

Nota integraal risicomanagement en weerstandsvermogen 2024 tot en met 2027

1. Besluit

Het algemeen bestuur van SamenTwente

Gelet op:

- Artikel 18 van de financiële verordening SamenTwente;
- Het Besluit begroting en verantwoording provincies en gemeenten

Besluit:

- Nota integraal risicomanagement en weerstandsvermogen 2024 tot en met 2027 vast te stellen;
- De oude nota "Van risicomanagement tot weerstandsvermogen 2018" in te trekken.

2. Inleiding

Dagelijks maken we afwegingen die van invloed kunnen zijn op het realiseren van maatschappelijke opgaven. De omgeving waarin SamenTwente dit doet is niet altijd voorspelbaar. We krijgen te maken met onzekerheden, risico's en kansen. Dit kan ertoe leiden dat het onzeker is of we onze doelstellingen zullen behalen. Goed risicomanagement helpt hierbij en helpt bij het nemen van onderbouwde besluiten. Risicomanagement zorgt er niet alleen voor dat risico's duidelijk worden, maar zorgt er vooral voor dat er maatregelen getroffen worden om risico's te beheersen.

Doel van deze notitie

Deze notitie beschrijft de uitgangspunten voor het risicomanagement bij SamenTwente en het hieraan gerelateerde weerstandsvermogen. Deze notitie biedt handvatten voor onze organisatie die helpend zijn voor zowel ons bestuur als de ambtelijke organisatie als het gaat om het managen en beheersen van risico's. Daarnaast zijn wij als gemeenschappelijke regeling volgens het Besluit begroting en verantwoording (BBV) wettelijk verplicht om risico's te inventariseren die van belang kunnen zijn voor onze financiële positie. Om de financiële consequenties van risico's op te kunnen vangen wordt weerstandsvermogen aangehouden. Dit zijn middelen die een buffer vormen om de financiële effecten van risico's op te vangen.

Kanttekeningen

Is risicomanagement dé oplossing voor het voorkomen van incidenten? Het antwoord is: nee. We kunnen namelijk nooit alle risico's in kaart brengen die zich in een bepaalde periode zouden kunnen voordoen. Simpelweg omdat risicomanagement geen exacte wetenschap is en bovendien zou dit ook niet doelmatig zijn. Risicomanagement vergroot wel de kans op succes, draagt bij aan de bewustwording van het werken met risico's en helpt onze organisatie om meer weloverwogen keuzes te maken.

Hebben risico's alleen een negatief effect? Ook hierop is het antwoord: Nee. Wanneer we in dit document spreken over risico's dan hebben we het ook over kansen. Kansen die gezien worden wanneer we het hebben over het realiseren van onze doelstellingen. Risicomanagement geeft dus niet alleen inzicht in de risico's, maar ook in de kansen.

2.1 Kaderstelling

Naast onze interne motivatie dat risicomanagement en afspraken hierover helpen bij het realiseren van doelstellingen, is er ook sprake van wet- en regelgeving die ons verplicht om hierover afspraken te maken.

Wettelijk kader

Het wettelijk kader voor dit document ligt besloten in BBV. Het BBV bevat voorschriften voor de inrichting van de begroting en de jaarstukken. Eén van de verplichtingen is het opnemen paragraaf weerstandsvermogen en risicobeheersing. Met het vaststellen van deze nota wordt het beleid voor de komende periode vastgelegd. Daarnaast zijn er verplichtingen gesteld vanuit de Baseline Informatiebeveiliging Overheid (BIO) en de NEN-7510 als het gaat om cyberrisico's en informatiebeveiliging en privacy risico's.

Provinciaal toezichtkader

De provincie Overijssel houdt toezicht op SamenTwente als gemeenschappelijke regeling. In het financieel toezichtkader voor gemeenschappelijke regelingen is opgenomen dat de provincie toetst of SamenTwente inzicht geeft in de risico's.

Financiële verordening SamenTwente

Met de financiële verordening stelt het algemeen bestuur op hoofdlijnen de financiële spelregels vast. In artikel 18 van onze financiële verordening 2024 is opgenomen dat het dagelijks bestuur tenminste eens in de vier jaar een nota risicomanagement ter vaststelling aanbiedt aan het algemeen bestuur.

2.2 Leeswijzer

De notitie begint met een managementsamenvatting waarin de belangrijkste uitgangspunten zijn opgenomen. In de navolgende hoofdstukken worden deze uitgangspunten uitgeschreven. Vervolgens wordt toegelicht hoe het risicomanagement op basis van deze uitgangspunten in de praktijk zijn uitwerking krijgt, welke aandachtspunten er zijn en welke rollen en verantwoordelijkheden bij risicomanagement horen. Deze notitie wordt afgesloten met een beschrijving van het weerstandsvermogen.

3. Managementsamenvatting

Het is belangrijk om periodiek de wijze waarop risicomanagement is ingericht tegen het licht te houden om te verbeteren en te optimaliseren. Daarnaast zijn er hiervoor ook aanleidingen vanuit de externe omgeving, zoals bijvoorbeeld het 'Besluit begroting en verantwoording' en diverse voor ons (aankomende) verplichte normen, zoals de BIO, NEN7510, NIS2, ISO 9001 en HKZ (Harmonisatie Kwaliteitsbeoordeling in de Zorgsector).

Afgezien van de externe invloeden, zien we zelf het belang groter worden voor effectief risicomanagement om onze doelstellingen te kunnen blijven behalen. Met risicomanagement willen we niet alleen ervoor zorgen dat de organisatie voldoet aan wettelijke verplichtingen, maar vooral ervoor zorgen dat effectief omgegaan kan worden met steeds veranderende en groeiende (cyber)dreigingen en uitdagingen die onze doelrealisatie in de weg kunnen staan.

Om ervoor te zorgen dat we binnen de gehele organisatie werken met een duidelijk en eenduidig kader voor risicomanagement, gebruiken we de NEN-ISO 31000 als handvat. Deze risicomanagementstandaard kan ons ondersteunen in het behalen van onze ambities op het gebied van risicomanagement, deze zijn:

- Doelgebonden: risicomanagement voegt directe waarde toe;
- Risicodialoog is prioriteit: het gaat niet om actueel houden van lijstjes;
- Eenduidig kader: uniformiteit werkwijze binnen de gehele organisatie;
- Integraal: risicomanagement doen we waar dat waarde toevoegt;
- Integraal: de juiste disciplines aan tafel;
- Integraal: aandacht voor strategisch risicomanagement en operationeel risicomanagement;

Voor het toepassen van risicomanagement is het van belang dat de processen van de organisatie waar nodig voldoende zijn beschreven en dat de rol van proceseigenaar én andere rollen voor het risicomanagement binnen de organisatie goed worden neergezet. Om het risicomanagement doelgebonden te maken en niet los te laten staan van de processen gaan we ook een applicatie gebruiken. Deze applicatie moet bijvoorbeeld een koppeling maken tussen doelen, risico's en maatregelen. Hiermee voorkomen we ook dat er op verschillende manieren en op verschillende locaties risicoregisters worden bijgehouden. Dit helpt bij het samen integraal werken aan doelrealisatie en daarmee dus ook aan risicomanagement (managen van onze doelen).

4. Onze ambitie op het gebied van integraal risicomanagement

Waarom (nu) belangrijk?

Risicomanagement is belangrijk omdat wij daardoor tijdig kunnen anticiperen op eventuele onverwachte invloeden op het kunnen behalen van onze doelstellingen en het uitvoeren van onze zorg- en dienstverlening. We merken dat risicomanagement steeds belangrijker wordt. Vanuit wet- en regelgeving moeten wij als overheidsorganisatie steeds meer aantonen dat we in control zijn als het gaat om risico's. Zie als voorbeeld de toenemende (nationale en internationale) eisen rondom informatiebeveiliging, -management en privacy maar ook regelgeving over Arbo en de veiligheid van medewerkers en de rechtmatigheidsverantwoording. Dit vergt voor risicomanagement een bredere blik dan alleen een financiële.

Waar staan we nu?

Risicomanagement kan op vele verschillende manieren ingericht worden. Om een beeld te vormen van ons huidige niveau gebruiken we een volwassenheidsmodel (zie figuur 1) dat uitgaat van 4 niveaus van risicomanagement. Op dit moment is ons risicomanagement ingericht op het voldoen wat ervanuit wet- en regelgeving van ons gevraagd wordt (niveau 2). Het is erg financieel gedreven met als focus,

het opstellen van de risicoparagraaf in de begroting en de jaarstukken. De koppeling met doelrealisatie kan versterkt worden. Zonder een goede koppeling met doelrealisatie is het moeilijk om risicomanagement te laten leven in de organisatie. Risicomanagement is weinig succesvol als de reden voor het uitvoeren hiervan gelegen is in het voldoen aan de wettelijke voorschriften. Volgens ons is een interne motivatie de beste drijfveer.



Figuur 1 Risico-volwassenheidsmodel NARIS

Onze ambitie

De focus ligt de komende jaren (2024-2027) op het door ontwikkelen en verder professionaliseren van risicomanagement naar het niveau van "Proactief". Dit willen we bereiken door:

1. Doelgericht, Integraal en uniform risicomanagement
Om het niveau van "Proactief" te bereiken is onze ambitie om risicomanagement *integraal* en zoveel als mogelijk uniform binnen de organisatie toe te passen. Met integraal verstaan we het breed invullen van risicomanagement (niet alleen financieel). We realiseren ons dat risicomanagement een bredere focus heeft dan enkel financieel. Daarom is het van belang om ook aandacht te hebben voor niet-financiële risico's zoals imago, proces, en bestuurlijke risico's/aansprakelijkheid. Managers zijn verantwoordelijk voor risicomanagement in hun werkveld. Om met deze brede bril naar risico's te kunnen kijken, zorgen we ervoor dat risico's identificeren een proces is waarbij meerdere disciplines bij betrokken zijn. Risicomanagement is geen afzonderlijke activiteit maar maakt integraal onderdeel uit van alle processen. We stimuleren het risicobewustzijn en voorkomen dat afdelingen op verschillende wijze met verschillende uitgangspunten voor risicomanagement werken. Het rekening houden met risico's en kansen willen we terugzien in het dagelijkse denken en handelen van alle medewerkers. Daarbij leggen we een duidelijke koppeling tussen doelrealisatie en risicomanagement. Waarbij we op strategisch niveau vooral kijken naar het behalen van doelstellingen uit het vierjarige strategische programma en de programmabegroting. Op het operationele niveau kijken we naar de door vertaalde doelstellingen in de (team) jaarplannen en de processen. Bij beide gaat het om tijdig anticiperen op onverwachte invloeden die effect hebben op onze doelstellingen. Het gebruiken van dezelfde werkwijze en uitgangspunten maakt het mogelijk om het strategische niveau met het operationele niveau te koppelen en te spreken van doelgericht, integraal en uniform risicomanagement.
2. Dialoog stimuleren
Het goede gesprek over risico's en risicobereidheid is de basis van ons risicomanagement. We moeten ervoor zorgen dat op alle ambtelijke en bestuurlijke niveaus bereidheid en ruimte is om over risico's te praten. Het gaat om het ontwikkelen van een gesprekscyclus waarbij het draait om bewustwording en het voeren van een open gesprek over risico's (risicodialoog). Een goed risicodialoog is wat ons betreft een gesprek over expliciet, realistisch en gestructureerd omgaan met onzekerheden (risico's en kansen) waarbij alle deelnemers aan het gesprek vrijmoedig spreken en openhartig luisteren¹. Bij de uitvoering van het risicodialoog stellen we drie vragen centraal:

1) Van Staveren, 2023

- Wat is ons doel?
- Wat is daarbij onzeker (wat zijn de risico's en kansen)?
- Wat staat ons vanuit onze risicobereidheid te doen?

Met de hierboven uiteengezette twee punten is onze ambitie dat risicomanagement meer gaat leven en meer wordt dan enkel een financieel technische exercitie eens per jaar voor de paragraaf weerstandsvermogen.

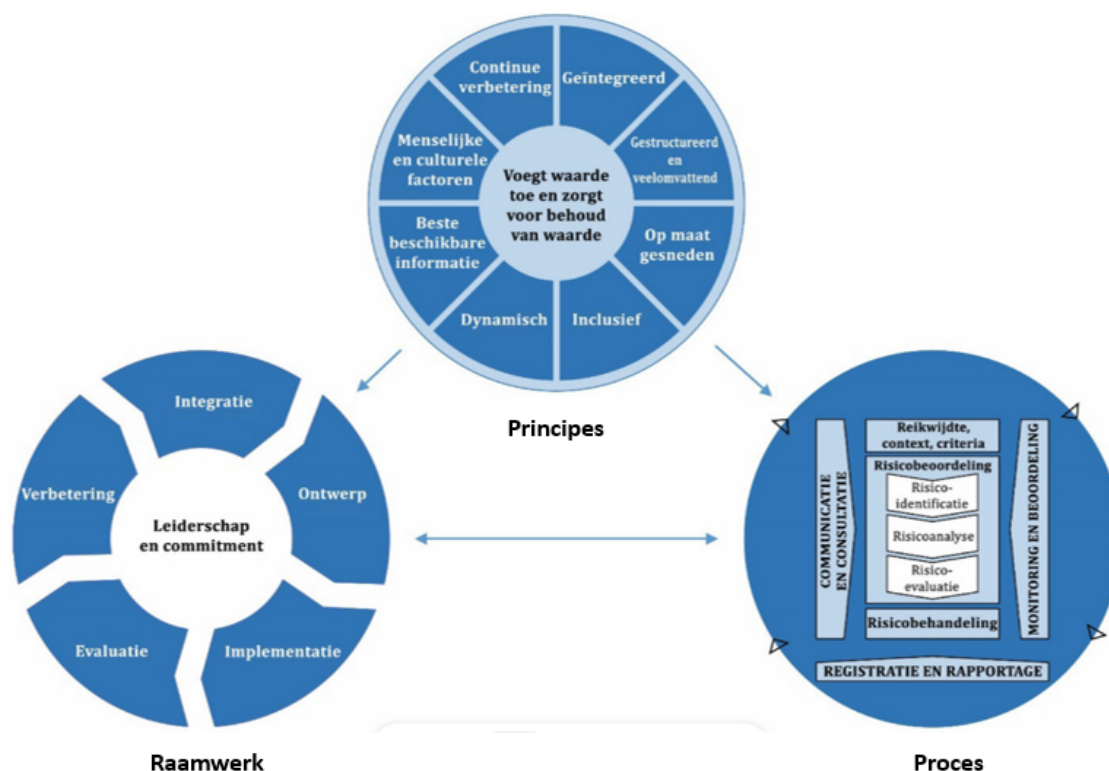
5. Integraal risicomanagement volgens de NEN-ISO 31000

Om het risicomanagement integraal bij SamenTwente in te kunnen richten is een raamwerk nodig. Hiervoor hebben wij gekozen voor de internationale standaard NEN-ISO 31000.

Waarom de NEN-ISO 31000

De NEN-ISO 31000 is een internationale richtlijn voor risicomanagement. Het heeft als doel om de kans op het behalen van doelstellingen te vergroten. Het voorziet daarvoor in een werkwijze op zowel strategisch als operationeel niveau voor de identificatie van kansen en bedreigingen in combinatie met de behandeling hiervan.

Deze richtlijn biedt een eenduidig raamwerk, taal en werkwijze voor de verschillende vormen van risicomanagement binnen een organisatie. De NEN-ISO 31000 is een vrij toe te passen richtlijn en kan door de organisatie zelf op maat worden gemaakt. Hierdoor wordt voorkomen dat risicomanagement naast de reguliere bedrijfsvoering komt te staan en gezien wordt als een ongewenste bureaucratische aanvulling op het dagelijkse werk. Bij diverse overheden wordt NEN-ISO 31000 dan ook veelvuldig toegepast. Wij zien de NEN-ISO 31000 als ondersteunend aan onze in hoofdstuk 4 verwoorde ambities. In onderstaande figuur is de NEN-ISO 31000 weergegeven. Deze norm zet de principes, het raamwerk en het proces van integraal risicomanagement uiteen.



Figuur 2 NEN- ISO 31000

Principes voor effectief risicomanagement (hoofdstuk 6.1)

De NEN-ISO 31000 geeft principes (te zien als randvoorwaarden) die ingevuld moeten zijn en continu gestimuleerd moeten worden om het risicomanagement binnen organisatie effectief te houden. De principes stellen de organisatie in staat om de effecten van onzekerheden op haar doelstellingen op goede en gestructureerde wijze te managen. Principes zijn richtinggevend voor de opzet van doelmatig en doeltreffend risicomanagement.

Raamwerk voor risicomanagement (hoofdstuk 6.2)

Het doel van het raamwerk voor risicomanagement is om de organisatie te helpen om risicomanagement in belangrijke activiteiten en functies te integreren. Zodat het rekening houden met risico's en kansen en alle relevante processen terug te vinden is. Doeltreffendheid van risicomanagement hangt hiervan af. Dit vereist draagvlak vanuit belanghebbenden en leiderschap commitment van het management en het bestuur. Het ontwikkelen van het raamwerk omvat het integreren, ontwerpen, implementeren, evalueren en verbeteren van risicomanagement in de hele organisatie. Waarbij de verschillende componenten samenwerken en op maat zijn gemaakt voor het specifieke proces (de activiteit). Zo krijgt het risicomanagement voor projectmanagement bijvoorbeeld een andere invulling dan het risicomanagement voor uitvoerende zorgprocessen (zoals het zetten van vaccinaties).

Het proces van risico's identificeren t/m behandeling (hoofdstuk 6.3)

Rekening houden met risico's en kansen in de processen impliceert dat je op een bepaald moment in een proces nadenkt over risico's en kansen en er vervolgens de juiste maatregelen bij bepaald. Voor het borgen van de uniformiteit biedt de NEN-ISO 3100 enkele vaste stappen. Een risicomanagement-proces start altijd met het vaststellen van reikwijdte, context en criteria. In het proces is communicatie en consultatie met belanghebbenden verankerd en wordt het monitoren en beoordelen van risico's geborgd. De NEN-ISO 31000 is geen "one size fits all". Er is ruimte voor proportionaliteit. Dat wil zeggen dat organisatieonderdelen en/of projecten met een hoog risicoprofiel en groot belang voor het functioneren van onze organisatie, het risicomanagement zwaarder kunnen aanzetten dan waar dat minder het geval is.

In de volgende hoofdstukken wordt aangegeven hoe de NEN-ISO 31000 wordt toegepast bij SamenTwente.

6. Toepassing bij SamenTwente

In dit hoofdstuk worden de uitgangspunten beschreven zoals wij dit gaan toepassen bij het ontwerpen, implementeren en evalueren van het risicomanagement van SamenTwente.

6.1 Toepassing principes voor effectief risicomanagement

De principes (te beschouwen als voorwaarden) vormen de basis voor het managen van risico's en kansen. De mate van en de invulling van de principes kan per organisatie verschillen en daarom dienen de principes ook op maat te worden gemaakt. Dit doen we op het moment dat we concreet processen gaan beschrijven of bestaande processen gaan aanpassen om het risicomanagement proces (de stappen) te integreren. Een voorbeeld hiervan is dat het risicomanagement dynamisch moet zijn. In praktijk betekent dat wij niet alleen op vaste geplande momenten moeten kijken naar risico's. Maar dat wij dat ook doen wanneer de externe of interne omgeving van de organisatie verandert. In bijlage 3 is beschreven welke principes vanuit de ISO 31000 worden gehanteerd en hoe wij deze gaan toepassen bij het ontwerpen, implementeren en evalueren van het risicomanagement van SamenTwente.

Risicomanagement en de processen van SamenTwente

Wanneer je als organisatie binnen de processen rekening wilt houden met risico's en kansen, dan is het van belang inzichtelijk te hebben hoe de processen verlopen. Hiervoor is het van belang dat we als organisatie heldere en actuele procesbeschrijvingen hanteren en beheren in het kwaliteitsmanagement-systeem. We streven naar actuele procesbeschrijvingen, maar ook geven we bijhorende proceseigenaren een duidelijke taak- en verantwoordelijkheid bij het tijdig rekening houden met risico's en kansen in zijn of haar proces.

Risico-register

Om zicht en grip te houden op je risico's is het van belang dat deze risico's ergens op een eenduidige wijze zijn vastgelegd. Dit voorkomt het zoeken naar (mogelijk verouderde) Excel documenten of ander-soortige documenten waarin de risico's staan.

Hiervoor gaan we een toegankelijke applicatie hanteren die ons gaat helpen bij het actueel houden van risico's en bijhorende maatregelen. Bovendien wordt het hierdoor mogelijk om risico's te aggregeren en om risico's rechtstreeks te koppelen aan processen.

Bij aggregeren gaat het bijvoorbeeld om het meenemen van de operationele risico's bij de beoordelingen op het strategische niveau.

Bij het koppelen aan processen gaat het om de maatregelen die worden bedacht. Die kunnen dan gelijk landen in de juiste processen om daar verbeteringen te realiseren (de risico barrière). Maar ook wordt het dan mogelijk om bij het evalueren (het actualiseren) van procesbeschrijvingen de al bekende risico's mee te nemen.

6.2 Toepassing effectief raamwerk voor risicomanagement

Het proces gaan we zoveel als mogelijk integreren binnen de bestaande processen van de organisatie. Hierbij maken we onderscheid in strategisch en operationeel risicomanagement.

Strategisch risicomanagement

Strategisch risicomanagement gaat over het managen van risico's gerelateerd aan onze strategie en lange termijn doelstellingen. Bij het nastreven van de gestelde doelen kunnen risico's aanwezig zijn, daarom moet nagedacht worden over welke bereidheid er is om risico te lopen. Dit noemen we risicobereidheid. Risicobereidheid (of risk appetite) hangt nauw samen met organisatie strategie en is daarmee onderdeel van strategisch risicomanagement. De risicobereidheid is de mate waarin een organisatie bewust risico's accepteert. Denk bijvoorbeeld aan informatiebeveiliging, 100% foutloos werken kan niet. Maar tegelijkertijd is belangrijk om te realiseren dat informatiebeveiligingsrisico's ook onderdeel zijn van het strategisch risicomanagement.

Het vaststellen van je risicobereidheid kan helpen bij het bepalen van de prioriteiten. Het bepalen van de risicobereidheid is taak van directie en management. Top down. Hierbij is het belangrijk om een terugkerende dialoog organiseren. Ter ondersteuning van de dialoog is volgens ons een risicomatrix (zie hoofdstuk 6.3.2) een goed instrument. Hiermee kan directie en management duidelijkheid verschaffen over de 10 tot 15 belangrijkste strategische risico's die de prestatie van onze organisatie beïnvloeden. Strategische risico's zijn risico's die inherent zijn aan het ontwikkelen en uitvoeren van beleid en zijn daarom ook niet per definitie altijd ongewenst.

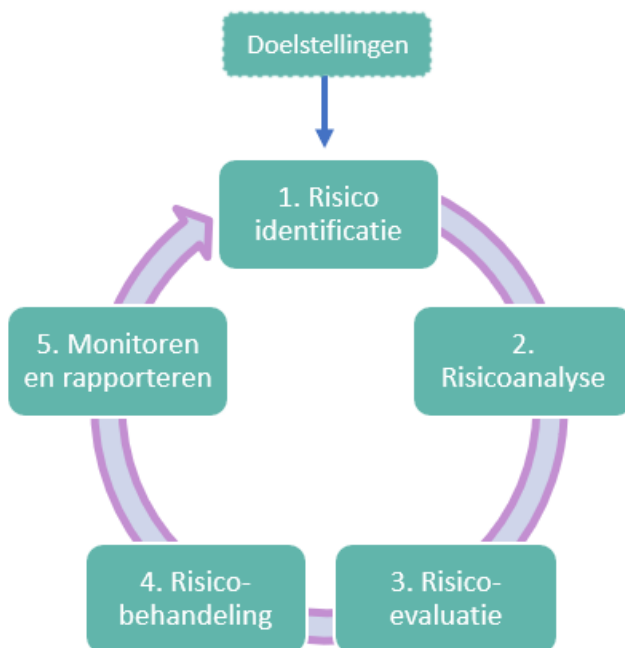
Zoals u in de inleiding heeft kunnen lezen wordt SamenTwente vanuit diverse wet- en regelgeving (BBV, BIO, NEN7510, NIS2 etc.) verplicht om risico's te inventariseren die van belang kunnen zijn voor onze financiële positie. Om de financiële consequenties van risico's op te kunnen vangen wordt weerstandsvermogen aangehouden. Ook dit is onderdeel van strategisch risicomanagement van SamenTwente.

Operationeel risicomanagement

Operationele risico's zijn veelal interne risico's, voortkomend uit de organisatie, die beheersbaar zijn en vermeden of zoveel als mogelijk opgelost moeten worden. Voorbeelden zijn risico's van onrechtmatig handelen, fouten in (geautomatiseerde) processen en ongeautoriseerde toegang. Operationele risico's kunnen risico's zijn die voortvloeien uit wet- en regelgeving (compliance) maar het gaat ook om risico's bij de uitvoering van onze taken zoals het uitvoeren van vaccinaties. Hierbij gaat het om het treffen van beheersmaatregelen en ervoor te zorgen dat er sprake van een continu proces van controleren en evalueren. Ook in het operationele risicomanagement is er sprake van risicobereidheid. Het gesprek hierover ligt dan op het niveau van teamleiders in afstemming met het management.

6.3 Het proces van risico's identificeren t/m rapporteren

Het risicomanagement proces, op strategisch en operationeel niveau, beschrijft de stappen van risico identificatie, analyse en evaluatie.



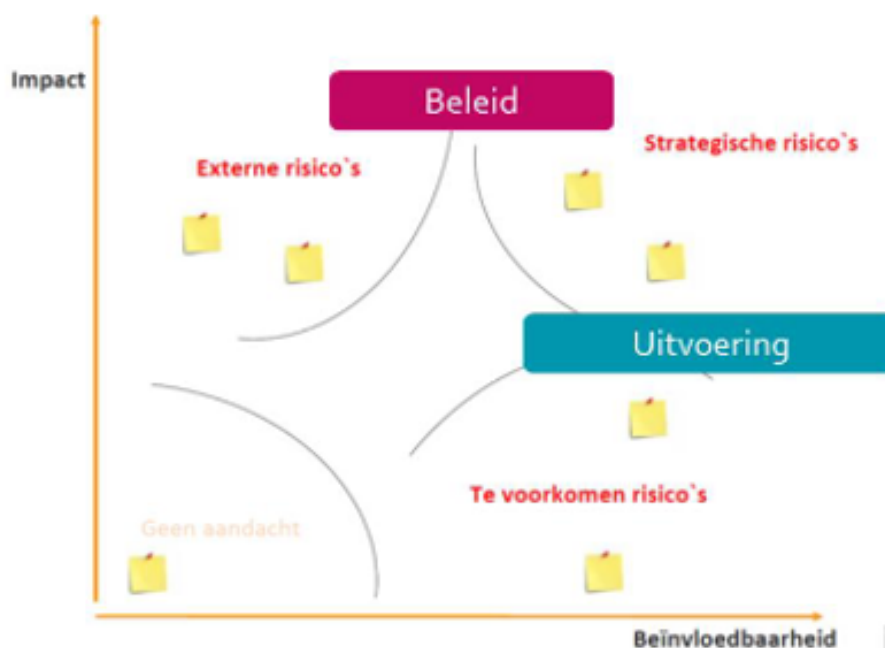
Dit risicomanagement proces gaan we toepassen waar dit waarde toevoegt aan het beter kunnen realiseren van doelstellingen. Op het strategische niveau zien we dat terug in de planning- en control cyclus en voor het operationeel niveau valt bijvoorbeeld te denken aan:

- Realisatie van jaar- en teamplannen.
- Projectmanagement

Op de volgende pagina's wordt het risicomanagement proces toegelicht.

6.3.1 Risico-identificatie

Bij de identificatie van risico's onderscheiden we operationele risico's (bijvoorbeeld fouten in geautomatiseerde processen), strategische risico's (bijvoorbeeld risico's die invloed hebben op de gestelde doelen in de programmabegroting) en externe risico's. Externe risico's worden gekenmerkt doordat de oorzaak van het risico zich buiten ons invloedsfeer bevindt, zoals een pandemie. Bij dit type risico moet wel een vertaalslag plaatsvinden naar de concrete risico's voor onze organisatie (bijvoorbeeld het risico dat extra taken uitgevoerd moeten worden door een pandemie, het risico dat er extra personeel ingezet moet worden dan begroot en/of het risico op tegenvallende opbrengsten). Zie [bijlage 2](#) voor een verdere uitwerking van de soorten en type risico's. Het typeren van risico's helpt bij het omgaan van risico's. Hieronder wordt schematisch per soort risico weergegeven of de mate van impact en beïnvloedbaarheid van het risico laag of hoog is. Hieruit valt op te maken dat bij het opstellen van beleid rekening gehouden moet worden met de externe en strategische risico's en dat bij de uitvoering door de organisatie de focus hoofdzakelijk ligt op strategische en te voorkomen/operationele risico's.



Figuur 3 Soorten risico's naar impact en beïnvloedbaarheid

6.3.2 Risicoanalyses

We vinden het onwenselijk om te sturen op alle risico's. Dit is niet doeltreffend risicomanagement. Bij de risicoanalyse gaat het er om ordening in de lijst met risico's aan te brengen, zodat de meeste tijd en energie gestoken kan worden in de beheersing van en sturing op risico's die de grootste impact kunnen hebben op onze doelstellingen. Uit de fase van risico-inventarisatie volgt een lijst met risico's die onderling erg verschillen. Om een ordening hieraan te brengen bepalen we:

- de geschatte omvang van het risico (impact op doelstelling);
- de waarschijnlijkheid dat het risico zich voordoet (kans).

Risicomatrix

Bij SamenTwente gaan we uit van deze risicomatrix:

Kans van optreden	Zeer waarschijnlijk	5						
	Waarschijnlijk	4						
	Is wel eens voorgekomen	3						
	Onwaarschijnlijk	2						
	Zeer onwaarschijnlijk	1						
			1	2	3	4	5	
Impact op doelstelling			Ze er klein	Klein	Gemiddeld	Groot		Ze er groot

Nadat we de risico’s hebben geïdentificeerd kan de kans en impact worden bepaald. Als hulpmiddel wordt de kans en impact ingedeeld in klassen van 1 t/m 5. Door het vermenigvuldigen van de scores op geschatte kans en impact, kan per risico een risicoscore worden uitgerekend. Bijvoorbeeld: kans klasse is 4 en de impact klasse is 3, dan is de risicoscore $4 \times 3 = 12$.

Voor financiële risico’s kan een geschat bedrag bepaald worden voor de impact. De risicoscore is een maatstaf voor de potentiële impact van het risico. Op basis van deze risicoscores kunnen risico’s worden gerangschikt. Hierbij geldt dat, hoe hoger de risicoscore:

- hoe groter de potentiële impact;
- hoe hogere prioriteit de aanpak van het risico heeft.

In de volgende paragrafen wordt toegelicht hoe de matrix is opgebouwd.

Kans klassen

We maken ook een inschatting van de waarschijnlijkheid dat het risico zich daadwerkelijk voor kan doen.

Klasse	Mate van waarschijnlijkheid	Percentage
1.	Zeer onwaarschijnlijk	10%
2.	Onwaarschijnlijk	30%
3.	Is wel eens voorgekomen	50%
4.	Waarschijnlijk	70%
5.	Zeer waarschijnlijk	90%

Toelichting op de klassen:

1. Zeer onwaarschijnlijk hanteren we voor risico’s waarvan het zeer onwaarschijnlijk is dat het risico zich voordoet. Denk hierbij bijvoorbeeld aan risico’s die op basis van ervaringscijfers slechts één keer in de 10 jaar voordoen.
2. Onwaarschijnlijk we voor risico’s waarvan het niet zo waarschijnlijk is dat het zich gaat voordoen. Bijvoorbeeld aan risico’s die op basis van ervaringscijfers één keer in de 5 jaar voordoen.
3. Is wel eens voorgekomen hanteren we voor risico’s die nog beide kanten op kunnen. Het kan zijn dat die zich voor doet, het kan ook zijn van niet. Denk hierbij aan risico’s die op basis van ervaringscijfers slechts één keer in de 2 jaar optreden.
4. Waarschijnlijk hanteren we voor risico’s waarvan het waarschijnlijk is dat die zich het komend jaar voordoet. Dit zijn risico’s die op basis van ervaringscijfers jaarlijks voordoen.
5. Zeer waarschijnlijk hanteren we voor risico’s waarvan het zeer waarschijnlijk is dat die optreden. Dit zijn risico’s die op basis van ervaringscijfers meerdere keren per jaar voordoen

Impact klassen

a. Impact klasse voor niet-financiële risico’s

Het bepalen van de omvang bij niet-financiële risico’s is anders dan bij risico’s met financiële gevolgen. De gevolgschade kan namelijk niet uitgedrukt worden in geld. Om toch de impact in risicoklassen hiervan te kunnen bepalen wordt gebruikt gemaakt van onderstaande risicoklassen. Onderstaande indelingen bieden handvatten voor de focus in sturing en beheersing van risico’s met niet financiële impact.

Klasse	Impact
1.	Zeer klein
2.	Klein
3.	Gemiddeld
4.	Groot
5.	Zeer groot

b. Impact klasse voor financiële risico's

Bij het bepalen van de geschatte financiële omvang gaan we uit van een situatie dat het risico zich daadwerkelijk voordoet. Vanuit de gedachte "als het risico zich voordoet, dan..." maken we een inschatting van het bedrag dat naar alle waarschijnlijkheid SamenTwente kwijt is als het risico zich voordoet.

Klasse	Bandbreedte in €	Risico bedrag in €
1.	25.000 < > 50.000	37.500
2.	50.000 < > 100.000	75.000
3.	100.000 < > 200.000	150.000
4.	200.000 < > 500.000	350.000
5.	> 500.000	P.M.

Er zijn risico's die verwaarloosbaar zijn omdat de kans dat ze zich voordoen zo klein is of de financiële gevolgen zo gering, dat het vanuit de doelmatigheidsoptiek niet aan te bevelen is om daar tegen maatregelen te treffen. Het is daarom wenselijk een ondergrens vast te stellen. SamenTwente hanteert voor het kwantificeren van de risico's een ondergrens van € 25.000 als uitgangspunt.

De risico's met een financieel risico onder deze grens kunnen wel benoemd worden, maar worden niet meegerekend. Indien de impact van een bepaald risico in klasse 5 valt en dus groter is dan € 500.000, dient voor dat risico ook het maximale verwachte gevolg in euro's aan te worden gegeven. Deze situatie zou zich vooral voor kunnen doen bij majeure projecten. Het maximale gevolg in euro's fungeert vervolgens als risicobedrag voor impactklasse 5.

Voor risico's met structurele gevolgen tellen alleen de verwachte gevolgen in de eerste drie jaar mee voor een dalend percentage (1e jaar 100%, 2e jaar 50% en 3e jaar 25% = totaal € 175%). Volgens deze aflopende lijn moeten de gevolgen van het risico na jaar 3 zijn opgevangen.

6.3.3 Risico-evaluatie

Nadat de risico's zijn geïdentificeerd en geanalyseerd komen we bij de risico-evaluatie fase. Het doel van deze derde stap in het risicomanagement proces is het ondersteunen van besluiten. Hierbij gaat het om sturing op en beheersing van risico's door beheersmaatregelen te treffen. Dit is een maatregel die de kans van het optreden of de gevolgen van het optreden van een risico verkleint. Hierbij is het van belang dat de maatregelen proportioneel zijn. Dit houdt in dat de kosten van de maatregel in verhouding staan tot de vermindering van de kans of de gevolgen en dat er niet onnodig veel maatregelen voor één risico genomen worden. Er zijn 4 mogelijkheden om te bepalen wat er met het risico moet gebeuren:

1. vermijden van het risico door te besluiten de activiteit waardoor het risico wordt veroorzaakt te stoppen of door doelstelling aan te passen;
2. verminderen van de impact van het risico door ofwel de omvang van het risico terug te brengen (door bijvoorbeeld fasering) ofwel de kans/waarschijnlijkheid van optreden terug te brengen;
3. overdragen/delen van het risico door bijvoorbeeld het beleid (en/of het proces) wat het risico met zich brengt uit te laten voeren door een andere partij. Hierbij kan gedacht worden aan garanties, derden aansprakelijk stellen, contracten en verzekeringen;
4. als geen van de bovenstaande opties (vermijden, verminderen, overdragen) mogelijk of wenselijk is, kan gekozen worden om het risico te accepteren. Dit kan ook het geval zijn bij externe risico's waarop we niet kunnen sturen. De keuze om een risico te accepteren wordt bewust gemaakt. We schatten de kans en het mogelijk financieel gevolg van een geaccepteerde risico in. Deze financiële impact wordt vervolgens opgenomen in ons risicoprofiel en wordt door het weerstandsvermogen gedekt ([hoofdstuk 9](#)).

Bruto en netto risico's

Vermijden elimineert een risico. Verminderen en overdragen verlagen de netto omvang van een risico:

Bruto verwachte omvang risico =	Verwachte gevolgschade van risico	
	Reductie risico door beheersmaatregelen	-/-
	Compensatie van derden / verhaal op derden	-/-
Netto verwachte omvang =	Nog te dekken gevolg van een risico (weerstandsvermogen)	

6.3.4 Risico-behandeling

Maatregelen voor de reductie van de impact van risico's liggen zowel op het strategische als op het operationele vlak. Het gaat hierbij niet alleen om het kiezen van maatregelen en het implementeren ervan, maar ook om het bewaken en controleren dat de gekozen maatregelen effect hebben en het zo nodig bijsturen hierop. Eerste aandachtspunt bij risicomanagement zijn de risico's die het hoogste scoren in de risicokaart (tabel 1). Ook belangrijk is om aandacht te hebben voor risico's die zelden voor komen maar als ze zich voordoen, dan is de impact enorm. Deze risico's worden ook wel zwarte zwanen genoemd. Onze organisatie heeft dit meegemaakt met de uitbraak van het coronavirus. Het beheersen van dit soort risico's is echter complex. Een beheersmaatregel kan zijn het hebben van een continuïteitsplan en zorgen dat je voldoende weerbaar bent door het organiseren van een financiële buffer.

6.3.5 Monitoren en rapporteren

Planning & control cyclus

Risicomanagement is een lerend proces. Het gaat om steeds beter omgaan met onzekerheden die onze doelen kunnen beïnvloeden. Risicomanagement past daarom goed binnen de bestaande planning & control cyclus van SamenTwente. In deze cyclus draait het om het maken van strategische plannen en het beheerst uitvoeren daarvan. Dit vraagt om sturing op doelen die we willen realiseren en verantwoording afleggen over het al dan niet realiseren daarvan. Daar hoort bij dat je bewust omgaat met onzekerheden, kansen en risico's en daar regelmatig het gesprek over voert.

Dialogoog organiseren

In onze planning & control cyclus werken we met een gesprekscyclus waarin we ook het gesprek over risico's terug willen laten komen. We voeren jaarlijks bij het opstellen van onze doelen het gesprek over risico's, kansen en beheersmaatregelen. Vanaf 2024 werken we met een viermaands-cyclus. Elke viermaanden voeren we zowel op het management- en teamleider niveau als op bestuurlijk niveau gesprekken over de realisatie van doelen, prestaties, beheersing van processen en van budgetten. Het gesprek over kansen en risico's wordt bij SamenTwente ook hier vormgegeven. We zijn deze gesprekken op dit moment steeds beter aan het structureren. Hierin leren we continue.

Rapporteren

In de paragraaf Weerstandsvermogen en risicobeheersing van de programmabegroting en jaarstukken brengen we tenminste de grootste risico's (top 10) periodiek in beeld. In het volgende hoofdstuk gaan we dieper in op het onderwerp weerstandsvermogen.

Bestuursvoorstellen

Het dagelijks bestuur heeft de opdracht van het algemeen bestuur om de gestelde doelen in de programmabegroting te behalen. Het dagelijks bestuur staat bij de uitvoering van de doelen soms voor complexe keuzes. Voor het maken van een bewuste keuze is het hebben van een goed beeld van de argumenten voor en tegen, met de hieraan gekoppelde risico's en risicobereidheid, noodzakelijk. Het is dus van belang dat in bestuursvoorstellen de risico's duidelijk worden benoemd en de afwegingen die hierbij zijn gemaakt of worden voorgesteld. Hierbij houden we rekening met de in bijlage 2 uiteengezette soorten risico's.

7. Belangrijke aandachtspunten bij risicomanagement

Sinds onze vorige beleidsnota "Van risicomanagement tot reserves en voorzieningen" uit 2018 is veel ervaring opgedaan met risicomanagement. Ook door het uitvoeren van (complexe) projecten en het evalueren hiervan hebben we lessen geleerd en aandachtspunten opgedaan die belangrijk zijn bij risicomanagement.

Verschillende vormen van risicobeheersing en tegendenkkracht organiseren

Het is belangrijk om bij (complexe) projecten waarbij veel (en soms tegengestelde) belangen spelen verschillende instrumenten in te zetten om risico's zichtbaar te maken, te voorkomen of beheersbaar te houden. Hierbij is het belangrijk om vooraf maar ook gedurende het project risico's in beeld te (blijven) brengen. Bij het in beeld brengen is het van belang om aandacht te hebben voor risico's met een kleine

kans maar met een grote impact. Om dit scherp in beeld te brengen organiseren wij voldoende tegen-denkkraft. Deze tegendenkkraft kan bijvoorbeeld intern georganiseerd worden door bij het inventariseren van risico's (bijvoorbeeld tijdens een risicodialoog) verschillende disciplines te betrekken. Hiermee borgen we dat er vanuit verschillende invalshoeken wordt gekeken. Er kan ook externe expertise ingehuurd worden door bijvoorbeeld het laten uitvoeren van een externe juridische toets of door het laten uitvoeren van een onafhankelijke risico-inventarisatie.

Risico optimisme

Inschatting van risico's gebeurt niet altijd rationeel en daardoor bestaat de kans dat risico's onderschat worden. Dit kan bijvoorbeeld door kosten laag in te schatten en/of het tijdsbeslag om een project te realiseren onbewust wordt onderschat. Het is belangrijk om vooraf te realiseren dat deze risico optimisme kan gebeuren. Het is belangrijk om een cultuur te creëren waarbij dit bespreekbaar is en altijd helder en transparant te communiceren over de mogelijke hogere kosten en/of langere tijd die met het project kan zijn gemoeid.

Het is niet mogelijk alle risico's in te schatten en risicobeheersing is geen garantie voor succes

De realiteit is ook dat het niet mogelijk is alle risico's die SamenTwente loopt op voorhand te onderkennen. In onze complexe samenleving doen zich altijd verrassingen voor. Deze kunnen grote impact hebben. Risico's kunnen zich ook altijd op onvoorziene wijzen manifesteren in een project.

Risicoregelreflex

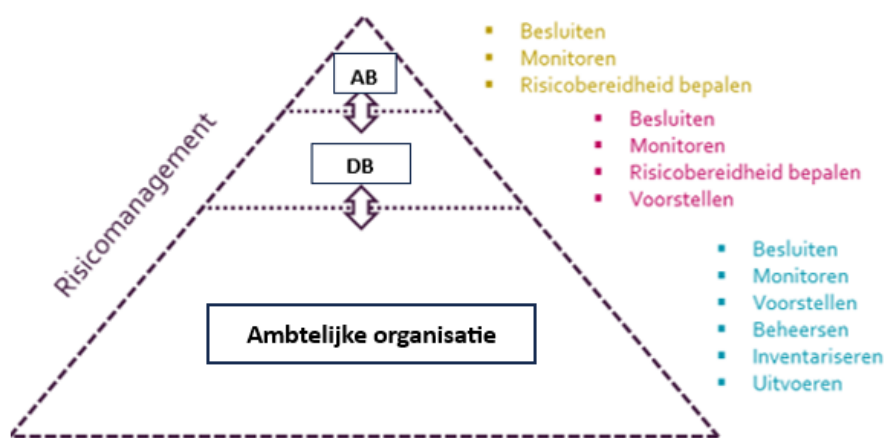
Wanneer een risico zich heeft voorgedaan in de vorm van een incident is meestal de reactie "dit had nooit mogen gebeuren en dus moeten we het liefst direct maatregelen treffen". Dit noemen we de risicoregelreflex. Dit reflex is soms adequaat, maar soms leidt dit ook tot een overmaat aan maatregelen die hoge kosten met zich meebrengen. Door bewust stil te staan en maatregelen goed te overwegen en incidenten te onderzoeken, kan SamenTwente goed omgaan met dit reflex.

8. Rollen en verantwoordelijkheden

Bij het ontwerpen en implementeren van risicomanagement is het van belang afspraken te maken over rollen en verantwoordelijkheden.

Hieronder is in figuur 4 schematisch weergegeven welke rollen het algemeen bestuur (AB), dagelijks bestuur (DB) en de ambtelijke organisatie hebben bij het risicomanagement binnen SamenTwente. Het algemeen bestuur en het dagelijks bestuur nemen voornamelijk besluiten waarbij risico's worden afgewogen, bepalen de risicobereidheid en monitoren via de planning en control cyclus de grootste risico's en het weerstandvermogen. Zij stellen de kaders waarbinnen de organisatie de risico's kan beheersen, mitigeren en/of accepteren. De ambtelijke organisatie heeft de grootste rol binnen het risicomanagement. Zij zorgt er met name voor dat het dagelijks bestuur en het algemeen bestuur risicobewuste keuzes kunnen maken. Het inventariseren, kwantificeren en beheersen ligt dan ook met name bij de organisatie. De medewerkers die verantwoordelijk zijn voor de uitvoering van doelen, projecten en processen zijn ook de risico-eigenaren van de hieraan gekoppelde risico's

Verantwoordelijkheden bij het uitvoeren van risicomanagement:



Figuur 4 Overzicht rollen en verantwoordelijkheden

Wie	Wat
Algemeen bestuur	Vaststellen kaders risicomanagement en weerstandsvermogen
	Vaststellen paragraaf weerstandsvermogen en risicobeheersing (in de begroting)
Auditcommissie	Adviseren van het algemeen bestuur over de rechtmatigheidsverantwoording en accountantscontroles.
Dagelijks bestuur	Verantwoordelijk voor realisatie van doelen en beheersen van risico's die daarmee gemoeid zijn.
	Rapporteren aan het algemeen bestuur over de belangrijkste risico's via bestuursvoorstellen en reguliere P&C cyclus
Centraal managementteam (CMT)	Verantwoordelijk voor sturing op en beheersing van organisatie brede strategische risico's en maatregelen .
	Zorgdragen voor vergroten risicobewustzijn
	Rapporteren aan dagelijks bestuur over risico's via bestuursvoorstellen en via de reguliere P&C cyclus
Managers	Verantwoordelijk voor sturing op en beheersing van risico's en maatregelen op afdelingsniveau.
	Zorgdragen voor vergroten risicobewustzijn
	Doorlopen van risicomanagementproces (inventarisatie en beoordeling van strategische risico's).
	Rapporteren aan het CMT over strategische risico's .
Financieel adviseurs/ business control	Stimuleren, adviseren en begeleiden van de managers bij het doorlopen van het strategische risicomanagementproces
Teamleiders	Verantwoordelijk voor sturing op en beheersing van risico's en maatregelen op teamniveau.
	Zorgdragen voor vergroten risicobewustzijn van medewerkers en begeleiding van medewerkers.
	Doorlopen van risicomanagementproces (inventarisatie en beoordeling van operationele risico's).
Medewerkers	Doorlopen van risicomanagementproces (inventarisatie en beoordeling van operationele risico's).
Kwaliteitsadviseurs	Stimuleren, adviseren en begeleiden van teamleiders en medewerkers bij het operationele risicomanagementproces.
	Zorgdragen voor vergroten risicobewustzijn.
Medewerker Verbijzonderde interne controle / auditors	Toetsen belangrijkste risico's in processen en de opzet, bestaan en werking van de beheersmaatregelen.
Concerncontroller	Toetst de kwaliteit van de organisatie brede strategische risico-inventarisatie en bewaakt de weerbaarheid van de organisatie.
	Zorgdragen voor vergroten risicobewustzijn.
	Verantwoordelijk voor het organisatie brede kader voor risicomanagement en weerstandsvermogen.
Adviseur crisisbeheersing GGD Twente	Inventariseren van en advisering over risico's die tot een crisis kunnen leiden
	Zorgdragen voor vergroten van risicobewustzijn
Chief Information Security Officer (CISO)	Bewaking van informatiebeveiliging-risico's en adviseren van de organisatie hierover.
	Zorgdragen voor vergroten risicobewustzijn
Functionaris Gegevensbescherming (FG)	Bewaking van privacy-risico's en adviseren van de organisatie hierover.
	Zorgdragen voor vergroten risicobewustzijn

9. Weerstandsvermogen

We zijn volgens het BBV verplicht om aan te tonen dat onze organisatie in staat is de gevolgen van risico's op te vangen zonder dat onze beleidsuitvoering in gevaar komt. Dit doen wij aan de hand van

de ratio weerstandsvermogen. Het weerstandsvermogen geeft aan in hoeverre onze organisatie in staat is (weerbaarheid) negatieve financiële consequenties van risico's zelfstandig op te vangen.

Het weerstandsvermogen bestaat uit de relatie tussen

- de beschikbare weerstandscapaciteit, zijnde de middelen en mogelijkheden waarover onze organisatie beschikt of kan beschikken om niet begrote kosten te dekken;
- de benodigde weerstandscapaciteit, zijnde alle risico's waarvoor geen maatregelen zijn getroffen en die impactvol kunnen zijn in relatie tot onze financiële positie.

Om het weerstandsvermogen te kunnen beoordelen, zetten we de *benodigde weerstandscapaciteit* af tegen de *beschikbare weerstandscapaciteit*. De uitkomst van deze berekening vormt de *ratio weerstandsvermogen*.

$$\text{Ratio weerstandsvermogen} = \frac{\text{Beschikbare weerstandscapaciteit}}{\text{Benodigde weerstandscapaciteit}}$$

Beschikbare weerstandscapaciteit

Om te kunnen beoordelen of we in staat zijn om risico's op te vangen wordt in beeld gebracht welke capaciteit we hiervoor beschikbaar hebben. Hierbij maken we onderscheid in incidentele en structurele weerstandscapaciteit.

Incidentele weerstandscapaciteit

Hieronder beschouwen we de algemene reserve van SamenTwente en de beschikbare egalisatiebestemmingsreserves. Ook stille reserves (verhandelbare bezittingen die gewaardeerd zijn lager dan de verkoopwaarde) maken onderdeel uit van incidentele weerstandscapaciteit. De gedachte hierachter is dat bij verkoop van deze bezittingen winst ontstaat die eenmalig inzetbaar is om tegenvallers op te vangen. Bij SamenTwente is geen sprake van stille reserves.

Structurele weerstandscapaciteit

De structurele weerstandscapaciteit bestaat veelal uit een structurele post onvoorzien en/of uit begrotingsruimte. In overeenstemming met het besluit van het algemeen bestuur ramen wij een post onvoorzien in de begroting maar de dekking hiervan is afkomstig uit de algemene reserve. Hiermee is de dekking van post onvoorzien feitelijk niet structureel. Als de begroting (inclusief de meerjarenraming) op een positief saldo sluit dan is er sprake van begrotingsruimte. Deze ruimte zou ook ingezet kunnen worden om structurele financiële tegenvallers op te kunnen vangen. SamenTwente heeft geen structurele begrotingsruimte en daarmee dus ook geen structurele beschikbare weerstandscapaciteit.

Benodigde weerstandscapaciteit

De benodigde weerstandscapaciteit wordt bepaald door de geïdentificeerde risico's uit te drukken in euro's. Dit betreffen alle risico's waarvoor geen/onvoldoende maatregelen zijn getroffen (netto verwachte omvang). Op deze wijze hebben we in beeld welke weerstandscapaciteit er nodig is om de financiële impact van risico's op te vangen als deze zich voordoen.

Ratio weerstandsvermogen en norm SamenTwente

SamenTwente streeft naar voldoende weerstandsvermogen. Dit staat gelijk aan een ratio weerstandsvermogen van maximaal 1,0. Als minimale toegestane ondergrens merken we de ratio weerstandsvermogen van 0,8 aan. We kiezen voor een minimale ondergrens zodat op het moment dat het weerstandsvermogen wordt aangesproken en de ratio onder de 1,0 komt, er ruimte is om een plan te maken hoe we het weerstandsvermogen weer aan te vullen.

Bijsturen op ratio weerstandsvermogen

We vinden het van belang om tijdig bij te sturen om te voorkomen dat het weerstandsvermogen onder onze norm komt of dreigt te komen. Als de ratio onder de 0,8 komt worden bij het volgende integrale afwegingsmoment van de ontwikkelingen/kaderbrief, programmabegroting of de jaarstukken afspraken gemaakt hoe bij te sturen om de ratio weer op het gewenste niveau te krijgen. Hierbij wordt het volgende afgesproken:

- positieve jaarrekeningresultaten prioritair bestemmen voor versterking van het weerstandsvermogen;
- het instellen van een spaarprogramma door toevoegingen te doen aan de beschikbare weerstandscapaciteit;
- bij beleid of besluiten met hoge risico's het risicoprofiel te verlagen voor zover mogelijk door het plan bij te stellen of de uitvoering uit te stellen.

10. Bijlagen

Bijlage 1. Termen en definities

Risicomanagement begint bij het spreken van dezelfde taal. Een juiste inschatting van een risico en haar effecten is alleen mogelijk wanneer we dezelfde definities hanteren. De belangrijkste definities worden hieronder beschreven.

Risico

Een risico is een onzekere en ongewenste gebeurtenis, waardoor het behalen van doelstellingen in gevaar komt. De doelstellingen kunnen onze strategische organisatie doelstellingen zijn maar ook kunnen ook operationele teamdoelstellingen zijn. Als er zekerheid is over het optreden van een gebeurtenis, dan is er géén sprake meer van een risico. Als de onzekere gebeurtenis geen gevolgen heeft voor het realiseren van doelstellingen, dan is er ook geen sprake van een risico. Binnen de definitie die in deze nota gehanteerd wordt gaan we uit van risico's waarbij er een negatief effect is op een doelstelling. Een positief effect op de doelstelling is een kans, maar kan op dezelfde manier behandeld worden als een risico.

Risicomanagement

Risicomanagement is een set aan gecoördineerde activiteiten om onze organisatie te sturen en te beheersen met betrekking tot risico's. Dit zodanig dat er meer zekerheid bestaat dat doelen worden gerealiseerd. Met andere woorden, risicomanagement is het managen van onze doelen.

Risicomanagementproces

Dit is een continue en systematisch proces waarbij in een organisatie risico's worden geïdentificeerd, geanalyseerd en geëvalueerd om ze beheersbaar te maken.

Weerstandscapaciteit

Weerstandscapaciteit bestaat uit middelen en mogelijkheden die SamenTwente heeft om onverwachte, niet-begrote kosten of tegenvallende inkomsten (door bijvoorbeeld optreden van een risico) te kunnen dekken. Hierbij wordt onderscheid gemaakt tussen benodigde (geïnterpreteerde risico's) en beschikbare weerstandscapaciteit (middelen en mogelijkheden). Daarnaast wordt er ook onderscheid gemaakt tussen incidentele en structurele weerstandscapaciteit. Onder incidentele weerstandscapaciteit wordt verstaan de capaciteit die SamenTwente heeft om eenmalige tegenvallers op te vangen. Onder structurele weerstandscapaciteit worden de middelen verstaan die permanent inzetbaar zijn om tegenvallers op te vangen.

Weerstandsvermogen

Weerstandsvermogen is de ratio van de beschikbare weerstandscapaciteit en de geïnterpreteerde risico's. Dit ratio geeft aan in hoeverre SamenTwente in staat is om niet begrote tegenvallers op te vangen zonder dat onze taakuitvoering in gevaar komt. Het weerstandsvermogen is eigenlijk een indicator van robuustheid van onze begroting.

Bijlage 2. Categorieën en soorten risico's

De meest voorkomende en herkenbare risico's zijn de financiële risico's. Daarnaast zijn er ook andere categorieën van risico's te onderscheiden. In deze nota wordt met risico's alle categorieën bedoeld, tenzij er expliciet wordt gesproken over financiële risico's. Te onderscheiden categorieën risico's:

Risico	Omschrijving
1. Politiek/bestuurlijk/imago	Dit soort risico's houden verband met beleid en besluitvorming met onevenredige overheidsinterventies in reactie op een gebeurtenis of ontwikkeling waarbij de verantwoordelijkheid voor risico-beheersing min of meer vanzelfsprekend wordt opgevat als taak van onze organisatie.
2. Financieel	Financiële risico's hebben te maken met tegenvallers in geldstromen (meer lasten en/minder of baten) zoals rijksuitkeringen, aanbestedingen, leningen en garanties, verstrekken en aantrekken van subsidies
3. Juridisch/wettelijk	Juridische risico's doen zich voor als er sprake is van: het niet voldoen aan wet- en regelgeving waaronder strijd met de algemene beginselen van behoorlijk bestuur en inbreuken op grondrechten; het niet voldoen aan contractuele verplichtingen; juridische gebondenheid zonder dat daar een besluit aan ten grondslag ligt
4. Fraude en integriteit	Risico's samenhangend met bedoeld en onbedoeld niet-integer handelen door bestuurders, ambtenaren of externe partners.
5. Organisatorisch	Een organisatorisch risico houdt verband met de manier waarop de organisatie is ingericht en haar werkzaamheden uitvoert. Dit betreft dan de samenwerking, processen, procedures en systemen die tekort schieten voor de (bijzondere) omstandigheden op enig moment of het ontbreken daarvan.
6. Informatie	Risico's die betrekking hebben op de duurzame toegankelijkheid van informatie (informatiebeheer); betrekking hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie (informatiebeveiliging); verband houden met de verwerking van persoonsgegevens (privacy).
7. Maatschappelijk	Maatschappelijke risico's voor SamenTwente houden verband met zowel ontwikkelingen in de samenleving waarop wij in de uitvoering moeten reageren op een manier waarop we nog niet (voldoende) zijn voorbereid en/of toegerust, als risico's die ontstaan door eigen beleidskeuzes gericht op een maatschappelijk doel.

Naast de verschillende risico categorieën zijn risico's ook in te delen in drie soorten: Te voorkomen/operationele risico's, strategische risico's en externe risico's

Omschrijving	Operationele risico's	Strategische risico's	Externe risico's
Voorbeelden	Fouten in (geautomatiseerde) processen, ongeautoriseerde toegang tot systemen, onrechtmatig handelen	Nieuwe activiteiten, samenwerkingen, subsidies,(des) investeringen, afweging kansen en bedreigingen	Pandemie en/of epidemie, wet- en regelgeving, economische en demografische ontwikkelingen
Kenmerken	Dit zijn risico's die betrekken hebben op de interne processen, vaak betrekking op gedrag en zijn sterk te beïnvloeden met maatregelen.	Dit zijn risico's die afhankelijk zijn van de gestelde doelen in de programmabegroting en bij (grote) projecten. Deze zijn goed te inventariseren en er kan een afweging plaatsvinden tussen acceptatie of beheersing van risico's.	Dit zijn risico's die worden gekenmerkt doordat de oorzaak van het risico zich buiten ons invloedsfeer ligt.
Beheersing	Deze risico's moeten proactief gemanaged worden door (het regelmatig) checken van processen via interne	Bij deze risico's dient de kans van optreden dan wel de mogelijke impact te worden verkleind. Bij deze risico's dient een terugkerende dia-	Vertaalslag maken naar concrete gevolgen voor de organisatie. Flexibiliteit van de organisatie. Scenario analyses en voldoende weerbaarheid organiseren.

	controles en regels rondom gedrag en be- sluitvorming.	loog te worden georgani- seerd over de risicobereid- heid en de gewenste maatre- gelen.	
--	--	--	--

Bijlage 3. Toelichting NEN-ISO 31000 principes

De NEN-ISO 31000 is een vrij toe te passen richtlijn en kan door de organisatie zelf op maat worden gemaakt. De NEN-ISO 31000 bestaat uit drie hoofdonderdelen; principes, raamwerk en het risicoproces. Deze bijlage geeft aanvullende informatie over de principes.

Principes NEN-ISO 31000

De principes zoals geïllustreerd in figuur geven richtlijnen van doelmatig en doeltreffend risicomanagement. Hieronder lichten we voor onze organisatie de belangrijkste principes toe en geven we ook aan hoe we deze in de praktijk toepassen.

Het doel van risicomanagement is het creëren en beschermen van waarde. Met andere woorden, goed risicomanagement verbetert de prestaties en ondersteunt het bereiken van doelstellingen.



a. *Geïntegreerd: Integraal risicomanagement*

Risicomanagement is pas waarde toevoegend als er sprake is van integraal risicomanagement. Hieronder verstaan we het breed invullen van risicomanagement. Dit betekent dat we bij risicomanagement niet alleen de wettelijke kaders volgen maar juist ook risicobewustzijn stimuleren. Risicomanagement is geen afzonderlijke activiteit maar maakt integraal onderdeel van alle processen (inclusief informatiebeveiliging en privacy). Dit houdt in dat we op alle niveaus risico's (alle processen) identificeren. Managers zijn verantwoordelijk voor risicomanagement in hun werkveld. Tegelijkertijd realiseren we ons ook dat bewust omgaan met risico's een onderdeel is van ieders werk. We richten ons bij integraal risicomanagement zoals toegelicht in onze ambitie op risicomanagement zowel op strategische risico's als operationele risico's. Hierbij ligt de focus niet alleen op risico's met financiële impact maar ook op risico's **zonder** een direct financiële impact. Bijvoorbeeld imago-, fraude-, juridische- en bestuurlijke risico's. Om met deze brede bril naar risico's te kunnen kijken, zorgen we ervoor dat risico's identificeren een proces is waarbij meerdere disciplines bij betrokken zijn.

b. *Gestructureerd*

Een gestructureerde benadering van risicomanagement draagt bij aan consistente en vergelijkbare resultaten. Werken op basis van één risicomanagementkader (raamwerk) binnen de gehele organisatie draagt bij aan een gestructureerde aanpak. Onze aanpak is cyclisch en sluit aan op de bestaande processen. Hierbij wordt het ontstaan van aparte werkwijzen en eilandjes op het gebied van risicomanagement zoveel als mogelijk tegengegaan.

c. *Dynamisch*

SamenTwente is verantwoordelijk voor een breed scala aan maatschappelijke taken. De maatschappij is continue in beweging en dit heeft ook impact op wat er van onze organisatie verwacht wordt. Zowel de interne als de externe context van onze organisatie is dynamisch waardoor risico's kunnen ontstaan, veranderen maar ook kunnen verdwijnen. Ons risicomanagement anticipeert hierop, detecteert dit en reageert hier op een tijdige en passende wijze op. Risico's komen voor in al onze doelstellingen, denk aan onze inhoudelijke doelstellingen vanuit GGD Twente, Veilig Thuis Twente en OZJT. Maar ook aan doelstellingen uit onze projecten en de bedrijfsvoering. Deze doelstellingen veranderen periodiek. We houden ons risicomanagement dynamisch door een koppeling te leggen tussen doelen en risico's. Daarnaast is het eenmalig inventariseren en analyseren van risico's onvoldoende. Het is een continue proces van identificeren, analyseren en evalueren. Bij wijzigingen in bijvoorbeeld de externe omgeving, als nieuwe wetgeving, is het noodzakelijk weer te kijken naar de risico's en bijhorende maatregelen. Alleen dan is sprake van risicomanagement.

d. *Menselijke en culturele factoren*

Goed risicomanagement kan pas plaatsvinden als er aandacht is voor menselijk gedrag en cultuur. Deze elementen hebben namelijk invloed op alle aspecten van risicomanagement en op elk niveau. We zorgen ervoor dat bij onze organisatie op alle ambtelijke en bestuurlijke niveaus bereidheid en ruimte is om open over risico's (en fouten) te praten. We spreken elkaar aan als dat niet zo is. Risico's nemen is onvermijdelijk maar erover communiceren ook. Een goede dialoog, het gesprek, over risico's en kansen zien wij als een belangrijke voorwaarde voor doeltreffend risicomanagement waarbij het spreken van dezelfde taal (definities) van belang is.

e. *Continue verbetering*

Eén van onze leidende principes is het zijn van een lerende organisatie. Dit betekent dat we ons risicomanagement continue verbeteren door leren en ervaring. Wie niet reflecteert op successen en fouten, stopt met leren. Door het gesprek over risico's en kansen zien we ook eerder potentiële verbeterpunten wat bijdraagt aan het zijn van een lerende organisatie