



# Boardletter

Gemeente Zutphen  
Boekjaar 2024



Aan het College van  
Burgemeester en Wethouders  
van de gemeente Zutphen  
Postbus 41  
7200 AA ZUTPHEN

**ONDERWERP**  
Board letter 2024

**DATUM**  
11 februari 2025

**KENMERK**  
25098-05972

Geacht college,

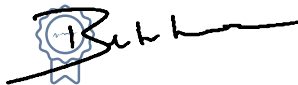
Als onderdeel van de jaarrekeningcontrole van boekjaar 2024 van de gemeente Zutphen rapporteren wij onze bevindingen uit de interim-controle.

In deze boardletter rapporteren wij de bevindingen naar aanleiding van onze controle, de belangrijkste risico's, ons beeld van de interne beheersing en indien van toepassing veranderingen die voor u relevant kunnen zijn. In de bijlage hebben wij een gedetailleerd overzicht opgenomen van onze bevindingen en aanbevelingen.

De bevindingen komen voort uit onze werkzaamheden in het kader van de jaarrekeningcontrole en zijn opgenomen voor zover wij het van belang achten om deze met u te communiceren. De bevindingen en aanbevelingen dienen te worden gelezen als constructieve aanwijzingen voor het college als onderdeel van een continue proces van het veranderen en verbeteren van de beheersing van de organisatie. Wij geven in deze boardletter op hoofdlijnen aan op welke wijze verbeteringen van de administratieve organisatie en de daarin opgenomen maatregelen van interne beheersing kunnen worden gerealiseerd. De gedetailleerde aanbevelingen en oplossingsrichtingen zoals beschreven in de management letter bieden het college handvaten voor de uitwerking.

Deze board letter is door ons opgesteld voor uw informatie en mag niet zonder onze uitdrukkelijke toestemming geheel of gedeeltelijk aan derden ter beschikking worden gesteld. Wij danken u en uw medewerkers voor de samenwerking en zijn graag bereid tot het verstrekken van nadere toelichting.

Met vriendelijke groet,  
Baker Tilly (Netherlands) N.V.



M.C.J.M. Bekker RA

1

# Kwaliteit interne beheersing



## Inleiding

# Kwaliteit van de interne beheersing

Deze boardletter bevat onze bevindingen ten aanzien van de interne beheersing (inclusief de IT-omgeving), die zijn gebaseerd op onze werkzaamheden in het kader van de jaarrekeningcontrole 2024. Deze werkzaamheden zijn dan ook niet gericht op het geven van een oordeel over de interne beheersing van uw organisatie als geheel.

Een goede interne beheersing maakt dat de risico's voor de organisatie beter beheersbaar zijn en de jaarrekeningcontrole effectiever en efficiënter kan plaatsvinden. Vanuit onze natuurlijke adviesfunctie willen wij bijdragen aan de verbetering van de bedrijfsvoering, onder andere door het analyseren van de IT-omgeving en de bedrijfsprocessen. Voorgaande jaren hebben wij onze bevindingen eveneens met u gedeeld. In deze board letter geven wij u een update van onze bevindingen.

Onze risicoanalyse richt zich op een betrouwbare totstandkoming van de jaarrekening. Dit betekent dat wij niet alle risico's die voor u als gemeente relevant zijn in onze controle meenemen. De risicoanalyse is een continue proces en stellen wij gedurende de controle indien nodig bij. De belangrijkste bij uw gemeente onderkende risico's / kernpunten in de controle zijn:

- Waardering van uw grondexploitatie;
- Voorwaardencriterium als onderdeel van de rechtmatigheidsverantwoording en dan specifiek de voorwaarden omtrent aanbestedingen;
- Prestatielevering inkopen;
- Handmatige betalingen;
- Risico dat het management van de gemeente de procesafspraken doorbreekt, hetgeen een standaard risico is vanuit onze beroepsregels. Dit risico ziet bij uw gemeente met name toe op de schattingsposten in de grondexploitatie en onderhoudsvoorzieningen.

In ons verslag van bevindingen rapporteren wij naar aanleiding van de jaarrekeningcontrole over bovenstaande punten.

In lijn met voorgaande jaren constateren we dat de organisatie aandacht heeft voor het optimaliseren van de inrichting van de interne beheersing. Het daadwerkelijk afwikkelen van bevindingen kost echter veel tijd kost, het merendeel van onze bevindingen staat dan ook al langer open. Vanuit concerncontrol is veel tijd en energie gestoken om betreffende punten af te wikkelen. Tegelijkertijd worden de verbetervoorstellen in de organisatie echter niet opgepakt. Het belang van een goed werkende AO/IB wordt niet door alle betrokken functionarissen voldoende wordt onderkend. Terwijl dit juist nu van groot belang is voor de gemeente Zutphen. Immers een goed werkende planning en control cyclus zorgt ervoor dat je goed en tijdig kunt bijsturen en raakt daarmee de gehele organisatie.

Recent is de Visie op Control vastgesteld, wij zijn van mening dat hiermee een belangrijke stap is gezet door de gemeente Zutphen. Het is van groot belang dat deze visie wordt uitgedragen door directie en management, alleen dan kan het gewenste resultaat bereikt worden.

We hebben geen significante tekortkomingen in de AO/IC geconstateerd.

## Kwaliteit van de interne beheersing

Wij constateren dat concerncontrol vanuit een duidelijke ambitie werkt en belangrijke verbeterplannen heeft voor het verder verankeren van noodzakelijke interne beheersing in de organisatie. Hiervoor is gestart met het beschrijven van de opzet van de belangrijkste processen en de aanwezige interne beheersingsmaatregelen om te komen tot een systeemgerichte controle. Daarentegen blijven op onderdelen de interne beheersingsmaatregelen in het proces nog onvoldoende zichtbaar. Als gevolg hiervan kan achteraf niet vastgesteld worden of de afgesproken procedures en interne controles wel hebben bestaan en gewerkt. De verbijzonderde interne controlefunctie kan niet systeemgericht controleren en wij als accountant ook niet. Dat laatste betekent dat een controle meer tijd kost voor zowel de gemeente als voor ons. Daarnaast neemt hierdoor ook het risico op fouten en onrechtmatigheden toe. Wij constateren dat het merendeel van onze bevindingen al langer onderhanden is.

Wij zijn van mening dat de VIC aan waarde kan winnen door meer systeemgericht te controleren, hierdoor kan ook een efficiency slag behaald worden. Om dit te kunnen bereiken is het van belang om de huidige processen in beeld te brengen. Hieruit moet blijken hoe interne controles er precies uitzien. Binnen uw gemeente zijn dergelijke beschrijvingen wel aanwezig, maar deze worden niet periodiek geactualiseerd. Wij adviseren u procesbeschrijvingen periodiek te actualiseren en om in de het proces aanwezige key-controls (processtap met feitelijke controlehandeling) te beschrijven op basis van de 6w's (wie, wat, waarom, waarmee, wanneer, waar vastgelegd) .

Een belangrijk onderdeel van de interne beheersing is de (verbijzonderde) interne controlefunctie. Deze werkt vanuit een duidelijke visie en heeft de ambitie om de organisatie te helpen om verdere verbeteringen en kwaliteitsslagen te maken op het gebied van interne beheersing. Er is sprake van een geformaliseerd en gestructureerd actueel controleplan, hetgeen de basis vormt voor de planning en uit te voeren werkzaamheden. Een kwalitatief goed intern controleplan bevat in onze optiek een opbouw die gebaseerd is op de financiële omvang van posten en stromen, waarin deze posten en stromen vervolgens worden gekoppeld aan relevante wet- en regelgeving en waarin de daaruit voortkomende relevante risico's zijn gedefinieerd. In onze optiek voldoet het controleplan 2024 hieraan. Daarnaast is met het vaststellen van de 'Visie op control' de focus van de gemeente Zutphen op het onderdeel control verankerd in de organisatie. Hierin wordt onder andere ingegaan op de rollen, taken en verantwoordelijkheden van de betrokkenen ingegaan. Doelstelling hiervan is om 'in control zijn' breed onder de aandacht te brengen en de betreffende vakafdelingen hierin te betrekken om zo een breed draagvlak te creëren.

## Kwaliteit van de interne beheersing

Tot en met boekjaar 2022 vormde de accountant een oordeel over de rechtmatigheid en bracht hierover verslag uit in de controleverklaring en het accountantsverslag. Met ingang van boekjaar 2023 is de rechtmatigheidsverantwoording onderdeel geworden van de jaarrekening en heeft het college van burgemeester & wethouders verantwoording afgelegd over de rechtmatigheid. Het totaal aan rechtmatigheidsbevindingen in 2023 bleef beneden de vastgestelde verantwoordingsgrens. De geconstateerde bevindingen hadden betrekking op begrotingsoverschrijdingen en het niet voldoen aan EU-aanbestedingsregels. Wij hebben als onderdeel van onze controle een getrouwheidsoordeel afgegeven over de jaarrekening als geheel, hiervan maakte de rechtmatigheidsverantwoording onderdeel uit. Wij hebben hierin geen afwijkingen geconstateerd van de door het college geconstateerde afwijkingen.

Recent is er landelijk onderzoek verschenen met de bevindingen en aanbevelingen op basis van de gemeentelijke rechtmatigheidsverantwoordingen. De belangrijkste bevinding, is het netto wegen van de rechtmatigheidsbevindingen. Hiermee wordt bedoeld dat de begrotingsonrechtmatigheden, die als acceptabel worden beschouwd (omdat ze vallen binnen het door de raad vooraf gestelde beleid) als rechtmatig worden geclassificeerd. In de kadernota rechtmatigheid is echter, in tegenstelling tot voorgaande jaren opgenomen dat deze onrechtmatig blijven en als zodanig 'meewegen' in de rechtmatigheidsconclusie, alleen dat voor de toelichting op deze onrechtmatigheden korthedshalve verwezen kan worden naar het vastgestelde beleid en de toelichting op de rekening van baten en lasten. Gezien het feit dat bovenstaand bij een groot deel van de gemeenten niet op een juiste wijze is verantwoord laat blijken dat de wet- en regelgeving op dit vlak vraagt om verduidelijking. Recent heeft de commissie BBV de kadernota Rechtmatigheid 2024 uitgebracht, hieruit blijken een aantal belangrijke wijzigingen ten opzichte van 2023. Deze hebben wij opgenomen in bijlage 3. Wij adviseren u de uitingen van de commissie BBV te volgen en de verantwoording in de jaarstukken 2024 aan te passen.

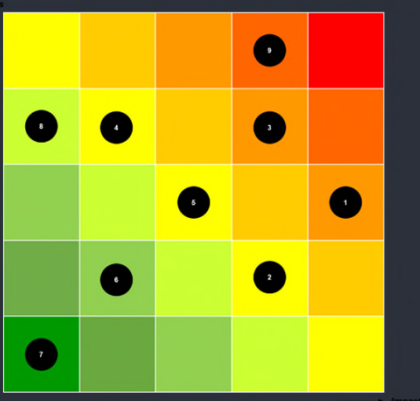
## Kwaliteit van de interne beheersing

| #       | Proces                          | Bevinding                      | Status 2024 | Status 2023 | Impact                                |
|---------|---------------------------------|--------------------------------|-------------|-------------|---------------------------------------|
| 2024.01 | Subsidieverstrekkings           | Vastleggen overwegingen        | ●           | n.v.t.      | Middel                                |
| 2024.02 | Subsidieverstrekkings           | Toetspunten                    | ●           | n.v.t.      | Middel                                |
| 2024.03 | Prestatielevering               | Onderbouwing                   | ●           | n.v.t.      | Hoog, want (mogelijk) frauderisico    |
| 2023.01 | Primaire registratie            | Wijzigen stamgegevens          | ●           | ●           | Hoog, want (mogelijk) frauderisico    |
| 2023.02 | Salarisadministratie            | Controle bezettingsoverzichten | ●           | ●           | Gemiddeld                             |
| 2023.03 | Huuropbrengsten                 | Indexatie huurovereenkomsten   | ●           | ●           | Laag                                  |
| 2019.01 | Administratie en verslaglegging | Memoriaalboekingen             | ●           | ●           | Hoog, want frauderisico               |
| 2019.05 | Inkopen                         | Aanbestedingen                 | ●           | ●           | Hoog, want (mogelijk) corruptierisico |
| 2019.06 | Inkopen                         | Prestatielevering              | ●           | ●           | Hoog, want (mogelijk) frauderisico    |
| 2019.07 | Subsidies                       | Inhoudelijke toets             | ●           | ●           | Gemiddeld                             |
| 2019.03 | Omgevingsvergunningen           | Functiescheiding               | ●           | ●           | Gemiddeld                             |

In het overzicht hiernaast zijn de bevindingen met de ingeschatte prioriteit opgenomen. Een gedetailleerde beschrijving van de detailbevindingen is opgenomen in bijlage. De kleur van de het symbool geeft de status van de constatering aan.

- opgelost
- actie ondernomen, maar nog niet afgerond
- geen actie ondernomen
- nieuwe bevinding
- gemeente heeft besloten bevinding niet op te volgen, zie ook bijlage 1

## Beheersing fraude- en corruptierisico's



# Fraude- en corruptierisico's

## Frauderisicoanalyse

De primaire verantwoordelijkheid voor het voorkomen en detecteren van fraude (waaronder corruptie) berust bij het college van burgemeester en wethouders. Deze verantwoordelijkheid betreft ook het onderhouden van een zodanige interne beheersing om het opmaken van de jaarrekening mogelijk te maken zonder dat deze afwijkingen van materieel belang bevat als gevolg van fraude of fouten.

De gemeente heeft jaren geleden een interne frauderisicoanalyse opgesteld, actualisatie van deze frauderisicoanalyse heeft echter sinds 2017 niet meer plaatsgevonden. Wij adviseren u deze frauderisicoanalyse op korte termijn te actualiseren.

Voor het opstellen van een frauderisicoanalyse kan gebruik worden gemaakt van een template. Hierin kan voor processen waar materiële opbrengsten-/kostenstromen mee zijn gemoeid, inzichtelijk worden gemaakt:

- ☐ Welke frauderisico's de gemeente onderkent;
- ☐ Wat de geschatte kans en impact van deze frauderisico's is;
- ☐ Wat de risicospons van de gemeente is, idealiter afgestemd op de risicobereidheid van de gemeente zoals vastgelegd in frauderisicobeleid;
- ☐ Welke interne beheersmaatregelen reeds getroffen zijn om onderkende frauderisico's te mitigeren;
- ☐ Welke eventuele restrisico's/leemtes in de interne beheersing resteren en hoe de gemeente deze ondervangt (bijvoorbeeld via de verbijzonderde interne controle).

De kans- en impactweging van frauderisico's kan via een risicomatrix weergegeven worden om op basis daarvan prioriteiten te stellen in de wijze waarop met risico's wordt omgegaan. Een voorbeeld van hoe een risicomatrix eruit kan zien is hiernaast opgenomen. Voor de duidelijkheid benoemen we graag dat er een relatie is tussen fraude en misbruik en oneigenlijk gebruik (M&O). M&O is namelijk een vorm van fraude waarbij de nadruk ligt op handelingen van derden in relatie tot het verkrijgen van overheidsbijdragen dan wel het betalen van heffingen. Wij raden u aan om bij het opstellen van een frauderisicoanalyse, ook expliciet aandacht te besteden aan M&O-risico's vanwege de verwevenheid tussen fraude en M&O.

Tot slot merken wij op dat het uitvoeren van een frauderisicoanalyse en het treffen van interne beheersmaatregelen, onderdeel vormen van het bredere 'frauderisicomanagement'. Frauderisicomanagement omvat namelijk ook het opstellen van frauderisicobeleid (waar M&O-beleid al dan niet onderdeel van kan vormen), het opstellen van een frauderesponsplan voor situaties dat een vermoeden van fraude bestaat en het periodiek intern evalueren in hoeverre frauderisicomanagement voldoende is ingericht en toereikend werkt binnen de organisatie.

## Fraude- en corruptierisico's

### Naleving M&O-beleid

Voor de duidelijkheid benoemen we graag dat er een relatie is tussen fraude en misbruik en oneigenlijk gebruik (M&O). M&O is namelijk een vorm van fraude waarbij de nadruk ligt op handelingen van derden in relatie tot het verkrijgen van overheidsbijdragen dan wel het betalen van heffingen. De naleving van het M&O-beleid weegt niet meer mee in het oordeel van de rechtmatigheidsverantwoording, eventuele bevindingen dienen echter wel gerapporteerd te worden in de paragraaf bedrijfsvoering. Wij raden u aan om bij het opstellen van een frauderisicoanalyse, ook expliciet aandacht te besteden aan M&O-risico's vanwege de verwevenheid tussen fraude en M&O, zie ook 'Kadernota Voorkomen en Bestrijden Misbruik en Oneigenlijk gebruik 2023'.

### Onze frauderisicoanalyse

Afgelopen jaren signaleren wij een toenemende aandacht voor fraude. Ook de rol van de accountant bij het signaleren van frauderisico's is afgelopen jaren veelvuldig besproken. Naar aanleiding van de rapportage van de AFM 'Scherper op frauderisico's' van 8 juni 2023 heeft onze beroepsorganisatie de aanpak van frauderisico's in de controle geëvalueerd en is deze zomer de concept Handreiking 1153 'Frauderisicoanalyse' gepubliceerd.

Tevens wijzen wij u op de gepubliceerde handreiking 1137 'Corruptie, werkzaamheden van de accountant', waarin aandacht geschonken wordt aan corruptierisico's. Wij willen u vragen om ook in de eigen frauderisicoanalyse aandacht te hebben voor mogelijke corruptierisico's binnen uw organisatie. De nadere guidance in Handreiking 1153 en 1137 kan er toe leiden dat dit gevolgen heeft voor de frauderisicoanalyse die wij voor onze controle van uw gemeente uitvoeren. Dit kan dan tevens betekenen dat wij in vergelijking met voorgaande jaren meer of andere frauderisico's identificeren.

## 2 IT-omgeving



## IT-omgeving

Als onderdeel van onze controleaanpak hebben wij werkzaamheden uitgevoerd om inzicht te krijgen in de toepassing van de IT-systemen in de bedrijfsprocessen en de daarbij (eventueel) behorende risico's.

Tijdens onze interim-controle hebben wij controlewerkzaamheden uitgevoerd op relevante IT-beheersingsmaatregelen die uw organisatie heeft genomen in de IT-processen; beheersen van de IT-operatie (IT-continuïteitsmaatregelen en uitbestede diensten), beheersen van updates (ontwikkelen en implementeren van nieuwe functionaliteit), beheersen van de identiteit van gebruikers (opzetten passende beveiligingsinstellingen) en beheersen van de bevoegdheden van gebruikers (verlenen en onderhouden van toegang). Afhankelijk van het belang van de IT-applicatie voor de jaarrekeningcontrole en uw organisatie hanteren wij een bepaalde scope waarbij wij de uitkomsten van uw IT-inrichting toetsen. Zie de onderstaande tabel voor de relevante IT-applicaties en de evaluatie van de IT-processen die door ons zijn gecontroleerd.

Veel handelingen die binnen organisaties plaatsvinden, worden geregistreerd door middel van automatisering. Daarbij zijn diverse interne beheersingsmaatregelen steeds vaker geautomatiseerd in softwarepakketten. Wij onderzoeken daarom de beheersing van uw IT-omgeving en rapporteren daarover in deze boardletter.

Op basis van de door ons uitgevoerde werkzaamheden in juli 2024 hebben wij onze inschatting van de kwaliteit van uw IT-systeem en/of applicaties opgenomen. Hierbij hebben wij de volgende onderverdeling gemaakt om de kwaliteit weer te geven:

-  Benodigd, verbetering op (korte) termijn
-  Adviespunt, verdere aanscherping mogelijk
-  Op dit moment voldoende

Bij het uitvoeren van onze werkzaamheden hebben wij gekeken naar de algemene onderwerpen rondom de beheersing van uw IT-omgeving zoals in de tabel hieronder opgenomen. Op de navolgende pagina's zullen wij onze bevindingen rapporteren.

| IT-proces     |                            |                                                                                       |                                                                                       |                                                                                       |
|---------------|----------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| IT-applicatie | Belang voor de organisatie | Authenticatie                                                                         | Autorisatie                                                                           | Wijzigingsbeheer                                                                      |
| Netwerk       | Belangrijk                 |  |  | N.v.t.                                                                                |
| IFinanciën    | Belangrijk                 |  |  |  |
| Suites        | Belangrijk                 |  |  |  |
| ADP           | Belangrijk                 | N.v.t.                                                                                | N.v.t.                                                                                |  |

## IT-omgeving

Als onderdeel van de jaarrekeningcontrole hebben wij inzicht gekregen in de cybersecurity-gerelateerde risico's die zouden kunnen leiden tot een potentiële afwijking van materieel belang in de jaarrekening (met betrekking tot zowel financiële als niet-financiële informatie). Hiervoor hebben wij inzicht gekregen in de mate waarin, en de overweging waarom de organisatie bepaalde informatiebeveiligingsmaatregelen heeft genomen om deze cyberrisico's te beperken.

Om het risico van cyberbeveiligingsbedreigingen (d.w.z. continuïteit van de dienstverlening en integriteit van de financiële verslaglegging) te verlagen, heeft uw organisatie een mix van beveiligingsmaatregelen geïmplementeerd. Met name op de onderdelen Identity en Recover scoort uw organisatie aanzienlijk lager dan de best-practice, op de onderdelen Protect, Detect en Response zijn wel belangrijke verbeterlagen ten opzichte van voorgaand jaar. Zie de Cybersecurity NIS2 scan in de bijlage.

We hebben geconstateerd dat zich in het boekjaar geen cyberbeveiligingsincidenten hebben voorgedaan die hebben geleid tot een afwijking van materieel belang in de jaarrekeningcontrole van uw organisatie. Onze controlewerkzaamheden zijn niet primair gericht op het doen van uitspraken over cyberbeveiliging en we hebben ook geen instructies van het management in die zin ontvangen voor het uitvoeren van meer diepgaande werkzaamheden. Hierbij kunnen wij u overigens wel in faciliteren.

In Nederland is de Cyberbeveiligingswet (verder: Cbw) in ontwikkeling welke vanaf 2025 verplicht zal worden en de EU richtlijn NIS2 (verder: Network and Information Systems Directive) implementeert. De wet is uit de consultatieronde en wordt na de zomer definitief gemaakt voor invoering naar verwachting in voorjaar 2025. Dit heeft betrekking op meerdere sectoren, waaronder de sector waar uw organisatie onder valt.

Er worden strengere eisen gesteld aan de beveiliging van netwerk- en informatiesystemen. Organisaties worden onder de Cbw meer dan nu verplicht om te zorgen voor de beveiliging van de hele keten waar zij deel van uitmaken. Op basis van het risico in de leveringsketen zullen zij cybersecurity maatregelen moeten opleggen aan hun leveranciers. Die groep leveranciers zal ook digitaal veiliger moeten gaan werken. Daarnaast komt er een verplichte registratie en meldplicht voor incidenten (naast degene die al bestaat voor privacy). Er worden maatregelen ingevoerd om de naleving van de NIS2 richtlijn te verzekeren, inclusief financiële sancties voor niet-naleving.

Wij adviseren om vanuit een actueel inzicht in de IT-objecten en gegevens in de keten waarvan uw organisatie deel uitmaakt de risico's te benoemen en maatregelen en contractuele afspraken scherp in beeld te hebben. Daarop aanvullend dienen vervolgens een aantal basis hygiëne maatregelen conform de nieuwe wet ingericht te worden. Wij hebben hiervoor een stappenplan ontwikkelt en kunnen u hierbij ondersteunen.

## Bijlage: Cybersecurity NIS2 scan

### Governance

#### Eigenaarschap en pro-activiteit is aanwezig.

Wij zien dat er aandacht en prioriteit wordt gegeven aan de kwaliteit van de huidige beveiliging. Ook zien wij dat er op dit moment een ontwikkeling plaatsvindt op het gebied van risicomanagement en formalisatie van beleid omtrent cybersecurity. Ter verbetering kan het bevoegd gezag de verantwoordelijkheden en taken voor cyber-risico's in de eigen organisatie verder formaliseren en er dient een beter overzicht te worden verkregen van de interne en externe stakeholders (ook in de keten).

### Identificatie

#### Identificeren van kritieke systemen vereist directe actie.

Wij zien dat het identificeren van kroonjuwelen, risico's en maatregelen (ook bij leveranciers) directe actie vereist. Denk hierbij aan het inzichtelijk maken van systemen, data en processen die essentieel zijn voor de continuïteit van uw bedrijfsvoering, en bepaal de impact wanneer deze niet meer operationeel zijn. Ook dient u adequate beveiligingsmaatregelen inzichtelijk te krijgen en uit te werken waarmee u of uw leveranciers de cyber-risico's afdekken.

### Bescherming

#### Uw bescherming heeft prioriteit.

De wijze waarop vervolgens de cyberrisico's door middel van maatregelen worden verlaagd kan verder worden verbeterd. Denk hierbij vooral aan het minimaal jaarlijks bijscholen van medewerkers op securitygebied en het up-to-date houden van IT hardware conform beveiligingsstandaarden.

### Detectie

#### Het detecteren is niet in lijn met uw risicobeeld.

Op basis van het model zien wij dat aandacht gegeven is aan monitoring, vulnerability scanning en pentesting, maar dat er verbeterpotentieel ligt om de cyberweerbaarheid van uw organisatie te verhogen. Denk hierbij aan het aanscherpen van de procedures omtrent toegangsbeheer en het verkrijgen van externe Assurance op beveiligingsmaatregelen van externe leveranciers.

### Reactie

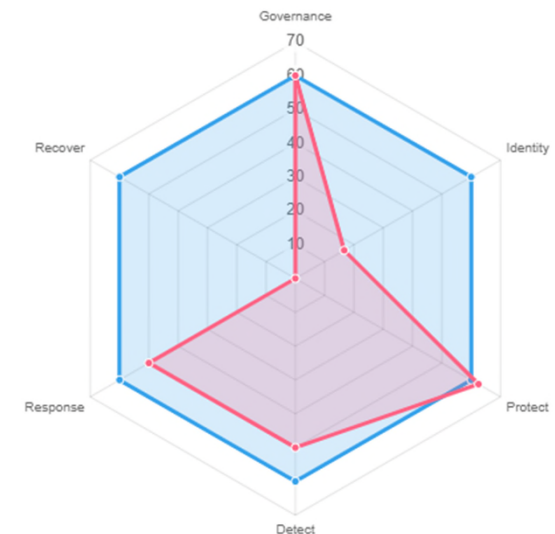
#### Reageren kan verder worden verbeterd.

Wij zien dat security incidenten worden geregistreerd en periodiek geanalyseerd. Ter aanscherping is het van belang dat u een crisis- en communicatieplan opstelt waarbij cyber ook onderdeel uitmaakt van de scoping, en in de praktijk test middels een simulatie van een cyber incident.

### Herstel

#### Herstellen vereist prioriteit.

Uw organisatie heeft geen herstelplan opgesteld om de schade te herstellen en de bedrijfsvoering te hervatten. Daarnaast oefent u niet regelmatig of de back-up voorzieningen adequaat kunnen herstellen en er is geen procedure om te leren van opgetreden cyberincidenten.



# Contact

**M.C.J.M. Bekker RA**  
Extern accountant  
+ 31 6 15 30 36 59  
m.bekker@bakertilly.nl

**E.R.M. (Emmy) Friesen MSc RA**  
Manager Audit  
+ 31 6 21 92 16 95  
e.friesen@bakertilly.nl

**KANTOORGEGEVENS**  
Baker Tilly (Netherlands) N.V.  
Burgemeester Roelenweg 14-18  
8021 EV Zwolle  
Postbus 508  
8000 AM Zwolle  
+31 38 425 86 00

Baker Tilly (Netherlands) N.V. trading as Baker Tilly is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities.

