard contracten of inkoopvoorwaarden een security en privacy paragraaf is opgenomen. Daarmee betrek je de businesspartners en leveranciers bij het IBP beleid.

Te leveren bewijs:
- Beschreven beleid over informatiebeveiliging en privacy (IBP)
- Goedkeuring beleid van senior management (in document zelf en/of vastlegging in MT stukken)
- Gedragscodes van de instelling
- Beschrijving programma voor veiligheidsbewustzijn (awareness programma)
- Het IBP-beleid is beschikbaar op intranet van de instelling
- Opname van IBP-paragraaf in inkoopvoorwaarden of in contracten met derden (gerelateerd aan ketenbeheer)
- Bij eventuele aanbestedingen wordt verwezen naar het IB&P beleid van de instelling, met daarin de verwachting dat een leverancier kan voldoen aan de relevante onderdelen van het IBP-beleid
- Periodieke herijking van het beleid (vastlegging in MT stukken en/of datering in beleidsdocument)

3.1.3 Planning/Roadmap

Onder het statement planning & roadmap (GO.03) wordt vooral gekeken of er planmatig gewerkt wordt aan het structureel verbeteren van de volwassenheid op het gebied van informatiebeveiliging en privacy.

Vaak is het voldoende om een jaarplan te hebben beschreven met daarin de belangrijkste acties op het gebied van IB&P. Neem daarbij de ambitie om volwassenheid 3 te halen als richting en destilleer op basis daarvan de uit te voeren acties (risicogebaseerd). Vaak kosten acties meer tijd dan het huidige jaar, waardoor je een roadmap krijgt voor de acties in opvolgende jaren als een meerjarenplanning. Wil je dit goed borgen, zorg er dan voor dat er een connectie te maken is met je architectuur (zie statement Architectuur) en zorg ervoor dat ook de benodigde middelen (geld, resources) opgenomen zijn in het plan, evenals de eigenaren van de benoemde acties.

Te leveren bewijs:
- Beschreven jaarplan/roadmap IB&P met concrete acties en benodigde middelen
- Jaarplan/roadmap IB&P is besproken en geaccordeerd door senior management (vastlegging in MT stukken)
- Tussentijdse periodieke rapportage over voortgang van de in het jaarplan benoemde acties
- Jaarlijkse herijking van het jaarplan/roadmap (vastlegging in MT stukken, datering jaarplan/roadmap IB&P in versiehistorie)

3.1.4 Architectuur

Bij dit statement wordt gekeken of de instelling zijn initiatieven baseert op een vooraf vastgestelde architectuur (GO.04). Als instelling kun je daarvoor een referentiearchitectuur gebruiken. Binnen de MBO-sector gebruiken we daarvoor de MORA. Zorg ervoor dat ergens in je beleid is vastgesteld dat je de MORA gebruikt als referentiearchitectuur.

Natuurlijk is het ook belangrijk dat bij alle nieuwe ontwikkelingen deze referentiearchitectuur ook daadwerkelijk gebruikt wordt (door een informatiemanager) in bijvoorbeeld een meerjarenplan voor digitalisering.

Te leveren bewijs:

- Beleid, waarin beschreven staat dat MORA als referentiearchitectuur wordt gebruikt
- Indien beschikbaar: architectuurdocumenten met vastlegging IST en SOLL situatie
- Indien beschikbaar: roadmap met activiteiten om van IST naar SOLL situatie te komen
- Vastlegging van besluitvorming over nieuwe ontwikkelingen, waarin ook aan de onderhavige architectuur getoetst is (beslisdocumenten en/of MT stukken)

3.1.5 Onafhankelijke toetsing

Onder onafhankelijke toetsing (GO.05) kun je de uitgevoerde zelfassessments opnemen en eventueel uitgevoerde interne audits. Daarnaast kun je verwijzen naar de externe audits zoals die uitgevoerd worden door Deloitte en eventueel de verplichte jaarrekening controle. Belangrijk is ook om aan te tonen dat de periodieke toetsing gedeeld is met het senior management (in rapportages of verslaglegging).

Je kunt ook denken aan de jaarrekening controle. Daar wordt vrijwel altijd ook gevraagd naar de staat van de ICT en specifiek naar de staat van informatiebeveiliging.

Te leveren bewijs:

- Beschrijving van 3 lines model (onderdeel Beleid IBP)
- Auditplan: welke audits zijn wanneer in komend jaar gepland (onderdeel jaarplan)
- Rapportage over de resultaten audit en opvolging zijn besproken met senior management (MT stukken)

3.1.6 Verantwoordingsinformatie

Dit is een statement (GO.06) uit het nieuwe toetsingskader (NBA 3.0), dit statement is nog geen onderdeel van de huidige audit. Maar dit statement is naar onze mening wel belangrijk om borging te realiseren in de instelling, daarom nemen we hem nu wel mee in deze handreiking. Het is goed om vanuit de tweede lijn periodiek verantwoording af te leggen aan de bestuurder en het management. Denk daarbij over terugkoppeling van dreigingen en risico's tot en met het rapporteren over beveiligingsincidenten en datalekken. Zorg dat deze rapportage onderdeel zijn of worden van de reguliere rapportage structuur.

Te leveren bewijs:

- Rapportagestructuur voor IB&P met benoeming eigenaren
- Periodieke rapportages IB&P (bijlage(n) MT stukken)

3.1.7 Eigenaarschap, rollen, verantwoording en verantwoordelijkheid

De statements over organisatie gaan vooral over eigenaarschap in de organisatie (OR.01 en OR.02). Veelal wordt dit onderdeel ook geadresseerd in het IB&P beleid in de vorm van het beschrijven van het 3-lines model, met eveneens de belegging van de rollen ISO, auditor en FG.

Eigenaarschap is eigenlijk niet de juiste term, zeker juridisch niet. Het gaat eigenlijk om verantwoordelijkheid. Belangrijk hierbij is om te onderkennen dat verantwoordelijkheden op het juiste niveau zijn belegd. Hierbij worden de termen Accountable en Responsible uit de RA(S)CI gebruikt.

- ➔ Accountable: eindverantwoordelijk en aanspreekbaar
- ➔ Responsible: verantwoordelijk voor de uitvoering

In een beleidsstuk hierover is het goed om op hoofdniveau de A en de R uit het RA(S)CI model op te nemen en dit stuk ook te bespreken met de genoemde verantwoordelijken. In dit gesprek leg je uit wat de verantwoordelijkheid precies inhoudt en wat je van de verantwoordelijke verwacht. Uiteindelijk stel je een RA(S)CI model op met de verantwoordelijkheden, dit model kun je opnemen in een beleidsstuk (bijvoorbeeld in een bijlage) en het beleidsstuk laat je goedkeuren door het verantwoordelijk management (in dit geval bij voorkeur het College van bestuur).

Uiteindelijk moet er een cultuur ontstaan waarbij op alle lagen in de instelling de verantwoordelijkheid voor het thema Informatiebeveiliging en Privacy gevoeld wordt (intrinsiek). Het veranderen van een cultuur kost veel tijd en vraagt een lange adem van ons als IBP professionals. Maak bijvoorbeeld een rondje langs alle directeuren en vraag ze concreet hoe je ze kunt helpen. Zorg dat je steun hebt van je CvB hierbij (daar begint de cultuurverandering).

In dit domein wordt ook gesproken over functiescheiding. Daarbij is het goed om de kernapplicaties als eerste voor ogen te houden. Zijn binnen de kernapplicaties de cruciale functies van elkaar gescheiden in verantwoordelijkheden? Bijvoorbeeld in de financiele administratie, in de HR administratie en in de studentenadministratie. Daar liggen de grootste potentiële risico's.
Denk ook aan de IT functies. Bijvoorbeeld: wie deelt de rechten uit, is er een goede scheiding tussen ontwikkelaars en beheerders? En ten slotte binnen beheer: is er een scheiding tussen regulier beheer en de systeemadministratie beheerders (met hoge rechten).

De verantwoordelijkheid en autoriteit met betrekking tot IBP dient duidelijk te zijn belegd in de organisatie. Dit omvat het identificeren van de personen en/of commissies die verantwoordelijk zijn voor het toezicht op IBP en het beoordelen van hun effectiviteit. Een duidelijke lijn van verantwoordelijkheid en rapportage moet bestaan en de betrokkenen beschikken over de nodige bevoegdheden en middelen om hun taken effectief uit te voeren.

De hoogste leidinggevenden (het bestuur of de directie) moeten voldoende betrokken zijn bij IBP. Het is cruciaal dat de hoogste leidinggevenden niet alleen betrokken zijn, maar ook dat zij actief bijdragen aan het formuleren en uitvoeren van het IB&P beleid en een voorbeeldrol vervullen. Daarbij is sectorale betrokkenheid, deelname OZON en periodiek overleg een vereiste.

Te leveren bewijs:

- Vastlegging van toewijzing rollen risico en security management (HRM functieprofielen, vaststelling in MT stukken)
- Vastlegging functiescheiding (in eerste instantie voor de kernapplicaties)
- RA(S)CI tabel om verantwoordelijkheden vast te leggen
- Verslag van/terugkoppeling over sectorale betrokkenheid, deelname OZON en periodiek overleg.

3.1.8 Risicomanagement

Bij risicomanagement (RM.01, RM.02, RM.03) is het vooral belangrijk om te kijken naar de risico's op het gebied van informatiebeveiliging en privacy (risicoinventarisatie). Zijn deze risico's goed in

beeld? Worden er frequent risicoanalyses gehouden? Zijn er duidelijke eigenaren aan te wijzen voor risico's en voelen die zich ook eigenaar van een risico? Zijn de risico's ook meegenomen in het jaarplan/roadmap IB&P?

Daarbij is het gestructureerd opvolgen van risico's belangrijk: na inventarisatie, ook analyse en opvolging door mitigerende maatregelen. Vanuit de tweede lijn heb je de verantwoordelijkheid om regelmatig eigenaren aan te spreken op de voortgang van het nemen van mitigerende maatregelen. Bij SURF is een Risico management toolkit beschikbaar, met goede tips hoe je een risicobeoordeling kunt uitvoeren.

In de praktijk kun je gebruik maken van het SURF dreigingsbeeld als uitgangspunt en is het belangrijk om van daaruit je strategische IB&P risico's te definieren en vast te leggen in een risicoregister. Je kunt als IBP functionaris heel goed beginnen met deze risico's zonder dat je risicomanagement voor je gehele organisatie hoeft op te pakken. Ook kun je de risico's uit de DPIA's en de BIV classificaties in je eigen risico register opnemen (inclusief opvolging).

Het risicomanagementproces binnen de organisatie moet beschreven zijn, met daarin aandacht voor identificatie, beoordeling en beheren van de risico's. Hoe vindt de systematische aanpak plaats voor het uitvoeren van risicobeoordelingen en worden deze beoordelingen regelmatig bijgewerkt om nieuwe of gewijzigde risico's te reflecteren? Ook moet de risicobereidheid van de instelling besproken worden met het verantwoordelijk management. Welke risico's is men bereid te lopen en welke absoluut niet?

De methoden en tools die worden gebruikt voor het risicomanagement, moeten adequaat zijn voor de aard en de complexiteit van de risico's die de organisatie loopt. De criteria voor risicoclassificatie en de procedures voor het vaststellen van risicobereidheid en risicotolerantie zijn afgestemd op de organisatie. Een proactieve en reactieve risicobeheerstrategie is aantoonbaar.

Het continu verbeteringsproces voor risicomanagement moet aantoonbaar zijn ingeregeld. Is er een mechanisme voor het evalueren van de effectiviteit van risicomanagementmaatregelen en het doorvoeren van verbeteringen waar nodig? Lessons learned worden verzameld en toegepast om het risicomanagementproces te versterken en de organisatie beter voor te bereiden op toekomstige risico's.

Te leveren bewijs:

- Beschreven risicomanagementproces met systematische aanpak risicobeoordeling vanuit optiek van de CISO
- Periodieke rapportage over (rest)risico's en voortgang van de geselecteerde maatregelen (bijlagen MT stukken)
- Het risicoregister (op termijn liefst instellingsbreed i.s.m. concerncontroller)
- Het vastleggen van afwijkingen als risico acceptatie, inclusief expliciete goedkeuring van het verantwoordelijk management
- Periodieke evaluatie van het proces en de risico's

3.2 Processen

Het aandachtsgebied processen bestaat uit de domeinen "personeelsmanagement", "configuration management", "incident/problem management", "change management", "datamanagement", "identity- &ccess management", "fysieke beveiliging", "bedrijfscontinuiteitsbeheer" en "ketenbeheer".

3.2.1 Personeelsmanagement

Bij personeelsmanagement (HR.01, HR.02, HR.03, HR.04, HR.05, HR.06) begint het met de standaard HR processen, zoals werving en selectie van personeel, in- en uitdienst procedures en een goed en gestructureerd personeelsbeleid met lange termijn personeelsplanning. Als dit op orde is, dan is het belangrijk om te controleren of deze HR-procedures goed toegepast en bewaakt worden door het management van de instelling.

Een aantal standaard belangrijke controles die je kunt uitvoeren is de indienst- en uitdienstprocedures en de koppeling met een instellingsaccount. Bij indienst is een vorm van screening van het personeel belangrijk, zeker bij personeel op kritische posities in de instelling (bijvoorbeeld beheerders met hoge rechten).

Bij de indienstname is bij voorkeur aandacht tijdens de onboarding voor informatiebeveilging en privacy. Kijk op kritische plekken ook goed naar afhankelijkheid van personeel. Is er nagedacht bij eventuele uitval of vervanging van deze kritische plekken?

Personeelsbeleid is een integraal onderdeel van de bedrijfsvoering; specifiek voor informatiebeveiliging zijn er de volgende aandachtspunten die aangetoond moeten kunnen worden:

- Zijn er procedures voor het **werven en selecteren** van personeel met VOG en screenings- en achtergrondcontroles voor nieuwe medewerkers, vooral voor diegene die toegang hebben tot gevoelige informatie?
- Is er een **inwerkprogramma** bij indiensttreding waarbij informatiebeveiliging ook geadresseerd wordt; ook specifiek voor bepaalde cruciale functies?
- Is er een **doorgroeipad** voor functies met eisen aan opleidingen/kennis/ervaring?
- Zijn er **effectieve trainingen** en **bewustwordingsprogramma's** die medewerkers informeren over hun verantwoordelijkheden op het gebied van informatiebeveiliging.
    - Worden deze trainingen regelmatig bijgewerkt?
    - Zijn alle medewerkers verplicht om deel te nemen aan deze programma's?
    - Wordt de effectiviteit van deze trainingen gemeten?
- Zijn er procedures voor **personeelsmutaties** zoals de overgang van medewerkers naar andere functies, promoties en beëindigingen van dienstverbanden, met betrekking tot het aanpassen van toegangsniveaus en het intrekken van rechten wanneer een medewerker de organisatie verlaat of haar/zijn rol verandert. Dit voorkomt ongeautoriseerde toegang tot systemen en informatie.
- Zijn er procedures voor **disciplinaire maatregelen** inzake ongepaste gedragingen of beveiligingsincidenten die medewerkers betreffen en hoe deze worden toegepast bij schendingen van beveiligingsbeleid?

Te leveren bewijs:

- Beschreven HR proces met aandacht voor werving en selectie, doorgroeimogelijkheden ook specifiek aangaande IB&P
- Inventarisatie van sleutelposities en opvang/achtervang mogelijkheden
- Inwerkprogramma (onboarding) met specifieke aandacht voor IBP
- Awareness en trainingsprogramma
- Autorisatiematrix en versiebeheer daarop
- IBP-beleid: Gedragscodes, incl. disciplinaire maatregelen

3.2.2 Service management processen

Een basisaanpak voor de servicemanagement processen is ITIL. Hierbij is het vooral de IT afdeling die deze processen goed ingeregeld moet hebben. Controleer of van configuration management, incident management, problem management en change management procesbeschrijvingen zijn en op welke wijze deze processen geadministreerd worden (bijvoorbeeld in Topdesk of een ander soortgelijk servicemanagement systeem).

Configuration management (CO.01, CO.02) wordt door veel instellingen onderschat, maar kun je beschouwen als het fundament onder goed IT Beheer. Immers als je niet goed weet wat je hebt aan IT middelen kun je ze ook niet beveiligen. Dus geef aandacht aan configuration management, dat gaat je enorm helpen om de risico's onder controle te krijgen. Veel beheersoftware heeft scanfunctionaliteit om configuratie items in beeld te brengen, maak daar ook goed gebruik van (denk aan Intune die weet welke werkplekken verbinding maken of aan serverbeheersoftware die weet welke servers er zijn, etc.).

Bij incident management (IM.01, IM.02, IM.03) is het belangrijk om naast de generieke procedures goed te kijken wat er gebeurt met security & privacy incidenten (inclusief doorkijk naar crisismanagement). Worden deze gemeld door de organisatie? Worden ze bij een servicedesk herkent en worden ze tijdig doorgezet naar de juiste specialisten? Dat moet je eerste focus zijn, security en privacy incidenten moeten zo spoedig mogelijk opgemerkt worden en vervolgens adequaat afgehandeld worden. Security en Privacy incidenten moeten ook ge-escaleerd kunnen worden bij grotere impact. Dus een IT crisis organisatie die incidenten met een grote impact oppakken is cruciaal. Zorg ook voor een koppeling met de crisis management organisatie van de instelling. Weet wanneer een incident zich ontwikkeld tot crisis en betrek tijdig het juiste management van de instelling.

Problem management (IM.04) wordt bij veel instellingen niet of nauwelijks gedaan, terwijl dit een proces is wat snel goed op te zetten is en erg belangrijk is om rust in je organisatie te creeren. Een organisatie zonder problem management is als een brandweer die alleen maar de brand blust en geen aandacht besteed aan brand preventie. Zorg dat je regelmatig je incidenten analyseert en bekijkt welke incidenten regelmatig terug komen. Bij deze incidenten zit er blijkbaar structureel iets niet goed en moet je onderzoeken wat de achterliggende oorzaak is van deze incidenten (root cause analyse). Leg deze vast als probleem en beleg de problemen bij een beheerder die tijd mag besteden aan het goed uitzoeken en oplossen van het probleem. Goed problem management (en oplossen van problemen) geeft rust aan je operationeel beheer en is erg belangrijk!

Tot slot is het erg belangrijk om grip te krijgen en te houden op je wijzigingen (CH.01, CH.02, CH.03, CH.04, CH.05, CH.06). Deze wijzigingen moeten worden beoordeeld op IB&P aspecten: de achterdeur moet niet opengezet worden door aanpassingen. Opnieuw, zijn er generieke procedures voor wijzigingen? Wordt de procedure altijd gevolgd? Hoe verwerk je wijzigingen van je leveranciers en van je belangrijkste applicaties. Let ook op het testen! Het is vaak erg ingewikkeld om een volledige test omgeving te hebben voor je gehele keten, maar hoe weet je dan zeker wat de impact is van een wijziging. Wat regel je om dat risico zo klein mogelijk te maken. Denk ook aan de noodprocedures, wanneer je een spoedwijziging moet doorvoeren.

Te leveren bewijs:

- Beschrijving van de processen configuration management (incl. licentiebeheer), incident management, problem management en change management met vastlegging rollen met TBV en escalatieproces.
- Vastlegging van periodieke reviews/ verbeteracties

- Configuration management: audits/reviews inzake configuratievastlegging in CMDB (actueel & volledig)
- Borging in procesbeschrijving(en) dat elke wijziging ook wordt doorgevoerd in de CMDB
- Incident management: specifiek aandacht in procesbeschrijving voor communicatie over IB&P incidenten
- Incident management: documentatie van incidenten (inzicht in service managementtool)
- Change management: wijzigingskalender van afgelopen jaar
- Problem management: documentatie van problemen en known errors (inzicht in service managementtool)
- Change management: documentatie van wijzigingen en testresultaten (inzicht in service managementtool)
- Change management: vastlegging werkwijze met aparte omgevingen OTAP
- Steekproef change management: Graag ontvangen wij alle relevante documentatie van een recente wijziging die is opgeleverd. Denk hierbij aan het opleverplan, acceptatieplan, acceptatiecriteria, autorisatie, overdrachtsdocumentatie, incidenten inclusief opvolging, gemaakte afspraken voor nazorg, evaluaties en managementrapportages.

3.2.3 Fysieke beveiliging

Bij fysieke beveiliging (PH.01, PH.02) draait het vooral om het beschermen van toegang tot je gebouwen en je kritische ruimtes. Daarbij zijn bijvoorbeeld data center ruimtes, je technische ruimtes (MER/SER) en de ruimtes waar mogelijk gevoelige persoonsgegevens liggen extra belangrijk.

Fysieke beveiligingsmaatregelen: welke maatregelen zijn getroffen om de organisatie te beschermen tegen ongeautoriseerde toegang? Met name toegang tot faciliteiten en datacenters zijn van belang om ingeregeld te hebben. Zijn er adequate controle- en toegangsmechanismen, zoals badge-systemen en beveiligingspersoneel?

Beveiligen van kritieke infrastructuren en apparatuur: zijn er maatregelen getroffen om apparatuur en gegevens op een veilige manier te beschermen tegen diefstal, sabotage of andere vormen van fysieke schade. Is de beveiliging van deze assets in overeenstemming met de risicoanalyse van de organisatie.

Nood- en evacuatieplannen: zijn er procedures en plannen voor noodsituaties en evacuaties, en worden deze regelmatig getest en bijgewerkt? Dit om ervoor te zorgen dat medewerkers goed voorbereid zijn en dat de continuïteit van de operaties wordt gewaarborgd in geval van een fysieke beveiligingsincident.

Beheer van bezoekers en leveranciers: zijn er duidelijk gedefinieerde procedures voor het identificeren, registreren en controleren van bezoekers en externe medewerkers die toegang hebben tot de faciliteiten en systemen.

Te leveren bewijs:

- Vastlegging fysieke beveiligingsmaatregelen & maatregelen diefstal/sabotage
- Vastlegging nood- en evacuatieplannen
- Procedures beheer van bezoekers en externe medewerkers

3.2.4 Identity & Access management

Bij Identity & Access management (IM.01, IM.02, IM.03, IM.04, IM.05) is het belangrijk om voor alle rollen in je organisatie de juiste rechten toe te wijzen. Medewerkers hebben de rechten die ze nodig hebben om hun werk goed uit te voeren. Maar het uitgangsprincipe is de juiste rechten, niet meer

maar ook niet minder. Van het goed beheren van je identeiten tot het beheren van je rollen en rechten.

Beleid en procedures voor toegang tot systemen en informatie: hoe worden identiteiten gecontroleerd en is er een duidelijke controle over wie toegang heeft tot welke systemen en gegevens. Is er een formeel proces voor het toewijzen, wijzigen en intrekken van toegangsrechten.

Authenticatie en autorisatie: worden sterke authenticatiemethoden toegepast, zoals multi-factor authenticatie, en zijn toegangsniveaus afgestemd op de rol en verantwoordelijkheden van medewerkers? Dit om te waarborgen dat alleen bevoegde personen toegang hebben tot gevoelige informatie.

Monitoring en auditing van toegangsactiviteiten: zijn er mechanismen om toegangspogingen en gebruik van systemen te volgen en te loggen. Hoe worden deze logs beoordeeld en gebruikt voor het detecteren van ongebruikelijke of ongeautoriseerde activiteiten.

Periodieke herziening van toegangsrechten: worden er regelmatige controles uitgevoerd om te verifiëren of de toegewezen toegangsrechten nog steeds gepast zijn en worden er aanpassingen gemaakt wanneer medewerkers hun rol of functie veranderen of de organisatie verlaten?

Te leveren bewijs:
- Beschreven beleid en procedures identity & Access Management (IAM)
- Autorisatiematrix per applicatie (rollen, rechten, beleidsregels)
- Procedures inzake monitoring en auditing van IAM
- Envelop NOOD procedure
- Overzicht superusers
- Periodieke verslagen inzake bevinidingen monitoring en toegang IAM

3.2.5 Data management

Bij data management (DM.01, DM.02, DM.03, DM.04, DM.05, DM.06) gaat het vooral om het proces van classificeren van je belangrijkste systemen. Probeer zoveel mogelijk terug te vallen op de classificatie uit de MORA, maar maak dat wel inzichtelijk hoe je dat doet. En bepaal wat de maatregelen zijn die je afhankelijk van je classificatie moet nemen (beschikbaarheid, integriteit en vertrouwelijkheid). Beschouw de uitkomsten van een BIV classificatie als een risicoanalyse en leg de resultaten vast in het risicoregister.

De maatregelen die bij een classificatie horen, dienen te worden vastgelegd. Denk hierbij aan versleuteling van gegevens, gegevensvalidatie en -verificatie.

Tot slot het onderwerp gegevensretentie en -vernietiging: zijn er duidelijke richtlijnen voor hoe lang gegevens worden bewaard en hoe verouderde of niet meer benodigde gegevens veilig worden vernietigd om privacyrisico's en juridische complicaties te voorkomen.

Te leveren bewijs:
- Beschreven beleid data management
- Eigenaar van data is benoemd en vastgelegd
- Classificatie data (BIV)
- Risicoregister
- Beschreven maatregelen zoals versleuteling en procedure gegevensvalidatie en -verificatie
- Vastlegging van afspraken en procedures over gegevensretentie en -vernietiging

3.2.6 Bedrijfscontinuiteitsmanagement

Bedrijfscontinuiteit (BC.01, BC.02, BC.03, BC.04, BC.05) gaat over het borgen van de beschikbaarheid van de belangrijkste bedrijfsprocessen van de instelling. Hier is het belangrijk om goed te kijken wat je vanuit IB&P in scope neemt. Ook is hier de koppeling met crisismanagement van je organisatie erg belangrijk. En vergeet niet regelmatig te oefenen en te testen!

Belangrijk is om in eerste instantie goed in beeld te hebben wat je meest kritische bedrijfsprocessen zijn. Daarvoor is het belangrijk om een BIA (Business Impact Assessment) op je processen uit te voeren. Met de resultaten van de BIA kun je vervolgens een business continuiteitsplan opstellen.

Is er een formeel bedrijfscontinuïteitsplan voor je IT omgeving (BCP) dat gedocumenteerd, getest en onderhouden wordt? Biedt dit een uitgebreid overzicht van hoe de organisatie haar kritieke processen kan voortzetten bij een IT verstoring? Zijn er scenario's gedefinieerd voor cyber security incidenten en of voor privacy incidenten. Hoe moet je dan acteren? Wat is de koppeling met het crisis management team en proces?

Bijwerken en testen van het BCP: wordt het plan regelmatig herzien en getest om te verzekeren dat het actueel en effectief blijft (OZON). Is er een gestructureerd proces voor het verwerken van feedback en het doorvoeren van verbeteringen op basis van de testresultaten en veranderende omstandigheden.

Te leveren bewijs:

- Beschreven bedrijfscontinuteitsplan (BCP)
- Afweging bedrijfscontinuiteit (BIA of soortgelijk)
- Bewustwordingscampagne/trainingen (periodiek)
- Testrapport BCP met bevindingen en verbeteracties (jaarlijks)

3.2.7 Ketenbeheer of leveranciersmanagement

Bij ketenbeheer of leveranciersmanagement (SC.01, SC.02, SC.03, SC.04) gaat het vooral over het beheersen van je externe leveranciers. Heb je goede afspraken gemaakt en liggen die vast in contracten. Weet je welke risisco's er spelen bij de leverancier die van toepassing kunnen zijn op jou als instelling?

Is er beleid en procedures voor het afnemen van diensten bij leveranciers en externe partners? Zijn er duidelijke criteria en processen voor het selecteren en evalueren van leveranciers op basis van hun informatiebeveiligingspraktijken?

Contractuele afspraken met leveranciers en partners: bevatten de contracten en SLA's specifieke eisen voor informatiebeveiliging en worden deze eisen nageleefd? Dit omvat ook het evalueren van de procedures voor het monitoren en beoordelen van de prestaties van leveranciers op het gebied van beveiliging. Periodiek wordt gerapporteerd over de geleverde dienstverlening en worden verbeteracties met elkaar besproken.

Hoe worden releases van de leveranciers ontvangen, getest en geimplementeerd. Wat heeft de leverancier zelf geregeld op het gebied van IB&P? Is er eenThird Party Mededeling (TPM)? Is er een ISO27001 certificering, een ISAE3402 type 2 verklaring of een SOC2 verklaring? Heb je die wel eens opgevraagd en weet je wat de status is?

Beëindigen van contracten en het beëindigen van relaties met leveranciers: is er een duidelijk proces voor het veilig beëindigen van toegang en het verwijderen van gegevens of apparatuur die aan leveranciers zijn verstrekt? Dit om te voorkomen dat vertrouwelijke informatie of assets onbeveiligd achterblijven na beëindiging van de samenwerking.

Te leveren bewijs:
- Beschreven contract management/ service level management proces/beleid met meetbare service levels
- Getekende contracten en/of Service Level Agreement's (SLA) (met jaarlijkse review)
- Periodieke Service Level Rapportages,
- Indien van toepassing: certificeringen vanuit leverancier
- Risicobespreking en -vastlegging met leveranciers (verslaglegging)
- Exitclausule opgenomen in contracten

3.2.8 Security baselines

Voor de invulling van de security baselines (SM.01) is het uitgangspunt om de SURF Security Baselines te volgen (gebaseerd op CIS controls). Als instelling kun je eventueel ook je eigen set aan baselines definieren, zorg er dan wel voor dat die goed vastliggen in het beleid en goed gekeurd zijn door het verantwoordelijk management.

Zijn er formele **security baselines** gedefinieerd voor alle relevante systemen en netwerken binnen de organisatie, en worden ze regelmatig bijgewerkt om nieuwe dreigingen en kwetsbaarheden te adresseren?
Toepassing en handhaving van de baselines: zijn er procedures voor het configureren en implementeren van systemen en voldoen deze procedures aan de vastgestelde baselines. Zijn er mechanismen voor het controleren van naleving en het identificeren van afwijkingen van de vastgestelde normen.
Training en bewustwording met betrekking tot de security baselines: zijn medewerkers en systeembeheerders voldoende opgeleid over de vereisten van de security baselines en het belang van naleving. Zijn er voldoende documentatie en richtlijnen beschikbaar om hen te ondersteunen bij het naleven van de baselines.
Herzien en aanpassen van de baselines: vinden er regelmatige reviews plaats om te verzekeren dat de baselines actueel blijven en relevant zijn voor de bestaande bedreigingen en kwetsbaarheden. Worden wijzigingen in de baselines goed beheerd en gecommuniceerd naar de betrokkenen.

Te leveren bewijs:
- Beschreven security baseline en procedure hoe hiermee om te gaan (incl. toepassing en handhaving)
- Awareness programma/ opleiding/ rapportage
- Vastlegging van reviews baselines met verbeteracties

3.3 Technische weerbaarheid

Het aandachtsgebied technische weerbaarheid onderkend onder meer de volgende onderwerpen:
- Multi Factor Authenticatie/Thuiswerken: betreft veilig van buitenaf inloggen.
- SOC SIEM: betreft 24 x 7 detectie van het netwerk (en respons).
- Pentesten: betreft periodiek gericht testen op kwetsbaarheden in het netwerk.
- Patchbeheer: betreft structureel bijwerken van de software (beveiligingsupdates).
- Infrastructuur: betreft beschikbaarheid van het netwerk en systemen.

- Security Policy: betreft inrichting technische beveiliging van het netwerk en systemen.
- Computer Operations: betreft automatische IT-processen (bijvoorbeeld back-up & restore).

De bovenstaande onderwerpen zullen veelal worden uitgevoerd (of onder regie worden uitbesteed) door de IT-afdeling. Hierover moet in begrijpelijke taal gerapporteerd worden aan het College van Bestuur. Bij deze rapportage hoort ook een financieel overzicht, zodat duidelijk is welke kosten/investeringen vereist zijn voor welke veiligheidsmaatregelen.

De onderwerpen Multi Factor Authenticatie/Thuiswerken, SOC SIEM en Security Policy vallen onder het zogenaamde Zero Trust principe.

3.3.1 Authenticatiemechanismes

Hierbij (SM.02) is het vooral belangrijk dat er een goed wachtwoordbeleid is opgesteld, met voldoende lange wachtwoorden. Zowel met regels voor normale accounts als voor accounts met hoge rechten.
Daarnaast is het belangrijk dat er duidelijke beleidsregels zijn voor het toepassen van Multi Factor Autorisatie (MFA). Minimaal is het inloggen op je kroonjuwelen beschermd door MFA.

3.3.2 Threat en Vulnarability management

Heb je als instelling een proces ingericht waarbij je regelmatig de nieuwe dreigingen beoordeelt en onderzoekt of er nieuwe kwetsbaarheden (SM.07) zijn gevonden. Dit vertaald zich in het tijdig bijwerken van kritieke applicaties en infrastructuur.

Scannen, beoordelen en categoriseren van kwetsbaarheden: welke tools voor kwetsbaarheidsscans worden ingezet en is er een gestructureerde aanpak voor het beheren van ontdekte kwetsbaarheden?
Prioritering en mitigatie van kwetsbaarheden: is er een duidelijk proces voor het prioriteren van kwetsbaarheden op basis van hun impact en waarschijnlijkheid. Zijn er procedures voor het implementeren van patches of andere maatregelen om kwetsbaarheden te verhelpen, en of deze maatregelen tijdig worden doorgevoerd.
Rapportage en communicatie over kwetsbaarheden: is er een effectief systeem voor het rapporteren van kwetsbaarheden aan de relevante teams en belanghebbenden. Is communicatie over kwetsbaarheden duidelijk en wordt er follow-up gedaan om te verzekeren dat alle kwetsbaarheden worden aangepakt?
Evalueren en herzien van het kwetsbaarhedenbeheerproces: Vinden er regelmatig evaluaties plaats om de effectiviteit van het kwetsbaarhedenmanagementsysteem te beoordelen en verbeteringen aan te brengen op basis van lessen geleerd en veranderende omstandigheden?

Te leveren bewijs:

- Beschreven kwetsbaarhedenbeheerproces inclusief scannen, beoordelen, categoriseren, prioriteren en rapporteren (incl. samenwerking met CSIRT)
- Tool(s) voor scannen, beoordelen en categoriseren kwetsbaarheden
- Periodieke rapportage over kwetsbaarheden
- Vastlegging van periodieke evaluatie met verbeteracties.

3.3.3 Patchmanagement

Het doel van dit patchmanagementbeleid (SM.06) is om de beveiligingsrisico's te minimaliseren door ervoor te zorgen dat software en systemen regelmatig en tijdig worden bijgewerkt met de nieuwste patches en updates. Installeer de patches of beveiligingsoplossingen niet te laat. Dan kan

dat ertoe leiden dat kwaadwillende personen bekende kwetsbaarheden misbruiken om ongeautoriseerde toegang tot de it-infrastructuur van je instelling te verkrijgen.

Denk aan de volgende onderdelen voor patch management beleid:
- **Patch Identificatie**: Regelmatige monitoring van patchmeldingen en kwetsbaarheden om potentiële risico's te identificeren.
- **Patch Prioriteit**: Kwetsbaarheden worden beoordeeld op basis van impact en urgentie, en patches worden geprioriteerd voor implementatie.
- **Testen en Implementatie**: Patches worden eerst getest in een gecontroleerde omgeving voordat ze worden uitgerold naar productiesystemen.
- **Documentatie**: Alle patchmanagementactiviteiten, inclusief identificatie, prioritisatie en implementatie van patches, worden gedocumenteerd voor toekomstige referentie en auditdoeleinden.
- **Rapportage en Monitoring**: Regelmatige rapportage over de patchstatus en monitoring van openstaande kwetsbaarheden om ervoor te zorgen dat systemen up-to-date blijven.

3.3.4 Testen van, inspectie van en toezicht op beveiliging

Worden er regelmatig security test uitgevoerd binnen de instelling (SM.05) en wordt er ook gezorgd voor adequate afhandeling van gevonden zwakheden.
Formele richtlijnen voor het uitvoeren van verschillende soorten tests moeten zijn vastgelegd. Voldoen deze richtlijnen aan erkende standaarden en worden ze regelmatig bijgewerkt.
- Penetratietests: periodiek uitvoeren van gecontroleerde aanvallen op systemen en netwerken om kwetsbaarheden te identificeren en te verhelpen.
- Kwetsbaarhedenscans: regelmatig scannen van systemen en netwerken op bekende kwetsbaarheden en configuratiefouten.
- Beveiligingstests: uitvoeren van tests zoals vulnerability assessments en red teaming om de effectiviteit van de beveiligingsmaatregelen te evalueren en te verbeteren.

Frequentie en scope van de uitgevoerde tests: Worden er regelmatige tests uitgevoerd volgens een vastgesteld schema en omvatten deze tests alle relevante systemen en netwerken. Is de scope van de tests adequaat om alle kritieke kwetsbaarheden en risico's te identificeren.
Documentatie en rapportage van de testresultaten: Worden er gedetailleerde rapportages gemaakt van de testresultaten, inclusief bevindingen en aanbevelingen voor verbeteringen. Worden deze rapportages effectief gecommuniceerd naar de betrokken teams en is er een gestructureerd proces voor het opvolgen van de bevindingen.
Herzien en verbeteren van de security testpraktijken: Vinden er periodieke reviews en evaluaties plaats om de effectiviteit van de security testing te beoordelen en aanpassingen te maken op basis van nieuwe dreigingen en kwetsbaarheden.

Te leveren bewijs:
- Beschreven richtlijnen voor testen in kader van beveiliging
- Vastlegging van de testresultaten
- Vastlegging van periodieke evaluaties met verbeteracties

3.3.5 Logging, Monitoring en Opvolging

Is er een **formeel beleid** dat bepaalt welke gegevens moeten worden gelogd, hoe logs moeten worden opgeslagen en hoe lange tijd logs worden bewaard (SM.04). Voldoet dit beleid aan wettelijke en regelgevende vereisten en wordt het effectief nageleefd.
- Monitoring: Continu monitoren van netwerken en systemen voor verdachte activiteiten en anomalieën die kunnen wijzen op een beveiligingsincident.

- Logging: Gedetailleerde registratie van systeem- en netwerkactiviteiten om verdachte gebeurtenissen te identificeren en te analyseren.

Implementatie van **logging en monitoring systemen**: wordt er adequaat gelogd op alle relevante systemen en applicaties en worden de logs verzameld en opgeslagen op een veilige manier. Zijn er monitoringtools geïmplementeerd om afwijkende of verdachte activiteiten te detecteren en te rapporteren.
Analyse en review van logs: worden logs regelmatig gecontroleerd en geanalyseerd op mogelijke beveiligingsincidenten. Zijn er procedures voor het onderzoeken van verdachte activiteiten en het ondernemen van actie op basis van de bevindingen uit de loganalyse.
Beheren en beschermen van loggegevens: Worden logs beschermd tegen ongeautoriseerde toegang en manipulatie, en zijn er procedures voor het veilig verwijderen of archiveren van logs wanneer ze niet langer nodig zijn. Zijn er mechanismen voor het testen van de effectiviteit van de logging en monitoringprocessen.

Te leveren bewijs:
- Formeel beleid en procedures monitoring en logging
- Ingerichte tool SOC SIEM, betreft 24 x 7 detectie van het netwerk (en respons)
- Periodieke rapportage inzake monitoring en logging

3.3.6 Beschikbaarheid en bescherming van infrastructuur
Te denken valt aan de volgende maatregelen (SM.08):
- **Firewalls en netwerkbeveiliging**: Implementeren van firewalls, intrusion detection/prevention systems (IDS/IPS) en andere netwerkbeveiligingsmaatregelen om ongeautoriseerde toegang en aanvallen te voorkomen.
- **Endpoint-beveiliging**: Beveiliging van eindgebruikersapparaten zoals computers, smartphones en servers door middel van antivirussoftware, anti-malware tools en endpoint detection and response (EDR) oplossingen.
- **Patchmanagement**: Regelmatig bijwerken van software en systemen met de nieuwste beveiligingspatches om bekende kwetsbaarheden te verhelpen.
- **Technologische Innovaties:** Bijblijven met de nieuwste ontwikkelingen en innovaties op het gebied van cybersecurity om te zorgen voor een up-to-date beveiligingsstrategie.

Te leveren bewijs:
- Vastlegging/documentatie van preventieve beveiligingsmaatregelen i.s.m. CSIRT.

3.3.7 Operationele procedures
Deze procedures zijn bedoelt om de efficientie en de effectiviteit van de geautomatiseerde IT-taken te verbeteren (OP.01, OP.02). Besteed speciale aandacht aan het zoveel mogelijk centraliseren van deze operationele taken en zorg ervoor dat deze taken beschreven en gedocumenteerd zijn in zogenaamde runbooks. Bij afwijkingen van de operationele procedures worden er triggers en/of rapportages verstuurd naar het verantwoordelijk IT personeel. Besteed speciale aandacht aan de procedures rondom backups en restore processen en besteed aandacht aan capaciteit management op de operationele IT omgeving.

Te leveren bewijs:
- Procedures voor (geautomatiseerde) job scheduling
- Run Books voor productietaken m.b.t. beheer en controle op interfaces voor de meest relevante systemen.

- Back-up en recovery beleid.
- Procedures voor back-up en herstel van systemen, applicaties, data en documentatie.
- Procedurebeschrijving van het testen van back-ups.
- Capaciteit- en prestatiemanagementbeleid
- Procedure voor het meten, analyseren en bewaken van performance metrics.

4 Na afloop van de audit

In dit hoofdstuk gaan we in op wat je kunt doen na afloop van de audit. Op welke wijze gebruik je de rapportage en zorg je ervoor dat jouw organisatie de uitkomsten van de audit positief kan gebruiken. De auditor zorgt ervoor dat de observaties worden ingebracht in Trustbound als bevinding. Hoe kun je die bevindingen gebruiken en inzetten in de gewenste groei naar volwassenheid. En tenslotte is het verstandig om een aantal zaken uit Trustbound op te ruimen.

4.1 Rapportage

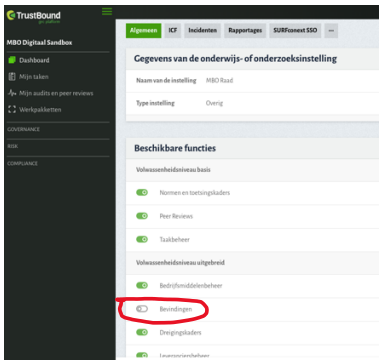
De auditor levert een uitgebreide rapportage op met daarin observaties en aanbevelingen. Deze rapportage kun je als instelling gebruiken om de volgende stappen in groei te maken. Het geeft goed aan waar je moet verbeteren en vooral op welke wijze je dat ook kunt laten zien en aantonen.

De rapportage kent ook een management samenvatting en het is aan te raden om de belangrijkste bevindingen te delen en te bespreken met jouw senior management (het Cvb, de verantwoordelijke directeuren en managers). Geef aan dat er een 2de audit aankomt binnen anderhalf jaar en dat je hulp nodig hebt om samen de groei in volwassenheid te maken. Deze rapportage kan helpen om het commitment en de betrokkenheid van de bestuurder te verhogen.

4.2 Bevindingen

We hebben afgesproken met de auditor dat naast de rapportage de bevindingen als “kans voor verbetering” opgevoerd gaan worden in Trustbound. Je kunt de bevindingen vinden onder de uitgevoerde Audits, zowel op de generieke statements als op de specifieke voor de kern systemen.

Er is ook een optie in de instellingen om de bevindingen module aan te zetten, zodat je alle bevindingen onder elkaar ziet staan. Je zet de “Bevindingen” administratie aan onder voorkeuren (het tandwieltje rechts boven aan het Trustbound scherm). Kies voor Algemeen en dan voor Bewerken. Het scherm ziet er dan ongeveer uit zoals hieronder, en selecteer dan “Bevindingen” (zet het schuifje naar “groen”) en dan Opslaan.



4.3 User management

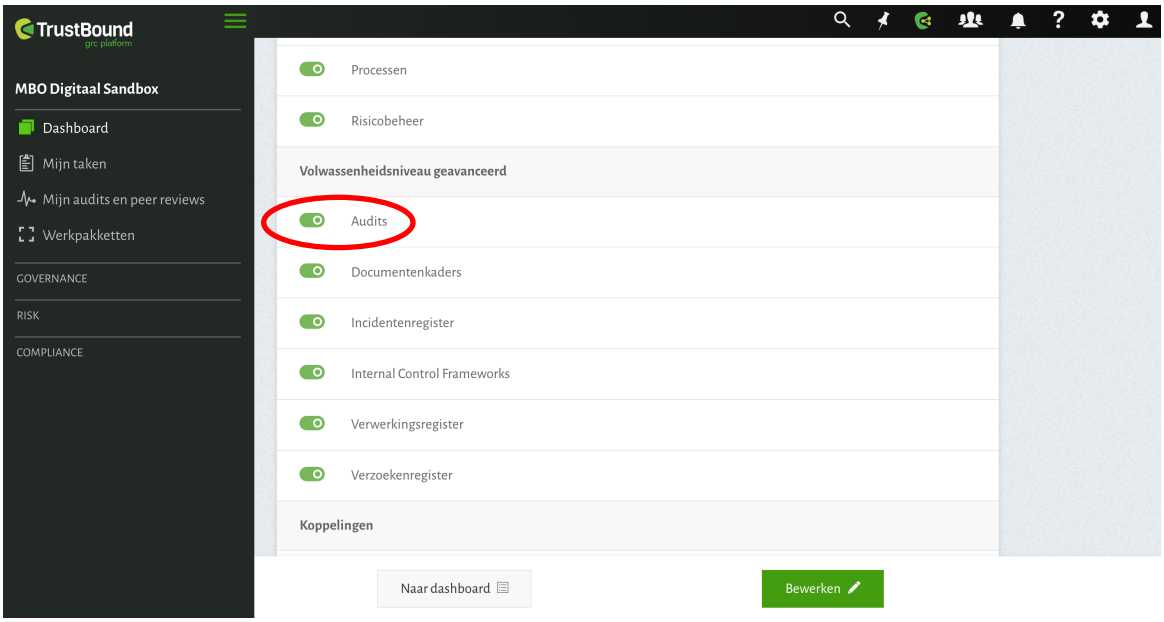
Als de audit is afgerond, en de auditoren hebben de bevindingen opgevoerd in Trustbound is het belangrijk om in ieder geval de rechten van de auditors in te trekken onder “Personen en Gebruikers”.

Bijlage 1 Handleiding Auditmodule in TrustBound

Stap 1: audit module activeren
Controleer of de auditmodule is aangevinkt.

Ga als beheerder van TrustBound naar het tandwieltje rechts bovenaan (voorkeuren).

Kies voor “Algemeen” en controleer of de functie “Audits” aanstaat. De functie audits zit onder het kopje “Volwassenheid geavanceerd”. Kies eerst voor “Bewerken” en selecteer dan de “Audits'' functie.



Stap 2: Opvoeren bedrijfsmiddelen
Om de kroonjuwelen in scope te nemen, is het noodzakelijk vooraf de bedrijfsmiddelen op te voeren in TrustBound. Dit doe je in twee stappen:

- Opvoeren van de leverancier van het kroonjuweel (als Externe organisatie)
- Opvoeren van het kroonjuweel als Bedrijfsmiddel

Als voorbeeld gaan we AFAS HR gebruiken. Als eerste gaan we naar Externe organisatie (onder “Governance”) en selecter je “nieuwe externe organisatie”.

Vul de velden als volgt in:

- Selecteer “Deze organisatie is alleen beschikbaar op centraal niveau”
- Voer de bedrijfsnaam in (bijvoorbeeld AFAS BV). Tip: naast de bedrijfsnaam zit een knop “TrustBound Smarthub”. TrustBound heeft al veel leveranciers opgevoerd, en die kun je daar opvragen. Dat scheelt veel intikwerk!
- Als de leverancier niet in Smarthub staat, voer dan in eerste instantie alleen de naam in, dat is voldoende.

Dan ga je het bedrijfsmiddel opvoeren. Opnieuw onder “Governance”, selecteer je “Bedrijfsmiddelen” en vervolgens voor “Nieuw”, Bedrijfsmiddel aanmaken in deze organisatie.
Vul de velden als volgt in:

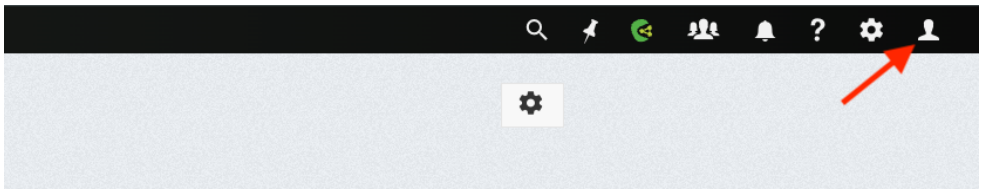
- Selecteer “Dit bedrijfsmiddel is allen beschikbaar op centraal niveau”

- Voor de naam van het product of systeem in. Tip: ook hier kun je veel bedrijfsmiddelen al selecteren via de TrustBound Smarthub. Veel velden zijn al standaard ingevuld, dat is erg handig!
- Kies onder “Leverancier” de zojuist opgevoerde “Externe organisatie”.
- De overige velden zijn ook interessant, maar voor nu nog niet relevant. Laat ze voor nu leeg.

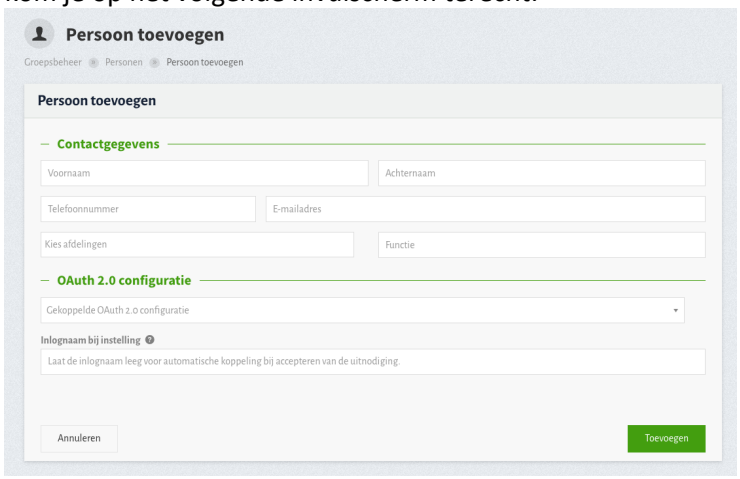
Herhaal dit voor elk kroonjuweel, zodat na deze stap alle kroonjuwelen zijn opgevoerd.

Stap 3: Opvoeren externe auditor als gebruiker
Je krijgt van de auditor doorgegeven welke personen jouw instelling gaan helpen bij het uitvoeren van de audit. Deze personen moeten opgevoerd worden in TrustBound als “gebruiker”.

Dat doe je onder het “poppetje” rechtsboven in het TrustBound scherm, en je kiest daar voor “Personen en Gebruikers”.

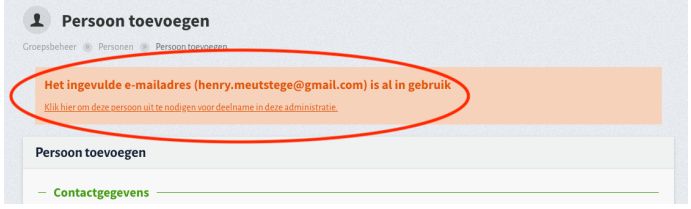


En kies vervolgens voor “Persoon invoegen” en vervolgens voor “Nieuwe persoon toevoegen”. Dan kom je op het volgende invulscherm terecht:



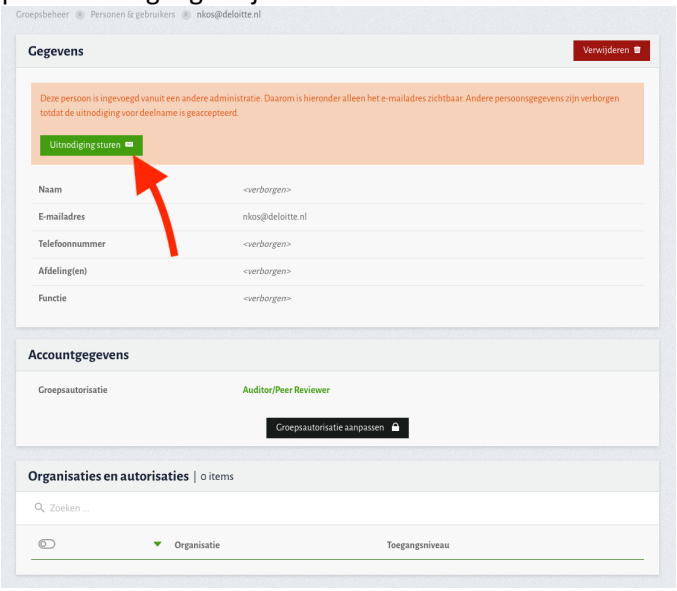
Vul hier de voornaam, achternaam en het e-mailadres in (dat is voldoende) en klik op “Toevoegen”.

Omdat de auditors bij meer instellingen aan het werk zijn krijg je een melding te zien na het opvoeren. Klik vervolgens op de link in de oranje gekleurde tekst.



Je krijgt dan de melding dat de persoon uit een andere administratie is toegevoegd. Geef de persoon de juiste rechten via “instellen groepsautorisaties”. Kies voor de rol “Auditor/Peer reviewer” en klik op “Toepassen”.

Tenslotte kun je de persoon een uitnodiging sturen, en na het bevestigen van de uitnodiging heeft de persoon toegang tot jouw administratie in TrustBound.



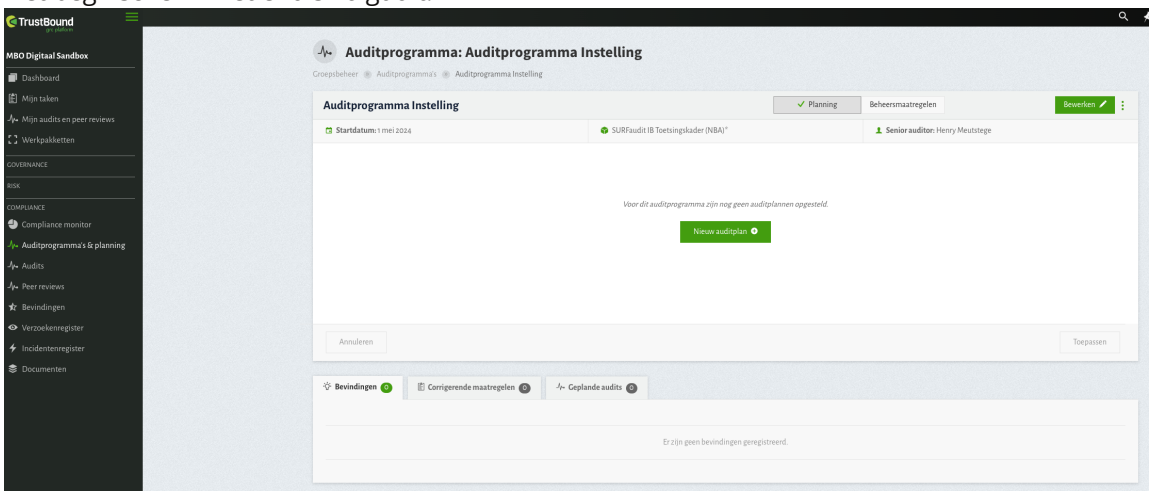
Stap 4: Opvoeren Auditprogramma
Er is vanuit TrustBound een generieke handleiding beschikbaar hoe je de auditmodule in TrustBound gebruikt. Neem deze er eerst bij, en lees hem door. Je vindt deze handleiding hier.

Maak nu voor je instelling een auditprogramma aan.
Vul de velden als volgt in:

- Selecteer dat het auditprogramma op centraal niveau beschikbaar is
- Geef het auditprogramma een titel, bijvoorbeeld “Auditprogramma [instellingsnaam]”
- Sla geauditeerde processen over (laat het leeg)
- Selecteer het SURFaudit IB Toetsingskader (NBA) als norm onder “Welke normen worden geauditeerd?”
- Geef de data op wanneer de audit wordt uitgevoerd, zet dit ruim op want dit bepaald in welke tijdsframe de externe auditor toegang heeft tot jouw TrustBound omgeving. Maar ook weer niet langer dan nodig.
- Vul senior auditor en auditor in. Dit is bij voorkeur het IB&P contactpersoon van de instelling zelf. Beide velden kunnen dezelfde personen zijn, maar je mag ook een collega invullen. Je selecteert uit de lijst van opgevoerde personen in TrustBound.
- Onder Externe auditor kun je de audit partij opvoeren (voor de mbo-instellingen is dat Deloitte).

Stap 5: Toevoegen audit(s)
Je hebt het auditprogramma aangemaakt en we gaan nu twee audits toevoegen. De eerste audit gaat over de generieke beheersmaatregelen, de tweede audit gaat specifiek over de beheersmaatregelen op de kroonjuwelen.

Het beginscherm ziet er als volgt uit:

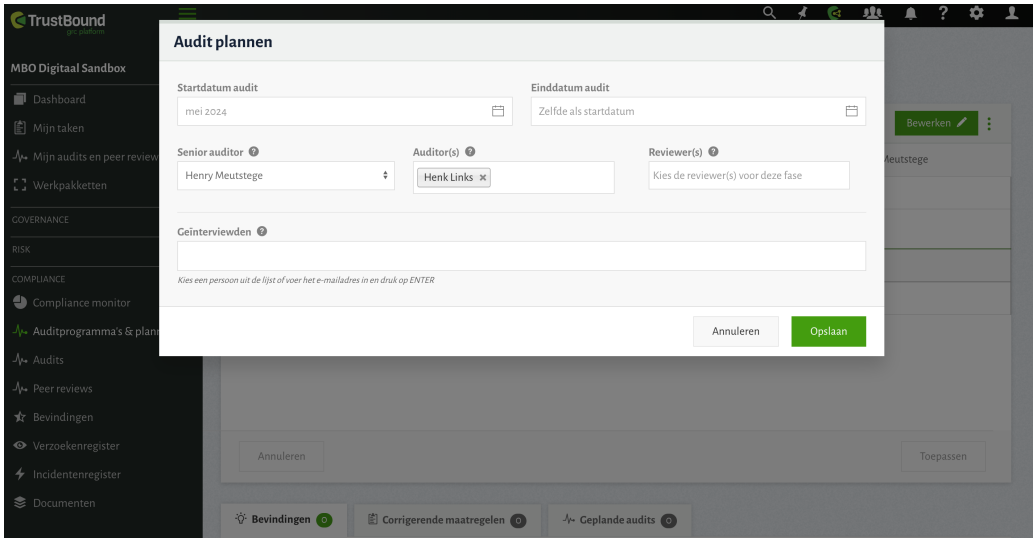


Kies hier voor “Nieuw auditplan”.
Vul de velden als volgt in:

- Naam, geef deze eerste audit bijvoorbeeld “Audit generiek”
- Laat de Senior auditor staan uit het auditprogramma
- Welk type controle wordt uitgevoerd. Kies hier voor conformiteitscontrole
- Welke auditmethoden worden gebruikt. Selecteer document onderzoek, interviews en observeren
- Het doel van de audit is vaststellen welke afwijkingen er zijn ten opzichte van de actuele status in het “werkpakket: SURFaudit IB Toetsingskader (NBA)”

De overige velden kun je voorlopig leeg laten.

We gaan nu de eerste audit “Plannen”. Klik op de rij van de aangemaakte eerste audit. Dan verschijnt het volgende venster:



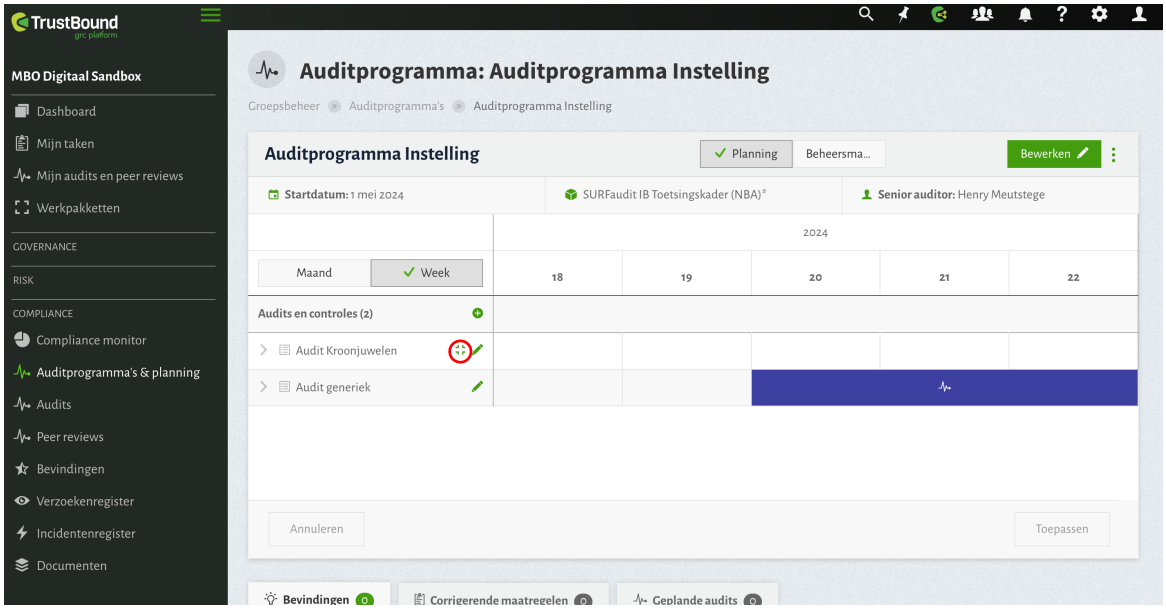
- Vul hier de startdatum en de einddatum in van de audit. Voeg onder Auditor(s) de externe auditor toe. **Let op**, deze moet je wel eerst opgevoerd hebben onder “Personen en Gebruikers”. De externe auditor heeft de autorisatie rol “Auditor/ Peer reviewer”. Daarmee kan de externe auditor alleen de audit module gebruiken.
- Laat vooralsnog de lijst met te interviewen personen leeg.

Je gaat nu de tweede audit toevoegen, deze audit is bedoelt om de kroonjuwelen in scope te nemen van het auditprogramma. In het scherm Auditprogramma staat nu 1 audit opgevoerd, klik op het + teken achter “Audits en controles”, daarmee voer je de tweede audit op als auditplan.
Vul de velden als volgt in:

- Naam, geef deze tweede audit bijvoorbeeld de naam “Audit Kroonjuwelen”
- Laat de Senior auditor staan uit het auditprogramma
- Welk type controle wordt uitgevoerd, kies hier voor conformiteitscontrole
- Welke auditmethoden worden gebruikt. Selecteer document onderzoek, interviews en observeren
- Het doel van de audit is vaststellen welke afwijkingen er zijn ten opzichte van de actuele status in het “werkpakket: SURFaudit IB Toetsingskader (NBA)”, maar dan specifiek voor de kroonjuwelen van de instelling.

De overige velden kun je voorlopig leeg laten. Kies voor “Opslaan”.

Let op, nu gaan je eerst de kroonjuwelen toevoegen aan de “Audit Kroonjuwelen”. Het scherm van het auditprogramma zal er ongeveer als volgt uitzien, selecteer de scope door te klikken op het hieronder rood omcirkelde teken.

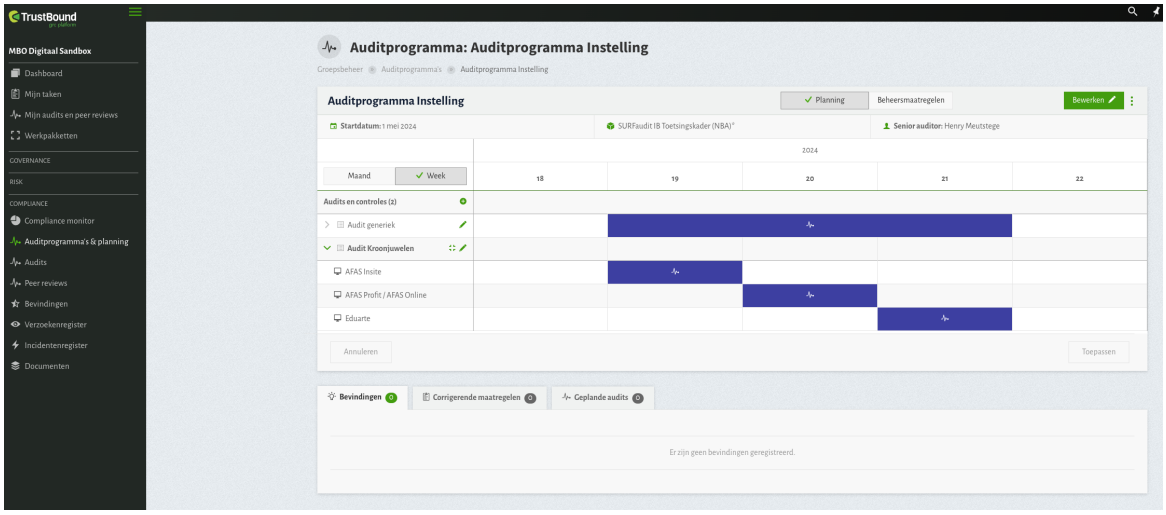


Je krijgt nu een selectie te zien van je opgevoerde “Leveranciers” en de opgevoerde “Bedrijfsmiddelen”. In deze handleiding gaan we er van uit dat de kroonjuwelen (zowel leveranciers als de bedrijfsmiddelen reeds zijn opgevoerd, zo niet moet je dit alsnog eerst doen!). Kies onder het tabje bedrijfsmiddelen de gewenste kroonjuwelen.

In het scherm van het auditprogramma kun je nu “Audit Kroonjuwelen” open klappen en je ziet de geselecteerde “bedrijfsmiddelen”. Maak nu een planning per bedrijfsmiddel aan, selecteer de rij van het eerste bedrijfsmiddel (bijvoorbeeld AFAS Insite) en vul het plannings scherm in voor dat

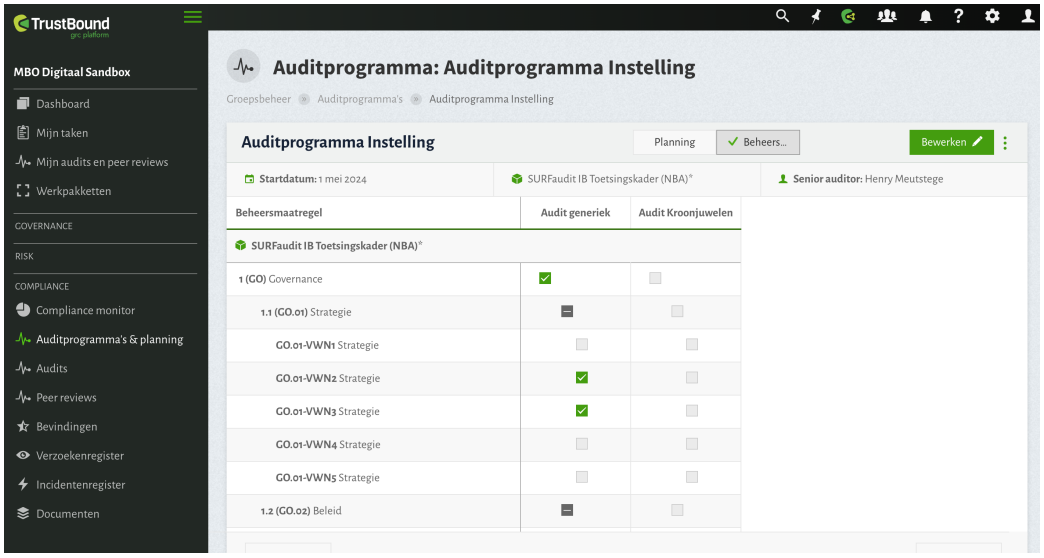
bedrijfsmiddel. Zie ook het eerdere scherm onder “Plannen”. Vul dezelfde gegevens in, en vergeet niet de Externe auditor toe te voegen.
Doe dit vervolgens voor elk “Bedrijfsmiddel”

Als je alles hebt gepland ziet het scherm er als volgt uit:



Stap 6: Selecteren beheersmaatregelen per Audit
Kies in het scherm van het auditprogramma voor “Beheersmaatregelen” (het tabje naast “Planning”). Je gaat nu de te auditen beheersmaatregelen selecteren. Hierbij kies je de beheersmaatregel van het huidige volwassenheidsniveau en het niveau wat je wilt behalen (dus bijvoorbeeld van niveau 2 en van het ambitie niveau 3). Begin met het selecteren van de generieke beheersmaatregelen uit “audit generiek” en vervolgens de specifieke maatregelen onder “Audit kroonjuwelen” (zie ook bijlage 2).

Bevestig de selectie van beheersmaatregelen door op “Toepassen” te klikken.



Bijlage 2 Maatregelen generiek en specifiek voor de kroonjuwelen

NBA-statements uitsplitsen per applicatie

Domeinnr	Domeinnaam	NBA-id	Statement	Generiek	Per applicatie
1	Governance	GO.01	Strategie	X	
		GO.02	Beleid	X	
		GO.03	Planning / Roadmap	X	
		GO.04	Architectuur	X	
		GO.05	Onafhankelijke assurance	X	
2	Organisatie	OR.01	Eigenaarschap, rollen, verantwoording en verantwoordelijkheid	X	
		OR.02	Functiescheiding	X	
3	Risk Management	RM.01	Framework voor Information Risk Management	X	
		RM.02	Risicobeoordeling	X	
		RM.03	Plan voor behandeling en beperking van risico's (inclusief risicoacceptatie)	X	
4	Personeelsbeheer	HR.01	Werving	X	
		HR.02	Certificering, training en scholing	X	
		HR.03	Afhankelijkheid van individuen		X
		HR.04	Verandering of beëindiging van functie		X
		HR.05	Kennisdeling		X
		HR.06	Veiligheidsbewustzijn	X	
5	Configuration Management	CO.01	Identificatie en onderhoud van configuratie-items	X	
		CO.02	Configuratiedatabase en baseline	X	
6	Incident/Problem Management	IM.01	Incident Management		X
		IM.02	Incident escalatie		X
		IM.03	Incidentrespons op (cyber) beveiligingsincidenten		X
		IM.04	Problem Management		X
7	Change Management	CH.01	Normen en procedures voor aanpassingen		X
		CH.02	Impact assessment, prioriteren en autoriseren		X
		CH.03	Noodaanpassingen		X
		CH.04	Testomgeving		X
		CH.05	Testen van aanpassingen		X
		CH.06	Promotie naar productie		X
8	Systeemontwikkeling	SD.01	Methodiek voor veilige softwareontwikkeling en -implementatie	X	
		SD.02	Toegang tot de productieomgeving door ontwikkelaars	X	
		SD.03	Data conversie en/of migratie	X	
9	Datamanagement	DM.01	Data (en systeem) eigenaarschap		X
		DM.02	Classificatie		X
		DM.03	Beveiligingseisen voor datamanagement		X
		DM.04	Inrichting van opslag en retentie		X
		DM.05	Uitwisseling van (gevoelige) gegevens		X
		DM.06	Verwijdering van data		X
10	Identity & Access Management	ID.01	Toegangsrechten		X
		ID.02	Administratie van toegangsrechten		X
		ID.03	Super Users		X
		ID.04	Noodtoegang (envelopprocedure/breek-het-glasprocedure)		X
		ID.05	Periodieke beoordeling van toegangsrechten		X
11	Security Management	SM.01	Security baselines	X	
		SM.02	Authenticatiemechanismes		X
		SM.03	Mobiele apparaten en telewerken	X	
		SM.04	Logging en Monitoring		X
		SM.05	Testen van, inspectie van en toezicht op beveiliging	X	
		SM.06	Patchmanagement	X	
		SM.07	Threat en Vulnerability Management	X	
		SM.08	Beschikbaarheid en bescherming van infrastructuur	X	
		SM.09	Onderhoud van de infrastructuur (inclusief LCM)	X	
		SM.10	Cryptographic Key Management	X	
		SM.11	Network security	X	
		SM.12	Capacity and Performance Management	X	
		SM.13	Bescherming van beveiligingstechnologie	X	
12	Fysieke beveiliging	PH.01	Fysieke beveiligingsmaatregelen	X	
		PH.02	Beheer van fysieke toegangsrechten	X	
13	IT-operatie	OP.01	Job processing	X	
		OP.02	Procedures voor back-up en herstel	X	
		OP.03	Capacity and Performance Management	X	
14	Bedrijfscontinuïteitsmanagement	BC.01	Bedrijfscontinuïteitsplanning	X	
		BC.02	Testen van Disaster recovery	X	
		BC.03	Offsite back-upopslag	X	
		BC.04	Gegevensreplicatie	X	
		BC.05	Crisismanagement	X	
15	Ketenbeheer	SC.01	Service Level Overeenkomst		X
		SC.02	Service Level Management		X
		SC.03	Supplier Risk Management		X
		SC.04	Interne beheersing bij derden		X

Bijlage 3 Eigenaren per statement uit het toetsingskader

Domeinnr	Domeinnaam	NBA-id	Statement	Accountable	Responsible
1	Governance	GO.01	Strategie	CVB	CISO
		GO.02	Beleid	CVB	CISO
		GO.03	Planning / Roadmap	CVB	CISO
		GO.04	Architectuur	CVB	Architect
		GO.05	Onafhankelijke assurance	CVB	Internal Audit
2	Organisatie	OR.01	Eigenaarschap, rollen, verantwoording en verantwoordelijkheid	CVB	Proces eigenaar
		OR.02	Functiescheiding	CVB	Proces eigenaar
3	Risk Management	RM.01	Framework voor Information Risk Management	CVB	Risco manager
		RM.02	Risicobeoordeling	CVB	Proces eigenaar
		RM.03	Plan voor behandeling en beperking van risico's (inclusief risicoacceptatie)	CVB	Proces eigenaar
4	Personeelsbeheer	HR.01	Werving	HR	Proces eigenaar
		HR.02	Certificering, training en scholing	HR	Proces eigenaar
		HR.03	Afhankelijkheid van individuen	HR	Proces eigenaar
		HR.04	Verandering of beëindiging van functie	HR	Proces eigenaar
		HR.05	Kennisdeling	HR	Proces eigenaar
		HR.06	Veiligheidsbewustzijn	HR	CISO
5	Configuration Management	CO.01	Identificatie en onderhoud van configuratie-items	IT	Configuratie manager
		CO.02	Configuratiedatabase en baseline	IT	Configuratie manager
6	Incident/Problem Management	IM.01	Incident Management	IT	Incident manager
		IM.02	Incident escalatie	IT	Incident manager
		IM.03	Incidentrespons op (cyber) beveiligingsincidenten	IT	Incident manager
		IM.04	Problem Management	IT	Incident manager
7	Change Management	CH.01	Normen en procedures voor aanpassingen	IT	Change manager
		CH.02	Impact assessment, prioriteren en autoriseren	IT	Change manager
		CH.03	Noodaanpassingen	IT	Change manager
		CH.04	Testomgeving	IT	Change manager
		CH.05	Testen van aanpassingen	IT	Change manager
		CH.06	Promotie naar productie	IT	Change manager
8	Systeemontwikkeling	SD.01	Methodiek voor veilige softwareontwikkeling en -implementatie	IT	Proces eigenaar
		SD.02	Toegang tot de productieomgeving door ontwikkelaars	IT	Proces eigenaar
		SD.03	Data conversie en/of migratie	IT	Proces eigenaar
9	Datamanagement	DM.01	Data (en systeem) eigenaarschap	Proces eigenaar	Functioneel beheer
		DM.02	Classificatie	Proces eigenaar	Functioneel beheer
		DM.03	Beveiligingseisen voor datamanagement	Proces eigenaar	Functioneel beheer
		DM.04	Inrichting van opslag en retentie	Proces eigenaar	Functioneel beheer
		DM.05	Uitwisseling van (gevoelige) gegevens	Proces eigenaar	Functioneel beheer
		DM.06	Verwijdering van data	Proces eigenaar	Functioneel beheer
10	Identity & Access Management	ID.01	Toegangsrechten	Proces eigenaar	Functioneel beheer
		ID.02	Administratie van toegangsrechten	Proces eigenaar	Functioneel beheer
		ID.03	Super Users	Proces eigenaar	Functioneel beheer
		ID.04	Noodtoegang (envelopprocedure/breek-het-glasprocedure)	Proces eigenaar	Functioneel beheer
		ID.05	Periodieke beoordeling van toegangsrechten	Proces eigenaar	Functioneel beheer
11	Security Management	SM.01	Security baselines	IT	IT Beheer
		SM.02	Authenticatiemechanismes	IT	IT Beheer
		SM.03	Mobiele apparaten en telewerken	IT	IT Beheer
		SM.04	Logging en Monitoring	IT	IT Beheer
		SM.05	Testen van, inspectie van en toezicht op beveiliging	IT	IT Beheer
		SM.06	Patchmanagement	IT	IT Beheer
		SM.07	Threat en Vulnerability Management	IT	IT Beheer
		SM.08	Beschikbaarheid en bescherming van infrastructuur	IT	IT Beheer
		SM.09	Onderhoud van de infrastructuur (inclusief LCM)	IT	IT Beheer
		SM.10	Cryptographic Key Management	IT	IT Beheer
		SM.11	Network security	IT	IT Beheer
		SM.12	Capacity and Performance Management	IT	IT Beheer
		SM.13	Bescherming van beveiligingstechnologie	IT	IT Beheer
12	Fysieke beveiliging	PH.01	Fysieke beveiligingsmaatregelen	Facilitair	IT Beheer
		PH.02	Beheer van fysieke toegangsrechten	Facitlitair	IT Beheer
13	IT-operatie	OP.01	Job processing	IT	IT Beheer
		OP.02	Procedures voor back-up en herstel	IT	IT Beheer
		OP.03	Capacity and Performance Management	IT	IT Beheer
14	Bedrijfscontinuïteitsmanagement	BC.01	Bedrijfscontinuïteitsplanning	CVB	Proces eigenaar
		BC.02	Testen van Disaster recovery	IT	IT Beheer
		BC.03	Offsite back-upopslag	IT	IT Beheer
		BC.04	Gegevensreplicatie	IT	IT Beheer
		BC.05	Crisismanagement	CVB	Proces eigenaar
15	Ketenbeheer	SC.01	Service Level Overeenkomst	Inkoop	Proces eigenaar
		SC.02	Service Level Management	Inkoop	Proces eigenaar
		SC.03	Supplier Risk Management	Inkoop	Proces eigenaar
		SC.04	Interne beheersing bij derden	Inkoop	Proces eigenaar

mbo digitaal

MBO Digitaal is een platform van MBO Raad voor samenwerking aan digitalisering in het mbo. MBO Digitaal werkt samen met alle mbo-instellingen en heeft sterke banden met MBO Voorzieningen, Kennisnet en Surf.

MBO Digitaal
Houttuinlaan 6
3447 GM Woerden

Telefoon *+31 (0) 348 – 75 35 00*
Email *info@mbodigitaal.nl*
Website *mbodigitaal.nl*