Nota Risicomanagement en Weerstandsvermogen gemeente Teylingen

April 2026
Concerncontrol

Inhoud

1. Inleiding 3
2. Wettelijk kader risicobeheersing 4
3. Uitgangspunten risicomanagement 5
4. Weerstandsvermogen 5
5. Risicomanagement 6
5.1 Definitie 6
5.2 Inventarisatie en beoordeling 6
5.3 Beheersing 6
5.4 Beheersing strategieën 7
5.6 Het risicoregister 8
6. Rollen en verantwoordelijkheden 9
6.1 Raad 9
6.2 College 9
6.3 Ambtelijke organisatie 9
Bijlage 1: Definities 10

1. Inleiding

Voordat een organisatie haar doelen haalt moet zij eerst een hele reis afleggen. Op deze weg komt een organisatie ook onzekere gebeurtenissen tegen die het behalen van deze doelen in gevaar brengt.

Risicomanagement richt zich op deze onzekere obstakels die tussen de organisatie en het behalen van haar doelstellingen staan. Voor een organisatie is het normaal om een zekere mate van risico te lopen, bij het uitvoeren van taken komen vrijwel altijd (inherente) risico's kijken. Een goed voorbeeld hiervan is het uitsturen van facturen. De organisatie kan met de allerbeste bedoeling en zorgvuldigheid de facturen opstellen en versturen. Dit sluit niet uit dat er een foutje insluipt en een bedrag net verkeerd wordt overgenomen waardoor lager wordt gefactureerd dan de bedoeling is. Een dergelijke fout is een risico in het facturatieproces. Als er geen risico's gelopen worden, worden er ook geen doelen behaald. Hoe wordt omgegaan met deze risico's is daarom binnen het risicobeheer van belang. Hier zijn verschillende smaken in; Gaan wij het risico beheersen? Of gaan we het risico verzekeren? Accepteren we wellicht het risico?

Statement/kernboodschap risicomanagement
Goed openbaar bestuur vraagt om een voortdurende balans tussen de leefwereld waarin inwoners de effecten van beleid ervaren en de systeemwereld van regels, procedures en verantwoording. Binnen gemeente Teylingen handelen bestuurders en ambtenaren vanuit gestelde normen en waarden, met oog voor zowel het belang van onze inwoners, als wet- en regelgeving.

In de uitoefening van hun publieke taak streven bestuurders en ambtenaren naar een zo volledig mogelijk inzicht in de bijbehorende risico's. Zij beoordelen deze risico's op uniforme wijze, met inachtneming van maatschappelijke impact. Ook treffen zij passende maatregelen om de risico's te beheersen. Dit proces is een gezamenlijke verantwoordelijkheid die de bestuurders en ambtenaren oppakken door continu te leren en te verbeteren.

Voor gemeente Teylingen geldt dat risico's onlosmakelijk verbonden zijn met het uitvoeren van hun taken. Daarbij gaat het niet alleen om interne processen, maar juist ook om de dienstverlening aan inwoners. In dat kader streven we bij onze gemeentelijke taken naar een balans tussen de systeemwereld, waarin regels, procedures en wet- en regelgeving centraal staan, en de leefwereld van onze inwoners, waarin maatwerk en goede dienstverlening voorop staan. Dit betekent dat wij altijd handelen binnen de kaders van de wet (rechtmatigheid), maar tegelijk oog hebben voor wat inwoners nodig hebben (doelmatigheid en dienstverlening). Wij erkennen dat het niet mogelijk is om alle risico's volledig af te dekken; keuzes en prioriteiten zijn noodzakelijk. Daarom richten wij onze inspanningen op de belangrijkste risico's en op maatregelen die zowel effectief als haalbaar zijn. Zo combineren wij een rechtmatige overheid met een mensgerichte en verantwoorde dienstverlening.

Om deze keuzes goed te maken is het belangrijk dat wij onze aanpak van risicomanagement verder ontwikkelen. Bij risicomanagement wordt vaak gesproken over 4 volwassenheidsfasen: fase 1 reactief, fase 2 wetgeving, fase 3 proactief en fase 4 waarde.



Gemeente Teylingen staat aan het einde van fase 2 (wetgeving).
De afgelopen jaren zijn er veel ontwikkelingen in het vakgebied audit & control. Er is steeds meer wet- en regelgeving (systeemwereld) en deze wordt steeds strenger. Gemeente Teylingen loopt steeds meer risico's op het gebied van fraude, privacy, informatieveiligheid, imagoschade of achterstallig onderhoud van gemeentelijke infrastructuur (met mogelijke veiligheids- en financiële gevolgen). Het is zaak dat gemeente Teylingen de volgende stap maakt in het volwassenheidsmodel van risicomanagement. De stap van fase 2: 'wetgeving' naar fase 3: 'proactief risicomanagement'. In fase 3 gaat het om het bepalen van risicobereidheid: welke risico's accepteert gemeente Teylingen bewust om haar doelstellingen te realiseren, en waar zijn extra maatregelen noodzakelijk.
Hierbij is het belangrijk om het risicobewustzijn te vergroten (risicodialogen/spel) en de kaders en richtlijnen rondom het weerstandsvermogen en risicomanagement vast te leggen in deze nota.
Deze zullen meer houvast geven in de dagelijkse praktijk als het gaat om de omgang met risico's en een gedeelde taal voorstellen.

Hoewel er waarde wordt gehecht aan het kwantificeren van risico's en het registreren hiervan is het minstens zo belangrijk om de risico's bespreekbaar te maken. Een lijst met risico's kan de indruk wekken dat alles onder controle is, terwijl dat in de praktijk pas zo is wanneer risico's actief besproken worden en waar nodig maatregelen worden getroffen. Daarom is het van belang dat risico's onderdeel worden van de PDCA (Plan Do Check Act) cyclus.

2. Wettelijk kader risicobeheersing

Hieronder staan de wettelijke kaders uit het Besluit begroting en verantwoording provincies en gemeenten (hierna: BBV) opgenomen (artikel 9 lid 2 sub b, artikel 11, lid 1 en 2, en artikel 26):

De begroting/jaarstukken bevat een paragraaf weerstandsvermogen en risicobeheersing.
Het weerstandsvermogen bestaat uit de relatie tussen:

a. de weerstandscapaciteit, zijnde de middelen en mogelijkheden waarover de gemeente beschikt of kan beschikken om niet begrote kosten te dekken;
b. alle risico's waarvoor geen maatregelen zijn getroffen en die van materiële betekenis kunnen zijn in relatie tot de financiële positie.

De paragraaf betreffende het weerstandsvermogen en risicobeheersing bevat ten minste:

a. een inventarisatie van de weerstandscapaciteit;
b. een inventarisatie van de risico's;
c. het beleid omtrent de weerstandscapaciteit en de risico's;
d. een kengetal voor de:
    1. netto schuldquote;
    2. netto schuldquote gecorrigeerd voor alle verstrekte leningen;
    3. solvabiliteitsratio;

4. grondexploitatie;
5. structurele exploitatieruimte; en
6. belastingcapaciteit;

e. een beoordeling van de onderlinge verhouding tussen de kengetallen in relatie tot de financiële positie.

Ook zijn er nog diverse andere wettelijke kaders die toezien op risicobeheersing. Denk hierbij bijvoorbeeld aan de Baseline Informatiebeveiliging Overheid op het gebied van informatieveiligheid. Wettelijke kaders die toezien op risico's op specifieke onderwerpen worden meegenomen bij de risico-inventarisatie voor die specifieke onderwerpen.

3. Uitgangspunten risicomanagement

Hieronder volgen de algemene uitgangspunten van gemeente Teylingen betreffende risico's.

- Gemeente Teylingen voldoet aan geldende wet- en regelgeving en geeft invulling aan de richtlijnen van het BBV.
- De norm is dat in het samenspel tussen raad/bestuur, college/directie en de ambtelijke organisatie transparant met risico's en maatregelen wordt omgegaan;
- Gemeente Teylingen legt risico's en beheersmaatregelen eenduidig en centraal vast in het risicoregister; en er wordt gestuurd op deze beheersmaatregelen.
- Het college/de directie weegt bij de voorbereiding van voorstellen de risico's mee en stelt vast op welke wijze de raad/het bestuur daarover geïnformeerd wordt;
- Gemeente Teylingen neemt bij projecten een paragraaf risico's en beheersmaatregelen op en wordt afgesproken hoe (waar nodig) de directeur of het bestuur op de hoogte gehouden worden;
- Gemeente Teylingen geeft via de P&C cyclus inzicht in de top 10 risico's. Daarbij hanteren we een drempelbedrag van €100.000 op basis van het gewogen financiële risico (kans x impact); risico's met een lagere omvang worden niet afzonderlijk opgenomen in de paragraaf weerstandsvermogen en risicobeheersing. Indien minder dan 10 risico's boven deze grens uitkomen, wordt de rapportage aangevuld met de eerstvolgende risico's op basis van hoogte van de benodigde weerstandscapaciteit, zodat in de paragraaf weerstandsvermogen en risicobeheersing inzicht wordt gegeven in de top 10 risico's. De drempel van €100.000 geldt uitsluitend voor opname in de paragraaf weerstandsvermogen; alle risico's blijven opgenomen in het risicoregister en tellen mee bij het berekenen van de benodigde weerstandscapaciteit.

Deze algemene uitgangspunten voor het omgaan met risico's en risicomanagement worden waar nodig in de volgende hoofdstukken toegelicht.

4. Weerstandsvermogen

Zoals gesteld loopt een organisatie per definitie risico's. Immers bij het bereiken van (vrijwel) ieder doel komen obstakels kijken. Eén van de manieren om risico's te beheersen is middels het opbouwen van weerstandsvermogen. Dit is de (financiële) capaciteit die aanwezig is in een gemeente mocht een risico zich voordoen om de eventuele financiële effecten op te vangen. Deze capaciteit bestaat uit de "vrij aanwendbare middelen". Dat zijn de buffers/middelen waar nog geen bestemming aan hangt. Denk hierbij aan een algemene reserve waar middelen in aanwezig zijn.

In hoeverre een organisatie in staat is om financiële tegenvallers op te vangen hangt af van:

- De risico's die de organisatie loopt.
- De middelen die de organisatie vrij kan maken om risico's op te vangen.

Hierbij zijn twee elementen belangrijk:

- Hoeveel middelen zijn nodig om eventuele tegenvallers op te kunnen vangen? Dit noemen we de benodigde weerstandscapaciteit.
- Hoeveel middelen zijn beschikbaar om eventuele tegenvallers op te kunnen vangen? Dit noemen we de beschikbare weerstandscapaciteit.

Het weerstandsvermogen geeft aan wat de verhouding is tussen de beschikbare en de benodigde hoeveelheid geld, en dus de mate waarin de organisatie in staat is om de ongewenste gevolgen van risico's op te vangen. Dit wordt uitgedrukt in onderstaande breuk:

$$\text{Weerstandsvermogen} = \frac{\text{beschikbare weerstandscapaciteit}}{\text{benodigde weerstandscapaciteit}}$$

5. Risicomanagement

Het vak risicomanagement bestaat in essentie uit twee disciplines. Aan de ene kant hebben we het inventariseren en beoordelen van risico's en aan de andere kant het beheersen van de risico's. In deze paragraaf behandelen we beide takken van sport. Het is daarbij belangrijk te benadrukken dat het niet alleen gaat om financiële risico's, maar om alle typen risico's die de organisatie kunnen raken: financieel, wet- en regelgeving, informatie, privacy, integriteit, reputatie, veilige werkomgeving en fraude.

5.1 Definitie

Risicomanagement is het systematisch herkennen, analyseren en beheersen van risico's die het behalen van organisatiedoelen kunnen belemmeren. Een risico is een gebeurtenis of ontwikkeling die, indien deze zich voordoet, kan leiden tot significante financiële, operationele, strategische of maatschappelijke gevolgen voor gemeente Teylingen, en waarover gemeente Teylingen enige mate van invloed of beheersing heeft[1]. Naast financiële schade kunnen risico's zich ook uiten in bijvoorbeeld reputatieschade, integriteitskwesties of verstoring van de dienstverlening.

5.2 Inventarisatie en beoordeling

De inventarisatie start met de vraag: *"Welke onzekere gebeurtenissen kunnen het behalen van onze doelen verstoren?"*.[1] Deze risico's worden beoordeeld op twee aspecten:

- Kans: de waarschijnlijkheid dat het risico zich voordoet, op een schaal van 1 (zeer klein) tot 5 (zeer groot).
- Impact: de ernst van de gevolgen, beoordeeld aan de hand van themaspecifieke impacttabellen, op een schaal van 1 (zeer klein) tot 5 (zeer groot).

De bruto risicoscore wordt berekend door kans x impact. Deze score bepaalt de zwaarte van het risico en vormt de basis voor verdere beheersing. De netto risicoscore wordt vergelijkbaar berekend, maar dan na beheersmaatregelen.

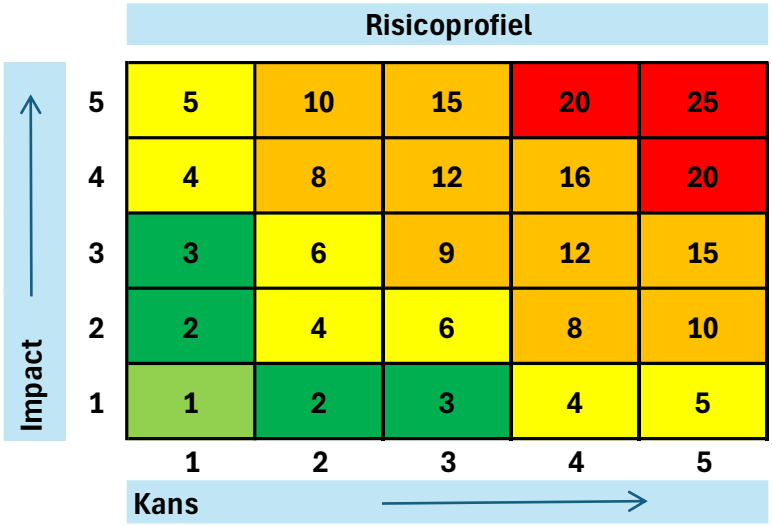
5.3 Beheersing

Beheersing is het beperken van risico's door passende maatregelen te nemen. Op basis van de bruto risicoscore wordt het risico ingedeeld in één van vijf categorieën:

[1] Gebeurtenissen die geheel buiten de invloedssfeer van gemeente Teylingen liggen, waarbij mitigerende maatregelen vanuit HLTsamen weinig tot geen impact hebben (zoals oorlog, natuurrampen van mondiale omvang of andere catastrofale gebeurtenissen), worden in dit kader niet als risico meegenomen.

- **Lichtgroen (1)**: Zeer laag risico: reguliere monitoring van het risico, verantwoordelijkheid bij de teammanager/projectleider.
- **Groen (2–3)**: Laag risico: specifieke monitoring van het risico, verantwoordelijkheid bij de teammanager/projectleider.
- **Geel (4–6)**: Gemiddeld risico: beheersmaatregelen gewenst, verantwoordelijkheid bij teammanager.
- **Oranje (8–16)**: Hoog risico: beheersmaatregelen formuleren en implementeren, verantwoordelijkheid bij teammanager en directeur
- **Rood (20–25)**: Zeer hoog risico: direct ingrijpen, beheersplan en monitoring verplicht, verantwoordelijkheid bij de directie

Deze indeling helpt bij het prioriteren van acties en het bepalen van verantwoordelijkheden.



5.4 Beheersing strategieën

Voor elk risico wordt een beheersstrategie gekozen. Er zijn vier mogelijkheden:

1. Accepteren – het risico wordt bewust genomen.
2. Reduceren – maatregelen verkleinen de kans of impact.
3. Verleggen – risico wordt overgedragen (bijv. via verzekering of contract).
4. Vermijden – activiteit of doelstelling wordt aangepast of beëindigd.

De keuze voor een strategie hangt af van de risicobereidheid van de organisatie. Na uitvoering van maatregelen wordt de netto risicoscore bepaald.

Voor risico's in de rode categorie is een beheersplan verplicht. Dit bevat:

- De gekozen strategie
- Toelichting op maatregelen
- Planning en effect
- Gewenste netto risicoscore

In lijn met het groeimodel volwassenheidsfasen wordt het risicomanagement de komende jaren verder ontwikkeld, waarbij een van de ontwikkelpunten is om in de paragraaf weerstandsvermogen meer inzicht te geven in de afwegingen tussen de risico's en de bijbehorende beheersmaatregelen.

5.5 Controle

De effectiviteit van beheersmaatregelen wordt getoetst via het Three Lines Model:

- Eerste lijn: teams zelf, via ingebouwde procescontroles.
- Tweede lijn: ondersteunende functies zoals financiën.
- Derde lijn: onafhankelijke toetsing, o.a. VIC, CISO, FG en concern control

Hiernaast zijn er nog externe controlepartijen zoals de accountant.

Deze controles zorgen voor inzicht in de werking van maatregelen en dragen bij aan continue verbetering van risicobeheersing.

5.6 Het risicoregister

Alle risico's met hun netto risicoscore worden vastgelegd in het risicoregister. Dit register voedt de P&C-producten en biedt inzicht in de ontwikkeling van risico's in de tijd. Minimaal halfjaarlijks wordt het register geactualiseerd. De top 10 risico's worden opgenomen in de paragraaf weerstandsvermogen en risicobeheersing en wordt gedeeld met bestuur/raad. Team Financiën ondersteunt bij het beheer van het register.

In het risicoregister worden onder andere het betreffende team, programma, omschrijving risico en impact, risicoscore, beheersstrategie, enzovoorts opgenomen.

Risicobewustzijn

Naast het registreren van risico's is het vergroten van risicobewustzijn een belangrijk aandachtspunt. Dit gebeurt op meerdere manieren:

- Risicospel: een interactieve manier om medewerkers bewust te maken van risico's en beheersmaatregelen.
- Frauderisicoanalyse: Concern Control stelt jaarlijks samen met de teammanagers een frauderisicoanalyse op.
- Intakeformulieren: risicovragen worden standaard meegenomen bij de start van projectplannen en programmaplannen.
- Grex (grondexploitaties) en Anterieure overeenkomsten: risico's worden bij de start en tijdens de uitvoering van grondexploitaties en bij het aangaan en uitvoeren van anterieure overeenkomsten (groeimodel n.a.v. 213a onderzoek) besproken en gevolgd.
- Bespreking in overleggen: risico's worden structureel besproken binnen teams, projectgroepen en managementoverleggen.

Door risicobewustzijn op deze manier structureel te integreren, wordt het risicoregister niet alleen een administratief overzicht, maar een levend instrument dat bijdraagt aan betere besluitvorming en beheersing van risico's.

6. Rollen en verantwoordelijkheden

De rollen en verantwoordelijkheden van de raad, het college en de ambtelijke organisatie zijn als volgt.

6.1 Raad

De raad stelt de kaders vast voor het beleid risicomanagement en weerstandsvermogen. De raad heeft daarmee een kaderstellende en controlerende rol.
Dit betreft onder meer:

- Vaststelling van de nota; inclusief de daarbij behorende kaders en uitgangspunten.
- Vaststelling van de paragraaf weerstandsvermogen en risicobeheersing in de begroting en jaarstukken;

6.2 College

Het college is verantwoordelijk voor:

- De uitvoering van het risicomanagementbeleid;
- Opstellen van een juiste paragraaf weerstandsvermogen.
- Het informeren van de raad over materiële risico's;
- Het opnemen van risico's en beheersmaatregelen in raadsvoorstellen.

6.3 Ambtelijke organisatie

De directie en teammanagers zijn verantwoordelijk voor:

- Het actief signaleren en registreren van risico's;
- Het uitvoeren van beheersmaatregelen;
- Het actualiseren van het risicoregister;
- Het voeren van risicodialogen binnen teams en projecten.

Bijlage 1: Definities

Het weerstandsvermogen geeft aan wat de verhouding is tussen de beschikbare hoeveelheid geld en de benodigde hoeveelheid geld, of de mate waarin de organisatie in staat is om de ongewenste gevolgen van risico's op te vangen. Dit wordt uitgedrukt in onderstaande breuk:

$$\text{Weerstandsvermogen} = \frac{\text{beschikbare weerstandscapaciteit}}{\text{benodigde weerstandscapaciteit}}$$

Beschikbare weerstandscapaciteit: hoeveel middelen zijn beschikbaar om eventuele risico's op te kunnen vangen. In het BBV (artikel 11.1) omschreven als 'de middelen en mogelijkheden waarover de organisatie beschikt of kan beschikken om niet begrote kosten te dekken'.

Benodigde weerstandscapaciteit: hoeveel middelen zijn nodig om eventuele risico's op te kunnen vangen (totaal van kans x impact van gekwantificeerde risico's).

Risicomanagement is het geheel aan activiteiten en maatregelen gericht op het expliciet en systematisch omgaan met en het beheersen van risico's.

Een risico is een onzekere gebeurtenis met (gewenste of ongewenste) gevolgen voor de organisatie. Deze gevolgen kunnen beleidsmatig en/of financieel zijn.

Beheersmaatregelen/beheersing: het stelsel van maatregelen en procedures die worden genomen om de onderkende risico's te ondervangen dan wel om de opkomende risico's te signaleren en het effect hiervan te beperken.

Accepteren van het risico: op basis van risicobereidheid kan een risico acceptabel zijn zonder beheersmaatregelen. Hierbij kan het zijn dat de kans en/of impact van het risico wel groot is.

Reduceren van het risico: de risico's worden beheerst met als doel de kans op voorkomen van een risico of de impact ervan te verminderen. Dit kan bijvoorbeeld door processen aan te passen.

Verleggen van het risico: men kan het risico verzekeren, uitbesteden of contracten sluiten.

Vermijden van het risico: dit kan door het stoppen van een activiteit of door de doelstelling te veranderen.

Beheersingsplan: bestaat in ieder geval uit:
- Keuze voor beheersingsstrategie
- Toelichting op de toekomstige/genomen maatregelen
- Planning van de invoer van de maatregelen
- Effect van de toekomstige/genomen maatregelen
- Te behalen netto risicoscore

De netto risicoscore: de risicoscore nadat we de benodigde beheersing hebben genomen. We kijken daarom, nadat we de benodigde beheersing hebben genomen, nogmaals naar de risicoscore. In welke mate is deze afgenomen? Door de kans maal impact te doen komt er, na beheersing, weer een score uit. Omdat we het hier hebben over de score na beheersing noemen we dit de netto risicoscore.

Het risicoregister: de verzameling van risico's met hun netto risicoscores.

De 1e-lijns controle betreft de controle ingebouwd in het proces zelf. De eerste lijn wordt gevormd door de teams zelf. Zij zijn verantwoordelijk voor het uitvoeren van processen en het nemen van beheersmaatregelen binnen hun werkgebied.

De 2e-lijns controle zijn de controles die de afdelingen zelf uitvoeren op hun eigen processen. Deze lijn wordt gevormd door ondersteunende functies zoals Financiën. Zij houden toezicht op de kwaliteit van de beheersmaatregelen, adviseren over risicobeheersing en zorgen ervoor dat risico's binnen de afgesproken kaders worden gemonitord. De tweede lijn ondersteunt de eerste lijn bij het naleven van beleid en richtlijnen, en draagt zo bij aan een consistent en betrouwbaar risicobeheer binnen de organisatie.

De 3e-lijns controle betreft de verbijzonderde interne controle (VIC) die wordt uitgevoerd door team VIC en heeft als doel om, onafhankelijk van de interne controle, vast te stellen of de interne controlemaatregelen (controle binnen de processen) zijn uitgevoerd en voldoende hebben gewerkt.