Nota risicomanagement 2025

Inhoud

1. Inleiding

Dit is de nieuwe Nota risicomanagement. De vorige versie van deze beleidsnota dateert uit 2015. Sindsdien hebben zich diverse externe en interne ontwikkelingen voorgedaan, zoals de invoering van de rechtmatigheidsverantwoording, een veranderd digitaal klimaat en een vernieuwde organisatiestructuur. Bovendien is in de afgelopen 10 jaar op diverse beleidsterreinen het gemeentelijk takenpakket uitgebreid, zijn nieuwe projecten gestart en zijn als gevolg hiervan nieuwe risico's ontstaan. Ook de cyberaanval van eind 2020 heeft het omgaan met risico's onmiskenbaar een nieuwe impuls gegeven.
Deze nieuwe Nota risicomanagement sluit aan bij de nieuwe situatie en heroverweegt de wijze waarop gemeente Hof van Twente risico's tracht te beperken en beheersen.

Nieuw onderdeel van deze Nota risicomanagement is het beleid over fraude, misbruik en oneigenlijk gebruik (M&O). Dit is een direct voortvloeisel van de invoering van de rechtmatigheidsverantwoording. Hierbij sluiten we aan bij bevindingen die de accountant in afgelopen jaren heeft gepresenteerd.

Het belangrijkste uitgangspunt voor het formuleren van de risico's is de strategie van de gemeente. Vanuit de strategie worden doelstellingen geformuleerd en acties in gang gezet. De risico's zitten hem erin dat als de acties niet slagen de organisatie dan risico loopt. Vervolgens is een centraal aspect van risicomanagement de cultuur binnen organisatie, politiek en bestuur. Van groot belang is daarbij het bewustzijn bij medewerkers, managers en bestuurders dat dagelijkse activiteiten, besluitvorming, juridische handelingen, advisering aan het college en de raad, en projectwerkzaamheden risico's met zich mee kunnen brengen waar bewust mee omgegaan dient te worden.

De noodzaak van een actief risicomanagement waarbij periodiek op ambtelijk en bestuurlijk niveau naar de risico's van de organisatie wordt gekeken, komt onder meer tot uiting in de vereiste rapportage van geïdentificeerde risico's in de risicoparagraaf van het jaarverslag en de programmabegroting. Daarmee is risicomanagement ook voor de gemeenteraad een terugkerend thema, die voortvloeit uit zijn kaderstellende en controlerende rol.

2. Doel en kader van risicomanagement

2.1 Doel

Het doel van de Nota Risicomanagement is om vast te stellen hoe Hof van Twente omgaat en om wil gaan met risico’s.
Risicomanagement is de afgelopen jaren structureel geïntegreerd in de bedrijfsvoering van Hof van Twente. Dit vereist een beleidskader dat aangeeft hoe risico's worden geïdentificeerd, beheerst en hoe de financiële veerkracht van de gemeente wordt berekend om onvoorziene uitgaven op te vangen.

Het doel van risicomanagement in Hof van Twente is dat in de bedrijfsvoering en het bestuur met regelmaat aandacht wordt geschonken aan het expliciet maken en beheersen van risico's, het bevorderen van risicobewustzijn en het nemen van bewuste beslissingen.

Het uitgangspunt van risicomanagement is om bestaande instrumenten en procedures te integreren onder één risicomanagementparaplu. Het gaat niet om een ingrijpend nieuw initiatief, maar om het samenbrengen van bestaande informatie en instrumenten tot een begrijpelijk en bruikbaar geheel. Hierbij sluiten we aan bij andere bestaande beleidsdocumenten, die verband houden met risicomanagement, namelijk de Nota Reserves & voorzieningen en de Nota Grondbeleid, maar ook met de vaste paragraaf Weerstandsvermogen en risicomanagement in programmabegroting en jaarverslag.

2.2 Kader

Hieronder worden zowel het externe als interne kader waarbinnen deze nota zich bevindt toegelicht.

Extern kader

De voornaamste externe voorschriften zijn opgenomen in het Besluit Begroting en Verantwoording provincies en gemeenten (hierna: BBV). In het BBV worden gemeenten verplicht een risicoparagraaf op te nemen in zowel de begroting als jaarrekening. Daarbij dient een weerstandratio, de verhouding tussen de risico's en de buffer die hiervoor wordt aangehouden, te worden weergegeven. De systematiek voor de berekening en de hoogte van deze ratio zijn keuzevrijheden voor de gemeenteraad. Hoofdstuk 3.1 gaat hier verder op in.

Daarnaast bieden de externe regelgeving uit de Gemeentewet, de Ambtenarenwet 2017, de Wet bescherming klokkenluiders, de Wet open overheid (Woo), en de Wet bevordering integriteitsbeoordelingen door het openbaar bestuur (Wet Bibob) een kader waarbinnen we als gemeente Hof van Twente ons risicomanagement vormgeven.

Jaarlijks stelt de gemeenteraad een normenkader vast waarbinnen de gemeente dient te handelen. Dit dient als kader waarbinnen de gemeente en de accountant controles uitvoeren.

Intern kader

Als interne regelgeving stelt de gemeenteraad verordeningen vast. Rondom risicomanagement is de belangrijkste daarvan de financiële verordening zoals artikel 212 Gemeentewet voorschrijft. In deze verordening staat dan ook beschreven:

- de cyclus van kaderstelling en verantwoording in de relatie tussen raad en college
- het niveau waarop de gemeenteraad de begroting autoriseert
- de verantwoordelijkheid van het college voor een systematische interne controle
- de verantwoordelijkheid van het college voor een adequate inrichting van de organisatie.
- de verplichting tot het vaststellen van deze Nota risicomanagement

Ook de verordening zoals deze door artikel 213 Gemeentewet voorschrijft speelt een rol in het risicomanagement. Hierin zijn de inrichting van de jaarlijkse accountantscontrole en de rol van de auditcommissie beschreven.

Daarnaast biedt de Nota Reserves & voorzieningen een belangrijk kader in de financiële beheersing binnen de gemeente. Hierin staat beschreven hoe de gemeente wenst om te gaan met het instellen, aanwenden en opheffen van diverse (bestemmings-)reserves en voorzieningen. Los van het feit dat het instellen en aanwenden van reserves en voorzieningen in praktijk gebonden is aan regelgeving, zijn het ook bij uitstek instrumenten om bewust en verantwoord om te gaan met risico’s die zich in de dagelijkse bestuurspraktijk kunnen voordoen.

3. Risicomanagement

Risicomanagement is een cyclisch proces,. in bijlage 1 staat deze cyclus gedetailleerd beschreven. In dit hoofdstuk wordt ingegaan op de fasen die wij hierbij onderscheiden en welke keuzes gemeente Hof van Twente hierbij maakt. Uitgangspunt hierbij is dat de gemeente zelfstandig een systematiek ontwikkelt, die onderbouwd is en die in praktijk ook wordt toegepast vanuit een duidelijk handelingsperspectief. Het BBV bevat namelijk geen voorgeschreven methodiek of normenkader. Dit betekent dat de gemeente zelf een afgewogen werkwijze kiest, een brede inventarisatie maakt van alle risico's die zich kunnen voordoen en een afweging maakt hoe met deze risico's wordt omgegaan.

3.1 Risicobeoordeling

Risicomanagement begint bij het signaleren van risico's. Dit is een cultuuronderdeel en vraagt om een permanente alertheid in alle onderdelen van de organisatie en dient terug te komen in de afwegingen die organisatie en bestuur dagelijks maken. Toch is er ook een duidelijke verankering van de risico-inventarisatie in de planning- en controlcyclus (P&C cyclus). Vast onderdeel van de programmabegroting en de jaarstukken (jaarverslag/jaarrekening) is de paragraaf weerstandsvermogen en risicobeheersing.
Bij het opstellen van de deze paragraaf worden de grootste financiële risico's geïnventariseerd en na beoordeling op waarschijnlijkheid, impact en reeds getroffen maatregelen gekwantificeerd.

Volgens het BBV dient in de paragraaf Weerstandsvermogen en risicobeheersing een vaste set financiële kengetallen opgenomen te worden. De bedoeling is dat deze kengetallen inzichtelijk maken hoeveel (financiële) ruimte de gemeente heeft om extra structurele of incidentele lasten op te kunnen vangen. Deze kengetallen bieden daarmee inzicht in de financiële positie van de gemeente.

- Netto schuldquote (=niveau schuldenlast t.o.v. eigen middelen)
- Netto schuldquote, gecorrigeerd voor leningen (die de gemeente aan derden heeft verstrekt)
- Solvabiliteitsratio (=mate waarin gemeente eigen financiële verplichtingen kan voldoen)
- Grondexploitatie
- Structurele exploitatieruimte
- Belastingcapaciteit

Weerstandsvermogen en weerstandsratio

Het kwantificeren van risico's gebeurt door een inschatting te maken van de financiële impact van het optreden van het risico. Vervolgens is van belang de kans dat het risico zich voordoet. Hierbij hanteren we eenduidig drie opties:

- Kans is klein: 25%
- Kans is middel: 50%
- Kans is groot: 75%

De categorieën zijn beperkt om een volgbare afweging te maken en schijnzekerheid te voorkomen. Aan de basis van deze beoordeling ligt immers een inschatting. Hierbij zijn 0% en 100% geen keuzeopties. Immers, wanneer het risico richting 0% gaat is dit verwaarloosbaar of niet aanwezig. Wanneer de kans richting 100% gaat is niet langer sprake van een onzekere gebeurtenis (risico) maar beschouwen we dit als zekerheid en worden (financiële) maatregelen getroffen. Dit uit zich bijvoorbeeld in het presenteren van een autonome ontwikkeling in een tussentijdse bestuursrapportage.

In het Besluit Begroting en Verantwoording provincies en gemeenten (BBV) worden gemeenten verplicht een risicoparagraaf (Paragraaf Weerstandsvermogen en risicobeheersing) op te nemen in zowel de programmabegroting als jaarstukken. Daarbij dient een weerstandratio weergegeven te worden. De systematiek voor de berekening en hoogte van deze weerstandsratio zijn keuzevrijheden voor de gemeenteraad.

Gemeente Hof van Twente kiest voor een overzichtelijke systematiek. Door de financiële impact te vermenigvuldigen met de kans komt het risicoprofiel tot stand.

De weerstandratio is de verhouding tussen het risicoprofiel en het weerstandsvermogen. Tot dit weerstandsvermogen rekenen we de vrij-besteedbare delen van de algemene reserve en de reserve majeure projecten.

Hierbij stelt de gemeenteraad de norm vast voor hoe hoog deze ratio minimaal moet zijn. In het verleden heeft de raad ervoor gekozen om de ratio te hanteren die minimaal ligt tussen de 1,0 en 1,4. Deze range wordt in het risicomanagement gekenmerkt als "voldoende".
Dit betekent bijvoorbeeld dat wanneer de gekwantificeerde risico's 4 miljoen euro bedragen en het weerstandsvermogen 6 miljoen euro bedraagt, de ratio uitkomt op 1,5. (6:4)

Komt de ratio onder de 1.0, dan dient de reserve aangevuld te worden tot dit niveau. Komt de ratio boven de 1.4 dan wordt het vermogen besteedbaar voor andere doelen en hoeft dit niet als buffer te worden aangehouden.
Voor de grondexploitatie wordt ditzelfde principe afzonderlijk gevolgd. Dit betekent dat binnen de reserve grondexploitaties een buffer wordt aangehouden om de gekwantificeerde risico's van alle lopende grondexploitaties, aankopen ed. tezamen op te vangen.
Op deze manier is de buffer van de gemeente groot genoeg om financiële tegenvallers op te vangen, maar niet zo groot dat middelen onnodig stil blijven staan.

3.2 Risicobeperking en beheersing

Naast het treffen van financiële maatregelen tracht de gemeente uiteraard zo veel mogelijk risico's te verkleinen. Dit gebeurt door het vergroten van bewustwording en het daarmee weloverwogen omgaan met risico's in de dagelijkse besluitvorming. Zo worden in beginsel bij periodieke risico-inventarisaties ter voorbereiding op bestuursrapportages gesprekken gevoerd met de eerste lijn, teamleiders, directie en de portefeuillehouder financiën.

Naast deze gesprekken dienen teams het onderwerp risicomanagement periodiek als thema in hun teamoverleg te agenderen. Het doel daarbij is dat risico's en beheersmaatregelen worden benoemd en een plaats krijgen binnen procesbeschrijvingen, projectplannen en projectrapportages.

Directie en management zullen aandacht blijven vragen voor risicomanagement binnen projecten, collegebesluiten, raadsbesluiten, beleidsontwikkeling en processen zodat zij hierop kunnen sturen.

Ter ondersteuning van de inbedding van het risicobewustzijn worden trainingen via de Hofacademie georganiseerd.

Een andere concrete uitwerking van de risicobeperking is het jaarlijkse interne controleplan. In het interne controleplan worden de risico's in processen en de daarbij behorende maatregelen beschreven. Dit kunnen bijvoorbeeld (aangescherpte) controles, het opvragen van bewijsstukken, het vierogenprincipe, toegangsbeheer, automatisering of logging zijn. In bijlage 3 is een overzicht weergegeven van het instrumentarium waarover gemeente Hof van Twente beschikt in risicobeperking en -beheersing.

4. Fraude, misbruik en oneigenlijk gebruik

Met de komst van de rechtmatigheidsverantwoording wordt ook van gemeenten verwacht dat zij beleid formuleren rondom misbruik en oneigenlijk gebruik (M&O). Het mitigeren van M&O is niet nieuw voor de gemeente, een overkoepelend vastgesteld beleid wel.

4.1 Overkoepelend kader

Het in dit hoofdstuk geformuleerde beleid is een uiteenzetting van belangrijke uitgangspunten om misbruik en oneigenlijk gebruik (hierna M&O) te bestrijden. Ook hier geldt dat het veelal een opsomming of kapstok is van reeds bestaande maatregelen en afspraken. Doelstelling is om de uitwerking van het beleid ten aanzien van voorkoming van M&O plaats te geven in de specifieke regelingen en bijbehorende verordeningen en processen. Overigens zijn de meeste wettelijke regelingen gebonden aan wettelijke eisen en minimumnormen voor het nemen van maatregelen ter bestrijding van fraude en misbruik.

4.2 Definities

Fraude, misbruik en oneigenlijk gebruik krijgen steeds meer aandacht in de gemeente. Dit kan namelijk grote financiële gevolgen hebben maar ook de normen en waarden waar de gemeenteraad, het college en de ambtelijke organisatie voor staan ondermijnen.
In verschillende wet- en regelgeving, zoals de Gemeentewet, de Ambtenarenwet 2017, de Wet bescherming klokkenluiders, de Wet open overheid (Woo) en de Wet bevordering integriteitsbeoordelingen door het openbaar bestuur (Wet Bibob) komt het thema fraude naar voren. De aandacht voor fraude, misbruik en oneigenlijk gebruik blijkt onder andere uit de enkele jaren geleden uitgevoerde frauderisicoanalyse. Daarnaast vormt ‘misbruik en oneigenlijk gebruik’ een toetsingscriterium bij de rechtmatigheidsverantwoording die het college moet opnemen bij de jaarrekening.

In de Financiële verordening van de gemeente is vastgesteld dat het college verantwoordelijk is voor het beleid en de interne regels voor het voorkomen van M&O om te voldoen aan de eisen van rechtmatigheid, controle en verantwoording. Daarnaast is de accountant verplicht om bij wettelijke controleopdrachten in hun controleverklaring te rapporteren over hun werkzaamheden op het gebied van fraude en continuïteit.
In deze nota wordt onderscheid gemaakt tussen de drie termen: fraude, misbruik en oneigenlijk gebruik. Waarbij de volgende definities gehanteerd worden;

Fraude

Onder fraude wordt verstaan opzettelijke misleiding om onrechtmatig voordeel te verkrijgen. In deze nota is de term intern gericht, dus op het handelen van personen binnen de gemeentelijke organisatie. Misbruik en oneigenlijk gebruik zijn daarentegen extern gericht. Enkele jaren geleden heeft Hof van Twente een frauderisicoanalyse laten uitvoeren om inzicht te creëren in de totaliteit van frauderisico's aanwezig binnen gemeente Hof van Twente. Het beoogde resultaat hiervan is een vergrote bewustwording en eventueel gerichte aanpak van frauderisico's. Zo kan de weerbaarheid van Hof van Twente worden vergroot. In bijlage 3 is een overzicht opgenomen van de instrumenten die ingezet worden voor frauderisicomanagement. Voorbeelden hiervan zijn het vierogenprincipe, de klokkenluidersregeling en logging.

De commissie BBV heeft in de Kadernota Rechtmatigheid de volgende definities van misbruik en oneigenlijk gebruik opgenomen.

Misbruik

Het opzettelijk niet, niet tijdig, onjuist of onvolledig verstrekken van gegevens met als doel ten onrechte overheidssubsidies of -uitkeringen te verkrijgen of niet dan wel een te laag bedrag aan heffingen aan de overheid te betalen. Het betreft hier een bewuste misleiding om onrechtmatig of onwettig voordeel te behalen. Niet elke misstap (fout) geldt als misbruik. Bij het maken van fouten is er meestal geen sprake van een opzettelijke handeling. Daarnaast is het begrip misleiding van betekenis in deze definitie. Misleiding heeft betrekking op het bewust verborgen houden van het misbruik.

Oneigenlijk gebruik

Het door het aangaan van rechtshandelingen, al dan niet gecombineerd met feitelijke handelingen, verkrijgen van overheidsbijdragen of het niet dan wel tot een te laag bedrag betalen van heffingen aan de overheid, in overeenstemming met de bewoordingen van de regelgeving maar in strijd met het doel en de strekking daarvan.
Als wet- en regelgeving oneigenlijk gebruik mogelijk maakt ('de mazen van de wet") is het noodzakelijk dat lokale wet- en regelgeving worden aangepast en/of duidelijker moet worden toegelicht.

4.3 Uitgangspunten/voorkomen en tegengaan misbruik en oneigenlijk gebruik

Bij alle processen waar sprake kan zijn van M&O of fraude moeten in de kaders voor deze regelingen waarborgen zijn opgenomen om dit te voorkomen. Extern geldt dat geen middelen de deur uitgaan zonder toetsing aan geldende regelgeving. Het is belangrijk dat o.a. de uitkeringen, subsidies en vergunningen naar de inwoners of bedrijven gaan die daar recht op hebben. Daarnaast is het van belang dat ook de duur en hoogte van het bedrag juist zijn. Een adequate toetsing van aanvragen en de interne controle en verbijzonderde interne controle gericht op rechtmatigheid spelen een belangrijke rol om intern toezicht te houden op het voorkomen en tegengaan van misbruik en oneigenlijk gebruik. Ditzelfde geldt indirect ook voor de accountantscontrole, ofschoon het opsporen van fraude en oneigenlijk gebruik geen expliciet doel is van deze controle.

Een bijzondere vorm van misbruik is ‘ondermijnende criminaliteit’. Een exacte definitie daarvan is moeilijk in een zin samen te vatten. Grofweg betekent het de vermenging van de onderwereld en de bovenwereld, de sluipende bedreiging van de integriteit van het openbaar bestuur, overheidsambtenaren en bedrijfsleven, bedreiging van bestuurders en ambtenaren, afpersingspraktijken, de innesteling van criminele fenomenen in buurten en woonwijken of het ontstaan van ‘vrijplaatsen’. Hierin komen M&O en fraude samen. Hierbij past een verwijzing naar het gemeentelijke en regionale beleid tegen ondermijning.

Om misbruik te voorkomen wordt niet alleen naar buiten gekeken, maar ook naar het eigen handelen. Intern gelden integriteitsregelingen, de ambtseed, functiescheiding in (financiële) processen, maar ook aanspreekgedrag en collegiale toetsing. In de gemeentelijke budgetregeling, die is opgenomen in het Organisatiebesluit, is de budgetbevoegdheid aan budgethouders en deelbudgethouders toebedeeld, waarbij nadrukkelijk waarborgen rondom het vierogenprincipe bij zowel opdrachtverlening als prestatiemeting en akkoordverklaring van facturen zijn opgenomen.

4.4 Misbruik en oneigenlijk gebruik in beleid en uitvoering

Zoals in hoofdstuk 4.2 beschreven richten definities van misbruik en oneigenlijk gebruik zich vooral op het misbruik door derden van publieke middelen. Het is aan ons om waarborgen aan te brengen om dit te voorkomen.

Voor activiteiten die vatbaar zijn voor M&O, geven we hieronder handvatten om op verschillende niveaus waarborgen in te richten, ter voorkoming of vermindering van het risico op M&O. Dit vormt een handleiding voor het voorkomen van M&O in onze regelgeving en uitvoering. Zowel beleidsmakers, juristen, inkopers als control kunnen dit hanteren als richtsnoer bij hun werkzaamheden.
We kiezen voor een procesmatige benadering, waarbinnen acht stappen worden onderscheiden, te weten:

1. Beleidsvoorbereiding
2. Regelgeving
3. Uitvoering
4. Voorlichting/communicatie
5. Controlebeleid
6. Maatregelenbeleid
7. Verantwoording
8. Evaluatie

Beleidsvoorbereiding

In de planfase wordt beleid opgesteld en worden verordeningen of subsidieregelingen voorbereid. Bij het opstellen van de regelingen wordt gezorgd dat de kans op M&O geminimaliseerd is. Medewerkers moeten zich zo vroeg mogelijk in het beleidsproces al afvragen of er sprake is van een voor M&O gevoelig beleidsterrein.

Regelgeving

Regelgeving moet zo min mogelijk ruimte bieden voor M&O. Dit wordt bereikt door heldere definities, een nauwkeurige omschrijving van doel en doelgroep en het opnemen van rechten, plichten en voorwaarden. In de regelgeving wordt ook opgenomen welke maatregelen of sancties worden toegepast bij geconstateerd M&O.
Daarnaast dienen in beschikkingen altijd (indien van toepassing) de volgende punten te worden vermeld: rechten, plichten, voorwaarden en mogelijke maatregelen of sancties.

Uitvoering

M&O spelen met name bij die activiteiten waarbij de informatie van derden/ belanghebbenden van groot belang is voor het verlenen of vaststellen van uitkeringen, subsidies, heffingen, belastingen en vergunningen. Processen waarbij gevoeligheden spelen, moeten voldoende maatregelen bevatten om de tijdigheid, juistheid, volledigheid en prestatielevering te toetsen van de door belanghebbende verstrekte gegevens. Dit wordt vastgelegd in de procesbeschrijvingen. Regelmatig dient te worden getoetst of wordt gewerkt conform de procesbeschrijving, bijvoorbeeld in de verbijzonderde interne controle (VIC). Uitgangspunt is dat de checks dan zichtbaar worden vastgelegd.

Medewerkers gaan goed na of door inwoner(s) of bedrijven aan de voorwaarden van bijvoorbeeld een subsidie of uitkering is voldaan. De door de klant of het bedrijf aangeleverde gegevens worden – indien mogelijk – geverifieerd. Op deze wijze worden toereikende controles uitgevoerd op het waarborgen van de getrouwheid en rechtmatigheid.

Voorlichting/communicatie

Voorlichting geven heeft een preventieve werking en is, in dit kader, vooral van belang om misbruik en oneigenlijk gebruik van een regeling te voorkomen en te ontmoedigen. Bij het beschrijven van de processen dient aandacht te worden gevraagd voor het risico op M&O. Door het onderwerp M&O als vast onderdeel op te nemen in gesprekken van de Verbijzonderde Interne Controle (VIC) wordt de interne communicatie over dit onderwerp levend gehouden.

Controlebeleid

Zoals hierboven beschreven, is het doel om belangrijke ‘checks’ te implementeren in de dagelijkse uitvoering, het management en de monitoring daarvan. In control termen wordt dan over de Interne Controle binnen de eerste en tweede lijn gesproken. Daarnaast toetst periodiek de VIC in de derde lijn, de opzet, het bestaan en de werking van de interne beheersmaatregelen ter voorkoming van M&O. Dit gebeurt op basis van een risico-gedreven controle aanpak. Met de invoering van de rechtmatigheidsverantwoording is de toets op M&O één van de voorwaarden geworden waaraan het college de uitvoering van haar taken toetst op rechtmatigheid. Daarmee komt dit onderwerp nadrukkelijker op de agenda van college en gemeenteraad.

Beleidsregels

Om te kunnen reageren op geconstateerd misbruik en/of oneigenlijk gebruik, is een adequaat maatregelenbeleid vereist dat aansluit op de regelgeving. Als norm hierbij wordt gehanteerd, dat tenminste het behaalde voordeel wordt weggenomen. Afhankelijk van de ernst van de situatie, wordt in voorkomende gevallen aangifte gedaan. Van het strikt toepassen van de beleidsregels gaat ook een preventieve werking uit.

Aandachtpunten hierbij zijn dat bepalingen met betrekking tot sancties en maatregelen opgenomen worden in de desbetreffende verordening c.q. regeling en het waarborgen dat het maatregelenbeleid in gelijke gevallen op gelijke wijze wordt toegepast. In geval van fraude (misdrijf) wordt in beginsel aangifte gedaan bij het de politie.

Verantwoording

Om inzicht te krijgen in de wijze waarop het M&O beleid wordt uitgevoerd en wordt nageleefd, moet verantwoording worden afgelegd. Dit wordt gerealiseerd door aan te sluiten bij de reguliere planning- en controlcyclus, waarbij in de jaarrekening de rechtmatigheidsverantwoording door het college wordt opgenomen. Daarnaast zal in de paragraaf bedrijfsvoering een nadere toelichting worden gegeven op de eventuele rechtmatigheidsfouten. De accountant betrekt de rechtmatigheidsverantwoording, inclusief de nadere toelichting in de paragraaf bedrijfsvoering, in zijn oordeel over de getrouwheid van de jaarstukken. Gaandeweg het jaar wordt de auditcommissie op de hoogte gebracht over de voortgang/resultaten van de interne controle, bijvoorbeeld na afronding van de interim controle van de accountant middels de managementletter.

Evaluatie

De bevindingen en aanbevelingen in bijvoorbeeld de VIC rapportages en het accountantsverslag gebruiken we (waar nodig) om van te leren en het beleid hiervan verder te verbeteren.

Bijlagen

Bijlage 1: Definities risicomanagement en risico

Ten aanzien van risicomanagement worden verscheidene definities gebruikt. Termen die veelal naar voren komen zijn; managen, voorkomen, risico's, kans, gevolg. Haisma (2003) geeft een definitie die al deze termen in zich heeft: *"Het nemen van beslissingen die gericht zijn op het voorkomen of minimaliseren van de nadelige gevolgen die het optreden van een risico met zich mee kan brengen."*

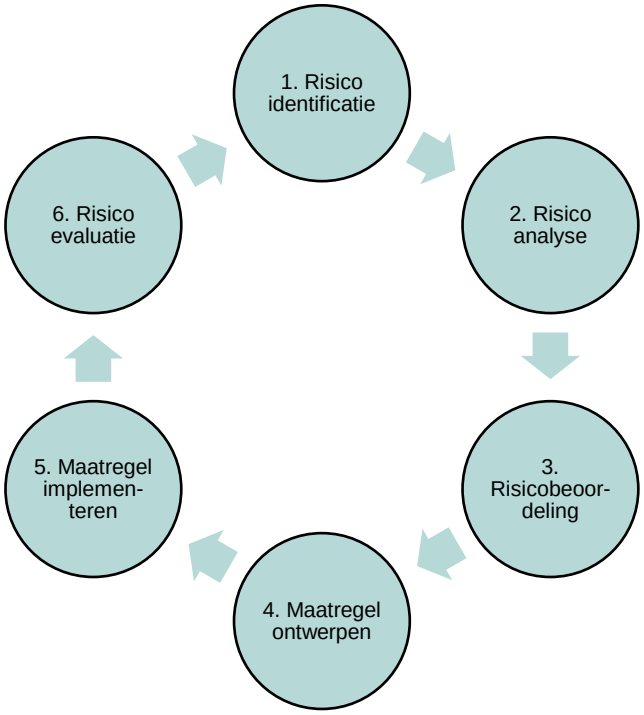
Om de term risicomanagement helder voor ogen te hebben, is het van belang te weten wat een risico is. Haisma (2003) geeft hier ook een definitie voor: *''Een risico is de kans op het optreden van een gebeurtenis, die een negatief gevolg voor de gemeente met zich mee kan brengen."*

Cyclus van risicomanagement

In de theorie van risicomanagement wordt veelal uitgegaan van het cyclische karakter van risicomanagement. Organisaties zijn namelijk continu onderhevig aan veranderingen. De risico-omgeving verandert ook voortdurend. De prioriteiten van de organisatie en het relatieve belang van risico's verschuiven daarmee. De risico's moeten daarom voortdurend bekeken, overwogen en afgewogen worden. In dit proces zijn de volgende stappen te onderscheiden:

1. identificatie
2. analyse
3. beoordeling
4. maatregelen ontwerpen
5. maatregelen implementeren
6. evaluatie o.b.v. rapportage (effect meten en mogelijk financieel gevolg in beeld brengen).

In figuur 1 is een overzicht weergegeven van de cyclus van risicomanagement.



Figuur 1. Risicomanagement Cyclus

Stappen 1 en 2: Risico's identificeren en analyseren

De eerste fase in het risicomanagementproces is het in kaart brengen van de risico's. Het doel van het in kaart brengen van de risico's is om te bepalen welke factoren de realisatie van de bestaande beleidsdoelen zowel positief als negatief kunnen beïnvloeden (hieronder kunnen eveneens nieuwe ontwikkelingen die op de gemeente afkomen, bijvoorbeeld nieuwe of gewijzigde wetgeving, worden gerekend). Basis voor het in kaart brengen van de risico's zijn de gewenste effecten die worden gesteld onder de het kopje *'Wat willen we bereiken?'*

Risico's zijn in diverse categorieën te onderscheiden. Meerdere indelingen zijn daarbij mogelijk. Wij hebben gekozen voor een indeling in:

1. Strategische risico's
2. Marktrisico's
3. Schaderisico's
4. Operationele risico's

1. Strategische risico's

Tot de strategische risico's behoren de rijksbezuinigingen die op gemeenten afkomen. Ook nieuwe wetgeving kan risico's met zich meebrengen, bijvoorbeeld als ze leiden tot lagere inkomsten of meer werk. Daarnaast behoren ook het niet halen van bestuurlijke doelen en niet ontvangen van externe bijdragen tot de strategische risico's. Ook de verbonden partijen

brengen strategische risico's met zich mee, door bijv. beperkte zeggenschap, economische ontwikkelingen en/ of slechte bedrijfsvoering bij verbonden partijen. Een ander strategisch risico bestaat uit de openeinderegelingen. Bijvoorbeeld de Wmo of jeugdzorg, waarbij de uitgaven van de gemeente in de loop der tijd fors kunnen toenemen. Tot slot kunnen ook in uitzonderlijke gevallen (bijvoorbeeld de hack in 2020) cyberrisico's strategisch van karakter zijn (zie hiervoor 4. Operationele risico's).

2. Marktrisico's

Tot de economische/marktrisico's behoren Lokale heffingen, financiering en grondexploitatie, fluctuaties in de rentestand, vastgoedmarkt, belastingen, de ontwikkeling van de werkloosheid. Dit zijn posten die direct financiële gevolgen hebben voor de gemeente. Financiering betreft hier de uitstaande en aangetrokken gelden. Hoe hoog is de te betalen of de te ontvangen rente en welke risico's worden hier gelopen? Grondexploitaties zijn ook gevoelig voor eventuele financiële gevolgen. Tegenvallende grondopbrengsten hebben direct financiële gevolgen.

3. Schade risico's

Hieronder vallen risico's die verband houden met juridische procedures zoals aansprakelijkheidstellingen. De vermogenspositie van de gemeente wordt aangetast door bijvoorbeeld claims van derden als gevolg van wettelijke- of contractuele aansprakelijkheid (bijv. letselschade, planschade, vermogensschade). Ook beschadiging of verlies van een materieel bezit zoals gebouwen, installaties, inventaris, ICT, vervoersmiddelen en goederen vallen onder deze categorie. Tot schaderisico's behoort ook fraude (zie hiervoor ook hoofdstuk 4) Laatste voorbeelden van schaderisico's vormen asbestverontreiniging en gebreken bij civiele kunstwerken van de gemeente.

4. Operationele risico's

Hieronder vallen risico's die verband houden met de wijze waarop de organisatie is ingericht, zoals organisatiestructuur, richtlijnen, regelgeving, administratieve organisatie (AO), interne controle (IC), protocollen, interne gedragsregels, etc.). Met name het verouderd, onjuist of onvolledig zijn hiervan is een risico. Een goede AO/IC beperkt het optreden van risico's.

Cyberrisico's vormen een belangrijk aspect binnen de operationele risico's. Deze risico's hebben onder andere betrekking op toegang tot het netwerk en/of applicaties door onbevoegden (intern of extern), het wijzigen of ontoegankelijk maken van informatie in dit netwerk en de applicaties, phishing, ICT-storingen en datalekken. Een bijkomend risico bij cyberbeveiliging en privacybescherming is de kans op boetes die de gemeente kan krijgen in

het kader van de AVG of NIS2-richtlijn (Cyberbeveiligingswet), ten gevolge van het niet naleven van deze wetgeving. NIS2 is een richtlijn die gemeenten verplicht passende en evenredige maatregelen te nemen om cyberbeveiligingsrisico's te beheersen.
Voor de operationele risico's en bijbehorende beheersmaatregelen verwijzen we ook naar het gemeentelijke continuïteitsplan.

De geïdentificeerde risico's worden op basis van de onderscheiden categorieën in het overzicht risico's Hof van Twente geplaatst. 2 keer per jaar wordt het overzicht risico's (zie bijlage I) geactualiseerd en vastgesteld door het college van B&W.

Stap 3 : Risicobeoordeling

Uit de identificatie en analyse kan een groot aantal risico's voortkomen. Het is onmogelijk en onwenselijk om te sturen op al de geïdentificeerde risico's. Door middel van het overzicht risico's Hof van Twente worden de belangrijkste risico's overzichtelijk in kaart gebracht. Zo kan qua tijd en energie gefocust worden op de risico's die de grootse impact op de organisatie en de gestelde doelen kunnen hebben. In dit overzicht worden de risico's gekwantificeerd. Het overzicht vormt een vast onderdeel van de paragraaf Weerstandsvermogen en risicobeheersing in de jaarlijkse programmabegroting en jaarverslag.
Bij het bepalen van de omvang van het risico wordt uitgegaan van een situatie dat het risico zich ook daadwerkelijk voordoet. De risico-eigenaar maakt een inschatting van de financiële impact wanneer het risico optreedt en de kans dat zich dit voordoet. Zoals eerder beschreven kan gekozen worden tussen drie categorieën (klein/middel/groot).

Stappen 4, 5 en 6: (Beheers-) maatregelen ontwerpen, implementeren en evalueren

Op basis van de uitkomsten van de eerste 3 stappen wordt bepaald hoe met de risico's moet worden omgegaan om de gevolgen van het optreden van risico's tot een minimum te beperken. De stappen 4 t/m 6 gaan over het omgaan met risico's. Hieronder benoemen we vier risicostrategieën, die gebruikt kunnen worden om (beheers)maatregelen te nemen met betrekking tot een risico. Deze risicostrategieën zijn:

Vermijden:
Hierbij wordt de kans/mogelijkheid van optreden van een bepaald risico opgeheven. Besloten wordt om bepaalde activiteiten op een andere wijze of zelfs helemaal niet uit te voeren. Vermijden is echter niet altijd een relevante categorie van maatregelen. Vermijden

kan namelijk tot gevolg hebben dat bestuurlijk/maatschappelijke doelstellingen die met bepaalde activiteiten worden beoogd niet kunnen worden gerealiseerd.

Verminderen:

Hierbij wordt beoogd de kans op optreden of het gevolg van optreden van het risico te verkleinen. Indien men de kans wil verkleinen moeten voorzorgsmaatregelen worden genomen. Bij een gevolggerichte maatregel is het echter zo dat men nu nadenkt over de maatregelen en eventuele voorbereidingen treft maar dat men de daadwerkelijke maatregel pas treft op het moment dat het risico optreedt.

Overdragen:

Overdragen van risico's aan een andere partij leidt niet direct tot het wegnemen van de oorzaken voor risico's maar wel tot een vermindering van de financiële impact voor het project, omdat verwacht wordt dat die andere partij in staat zal zijn het risico beter te managen of te dragen.

Accepteren: Het accepteren van een risico is ook nog een mogelijkheid,

Per risico zal bepaald worden welke strategie het beste ingezet kan worden. In het algemeen neemt de gemeente Hof van Twente een vooruitstrevende en ondernemende houding aan. Dit impliceert, dat risico's niet altijd vermeden kunnen worden. Ambitieuze vernieuwingsprojecten, ruimtelijke ontwikkelingen en een uiteenlopend palet aan gemeenschapsvoorzieningen, het zijn voorbeelden van situaties die van nature met risico's gepaard kunnen gaan. Inzet is daarbij om de risico's te kennen, de gevolgen ervan te hebben doordacht en via afgestemde maatregelen deze zoveel mogelijk te beheersen.
Dit geldt bijvoorbeeld voor het risico dat projecten door markt- en prijsontwikkelingen (fors) duurder uitvallen dan geraamd.

Bijlage 2: Instrumentarium risicobeheersing

Onderstaand volgt een overzicht van het instrumentarium waarover gemeente Hof van Twente beschikt in haar risicobeheersing.

A: Interne controleplan

Het jaarlijkse interne controleplan dat door het college wordt vastgesteld vormt de basis voor de interne controles van diverse processen waarin financiële beheershandelingen naar voren komen. Bevindingen en aanbevelingen van de accountant vormen mede de basis voor de opzet.

B: Accountantscontrole

De jaarlijkse accountantscontrole bestaat uit een interimcontrole en een eindcontrole. De bevindingen en aanbevelingen uit zowel de Managementletter als het Controlerapport geven aanleiding en bruikbare informatie om bestaande en nieuwe risico's en de effectiviteit van de maatregelen te volgen, te beoordelen en te organiseren.

C: Klokkenluidersregeling

Met de klokkenluidersregeling kunnen ambtenaren melding maken van misstanden met betrekking tot de gemeentelijke organisatie. Daarbij moet sprake zijn van een op redelijke gronden gebaseerd vermoeden. Dit kan ook een misstand zijn met betrekking tot fraude.

D: Gedragscode ambtelijke en bestuurlijke integriteit en de ambtseed

Deze gedragscode draagt de normen en waarden van de organisatie uit en bevordert de onderlinge communicatie daarover. Bij de ambtseed verklaart de medewerker uitdrukkelijk zich als een goede ambtenaar te gedragen. Hierdoor spelen de gedragscode en de ambtseed een belangrijke rol bij het bevorderen van het integriteitsbewustzijn en het voorkomen van fraude.

E: Vertrouwenspersoon

De organisatie beschikt over enkele interne (en externe) vertrouwenspersonen. Deze begeleiden medewerkers wanneer ze in aanraking komen met ongewenst gedrag binnen de organisatie en dit hebben gemeld aan de vertrouwenspersoon. Bijvoorbeeld bij fraude binnen de organisatie.

G: Meer inzet op professionaliseren contractmanagement

Door meer in te zetten op contractmanagement kunnen contracten met partijen scherper worden gecontroleerd, waardoor de gemeente deze partijen beter op de overeengekomen afspraken kan wijzen. Het risico dat de partij bijvoorbeeld te hoge kosten in rekening brengt, kan met deze beheersmaatregel worden verkleind. Ook kan de relatie tussen opdrachtgever en opdrachtnemer verder worden geprofessionaliseerd.
De prestatielevering is een aansluitende maatregel. Hierbij wordt gecontroleerd of leveranciers hebben geleverd. Daarmee wordt het risico beheerst dat ingekochte goederen niet overeenstemmen met geleverde goederen.

H: Pentesten en controleren autorisaties

Met het regelmatig uitvoeren van pentesten kunnen kwetsbaarheden in systemen gevonden en aangepakt worden. Daardoor wordt het voor onbevoegden lastiger om in het netwerk of applicaties te komen en wijzigingen aan te brengen, zodat daar vervolgens voordeel uit kan worden genoten. Het regelmatig controleren van de autorisaties helpt ook bij het beheersen van dit risico.

I: Logging

In een aantal systemen worden de gebeurtenissen en handelingen automatisch bijgehouden en geregistreerd. Hierdoor kan achteraf gecontroleerd worden wie (wanneer) in het systeem heeft gezeten en of daar een goede reden voor was. Met het loggen van gegevens wordt het lastiger om fraude te plegen. De workflow in Youforce wordt bijvoorbeeld gelogd.

J: Toezicht en controle

Een manier waarop zorgfrauderisico's verminderd kunnen worden, is door meer toezicht en controle. Bijvoorbeeld bij het risico op malafide zorgaanbieders die onder contract van de gemeente staan, het risico op zorgverlening door ongekwalificeerde personen en het risico op besteding van het persoonsgebonden budget aan andere doelen. Voor de uitvoering van deze beheersmaatregel worden toezichthouders aangewezen. Taken van de toezichthouders bestaan uit: proactief/preventief kwaliteits- en rechtmatigheidsonderzoek en het ontvangen en beoordelen van meldingen/signalen.

K: Barrièremodel

Het barrièremodel is opgesteld door verschillende partijen (Samen14: gemeenten, politie, het OM, etc) om zorgfraude aan te pakken, Met dit model worden bij aanbestedingen aan de

voorkant strengere eisen gesteld aan zorgaanbieders. Vervolgens worden van gegunde zorgaanbieders risicoschattingen gemaakt die gekoppeld zijn aan een stoplichtmodel. Als de zorgaanbieder rood kleurt, kan de gemeente verbetermaatregelen opleggen of de overeenkomst beëindigen.

L: Gustos-controles

Dit zijn integrale controles die met verschillende ketenpartners (douane, politie, sociale recherche) van de gemeente 5 tot 6 keer per jaar worden uitgevoerd. Tijdens deze controles worden adressen van woningen en bedrijven bezocht, waarbij een onderbuik gevoel van uiteenlopende vormen van fraude en ondermijningsactiviteiten bestaat.

M: Sociale Recherche

Op het gebied van sociale zaken vinden er gerichte controles plaats naar fraude door de sociale recherche. Naar aanleiding van meldingen of signalen van bijvoorbeeld zwartwerken, woonfraude of zorgfraude wordt dan (strafrechtelijk)onderzoek ingesteld.

N: Handhaving en toezicht

Door (extra) toezicht en handhaving kunnen vergunningsfrauderisico's beter beheerst worden. Bijvoorbeeld wanneer een persoon zich niet aan de bouwvereisten van de vergunning houdt of fouten in de vergunningsprocedure opzettelijk worden genegeerd.

O: Overleggen bewijsstukken

Een aantal frauderisico's kunnen voorkomen worden door het overleggen van bewijsstukken. Het risico op diplomafraude kan de gemeente beheersen door diploma's op te vragen of deze fysiek mee te laten nemen en de kans op identiteits- of gegevensfraude kan verminderd worden door het laten overleggen van een geldig ID-bewijs. Bij de aanvraag van een uitkering of bijstand kan ook nog om andere bewijsstukken worden gevraagd, bijvoorbeeld bankafschriften of huurcontracten.

P: Raadplegen systemen en systeemkoppelingen

Naast het opvragen van bewijsstukken kunnen ook verschillende systemen geraadpleegd worden om risico's op gegevens- en identiteitsfraude te beheersen. Bij het uitkeren van bijstand of een uitkering kunnen persoonsgegevens in het BRP en Suwinet geraadpleegd worden. Gegevensfraude bij een vergunningaanvraag kan voorkomen worden door in het kadaster, bestemmingsplan of archief te raadplegen. Het BRP-systeem is aan een aantal

procedures gekoppeld, bijvoorbeeld aan de verkiezingsprocedure of het aanvragen van scheidingsdocumenten.

Q: Sanctiebeleid

Sanctiebeleid richt zich op het adequaat reageren en passende maatregelen treffen in het geval van misbruik en oneigenlijk gebruik. Bijvoorbeeld bij het verstrekken van bijstand of uitkeringen. Sancties kunnen bestaan uit boetes, terugvorderingen van voorzieningen waarvan misbruik is gemaakt en (tijdelijke) uitsluiting van aanspraak op voorzieningen/bijstand. De beheersmaatregel draagt bij aan het voorkomen van risico's, doordat de sancties afschrikkend werken.

R: Beperking volmachten verkiezingen

Tijdens de verkiezingen mogen gemachtigden voor maximaal twee andere kiezers stemmen middels een volmacht.

Bijlage 3: Rollenoverzicht

Risicomanagement begint bij bewustwording. Medewerkers, bestuur en management moeten nut en noodzaak hiervan inzien. Alle actoren zoals raadsleden, collegeleden, directieleden, teamleiders, projectleiders en medewerkers dienen zich bewust te zijn van hun verantwoordelijkheden en hun rol inzake risicomanagement. Herhaaldelijk dient aandacht voor dit onderwerp gevraagd te worden. Maar evenzo belangrijk is de inbedding in de manier van werken binnen Hof van Twente. Door structureel samen naar risico's te kijken, wordt het onderdeel van onze cultuur en werkwijze. Daarbij hebben de verschillende actoren ieder een andere rol. In onderstaande beschrijving zijn de diverse rollen op hoofdlijnen nader uitgewerkt.

Organisatie

Gemeentesecretaris

Als eindverantwoordelijke voor de ambtelijke organisatie vervult de gemeentesecretaris en belangrijke rol om het belang van risicobewustzijn en risicomanagement in de organisatie uit te dragen. De gemeentesecretaris ziet erop toe dat politiek-bestuurlijke risico's worden gesignaleerd, gemanaged en gemonitord en in relatie worden gebracht met de strategische belangen van de organisatie. Hiervoor is van belang dat in college- en raadsvoorstellen op een goede (integrale) manier wordt ingegaan op beleidsmatige en financiële risico's die aan de voorgestelde besluiten verbonden zijn.

Teamleiders

Teamleiders zijn verantwoordelijk voor de feitelijke inrichting van processen, waarbij de risicoanalyse en risicobereidheid moeten worden omgezet in het feitelijk beheersen van de risico's. De teamleiders zullen interne beheersingsmaatregelen in de processen en interne controleprocedures inrichten, bijdragen aan een risicobewuste cultuur en meewerken aan de monitoring van de effectiviteit van de interne beheersing. Eventuele afwijkingen dienen de teamleiders te verklaren.

Projectleiders en programmaleiders

Tijdens de uitvoering van projecten en programma's dient de projectleider/programmaleider in verschillende fases de risicomanagementcyclus te doorlopen.
Dat wil zeggen dat bij de verkenningsfase de risico's in beeld gebracht worden en dat tijdens de ontwikkelingsfase aangegeven wordt hoe hiermee moet worden omgegaan. Vervolgens moet dit continu de aandacht hebben en onderwerp van gesprek zijn met opdrachtgever en/

of stuurgroep. De projectleider/programmaleider draagt er zorg voor, dat in college- of raadsvoorstellen, die gaan over het project, of programma een volledig beeld wordt geschetst van de risico's en dat hierover in projectrapportages/programmarapportages verantwoording wordt afgelegd.

Medewerkers

In het dagelijkse werk dienen medewerkers zich bewust te zijn van de risico's die er zijn, deze te signaleren en mee te denken hoe hiermee om moet worden gegaan. Zij leveren een belangrijke bijdrage aan het bestaan en in stand houden van een hierbij passende cultuur. Bij beleidsvorming dient dit aandacht te krijgen in adviesnota's. Binnen projecten dient risicomanagement een belangrijk onderdeel te zijn in projectplannen en projectrapportages. Daarnaast dienen teamleiders door gesprekken met medewerkers (teamoverleg, werkbesprekingen, jaargesprekken) risico's en beheersmaatregelen te benoemen in het dagelijkse werk. Waar mogelijk dient dit vastgelegd te worden in (bestaande) procesbeschrijvingen of werkinstructies.

Concernstaf

De rol van de concernstaf is tweeledig. Enerzijds is ze verantwoordelijk voor het faciliteren van de inrichting van een adequaat risicomanagementsysteem ten behoeve van het bestuur, het management en de medewerkers. Bijvoorbeeld bij het ondersteunen van risicobeleid, risicoanalyses en risicobewustzijn. De onafhankelijke positie van de concernstaf in de organisatie draagt in belangrijke mate bij aan het rendement van risicomanagement. Anderzijds heeft de concernstaf een monitoringfunctie. De bestuurders en de teamleiders zijn in eerste lijn verantwoordelijk voor de monitoring van zowel de effectiviteit van de interne beheersmaatregelen alsmede van het risicomanagementsysteem. De coördinatie van de interne controle heeft hier een grote rol in.

Accountant

Buiten de organisatie bevindt zich een externe accountant met een assurancefunctie. Hij heeft vanuit zijn activiteiten uit hoofde van de jaarrekeningcontrole veelal aandacht voor het effectief functioneren van (onderdelen van) het risicomanagementsysteem, aangezien dat systeem een belangrijke randvoorwaarde is voor de totstandkoming van betrouwbare managementinformatie en -rapportages. Bovendien voert de externe accountant een marginale beoordeling uit van het jaarverslag van de gemeente, waartoe ook de risicoparagraaf behoort (paragraaf weerstandsvermogen). De ervaringen van de afgelopen

jaren is, dat de externe accountant vanuit zijn natuurlijke adviesfunctie zijn bevindingen met betrekking tot het risicomanagementsysteem rapporteert aan het college en aan de raad (managementletter).In de managementletters van de afgelopen jaren verzoekt de accountant inzicht te geven in de risico's op fraude binnen de gemeente.

College van burgemeester en wethouders

In het duale stelsel is het college van B&W primair de eigenaar van alle risico's. Besturen gaat niet zonder risico's. Dit gegeven vraagt om extra aandacht bij besluitvormingsprocessen. De Raad draagt, in het kader van zijn kaderstellende en controlerende rol, eindverantwoordelijkheid voor alle risico's in de gemeente. College van B&W en Raad hebben om die reden beiden belang bij de juiste informatie over de risico's, die het realiseren van de doelstellingen kunnen belemmeren. Door risico's vroegtijdig te onderkennen, kunnen adequate maatregelen worden genomen die de gevolgen van risico's beperken.

Gemeenteraad

De raad heeft een belangrijke rol in het gemeentelijk risicomanagement. Beschouwen we de cyclus die in de nota Risicomanagement als uitgangspunt is gekozen, dan heeft de raad vanuit zijn kaderstellende en controlerende rol wezenlijke taken in de fasen 1 (risico-identificatie) en 6 (risicoevaluatie).
Wat betreft risico-identificatie heeft de raad een signalerende functie door het stellen van vragen op uiteenlopende manieren, van schriftelijke vragen, vragenuurvragen, vragen over raadsvoorstellen in raadsvergaderingen tot het stellen van vragen over hetgeen via de actieve informatievoorziening vanuit het college mondeling of in raadsbrieven is gepresenteerd. In de navolgende tabel is illustratief een scala aan vragen verwoord die gedurende een jaar uit oogpunt van risicomanagement gesteld kunnen worden en welke momenten daarvoor aangegrepen kunnen worden.
Wat betreft de risico-evaluatie gaat het daarbij met name om die momenten waarop verantwoording en reflectie op een afgelopen periode centraal staan. Denk aan de bestuursrapportages en de jaarstukken (jaarverslag en jaarrekening), maar ook evaluatierapporten of rekenkameronderzoek kan hiertoe de aanleiding vormen. In de verantwoordingsdebatten die hierover gaan zou de vraag hoe de gemeente is omgegaan met risico's een vanzelfsprekendheid moeten zijn.

Bijlage 4: Risico's en maatregelen betreffende informatieveiligheid

Analyse

Onderstaand is de analyse van de te onderscheiden informatiebeveiligingsrisico's en een gekozen mitigatie-aanpak weergegeven. Deze is nader uitgewerkt in de Notitie informatiebeveiligingsrisico's d.d. 25 februari 2025.

1. Datalekken

Analyse: Datalekken kunnen optreden door ongeautoriseerde toegang of onzorgvuldig handelen met gevoelige gegevens, zoals verlies van apparaten of verkeerd verzonden e-mails. Dit kan gevolgen hebben voor de privacy van burgers en reputatie van de gemeente.
Mitigatie:

- Encryptie van gegevens, zowel in rust als in transit.
- Beveiligde e-mailcommunicatie en gecontroleerd verzenden van gevoelige informatie.
- Training en procedures voor medewerkers over het veilig omgaan met gegevens.
- Beveiliging van eindapparatuur (bijvoorbeeld via versleuteling laptops en telefoons).
- Incident response plan voor het geval een datalek plaatsvindt.

2. Malware

Analyse: Malware kan systemen infecteren, gegevens stelen of systemen saboteren, en komt vaak via e-mailbijlagen of websites. We kunnen aanzienlijke schade ondervinden als systemen worden geïnfecteerd.
Mitigatie:

- Antivirussoftware en firewalls installeren en up-to-date houden.
- E-mailfilters om schadelijke bijlagen te blokkeren.
- Regelmatige software-updates en patchbeheer.
- Bewustwordingstraining over het herkennen van verdachte e-mails en websites.
- Security response in geval van verdachte activiteiten.

3. Ransomware

Analyse: Ransomware versleutelt gegevens en vraagt losgeld voor de decryption key. Het kan de gemeentelijke dienstverlening ernstig verstoren.
Mitigatie:

- Back-ups van kritieke gegevens op offline locaties volgens 3-2-1 principe.
- Netwerksegmentatie om verspreiding van ransomware te voorkomen.
- Gebruik van multi-factor authenticatie (MFA) om toegang tot systemen te beveiligen.
- Incident response plan voor ransomware-aanvallen, inclusief communicatieprotocol.

4. Phishing

Analyse: Phishing-aanvallen misleiden medewerkers om persoonlijke informatie te delen, zoals inloggegevens, wat kan leiden tot compromittering van systemen.

Mitigatie:

- E-mailbeveiliging zoals DMARC, SPF en DKIM.
- Actieve link- en webscanning om malafide sites te herkennen.
- Training voor medewerkers om verdachte e-mails te herkennen.
- Multi-factor authenticatie (MFA) voor kritieke systemen.
- Simulatie van phishing-aanvallen om de paraatheid van medewerkers te testen.

5. Insider Threats

Analyse: Bedreigingen van binnenuit kunnen zowel onopzettelijk (door fouten) als opzettelijk zijn, en kunnen leiden tot het lekken of stelen van gevoelige informatie. Mitigatie:

- Toegangsbeheer door het principe van minimaal noodzakelijke toegang toe te passen.
- Monitoring van gebruikersactiviteiten (logbestanden en anomaliedetectie).
- Bewustwordingstraining om onbedoelde fouten te minimaliseren.
- Gedragscodes voor medewerkers.

6. Verlies van apparatuur of gegevens

Analyse: Verlies van apparaten kan leiden tot de onbedoelde blootstelling van gevoelige informatie als ze niet goed beveiligd zijn.

Mitigatie:

- Versleuteling van mobiele apparaten (laptops, telefoons, USB's).
- Beleid voor het melden van verlies van apparatuur.
- Apparaten met wachtwoorden en biometrische beveiliging.
- Remote wipe-mogelijkheden voor apparaten bij verlies.

7. Kwetsbaarheden in software

Analyse: Verouderde software bevat vaak beveiligingslekken die door hackers kunnen worden misbruikt.

Mitigatie:

- Regelmatige software-updates en patchbeheer (minimaal 2x per jaar).
- Kwetsbaarheidsmanagementprogramma om de risico's van verouderde software te beheren.

8. Configuratiefouten

Analyse: Fouten in de configuratie van systemen kunnen de toegang tot netwerken en gegevens blootstellen.

Mitigatie:

- Regelmatige configuratieaudits en het toepassen van best practices.
- Automatiseren van configuratiebeheer om menselijke fouten te minimaliseren.
- Beperkingen op toegangsrechten op basis van functies en noodzaak.

9. Natuurrampen of onvoorziene gebeurtenissen

Analyse: Onvoorziene gebeurtenissen zoals brand, stroomuitval of overstromingen kunnen de gemeentelijke dienstverlening verstoren.

Mitigatie:

- Inzet van back-up voorzieningen bij elektriciteitsuitval zoals UPS en een generator.
- Brandblus apparatuur.
- Continuïteitsplanning en Disaster Recovery-strategieën.
- Back-ups op geografisch gespreide locaties.
- Oefeningen voor crisismanagement en het regelmatig testen van de plannen.

10. Nalevingsrisico's

Analyse: Niet naleven van wet- en regelgeving zoals de AVG kan leiden tot juridische gevolgen en boetes.

Mitigatie:

- Compliance-programma om te voldoen aan relevante wet- en regelgeving.
- Regelmatige audits en reviews van processen en systemen.
- Bewustwordingstrainingen voor medewerkers over de verplichtingen van de AVG en andere wetgeving.

11. Onduidelijkheid/wijziging in rollen/functies en toegang

Analyse: Onvoldoende afgebakende rollen en rechten tot informatie kunnen leiden tot onrechtmatige toegang tot gevoelige gegevens.

Mitigatie:

- Rolgebaseerd toegangsbeheer (RBAC).
- Regelmatige toegangstoewijzing en -beoordeling.
- Beleid en procedures voor het aanpassen van toegang bij functiewijzigingen of vertrek van medewerkers (logische toegangsbeveiliging).

12. Leveranciersrisico's

Analyse: Leveranciers kunnen onbevoegde toegang verschaffen tot gemeentelijke systemen en gegevens.

Mitigatie:

- Leveranciersbeheer met strikte beveiligingseisen in contracten.
- Audits van leveranciers op hun beveiligingspraktijken.
- Beperkingen op toegangsrechten voor leveranciers tot enkel noodzakelijke systemen (Jumphost).

Door deze risico's te analyseren en gerichte maatregelen te nemen, kan de gemeente de informatiebeveiliging verbeteren en de impact van potentiële incidenten verkleinen.