

Risicomanagement voor gemeenten

Handreiking



Naam document

Risicomanagement voor gemeenten op basis van de BIO2

Versienummer

1.0

Versiedatum

28-05-2025

Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).



INFORMATIE
BEVEILIGINGS
DIENST

Vereniging van Nederlandse Gemeenten / **Informatiebeveiligingsdienst** voor gemeenten (IBD)



Tenzij anders vermeld, is dit werk verstrekt onder een Creative Commons Naamsvermelding-Niet Commercieel-Gelijk Delen 4.0 Internationaal licentie. Dit houdt in dat het materiaal gebruikt en gedeeld mag worden onder de volgende voorwaarden: Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:

De IBD wordt als bron vermeld.

Het document en de inhoud mogen commercieel niet geëxploiteerd worden.

Publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door de IBD en / of de Vereniging van Nederlandse Gemeenten.

Iedere kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Wanneer dit werk wordt gebruikt, hanteer dan de volgende methode van naamsvermelding: "Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten", licentie onder: CC BY-NC-SA 4.0.

Bezoek <http://creativecommons.org/licenses/by-nc-sa/4.0> voor meer informatie over de licentie.

Rechten en vrijwaring

De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Met dank aan

De gemeenten en samenwerkingsverbanden die hebben bijgedragen aan de totstandkoming van dit document.

Wijzigingshistorie:

Versie	Datum	Wijziging / Actie
1.0	28-05-2025	Eerste versie

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Inhoud

1.	Managementsamenvatting	5
2.	Inleiding	7
2.1.	Wat is risicomanagement	7
2.2.	Waarom is dit belangrijk	7
2.3.	Leeswijzer	8
3.	Wet en regelgeving	10
3.1.	De richtlijn NIS2 en de Cyberbeveiligingswet (Cbw)	10
3.2.	Wat zegt de Cbw over risicomanagement?	10
3.3.	De BIO	11
3.4.	De ISO 27005 aanpak	12
3.5.	Samenvattend	18
4.	Niveaus in risicomanagement	19
5.	Rollen en verantwoordelijkheden in relatie tot risicomanagement	20
5.1.	De bestuurder	20
5.2.	De gemeentesecretaris	21
5.3.	De lijnmanagers of proceseigenaren	22
5.4.	De informatiemanager	23
5.5.	De concerncontroller	24
5.6.	De CISO	25
5.7.	De PO	25
5.8.	Ondersteunende rollen	26
5.9.	Samenvattend	26
6.	Uitgangspunten Risicomanagement voor gemeenten	27
6.1.	Actor	27
6.2.	Kans	28
6.3.	Impact	29
7.	Risicomanagement aanpakken voor gemeenten	30
8.	De Business Model Canvas methode	30
8.1.	Stap 0 – Context vaststellen	31
8.2.	Stap 1 – Bepaal welke processen risicoanalyse behoeven (BIA-fase)	32
8.3.	Stap 2 – Organiseer een groepsessie met de juiste deelnemers	33
8.4.	Stap 3 – Vul gezamenlijk het BMC in	33

8.5.	Stap 4 – Identificeer risico's per canvasblok	33
8.6.	Stap 5 – Waardeer risico's (kans × impact)	34
8.7.	Stap 6 – Behandel risico's volgens ISO 27005	35
8.8.	Stap 7 – GAP-analyse en actieplan tegen BIO2-maatregelen	35
8.9.	Stap 8 – Maak de resultaten concreet.....	36
8.10.	Bijlagen en hulpmiddelen en links:.....	36
9.	De MAPGOOD methode	37
10.	Hoe zit het met de relatie tussen de ISO27005 aanpak en andere risicomanagement standaarden.....	37
11.	Van risicoanalyse naar structureel risicomanagement binnen het ISMS.....	40
11.1.	Vertaling naar beleid en doelstellingen	40
11.2.	Vastleggen in risicoregister en maatregelregister	40
11.3.	Monitoring en rapportage (Check-fase).....	41
11.4.	Integratie in de Planning & Control-cyclus	41
11.5.	Evaluatie via interne audit en management review.....	41
11.6.	Continue verbetering (Act-fase)	42
11.7.	Risicoacceptatie, escalatie en waiver-procedure	42
11.8.	Koppeling met andere cybersecurity- en beheerprocessen	43
11.9.	Rollen en verantwoordelijkheden	43
12.	Bijlage: Definities en kaders voor risicomanagement in gemeentelijke context	45
12.1.	Dreiging	45
12.2.	Kwetsbaarheid.....	45
12.3.	Actor	45
12.4.	Risico.....	45
12.5.	Incident.....	45
13.	Methodieken in samenhang.....	46
13.1.	Business Model Canvas (BMC)	46
13.2.	Proces Risico Model Gemeente (PRMG).....	46
13.3.	MAPGOOD.....	46
14.	Bijlage risicomatrix.....	47
15.	BMC en PRMG model	48

1. Managementsamenvatting

Met de komst van de cyberbeveiligingswet (Cbw) en de BIO2 waarmee in Nederland invulling wordt gegeven aan de NIS2 krijgt risicomanagement een prominente rol om de cyberveiligheid van organisaties te verhogen. Risicomanagement is het systematisch identificeren, beoordelen en beheersen van onzekerheden die de doelen van een organisatie kunnen bedreigen, zodat weloverwogen keuzes kunnen worden gemaakt en schade wordt voorkomen of beperkt.

Deze handreiking biedt een gestructureerde en praktische aanpak voor het uitvoeren van risicoanalyses op gemeentelijke processen, in lijn met de ISO 27005-nor. Door gebruik te maken van het Business Model Canvas (BMC) en het Proces Risico Model Gemeente (PRMG), wordt het voor proceseigenaren mogelijk om risico's niet alleen systematisch te identificeren, maar ook visueel inzichtelijk te maken. De methode is specifiek bedoeld voor gemeentelijke (kritieke) processen, die voorafgaand worden geselecteerd op basis van een beknopte Business Impact Analyse (BIA) met behulp van de door de IBD opgestelde impacttabel. Deze analyse helpt gemeenten te bepalen welke processen bijzondere aandacht verdienen vanwege hun potentieel grote impact op beschikbaarheid, integriteit, vertrouwelijkheid, privacy en bestuurlijke gevolgen.

De kern van de aanpak is een gestructureerde groepssessie waarin, onder leiding van de proceseigenaar en eventueel ondersteund door een CISO, een PO of andere adviseurs, het volledige BMC van het proces wordt ingevuld. Vervolgens worden, per onderdeel van het BMC, risico's benoemd, geclassificeerd op Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) langs de productiemiddelen: Mens, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving en Diensten (MAPGOOD), en gewaardeerd op basis van kans en impact.

Risico's die boven de vooraf vastgestelde risicobereidheid uitkomen, worden volgens de methodiek van ISO 27005 behandeld. De risicobehandeling houdt in dat er per risico een keuze gemaakt wordt of deze vermeden, verminderd, overgedragen dan wel geaccepteerd wordt. De gekozen maatregelen worden gecategoriseerd naar hun aard (organisatorisch, personeel, fysiek, technisch) en geëvalueerd op effectiviteit. Daarna volgt een GAP-analyse op basis van de BIO2-maatregelen om te controleren welke maatregelen al zijn ingevoerd en waar nog actie nodig is.

De aanpak zorgt niet alleen voor bewustwording en eigenaarschap bij proceseigenaren, maar levert ook concrete resultaten op:

- een volledig ingevuld BMC/PRMG;
- een geprioriteerd risicoregister;
- een actielijst en een maatregelenoverzicht.

Deze output kan direct worden opgenomen in het gemeentelijk ISMS, als input voor een informatiebeveiligingsplan, en als onderbouwing voor audits en toezicht. Door het proces

cyclisch in te richten, wordt ook de basis gelegd voor continue monitoring en verbetering, zoals voorgeschreven door de ISO 27001 en ISO 27005.

Disclaimer:

Over het gebruik van het Business Model Canvas

In deze handreiking gebruiken we het Business Model Canvas (BMC) als basis. Dit model is ontwikkeld door [Alexander Osterwalder en Strategyzer AG](#), en mag vrij gebruikt en aangepast worden dankzij de Creative Commons-licentie CC BY-SA 4.0. De aanvullingen die je hier ziet — zoals de koppeling met MAPGOOD, de BIV-classificatie en de procesgerichte risicoanalyse — zijn speciaal ontwikkeld voor toepassing binnen gemeenten. Ook deze aanvullingen stellen we beschikbaar onder CC BY-SA 4.0, zodat anderen ermee aan de slag kunnen, zolang de bovengenoemde bron maar netjes vermeld wordt.

2. Inleiding

2.1. Wat is risicomanagement

Risicomanagement is het proces van systematisch identificeren, analyseren, evalueren en beheersen van potentiële risico's die de doelstellingen van een organisatie kunnen bedreigen. Het doel van risicomanagement is om onzekerheden inzichtelijk te maken en bewust keuzes te maken over hoe met deze risico's wordt omgegaan: accepteren, vermijden, verminderen of overdragen. Door risico's vroegtijdig te onderkennen en beheersmaatregelen te treffen, kunnen organisaties hun weerbaarheid vergroten, beter inspelen op veranderingen en de kans op verstoringen of schade verkleinen. Risico's kunnen zowel een positieve als een negatieve uitwerking hebben op de doelstelling van de organisatie. Risicomanagement is daarmee een belangrijk onderdeel van goed bestuur en draagt bij aan continuïteit, veiligheid en het behalen van strategische doelen.

Voorbeeld van een positief risico:

Succesvolle online dienstverlening overstijgt verwachtingen.

- Context: Een gemeente lanceert een nieuw digitaal loket voor het aanvragen van uittreksels, rijbewijzen en parkeervergunningen. De verwachting was een geleidelijke toename in gebruik.
- Risico: Het systeem blijkt veel populairder dan voorzien, waardoor er in korte tijd veel meer aanvragen binnenkomen dan verwacht.
- Impact: Het succes draagt bij aan de doelstellingen rond digitale dienstverlening, maar leidt tot capaciteitsproblemen bij de afhandeling van aanvragen, performance-issues bij het systeem en extra druk op de servicedesk.
- Beheersmaatregel: Schaalbare cloudoplossing inzetten en een flexibele schil aan personeel organiseren. Daarnaast monitoring van piekmomenten en automatische doorgeleiding naar selfservice-informatie.

Voorbeeld van een negatief risico:

Cyberaanval op burgerzakenapplicatie.

- Context: De gemeentelijke burgerzakenapplicatie wordt doelwit van een ransomware-aanval.
- Risico: Niet beschikbaarheid van essentiële diensten zoals aangifte geboorte, overlijden, of aanvragen identiteitsbewijs.
- Impact: Grote verstoring van dienstverlening, schade aan vertrouwen van inwoners, en mogelijk boetes bij datalekken (AVG).
- Beheersmaatregel: Implementatie van monitoring en respons, segmentering van het netwerk, zero trust, actuele back-ups en een geoefend cybercrisisplan (Om wat voorbeeld maatregelen te noemen)

2.2. Waarom is dit belangrijk

Risicomanagement is voor Nederlandse gemeenten van groot belang omdat zij verantwoordelijk zijn voor een breed scala aan publieke taken, variërend van jeugdzorg en

ruimtelijke ordening tot burgerzaken en informatievoorziening. Fouten of verstoringen in deze processen kunnen directe gevolgen hebben voor inwoners, bedrijven en het vertrouwen in het openbaar bestuur. Daarnaast werken gemeenten steeds vaker samen in ketens, maken zij gebruik van complexe ICT-systemen en zijn zij gebonden aan strikte wet- en regelgeving zoals de BIO, AVG en (aankomende) Cbw als nationale wetgeving in het kader van de NIS2 richtlijn. Goed risicomanagement helpt gemeenten om tijdig inzicht te krijgen in kwetsbaarheden, afgewogen besluiten te nemen over de inzet van mensen en middelen, en de dienstverlening aan inwoners continu en veilig te houden. Het draagt ook bij aan bestuurlijke verantwoording en het aantoonbaar 'in control' zijn.

2.3. Leeswijzer

Dit document biedt een gestructureerde aanpak voor risicomanagement in gemeentelijke processen, met specifieke aandacht voor de implementatie van de Cbw en de BIO2. De inhoud is bedoeld voor gemeentelijke professionals die betrokken zijn bij het waarborgen van de cyberveiligheid en het uitvoeren van risicoanalyses binnen hun organisatie.

Hoofdstukken:

1. **Wat is risicomanagement:** In dit hoofdstuk wordt het concept risicomanagement uitgelegd, met de nadruk op het systematisch identificeren, beoordelen en beheersen van risico's om de organisatiedoelen te beschermen.
2. **Waarom is dit belangrijk:** Hier wordt het belang van risicomanagement voor gemeenten toegelicht, waarbij de nadruk ligt op de verantwoordelijkheden die gemeenten dragen voor publieke taken en de impact van risico's op de dienstverlening aan burgers en bedrijven.
3. **Wet- en regelgeving:** Dit deel behandelt de relevante wet- en regelgeving, zoals de NIS2 en de Cyberbeveiligingswet (Cbw), en de verplichtingen die voortkomen uit deze wetten voor gemeenten op het gebied van risicomanagement.
4. **De NIS2 en de Cbw):** In dit hoofdstuk wordt dieper ingegaan op de eisen die NIS2 stelt aan risicomanagement en de manier waarop de Cbw gemeenten verplicht om risicobeheer op te zetten en te onderhouden.
5. **De BIO2:** De Baseline Informatiebeveiliging Overheid 2 (BIO2) wordt besproken, met de focus op hoe gemeenten deze baseline kunnen toepassen om de informatiebeveiliging te waarborgen en risicomanagement effectief te implementeren.
6. **De ISO 27005 aanpak:** Dit hoofdstuk biedt een gedetailleerd overzicht van de ISO 27005-norm, die gemeenten kan helpen bij het uitvoeren van risicomanagement specifiek voor informatiebeveiliging.
7. **Niveaus in risicomanagement:** Hier worden de verschillende niveaus van risicomanagement (strategisch, tactisch en operationeel) beschreven en de rol van gemeentelijke medewerkers in elk van deze niveaus.
8. **Rollen en verantwoordelijkheden in risicomanagement:** Dit hoofdstuk geeft inzicht in de verschillende rollen die betrokken zijn bij het risicomanagementproces, van de gemeentesecretaris en bestuurders tot de CISO en proceseigenaren.
9. **Risicomanagement aanpakken voor gemeenten:** Hier worden praktische stappen beschreven voor het uitvoeren van risicoanalyses en het identificeren van kritieke gemeentelijke processen met behulp van methoden zoals het Business Model Canvas (BMC) en MAPGOOD.

Het document eindigt met een samenvatting van de aanpak, waarbij de nadruk ligt op de integratie van risicomanagement in de gemeentelijke planning en control cyclus en het belang van continue verbetering.

3. Wet en regelgeving

3.1. De richtlijn NIS2 en de Cyberbeveiligingswet (Cbw)

De Network and Information Security Directive 2 (NIS2-richtlijn), die vanaf 17 oktober 2024 in Nederland van kracht is geworden en die via de Cyberbeveiligingswet (Cbw) een nationale uitwerking gaat krijgen, legt een stevige nadruk op risicomanagement als kernverantwoordelijkheid van essentiële en belangrijke entiteiten. In artikel 21 van de richtlijn worden elementen genoemd die opgelegd worden aan organisaties ten aanzien van het treffen van passende en evenredige technische, operationele en organisatorische maatregelen.

3.2. Wat zegt de Cbw over risicomanagement?

De Cbw stelt in artikel 2 dat organisaties passende maatregelen moeten nemen op basis van een risicoanalyse, met als doel om:

- de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van netwerk- en informatiesystemen te waarborgen;
- cyberdreigingen te voorkomen, op te sporen, inzichtelijk te maken, te beperken en te herstellen;
- incidenten met grote impact te voorkomen.

3.2.1. Verplichte maatregelen (NIS2, artikel 21, lid 2)

In de Cbw worden de maatregelen uit de NIS2 in artikel 21 opgesomd die een relatie hebben met risicomanagement (zorgplicht), waaronder (niet letterlijk overgenomen):

1. Beleid inzake risicobeoordeling en beveiliging van informatiesystemen en OT.
2. Incidentbehandeling (incident response).
3. Assetmanagement (Heeft een gemeente inzicht in alle assets (inclusief OT) waarvan de weerbaarheid beheerd moet worden).
4. Business continuity (BCM), zoals back-up beheer en disaster recovery.
5. Beveiliging van de toeleveringsketen (**supply chain security**).
6. Beveiligingsarchitectuur en toegangsbeheer.
7. Encryptie en andere vormen van gegevensbescherming.
8. Training en bewustwording bij personeel.
9. Beleid en procedures voor het gebruik van cryptografie en beveiligingsupdates.

3.2.2. Risicomanagement is geen eenmalige actie

De NIS2 benadrukt dat risicomanagement **een continu proces** is, afgestemd op de dreigingen en het belang van de diensten die een organisatie levert. Het is géén checklist of momentopname, maar een structurele aanpak waarbij regelmatig wordt herzien of de genomen maatregelen nog toereikend zijn.

3.2.3. Aansprakelijkheid en governance

Een belangrijk nieuw element is dat het **bestuur van de organisatie verantwoordelijk en aansprakelijk** is voor de implementatie van risicomanagementmaatregelen. Bestuurders moeten dus actief betrokken zijn bij de beveiligingsstrategie en keuzes maken, erop sturen en zich laten informeren.

3.3. De BIO

De Baseline Informatiebeveiliging Overheid 2 (BIO2) is het verplichte normenkader voor informatiebeveiliging bij alle overheidsorganisaties. Het biedt een framework, richtlijnen, algemene principes en verplichte overheidsmaatregelen voor het initiëren, implementeren, onderhouden en verbeteren van informatiebeveiliging binnen overheidsorganisaties en hun ketens. Het doel van de BIO2 is om de informatieveiligheid overheidsbreed op een gemeenschappelijk basisniveau te brengen en daardoor ook de ketenpartners een basis van vertrouwen te geven bij gegevensuitwisseling. De aanpak conform BIO2 vraagt inspanning door ketenorganisaties en eenduidige samenwerking.

De BIO is samengesteld uit de aanpak van de NEN-EN-ISO/IEC 27001 (het managementsysteem), de beheersmaatregelen en implementatierichtlijnen uit de NEN-EN-ISO/IEC 27002 en aanvullende verplichte overheidsspecifieke maatregelen en -richtlijnen.

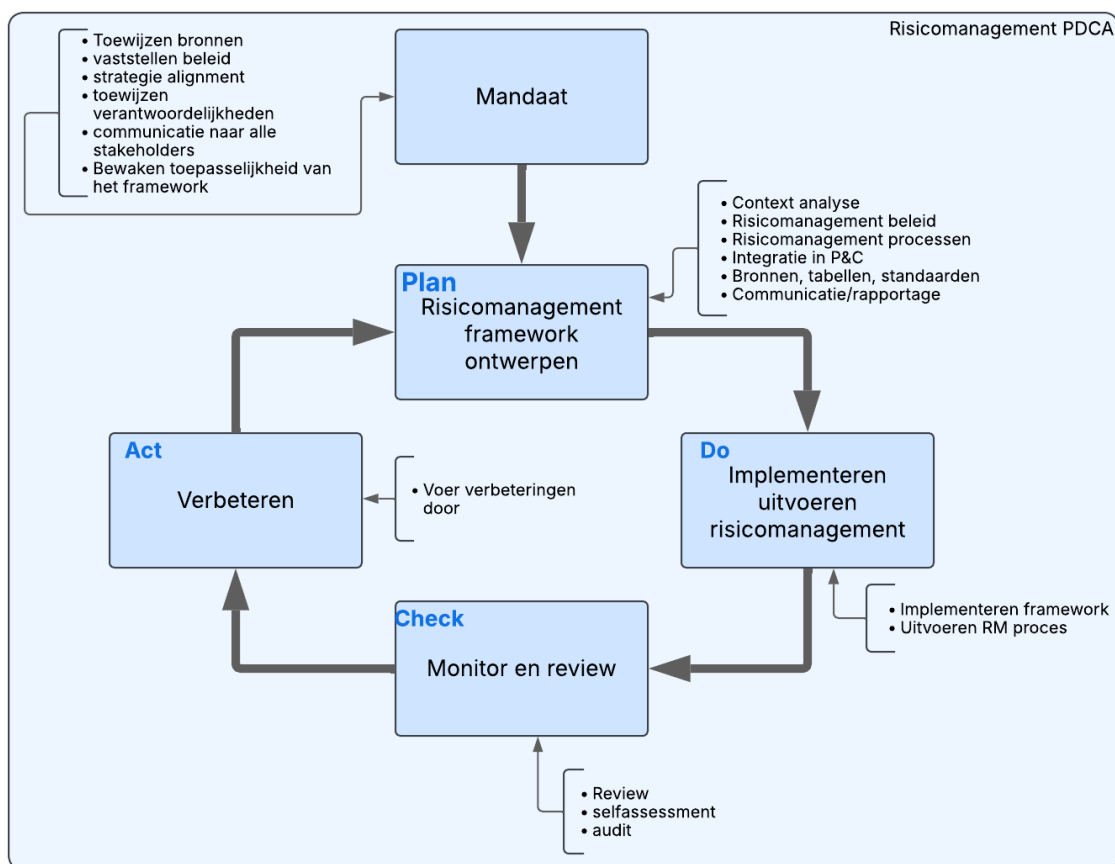
Het feit dat de BIO2 is uitgebreid met de NEN-EN-ISO/IEC 27001 betekent dat een ISMS moet worden ingericht, waarbij risicomanagement een prominente rol heeft. In de NEN-EN-ISO/IEC 27001 staat dit verwoord bij clausules:

PLAN fase:

- 6.1.1 Risicobeoordeling: De organisatie moet risico's en kansen vaststellen die het ISMS beïnvloeden.
- 6.1.2 Risicobeoordeling: De organisatie moet een risicobeoordelingsprocedure definiëren en toepassen.
- 6.1.3 Risicobehandeling: de organisatie moet een risicobehandelingsprocedure definiëren en toepassen, hier wordt voor een methode verwezen naar de ISO31000/ISO27005.

DO fase:

8.2 Risicobeoordeling van informatiebeveiliging: Op basis van de criteria uit 6.1.2 uitvoeren van risicoanalyses en de documentatie bewaren.

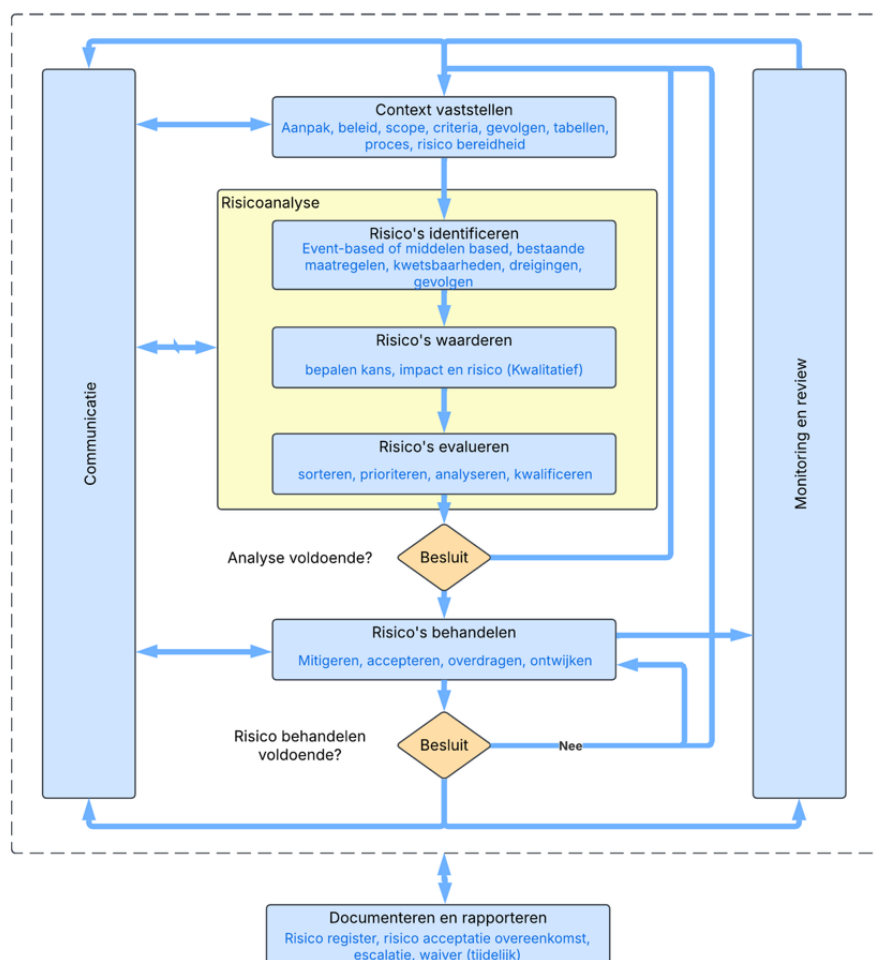


Afbeelding: Risicomanagement PDCA cyclus

3.4. De ISO 27005 aanpak

NEN-ISO/IEC 27005 is een internationale standaard die richtlijnen geeft voor het uitvoeren van risicomanagement op het gebied van informatiebeveiliging. De ISO 27005 is een afgeleide van NEN-ISO/IEC 31000, maar speciaal aangepast voor de 2700x serie. Deze standaard ondersteunt organisaties bij het opzetten, onderhouden en continu verbeteren van een risicomanagementproces dat aansluit op het Information Security Management System (ISMS) zoals beschreven in ISO 27001.

ISO 27005 schrijft geen specifieke methode voor, maar biedt een raamwerk waarin risico's stapsgewijs worden herkend, beoordeeld, behandeld en gemonitord. Hierdoor blijft informatiebeveiliging afgestemd op de context van de organisatie en op veranderingen in dreigingen, kwetsbaarheden en bedrijfsactiviteiten. Onderstaand een overzicht van het risicomanagement proces uit de ISO/IEC 27005:



Afbeelding: risicomanagement volgens de NEN-ISO/IEC 27005 (en de NEN-ISO/IEC 31000)

3.4.1. Context vaststellen

De eerste stap in het risicomanagementproces is het vaststellen van de context. Dit betekent dat de organisatie scherp in beeld brengt wat haar doelen zijn, welke informatie essentieel is voor het behalen van die doelen en de uitvoering van taken, welke systemen worden gebruikt en binnen welke wettelijke en andere kaders wordt gewerkt. Bij gemeenten gaat het dan bijvoorbeeld om (essentiële) processen en de daaraan ondersteunende bedrijfsvoering, de verwerking van persoonsgegevens volgens de AVG en (straks) de eisen vanuit de Cyberbeveiligingswet (Cbw), die voortkomt uit de Europese NIS2-richtlijn en andere wet- en regelgeving.

Een belangrijk onderdeel van deze stap is het bepalen van de risicobereidheid: welk niveau van risico is nog acceptabel binnen de organisatie? Sommige risico's, zoals een kortstondige verstoring van een niet-kritiek systeem, kunnen worden geaccepteerd.

Andere risico's, zoals langdurige uitval van een kernregistratie of datalekken met grote maatschappelijke of juridische gevolgen, zijn per definitie onacceptabel. Deze grenzen worden meestal vastgelegd in beleidsdocumenten of risicoprofielen. Een bron voor het vaststellen van de risicobereidheid van de gemeente is de controller die moet nadenken over weerstandsvermogen. Daarnaast kunnen risico's en maatregelen ook leiden tot hogere kosten die het noodzakelijk kunnen maken dat de raad erover gaat. Een andere bron die bij de context hoort is het dreigingsbeeld Nederlandse gemeenten van de IBD (LINK).

Om risico's goed te kunnen inschatten en vergelijken is het noodzakelijk om gebruik te maken van gestandaardiseerde tabellen voor kans en impact. In een impacttabel wordt bijvoorbeeld vastgelegd wanneer iets als 'zeer laag', 'laag', 'middel' of 'hoog' tot 'zeer hoog' wordt beschouwd, uitgedrukt in concrete gevolgen voor dienstverlening, privacy, financiën of imago. Door dit vooraf vast te leggen, kunnen risicoanalyses binnen en tussen organisaties op een uniforme manier worden uitgevoerd. Dit is met name van belang in ketens waarin meerdere gemeenten of leveranciers samenwerken (dit geldt ook voor een GR). Maar ook voor een bestuurder of manager is het nodig om risico's die door verschillende personen of op verschillende momenten zijn gewaardeerd, onderling te kunnen vergelijken. Voor gemeenten heeft de IBD een [kans en impacttabel](#) beschikbaar gesteld.

3.4.2. Risico identificatie

Na het vaststellen van de context, worden de mogelijke risico's geïdentificeerd. In deze stap wordt onderzocht welke dreigingen relevant zijn voor de organisatie. Denk aan kwaadwillende aanvallen (zoals ransomware), menselijke fouten (zoals verkeerd verzenden van bestanden), technische kwetsbaarheden (zoals verouderde software), maar ook fysieke risico's zoals brand of waterschade.

Daarbij wordt gekeken naar welke bedrijfsmiddelen (assets) kwetsbaar zijn voor deze dreigingen. Bedrijfsmiddelen kunnen gegevens zijn (bijvoorbeeld persoonsgegevens), maar ook processen (zoals de afhandeling van een aanvraag) of systemen (zoals het zaakstelsel of een BRP-applicatie). Door de samenhang te analyseren – dreiging + kwetsbaarheid + waardevol bedrijfsmiddel (proces) – ontstaat een helder beeld van waar de risico's zitten. Modellen zoals [MAPGOOD](#) uit de diepgaande risicoanalyse aanpak kunnen hierbij helpen om systematisch over alle aspecten na te denken, van mensen en apparatuur tot processen en dienstverlening. Een andere bron met voorbeelden van dreigingen zit in de bijlage van de NEN-EN-ISO/IEC 27005.

3.4.3. Risico's waarden

Wanneer de risico's zijn geïdentificeerd, volgt de analysefase. In deze stap wordt voor elk risico bepaald wat de kans is dat het zich voordoet, en wat de impact zou zijn als dat gebeurt. Dit doen we in de door de IBD beschikbaar gestelde methode op een schaal van 1 tot 5. Bijvoorbeeld: een risico met een kans van 3 (waarschijnlijk) en een impact van 4

(aanzienlijke schade) krijgt een risicoscore van 12 (kans x impact). De risicomatrix staat in hetzelfde bestand waar hier naar verwezen wordt.

Door een risicomatrix te gebruiken kunnen risico's onderling worden vergeleken en kan worden bepaald welke risico's prioriteit moeten krijgen. Belangrijk is dat de inschaling zoveel mogelijk objectief en gestandaardiseerd gebeurt, zodat analyses tussen afdelingen binnen of tussen gemeenten onderling vergelijkbaar blijven. Zeker in ketens, waar meerdere partijen verantwoordelijk zijn voor onderdelen van een proces, is deze uniformiteit essentieel.

3.4.4. Risico evaluatie

Na de analyse volgt de beoordeling: hoe verhoudt elk risico zich tot de eerder vastgestelde risicobereidheid? Hier wordt besloten of een risico acceptabel is, of dat het behandeld moet worden.

Een laag risico hoeft meestal niet direct een actie op te roepen, maar moet wel worden geregistreerd. Een middelhoog risico wordt vaak behandeld als er eenvoudig effectieve maatregelen te nemen zijn. Hoog risico moet in principe altijd aanleiding zijn voor actie, of er moet een expliciet besluit worden genomen om het risico – tijdelijk – te accepteren en dat vast te leggen in een document. Het besluit om een risico tijdelijk te accepteren wordt genomen door het bestuur. Na een vastgestelde periode wordt opnieuw bepaald wat er moet gebeuren, tenzij inmiddels de belemmeringen voor het mitigeren van het risico zijn opgeheven.

De beoordeling kan ook leiden tot een escalatie: als een risico boven het geaccepteerde niveau ligt, moet het management een besluit nemen over behandeling of tijdelijke acceptatie. Deze stap vormt dus de brug tussen analyse en besluitvorming.

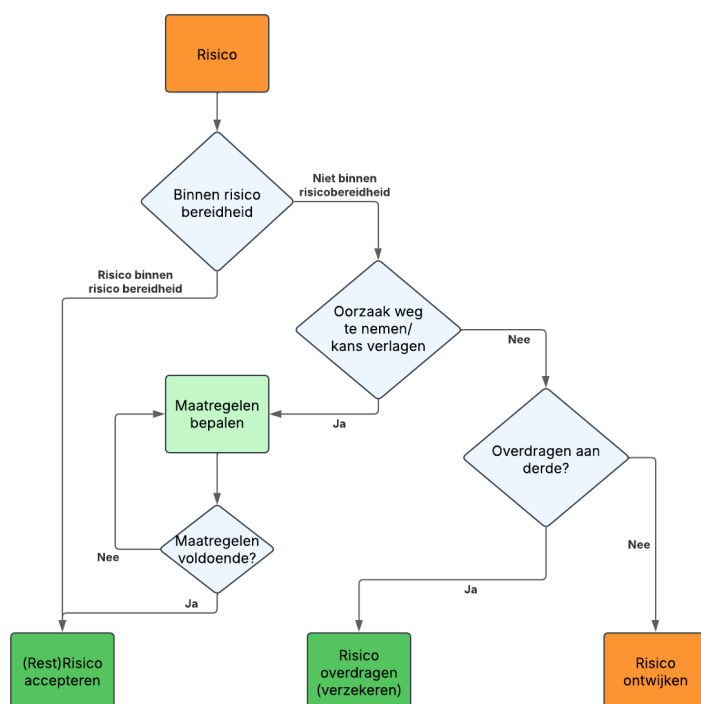
3.4.5. Risico's behandelen

Bij de behandeling van risico's kiest de organisatie één of meerdere strategieën. De meest voorkomende strategie is risicoreductie: het nemen van maatregelen die de kans of impact van het risico verkleinen. Denk aan technische maatregelen (zoals authenticatie of encryptie), organisatorische maatregelen (zoals procedures en opleidingen), personele maatregelen (een VOG vragen of geheimhoudingsovereenkomst), fysieke maatregelen (zoals noodstroom of bewaking) of contractuele afspraken met leveranciers.

Soms wordt een risico vermeden door de activiteit stop te zetten of anders te organiseren. Een andere optie is overdracht, bijvoorbeeld door het risico te verzekeren of uit te besteden. Tot slot kan een risico geaccepteerd worden als het past binnen de risicobereidheid en als er voldoende onderbouwing is.

Bij elke maatregel is het van belang om het restrisico opnieuw in te schatten. Soms blijft er ondanks maatregelen een rest-risico over dat nog steeds niet acceptabel is, en dus aanleiding geeft tot aanvullende acties.

Onderstaand een risicobehandelschema om duidelijk te maken hoe de keuzes samenhangen:



Afbeelding: Risicobeslisboom

3.4.6. De 4 keuzes van risico behandelen zijn:

Risico verminderen of mitigeren (Risk reduction)

Risicoreductie betekent dat maatregelen worden genomen om de kans dat het risico optreedt te verkleinen, of de impact te beperken als het zich toch voordoet. Vaak gebeurt dit door maatregelselectie uit de ISO27002 of een andere bron.

Toepassing: Dit is de meest gebruikte strategie, zeker binnen informatiebeveiliging. Het doel is om risico's terug te brengen tot een acceptabel niveau (restrisico).

Voorbeeld: Een organisatie implementeert tweefactor-authenticatie om de kans op ongeautoriseerde toegang te verkleinen. Of een datacenter wordt uitgerust met een noodstroomvoorziening om impact bij stroomuitval te beperken.

Risico acceptatie (Risk acceptance)

Soms besluit een organisatie om een risico bewust te accepteren, zonder aanvullende maatregelen te nemen. Dit gebeurt alleen als het risico binnen de vastgestelde

risicobereidheid valt, of als maatregelen disproportioneel duur of complex zijn ten opzichte van de verwachte schade.

Toepassing: Vaak gebeurt dit na overleg met het management of de CISO. Er kan ook sprake zijn van tijdelijke acceptatie, in afwachting van toekomstige maatregelen. Acceptatie moet expliciet worden afgewogen en vastgelegd om te voorkomen dat risico's onterecht worden genegeerd en in de toekomst vergeten worden.

Voorbeeld: Een ICT-systeem draait op een oude versie van software waarvoor (nog) geen update beschikbaar is. De kans op misbruik is laag en er zijn monitoringmaatregelen actief. Het risico wordt tijdelijk geaccepteerd met herbeoordeling over zes maanden.

Risico overdragen (Risk transfer)

Bij risico-overdracht wordt het risico of de gevolgen ervan verlegd naar een derde partij. Dit betekent niet dat het risico verdwijnt, maar wel dat de verantwoordelijkheid of financiële gevolgen bij een ander worden gelegd.

Toepassing: Dit gebeurt vaak via outsourcing, verzekeringen of contracten met leveranciers waarin beveiligingsverplichtingen zijn opgenomen.

Voorbeeld: Een gemeente sluit een cyberverzekering af die de kosten dekt van herstel en juridische claims na een datalek. Of een leverancier van een SaaS-applicatie wordt contractueel verplicht tot specifieke beveiligingsmaatregelen en aansprakelijkheid bij schade.

Risico ontwijken (Risk avoidance)

Bij risicovermijding wordt ervoor gekozen om de activiteit die het risico veroorzaakt niet (meer) uit te voeren. Hiermee wordt het risico volledig weggenomen, maar mogelijk ook de kans op waardecreatie of innovatie.

Toepassing: Deze strategie wordt vooral gebruikt bij risico's met een onacceptabel hoge impact, waarbij beheersmaatregelen onvoldoende soelaas bieden of te kostbaar zijn.

Voorbeeld: Een gemeente besluit om geen gebruik te maken van een app voor burgers als blijkt dat de leverancier persoonsgegevens onversleuteld opslaat en de risico's op datalekken hoog zijn. Door het project te stoppen, wordt het risico vermeden.

Het risico's behandelen wordt afgesloten met een vraag of alle risico's voldoende zijn behandeld, zijn de juiste keuzes gemaakt. Zijn er eventueel nog open eindjes waar wat mee gedaan moet worden.

3.4.7. Documenteren en rapporteren

Tot slot wordt expliciet vastgelegd wat met welk risico is gedaan, welke risico's worden geaccepteerd en welke niet, hoe deze worden behandeld en wie de risico- en

maatregelen is. Dit gebeurt vaak in overleg met de CISO en de PO, proceseigenaren en het management. De acceptatie moet worden onderbouwd en voorzien zijn van context: waarom is dit risico acceptabel, voor hoe lang, en wie heeft het besluit genomen? Hiermee wordt geborgd dat er sprake is van bewuste keuzes, en ontstaat een dossier waarmee ook bij audits of toezicht duidelijk is hoe er met risico's wordt omgegaan. De risico's en maatregelen worden met hun eigenaren en opvolg acties vastgelegd in het risicoregister van het ISMS ondersteunend informatiesysteem.

3.4.8. Risico monitoring en review

Risicomangement is een continu proces. Daarom wordt in deze fase vastgesteld hoe risico's en maatregelen worden bewaakt.

Nieuwe dreigingen, veranderingen in systemen of processen, of incidenten kunnen aanleiding zijn om risico's opnieuw te beoordelen. Gemeenten doen dit bijvoorbeeld jaarlijks of bij grote wijzigingen, maar ook na audits of beveiligingsincidenten.

Het binnen de gemeente centraal bijhouden van een actueel risicoregister is essentieel om inzicht te behouden en verantwoording af te kunnen leggen. Het register maakt het ook mogelijk om trends te signaleren, bijvoorbeeld een toename in risico's door afhankelijkheid van cloudleveranciers of een toename van phishing.

3.4.9. Communicatie

In alle stappen van het proces is communicatie essentieel. Risicoanalyses en besluiten over behandeling of acceptatie raken vaak meerdere afdelingen en stakeholders. Denk aan ICT, juridische zaken, privacy, het managementteam of ketenpartners. Door belanghebbenden actief te betrekken, ontstaat draagvlak en worden risico's beter beheersbaar.

Daarnaast is het belangrijk om de resultaten van risicoanalyses begrijpelijk te rapporteren. Niet elke beslisser is een expert in cybersecurity, maar moet wél kunnen inschatten wat de risico's betekenen voor de dienstverlening of voor de organisatie als geheel. Beschrijf risico's ondubbelzinnig en probeer de relatie te leggen met bestuurlijke risico's die ook in de kans- en impact tabel staan.

Gebruik de BMC- en PRMG-modellen voor communicatie naar het hoger management.

3.5. Samenvattend

De wet- en regelgeving schrijft niet voor hoe je risico's moet beheersen of welke methode je daarvoor gebruikt. Echter in de BIO2 en de onderliggende norm de NEN-EN-ISO/IEC 27001 staat wel dat voor de behandeling van risico's gekeken kan worden naar de ISO 31000 en de daarvan afgeleide NEN-EN-ISO/IEC 27005. Deze laatste is een framework

die specifiek gemaakt moet worden voor de toepassing binnen een bepaald type organisatie.

4. Niveaus in risicomanagement

Binnen risicomanagement onderscheiden we doorgaans drie niveaus van risico's: strategische risico's op organisatieniveau, tactische risico's op procesniveau en operationele risico's op het niveau van informatiesystemen. Elk type risico heeft zijn eigen kenmerken, impact en betrokken stakeholders, maar ze zijn onlosmakelijk met elkaar verbonden.

Strategische risico's zijn risico's die de organisatie in haar geheel raken en invloed hebben op het behalen van beleidsdoelen, reputatie, politieke legitimiteit en lange termijn continuïteit. Denk bijvoorbeeld aan wijzigingen in wetgeving, tekorten op de arbeidsmarkt of het falen van ketensamenwerking. Deze risico's worden doorgaans beheerd door het college van B&W, directie en concerncontroller. Zij stellen de risicobereidheid vast, prioriteren risico's en nemen besluiten over investeringen in beheersmaatregelen.

Tactische risico's, oftewel procesrisico's, doen zich voor op het niveau van domeinen, afdelingen of ketenprocessen. Ze raken de manier waarop de organisatie haar taken uitvoert en betreffen zaken als onvoldoende capaciteit, fouten in uitvoering of afhankelijkheden in processen. Proceseigenaren, domeinmanagers en teamleiders zijn hier de belangrijkste stakeholders. Zij vertalen de strategische doelen naar uitvoerbare plannen en moeten ervoor zorgen dat processen beheerst verlopen, onder andere door periodieke risicobeoordelingen en het treffen van beheersmaatregelen.

Operationele risico's hebben betrekking op het functioneren van informatiesystemen, gegevensstromen en technische infrastructuur. Denk aan uitval van applicaties, datalekken, of kwetsbaarheden in software. Deze risico's worden beheerd door functioneel beheerders, informatieadviseurs/managers, de I&A-afdeling en de (T)ISO. Zij zorgen ervoor dat de systemen voldoen aan beveiligingseisen, beschikbaar zijn en op een beheerste manier worden gewijzigd of geïntegreerd.

Er is samenhang en beïnvloeding tussen de drie niveaus. Een kwetsbaarheid in een informatiesysteem (operationeel) kan leiden tot een verstoring van een cruciaal proces (tactisch), wat op zijn beurt het vertrouwen van burgers schaadt of het behalen van beleidsdoelen in gevaar brengt (strategisch). Omgekeerd kunnen strategische keuzes, zoals digitalisering of outsourcing, nieuwe risico's introduceren op tactisch en operationeel niveau. Daarom is afstemming tussen de verschillende lagen essentieel.

Naast het kijken naar een proces of een informatiesysteem kunnen er ook Risico's zijn die gemeentebreed spelen, dus die diep verweven zijn met de organisatiebrede processen, governance en cultuur. Ze overstijgen individuele systemen of processen en hebben

impact op de integrale informatiebeveiliging (BIV) en compliance. Deze risico's zijn strategisch omdat het hier gaat om organisatiebrede tekortkomingen die voortkomen uit het ontbreken van beleid, regie en sturing op kernthema's als IAM, contractmanagement en cultuur. Deze risico's kunnen ook tactisch zijn omdat de vertaling van beleid naar processen en ondersteuning in de lijnorganisatie ontbreekt of niet goed werkt.

Effectief risicomanagement vraagt om samenwerking tussen bestuurders, management, proceseigenaren, I&A-professionals en control-functies. Iedere stakeholder heeft vanuit zijn of haar rol de verantwoordelijkheid om risico's te signaleren, te beoordelen en waar mogelijk te beheersen, maar alleen samen ontstaat er een integraal beeld van de risico's waarmee de gemeente wordt geconfronteerd.

5. Rollen en verantwoordelijkheden in relatie tot risicomanagement

5.1. De bestuurder

Risicomanagement is niet langer een technisch of uitvoerend vraagstuk — het is een bestuurlijke verantwoordelijkheid. Bestuurders, zoals het college van burgemeester en wethouders, spelen een sleutelrol in het stellen van kaders, het bepalen van risicobereidheid en het tonen van voorbeeldgedrag.

Bestuurders zijn eindverantwoordelijk voor het realiseren van maatschappelijke doelen binnen hun gemeente, en dus ook voor het beheersen van risico's die die doelen in gevaar kunnen brengen. Denk aan risico's rondom privacy, dienstverlening, financiële continuïteit of maatschappelijke onrust bij uitval van systemen. Bestuurders hoeven niet elk risico in detail te kennen, maar moeten voldoende regie en inzicht hebben om kritische keuzes te maken: wat accepteren we, wat moet gemitigeerd worden, en waar investeren we in?

Daarvoor is een goed werkend systeem van risicomanagement nodig, waarin risico's systematisch worden geïdentificeerd, geëvalueerd en gemonitord — en waarin signalen van onderaf daadwerkelijk boven komen. De bestuurder moet zorgen voor:

- Heldere bestuurlijke kaders: vaststellen van beleid, normen, en risicobereidheid.
- Governance en eigenaarschap: benoemen van rollen en verantwoordelijkheden in de lijn.
- Integraal toezicht: risicomanagement integreren in P&C-cyclus, audits, informatieveiligheid en compliance.
- Stimuleren van een open cultuur: ruimte bieden aan medewerkers om risico's bespreekbaar te maken.

Binnen het samenspel met de gemeentesecretaris, concerncontroller, CISO en domeinmanagers, is het de taak van de bestuurder om te zorgen dat risicomanagement

niet als 'extra taak' wordt gezien, maar als een integraal onderdeel van goed bestuur. In de Cbw is de bestuurlijke verantwoordelijkheid voor digitale weerbaarheid expliciet benoemd, inclusief aansprakelijkheid bij nalatigheid.

Kortom, risicomanagement begint niet bij een tool of een maatregel, maar bij bestuurlijke betrokkenheid, zichtbaarheid en besluitvaardigheid. Bestuurders maken daarmee het verschil tussen een papieren aanpak en een organisatie die écht in control is.

5.2. De gemeentesecretaris

De gemeentesecretaris vervult een cruciale spilfunctie in het risicomanagement van een gemeente. Als hoogste ambtelijke adviseur van het college én algemeen directeur van de ambtelijke organisatie, bevindt de gemeentesecretaris zich op het kruispunt van strategie, operatie en bestuurlijke besluitvorming. In die positie is hij of zij bij uitstek geschikt om de randvoorwaarden te creëren voor een volwassen, samenhangend en gedragen risicomanagementsysteem.

Waar de bestuurder kaders stelt, zorgt de gemeentesecretaris voor de verankering van risicomanagement in de organisatie. Dit betekent niet dat de gemeentesecretaris zelf risicoanalyses uitvoert, maar wel dat hij of zij de mensen en middelen beschikbaar stelt en zorgt voor een cultuur en houding die nodig zijn om risico's tijdig te signaleren, structureel te bespreken en transparant te rapporteren.

Concreet houdt dit in dat de gemeentesecretaris:

- Risicomanagement verbindt aan strategische- en concern-brede thema's, zoals digitalisering, ketensamenwerking, informatievoorziening en dienstverlening.
- Stuurt op integraliteit, bijvoorbeeld door risicomanagement te koppelen aan de planning- en control-cyclus, informatieveiligheidsbeleid, privacy, interne audits en kwaliteitszorg.
- Toeziet op het mandaat en de positionering van sleutelfuncties zoals de CISO, privacy officer, concerncontroller en informatiemanagers, en bevordert dat zij elkaar versterken.
- Een risicobewuste organisatiecultuur stimuleert, waarin risico's niet weggemoffeld worden, maar bespreekbaar zijn — ook richting het bestuur.
- Voorzitterschap neemt van de ambtelijke risicodialoog, waarin risico's, beheersmaatregelen en voortgang worden besproken op concernniveau.

In de praktijk is de gemeentesecretaris degene die het verschil kan maken tussen gefragmenteerde risicosignalen en een structurele, samenhangende aanpak. Zeker in het licht van de opkomst van thema's als digitale weerbaarheid, ketenafhankelijkheid en NIS2-verantwoordelijkheden, is een actieve, betrokken en verbindende gemeentesecretaris onmisbaar.

Door risicomangement te positioneren als onderdeel van goed leiderschap en integrale sturing, helpt de gemeentesecretaris om risico's niet alleen te beperken, maar ook te benutten als kans om te verbeteren en te vernieuwen.

5.3. De lijnmanagers of proceseigenaren

Binnen gemeenten ligt de dagelijkse verantwoordelijkheid voor het beheersen van risico's in belangrijke mate bij de lijnmanagers en proceseigenaren. Zij staan het dichtst bij de uitvoering en kennen de inhoud, knelpunten en afhankelijkheden van processen als geen ander. Daarmee zijn zij de eersten die risico's kunnen signaleren én degenen die er direct op kunnen en moeten handelen.

De lijnmanager of proceseigenaar is verantwoordelijk voor het behalen van doelstellingen binnen het eigen domein — of dat nu gaat om bijvoorbeeld burgerzaken, jeugdzorg, vergunningverlening of ICT. Risicomangement maakt integraal deel uit van die verantwoordelijkheid. Het gaat hierbij niet alleen om het signaleren van incidenten achteraf, maar vooral om het proactief inschatten van kwetsbaarheden en het treffen van beheersmaatregelen vooraf door middel van een risicoanalyse.

Vanuit deze rol wordt verwacht dat de lijnmanager of proceseigenaar:

- Risico's herkent en benoemt in het eigen procesgebied, bijvoorbeeld via sessies met het team, dashboards, audits of ketenanalyses.
- In gesprek gaat met informatiemanagers, privacy- en beveiligingsfunctionarissen, om risico's niet alleen technisch, maar ook juridisch en organisatorisch goed te duiden.
- Maatregelen afweegt en implementeert, op basis van prioriteit, impact, capaciteit en kosten.
- Actief deelneemt aan risicodialogen binnen de organisatie, om bevindingen te delen, knelpunten bespreekbaar te maken en verantwoording af te leggen over genomen maatregelen.
- De aanpak van risico's en kwetsbaarheden structureel borgt in verbetertrajecten, projectvoorstellen en de jaarlijkse P&C-cyclus.

Deze verantwoordelijkheid wordt in de praktijk soms onderschat of onvoldoende gefaciliteerd. Zeker wanneer lijnmanagement en proceseigenaarschap niet formeel zijn belegd, of als het ontbreekt aan inzicht in afhankelijkheden met bijvoorbeeld ICT, wet- en regelgeving of ketenpartners. Hier ligt een belangrijke rol voor de organisatieleiding om deze rol duidelijk te positioneren en te ondersteunen met formats, tooling en ondersteuning.

De lijnmanager of proceseigenaar is daarmee de sleutel tussen strategie en operatie, en zorgt ervoor dat risicomangement niet blijft hangen op beleidsniveau, maar daadwerkelijk landt in het primaire proces.

Zie ook ons kennisproduct: [handreiking risicomangement voor lijnmanagers](#).

5.4. De informatiemanager

Goed informatiemanagement is binnen gemeenten een essentiële voorwaarde voor het beheersen van risico's en het borgen van digitale weerbaarheid. Gemeentelijke dienstverlening is sterk afhankelijk van betrouwbare en toegankelijke informatie, vaak verdeeld over meerdere systemen, afdelingen en ketenpartners. Om risico's goed te kunnen inschatten en maatregelen effectief te kunnen nemen, is inzicht nodig in de informatie zelf: wat het is, waar het is, hoe het wordt gebruikt en door wie.

Informatiemanagement gaat verder dan alleen het ondersteunen van functionele wensen van gebruikers. In moderne gemeentelijke organisaties vervult de informatiemanager/adviseur informatiemanagement een **brugfunctie** tussen de bedrijfsvoering, beleidsafdelingen, de ICT-organisatie en leveranciers. Deze rol is cruciaal om niet alleen de informatiearchitectuur en procesondersteuning te optimaliseren, maar ook om structureel aandacht te besteden aan **niet-functionele eisen** zoals:

- **Informatiebeveiliging:** Waarborgen van beschikbaarheid, integriteit en vertrouwelijkheid.
- **Privacy:** Naleving van de AVG, inclusief data-minimalisatie en juiste verwerkingsgrondslagen.
- **Continuïteit:** Inzicht in welke informatie kritisch is voor processen, en dus prioriteit moet krijgen bij herstel.
- **Risicobeheersing:** Signaleren van risico's, koppelen aan informatiesystemen, processen én ketenafspraken.

Een informatiemanager draagt bij aan het opstellen van informatieregisters, het identificeren van informatiestromen, en het duiden van de waarde van informatie binnen processen. Dit maakt het mogelijk om risico's per informatiestroom of per informatiesysteem te beoordelen, en te bepalen waar maatregelen nodig zijn — zowel organisatorisch als technisch. Denk bijvoorbeeld aan het opstellen van logging-eisen, classificatie van informatie, eisen aan versleuteling of afspraken over bewaartermijnen en toegang.

Vanuit governance-perspectief is het belangrijk dat informatiemanagement geborgd is met helder eigenaarschap. De toewijzing van informatie-eigenaren (veelal lijnmanagers of proceseigenaren) moet gepaard gaan met verantwoordelijkheden op het gebied van besluitvorming, beveiligingseisen en compliance. De informatiemanager is daarbij niet verantwoordelijk voor alle inhoudelijke keuzes, maar wel de facilitator die de samenhang bewaakt en zorgt dat deze thema's op de agenda blijven staan.

5.5. De concerncontroller

De concerncontroller is binnen de gemeente verantwoordelijk voor de borging van rechtmatigheid, doelmatigheid en doeltreffendheid van het gemeentelijk handelen. In de context van risicomanagement betekent dit dat de concerncontroller een cruciale rol speelt bij het structureel verbinden van inhoudelijke risico's aan financiële gevolgen, bestuurlijke keuzes en de P&C-cyclus.

Waar proceseigenaren risico's signaleren en beheersmaatregelen voorstellen, is het aan de concerncontroller om te toetsen of deze risico's ook financieel beheersbaar zijn. Wordt het risico binnen de eigen begroting opgevangen? Moet er dekking worden gezocht in het weerstandsvermogen? Of vraagt het om beleidsmatige bijsturing of prioritering op strategisch niveau?

De controller heeft hierbij meerdere rollen:

- Bewaker van integraliteit: het verbinden van risicoanalyses op operationeel en tactisch niveau aan strategische besluitvorming.
- Toetsers van risicobereidheid en acceptatie: de controller bekijkt of de acceptatie van risico's binnen afgesproken kaders valt, en brengt in beeld waar (financiële) overschrijding dreigt.
- Verantwoordelijk voor de onderbouwing van het weerstandsvermogen: op basis van een goed risicoprofiel, zoals vastgelegd in bijvoorbeeld een risicoregister, stelt de controller vast welke financiële buffers nodig zijn.
- Schakel tussen financiën, beleid en bedrijfsvoering: door risico's bespreekbaar te maken in directie- of MT-overleggen, en waar nodig bestuurlijke interventies voor te bereiden.
- Ondersteuner van de risicodialoog: de concerncontroller is vaak mede voorzitter of adviseur in risicodialogen op concernniveau, waarin de balans tussen risico, beheersing en ruimte voor innovatie aan bod komt.

Daarnaast is de concerncontroller gebonden aan de wettelijke kaders, zoals het Besluit Begroting en Verantwoording (BBV), waarin expliciet aandacht is voor risicobeheersing, weerstandsvermogen en rechtmatigheid. De controller draagt er zorg voor dat deze onderwerpen terugkomen in de programmabegroting en jaarstukken, en dat de gemeenteraad op een begrijpelijke manier geïnformeerd wordt over de belangrijkste risico's en de mate waarin de gemeente 'in control' is.

In een tijd waarin gemeenten te maken hebben met complexe opgaven, krappe budgetten en toenemende digitale afhankelijkheden, is een proactieve, goed gepositioneerde concerncontroller onmisbaar. Niet als 'boekhouder van de risico's', maar als strategische adviseur en verbinder die helpt om keuzes transparant, verantwoord en onderbouwd te maken.

5.6. De CISO

De CISO is binnen de gemeente verantwoordelijk voor de integrale aanpak van informatiebeveiliging. Vanuit die rol draagt de CISO zorg voor het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van gemeentelijke informatievoorziening — niet alleen binnen de ICT-afdeling, maar juist ook in de processen en samenwerkingen waarin informatie wordt verwerkt.

In het kader van risicomanagement vervult de CISO een sleutelrol als bewaker van digitale weerbaarheid en adviseur van directie en bestuur. De CISO zorgt ervoor dat risico's op het gebied van informatiebeveiliging tijdig worden gesignaleerd, geanalyseerd en afgestemd met de relevante proceseigenaren, informatiemanagers en lijnverantwoordelijken. Daarbij let de CISO niet alleen op technische kwetsbaarheden, maar juist ook op organisatorische en menselijke risico's, zoals onvoldoende bewustzijn, gebrekkige toegangssturing of ketenafhankelijkheden.

De CISO:

- Bevordert een risicogebaseerde benadering van beveiliging, conform de BIO, Cbw (NIS2) en gemeentelijke beleidskaders;
- Bewaakt risicoanalyses op het gebied van informatiebeveiliging, waaronder DPIA's, BMC-analyses, MAPGOOD-analyses of technische kwetsbaarheidsscans;
- Adviseert over beheersmaatregelen en toetst of deze passend, proportioneel en uitvoerbaar zijn;
- Maakt risico's zichtbaar op concernniveau, onder meer via rapportages, dashboards en deelname aan risicodialogen;
- Stelt prioriteiten op basis van dreigingen, kwetsbaarheden en dreigingsbeelden, zoals van de IBD of het NCSC.

De CISO is daarmee de specialist en verbinder die ervoor zorgt dat risico's in de digitale omgeving niet blijven liggen, maar worden opgepakt waar dat hoort: in de lijn. Tegelijkertijd adviseert hij of zij over de acceptatie van restrisico's en waar mogelijk het treffen van aanvullende maatregelen of escalatie naar het bestuur als een proceseigenaar risico's negeert of geen maatregelen wil treffen.

5.7. De PO

De Privacy Officer (PO) heeft een beleidsmatige taak in het waarborgen van de naleving van de AVG binnen de gemeente. Binnen risicomanagement vervult de PO een essentiële rol in het signaleren van privacyrisico's, adviseren over passende maatregelen en bewaken van rechtmatigheid bij gegevensverwerking.

De PO kijkt bij risicoanalyses niet alleen naar juridische compliance, maar helpt ook om de impact op betrokkenen – inwoners, cliënten, ondernemers – expliciet mee te nemen in de beoordeling van risico's. Dit gebeurt onder meer in DPIA's, maar ook als sparringpartner in procesontwerp, aanbestedingen of incidentafhandeling.

De Privacy Officer:

- Identificeert privacyrisico's bij nieuwe of gewijzigde verwerkingen;
- Adviseert bij risicoanalyses, zoals DPIA's of in het BMC/PRMG bij klantgerichte processen;
- Stimuleert gegevensminimalisatie, transparantie en rechtmatigheid bij beleids- en systeemontwikkeling;
- Maakt risico's rond datadeling, bewaartermijnen, doelbinding en grondslagen inzichtelijk;
- Is betrokken bij het opstellen van beheersmaatregelen die passen binnen de juridische kaders van de AVG;
- Is onafhankelijk in de advisering, maar werkt nauw samen met de CISO, informatiemanagers en proceseigenaren.

De PO helpt gemeenten om niet alleen 'in control' te zijn op papier, maar ook maatschappelijk verantwoord om te gaan met persoonsgegevens. Daarmee is de Privacy Officer een belangrijk geweten én gids in het risicomanagementlandschap, met een scherp oog voor de belangen van inwoners en de reputatie van de gemeente.

5.8. Ondersteunende rollen

Naast de kernrollen zijn ook ondersteunende functies zoals ICT/I&A, inkoop, contractmanagement, functioneel beheer en juridische zaken essentieel voor een effectief risicomanagementproces.

De I&A-functie zorgt voor een stabiele en veilige digitale infrastructuur en levert cruciale input over kwetsbaarheden en technische afhankelijkheden.

Inkoop en contractmanagement spelen een belangrijke rol bij het borgen van risicobeheersing in afspraken met leveranciers, bijvoorbeeld door het opnemen van eisen rond beschikbaarheid, beveiliging en privacy.

Functioneel beheerders signaleren operationele knelpunten vroegtijdig en vertalen deze naar concrete verbeteringen.

Juridische ondersteuning helpt bij het inschatten van juridische risico's en borgt dat maatregelen in lijn zijn met wet- en regelgeving.

Door deze functies actief te betrekken ontstaat een breed gedragen, multidisciplinaire aanpak waarbij risico's vanuit verschillende perspectieven worden herkend, beoordeeld en beheerst.

5.9. Samenvattend

In gemeentelijk risicomanagement speelt iedere rol een eigen, onmisbare bijdrage.

Bestuurders bepalen de kaders en risicobereidheid; de gemeentesecretaris verbindt strategie met uitvoering en zorgt voor samenhang.

Lijnmanagers en proceseigenaren dragen verantwoordelijkheid voor het herkennen en beheersen van risico's in de dagelijkse praktijk.

De concerncontroller bewaakt de financiële dekking en integraliteit van risico's binnen de P&C-cyclus en het weerstandsvermogen.

De CISO borgt digitale weerbaarheid door risico's vanuit informatiebeveiliging gestructureerd op te pakken en te vertalen naar maatregelen.

De Privacy Officer waarborgt daarbij dat risico's rondom persoonsgegevens in lijn zijn met de AVG en maatschappelijke verwachtingen.

Samen vormen zij de basis voor een integrale, werkbare en toekomstbestendige aanpak van risicomanagement binnen de gemeente.

6. Uitgangspunten Risicomanagement voor gemeenten

6.1. Actor

In de aanpak die hier beschreven wordt gaan we uit van een "gemiddelde actor", dat wil zeggen dat als een gemeente bij een risicoanalyse van een proces of informatiesysteem een "zwaardere" of meer capabele actor (of minder) relevant vindt dan moet de kans respectievelijk met 1 punt worden verhoogd of verlaagd.

Bij informatie- en cyberdreigingen onderscheiden we verschillende actoren, die elk een specifieke rol spelen in het dreigingslandschap. Hier zijn de belangrijkste actoren:

Staatsactoren (Nation-State Actors) +1

Dit zijn overheidsinstanties of groepen die betrokken zijn bij cyberaanvallen voor politieke, militaire of economische doeleinden. Ze kunnen betrokken zijn bij spionage, sabotage of beïnvloeding van buitenlandse verkiezingen.

Cybercriminelen

Dit zijn individuen of groepen die zich bezighouden met illegale activiteiten online, zoals het stelen van gegevens, het uitvoeren van ransomware-aanvallen, en het gebruiken van malware om systemen te infiltreren en schade te veroorzaken. Ze hebben vaak financiële motieven.

Hackers

Hackers kunnen goed- of kwaadwillend zijn. Ethical hackers worden ingehuurd om

systemen te testen en kwetsbaarheden op te sporen, terwijl criminele hackers systemen inbreken om gegevens te stelen of schade aan te richten.

Hactivisten

Dit zijn groepen of individuen die hacken voor politieke of sociale doelen. Ze gebruiken cyberaanvallen om hun standpunten kracht bij te zetten of om aandacht te vestigen op bepaalde kwesties (bijv. milieu, mensenrechten).

Interne bedreigingen (Insiders)

Werknemers of andere personen met toegang tot een organisatie kunnen opzettelijk of onopzettelijk schade veroorzaken door bijvoorbeeld gegevens te lekken, systemen te saboteren of zwakke plekken in beveiligingssystemen uit te buiten.

Bedrijven en leveranciers (supply chain)

Externe leveranciers en partners die toegang hebben tot een organisatie's netwerken en systemen, kunnen een risico vormen als ze zelf kwetsbaar zijn. Aanvallen via de toeleveringsketen worden steeds gebruikelijker.

6.2. Kans

Het is belangrijk dat de risicomanagement methode goede definities voor kans en impact heeft beschreven. Door het stellen van deze duidelijke definities worden verschillende risico's vergelijkbaar. Men kan dus op basis van risico score prioriteiten stellen en risicoanalyses worden herhaalbaar en deelbaar. Iemand anders zou voor hetzelfde risico op dezelfde score uitkomen op basis van de definities. Deze definities zijn door de IBD centraal beschikbaar gesteld.

De definitie van "kans" in risicomanagement verwijst naar de waarschijnlijkheid dat een bepaalde gebeurtenis kan voordoen, en een nadelig effect heeft op de gemeente, het bedrijfsproces of het informatiesysteem. Het begrip "kans" is cruciaal omdat het helpt bij het inschatten van de ernst van een risico en bij het prioriteren van maatregelen om die risico's te beheersen. Bij het beoordelen van de kans moeten verschillende aspecten worden overwogen, vooral in het licht van verschillende soorten risico's, zoals moedwillige aanvallen, gebruikersfouten en natuurrampen.

De kans kan worden uitgedrukt als een percentage, een frequentie (zoals "eens in de tien jaar") of als een schaalwaarde van 1-5 (met omschrijving zoals zeer laag, laag, medium, hoog en zeer hoog). Het is belangrijk dat alle gemeenten hiervoor eenzelfde schaal gebruiken bij de waardering van risico's. Voor gemeenten hebben we een 5 puntsschaal vastgesteld in de [kans- en impacttabellen](#).

Verschillende factoren zijn:

Natuurrampen

Hoewel de gevolgen van klimaatverandering voor sommige gemeenten een beperkte rol speelt is niet uit te sluiten dat hier meer rekening mee gehouden moet worden.

Beïnvloedende factoren: Geografische locatie, klimatologische omstandigheden, en historische gegevens over eerdere natuurrampen.

Kansberekening: Gebaseerd op statistieken en trends in het gebied.

Aanpak: Voorbereidingsmaatregelen zoals noodplannen, robuuste infrastructuur en verzekeringen kunnen de impact beperken.

Moedwillige Aanvallen

Hierbij gaat het om aanvallen door actiegroepen, georganiseerde criminaliteit of statelijke actoren.

Beïnvloedende factoren: Motivatie en bekwaamheid van aanvallers, waarde van het doelwit of de informatie, en de beveiligingsmaatregelen die momenteel zijn geïmplementeerd.

Kansberekening: Gebaseerd op dreigingsanalyses en informatie over mogelijke aanvallers en kwetsbaarheden. Wat hier ook een rol kan spelen is de soort informatie en het belang dat een aanvaller hierbij kan hebben. Hier ligt ook een relatie met het dreigingsbeeld van de IBD.

Aanpak: Implementatie van organisatorische, fysieke, technische en personele beveiligingsmaatregelen zoals firewalls en intrusion detection systemen, evenals training van personeel in beveiligingsbewustzijn.

Fouten van Eindgebruikers

Deze categorie betreft de meeste incidenten die bij gemeenten optreden.

Beïnvloedende factoren: Bewustzijnsniveau, training, complexiteit van systemen, motivatie en werkdruk.

Kansberekening: Afgeleid uit historische gegevens en gedragspatronen van gebruikers en opgetreden incidenten.

Aanpak: Regelmatige bewustwordingstrainingen, gebruik van technologieën zoals spamfilters en MFA, en het beperken van gebruikersrechten om de kans op menselijke fouten te verminderen.

6.3. Impact

Bij de impact moet niet alleen aan financiële impact gedacht worden maar moeten ook de volgende aspecten worden meegewogen volgens de inleiding van de BIO2 bij impact van risico's:

- Politieke schade aan een bestuurder;
- Schade voor de burger;
- Diplomatieke schade (waarschijnlijk voor de meeste gemeenten minder van toepassing);
- Financiële gevolgen;
- Directe imagoschade;
 - Verlies van publiek respect of vertrouwen;
 - Organisatie brede negatieve publiciteit;
- Significant verlies van motivatie van medewerkers;
- Belangrijk verlies van management control.

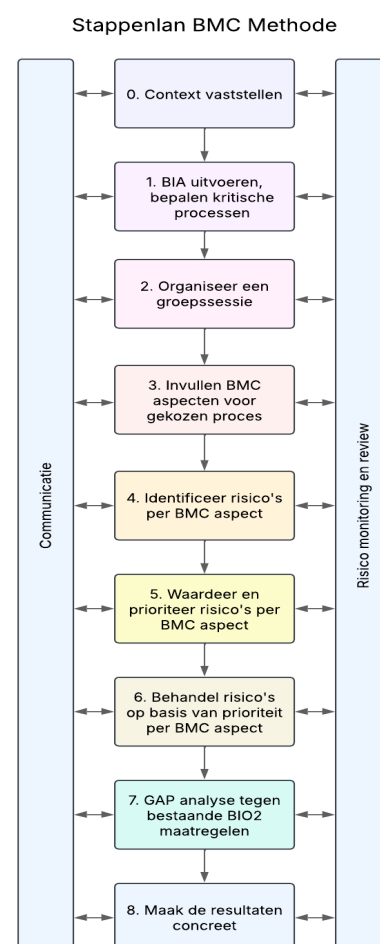
De impact wordt beschreven in een 5 puntsschaal. Bijvoorbeeld bij een 5 puntsschaal voor de impact 1-5 (zeer laag, laag, midden, hoog en zeer hoog) moet worden beschreven wat dit dan exact inhoudt. Deze impact is voor gemeenten uitgewerkt en staat in de [kans- en impacttabellen](#).

7. Risicomanagement aanpakken voor gemeenten

Het uitvoeren van risicoanalyses op de gemeentelijke kritieke processen is een belangrijk onderdeel van het ISMS. Door de belangrijkste risico's op de kritieke gemeentelijk hoofdprocessen in kaart te brengen krijgt het management focus op de belangrijkste risicogebieden. Daarnaast zijn de risicoanalyses op de risicoprocessen nodig bij het opstellen van de verklaring van toepasselijkheid (VVT). Omdat de kritieke processen voor alle gemeenten min of meer gelijk zullen zijn, zijn de uitkomsten van de analyses ook te delen en te hergebruiken voor andere gemeenten. Deze aanpak heeft tot doel een systematische, gestructureerde en herhaalbare manier van werken te hanteren. Daarbij maken we gebruik van het Business Model Canvas aanpak en/of de MAPGOOD-methode welke beide zijn gebaseerd op de NEN/ISO 27005.

Uitgangspunten:

- De scope van het ISMS en dus ook van het risicomanagement wordt bepaald door de voor de organisatie kritische processen.
- Voor het bepalen van de kritieke processen wordt uitgegaan van de lijst met hoofdprocessen die door het project BIO2 [is opgesteld](#).
- Qua detailinrichting zullen de processen bij gemeenten verschillen maar in hoofdlijnen zijn deze generiek. Deze aanpak richt zich dus op het deel wat generiek is. Voor gemeente specifieke risico's zullen gemeenten, indien nodig, aanvullende risicoanalyses moeten uitvoeren.
- Doordat het business model canvas als startpunt gebruikt wordt, is het voor deze risicoanalyses niet nodig om procesbeschrijvingen te hebben.
- De hier omschreven aanpak is vooral geschikt voor het bepalen van meer generieke risico's. Voor het bepalen van detailrisico's en het uitvoeren van risicoanalyses op applicaties kan beter de MAPGOOD methode gehanteerd worden.
- De output van de Business Impact Analyse (BIA), de BMC en de MAPGOOD-aanpak zijn geschikt om te hergebruiken voor bijvoorbeeld het Bedrijfscontinuïteitsproces. Daarnaast zijn het compacte overzichten die te gebruiken zijn om te communiceren en te rapporteren.



8. De Business Model Canvas methode

Deze paragraaf biedt een praktisch stappenplan waarmee proceseigenaren, ondersteund door bijvoorbeeld een CISO of informatieadviseur, zelfstandig een risicobeoordeling

kunnen uitvoeren. De methode is gestoeld op de ISO 27005-structuur, en vertaalt de risicoanalyse naar een groepsessie op basis van het Business Model Canvas (BMC) en Proces Risico Model Gemeente (PRMG). De aanpak maakt risico's visueel en tastbaar, is geschikt voor kritieke processen, en levert direct bruikbare output op zoals een ingevulde BMC, een risicoregister, een gap-analyse, maatregelenlijst, actielijst (input voor informatiebeveiligingsplan), en een risicoverdeling over het PRMG.

8.1. Stap 0 – Context vaststellen

Relatie met ISO 27005: Deze stap correspondeert met "Establishing the context". Het vastleggen van context is cruciaal voor consistente risicobeoordeling, en het vormt de basis voor effectieve communicatie en continue monitoring van veranderingen. Doel van deze stap: Begrijpen van de specifieke context waarin risico's worden geïdentificeerd en geanalyseerd.

Focus: Tactisch en operationeel niveau.

Vraag: Wat beïnvloedt de aard, kans en impact van risico's?

Typische elementen:

- Activiteiten, processen, diensten en informatieobjecten binnen scope.
- Dreigingen (threats), kwetsbaarheden (vulnerabilities), assets en risico-eigenaars.
- Toepassing van risico-criteria (bijv. impact op BIV).
- Risicobereidheid van de organisatie.
- Relevante bronnen.
 - Dreigingsbeeld Nederlandse gemeenten.
 - De kans- en impacttabellen.
 - Wet- en regelgeving.
 - Eerder uitgevoerde risicoanalyses.
 - Opgetreden incidenten.
 - Eerder uitgevoerde BIA / Resultaten van BCM
 - Etc. (eigenlijk alles wat relevant kan zijn voor de uit te voeren risicoanalyse)

Uitkomst:

Een afbakening/scope van de risicoanalyse: waar kijken we naar, welke dreigingen zijn relevant, hoe beoordelen we risico's (criteria), en welke methode gebruiken we (bijv. MAPGOOD, BIA, etc.).

Let op: de contextanalyse van het ISMS is niet hetzelfde als de context analyse van de risicoanalyse. Dit zijn de verschillen:

Aspect	ISO 27001 (Contextanalyse)	ISO 27005 (Context risicoanalyse)
Niveau	Strategisch	Tactisch/operationeel

Doel	Begrijpen van externe en interne invloeden op het ISMS	Begrijpen van scope en randvoorwaarden voor risicoanalyse
Uitkomst	Scope ISMS, stakeholders, eisen	Scope risicoanalyse, risicocriteria
Richt zich op	Organisatiebreed ISMS	Specifieke risico's en informatie binnen scope

8.2. Stap 1 – Bepaal welke processen risicoanalyse behoeven (BIA-fase)

Alle gemeentelijke processen moeten aan de Cbw / BIO voldoen, Het gaat er bij de BIA-stap om vast te stellen welke gemeentelijke processen kritiek zijn en dat deze waarschijnlijk meer of andere maatregelen nodig hebben. Check eerst of voor het proces al een BIA is uitgevoerd door de lijst met processen (LINK) en BIA-impact te raadplegen. Is dat niet het geval: Start met een eenvoudige Business Impact Analyse (BIA). Gebruik de impact tabellen van de IBD om processen te scoren op impactaspecten (beschikbaarheid, integriteit, vertrouwelijkheid, privacy, politieke schade, etc.). Classificeer het proces als kritiek als op een van de aspecten hoog of zeer hoog gescoord wordt. Voeg de uitgevoerde mini-BIA resultaten toe aan de lijst met (kritieke processen). Sorteert de gevonden processen zodat het proces dat op de meeste impact aspecten hoog/zeer hoog scoort bovenaan in de lijst komt. Bepaal ook de RTO en RPO van het proces in deze stap en leg ook vast of uitgegaan wordt van een gemiddelde actor of een specifieke actor (bijvoorbeeld cyber crimineel, script kiddie, kwaadwillende insider etc.). Deze stap wordt door de proceseigenaar uitgevoerd eventueel met ondersteuning van de CISO/PO. [Zie ook BCM.](#)

Doel: Alleen voor kritieke processen wordt een uitgebreide BMC-risicoanalyse uitgevoerd.

Relatie met ISO 27005: De contextbepaling van risico's start met inzicht in kritieke processen. Monitoring gebeurt via periodieke herbeoordeling van procesclassificaties. Communicatie met proceseigenaren en management is essentieel om draagvlak voor het onderscheid tussen kritisch en niet-kritisch te krijgen.

Input voor deze stap is de [kans- en impacttabel gemeenten van de IBD](#) waartegen gemeenteprocessen kunnen worden gewaardeerd, gebruik de hoogste waardering als proces impact waarde.

Output van deze stap is een lijst met processen die gewaardeerd zijn op de aspecten: Beschikbaarheid, Integriteit, Vertrouwelijkheid, Privacy en de verplichte BIO2 aspecten: politieke schade, diplomatieke schade, financiële impact, directe imagoschade, significant verlies van motivatie medewerkers en belangrijk verlies van management control. De RTO- en RPO-vaststelling en de actor.

8.3. Stap 2 – Organiseer een groepsessie met de juiste deelnemers

De proceseigenaar organiseert een sessie waarin de risicoanalyse wordt uitgevoerd. De volgende rollen zijn gewenst:

- Proceseigenaar
- Informatiebeveiligingsadviseur / CISO
- Procesmedewerker(s)
- Applicatiebeheerder of leverancier
- PO (indien relevant)
- I&A / IV-adviseur

Vorbereiding:

- Groot vel papier of fysiek of digitaal whiteboard met leeg BMC-sjabloon (kan dan ook met Teams worden uitgevoerd)
- Post-its in verschillende kleuren per stap of digitale equivalent
- Kans- en Impacttabel van de IBD
- BIO2-maatregelenlijst voor GAP-analyse

Relatie met ISO 27005: Consultatie van stakeholders is een expliciete stap in ISO 27005. Door de juiste rollen te betrekken, wordt informatie verzameld en gedeeld over risico's. Tussentijds herijken of herhaling van deze sessies is onderdeel van monitoring en review.

8.4. Stap 3 – Vul gezamenlijk het BMC in

Gebruik het Business Model Canvas om het proces in kaart te brengen vanuit tien vaste blokken (bijv. kernactiviteiten, partners, klantsegmenten). Zorg eerst voor een gezamenlijke invulling en consensus over het proces dat in kaart wordt gebracht.

Doel: Begrip van het proceslandschap en afhankelijkheden vóórdat risico's worden benoemd.

Relatie met ISO 27005: Contextbepaling vereist kennis van processen en bedrijfsmiddelen. Inzicht in het BMC is essentieel voor monitoring (wanneer het proces wijzigt) en communicatie met interne belanghebbenden. Zie voor een voorbeeld de bijlage.

8.5. Stap 4 – Identificeer risico's per canvasblok

Laat de deelnemers per canvasblok risico's benoemen en deze op post-its schrijven. Elk risico bevat:

- Korte beschrijving van de gebeurtenis eventueel aangevuld met het effect op het proces en de gemeente. Gebruik de MAPGOOD-gebeurtenissen uit de diepgaande risicoanalyse ter inspiratie.



BMC Aspect	Risiconummer	Risico Omschrijving
	leeg1	
	leeg2	
	leeg3	
	leeg4	
	leeg5	
	leeg6	
	leeg7	

- B, I en/of V aanduiding, dit helpt later bij het zoeken naar maatregelen
- MAPGOOD-dimensie, ook dit helpt bij later zoeken naar maatregelen.
- Wie de eigenaar van het risico is.

Plak risico's op het juiste canvas aspect. Laat de groep aanvullen, corrigeren en groeperen zodat gelijksoortige risico's bij elkaar komen te staan. Bepaal dan ook of het om hetzelfde risico gaat of omdat het om verschillende risico's gaat. Hier kan een scope worden aangebracht door alleen te zoeken naar cyberrisico's. Indien dat niet gebeurt zullen alle proces risico's gevonden worden, het voordeel is dan dat de proces eigenaar zich bewust wordt van alle proces risico's die er zijn. Zet eventueel bij het gevonden risico een "C" voor cyber en een "P" voor proces risico. Gebruik voor vastlegging de spreadsheet template die de IBD hiervoor ontwikkeld heeft.

Het duidelijk ondubbelzinnig noteren van geïdentificeerde risico's maakt het eenvoudiger om de stappen te nemen die volgen op de risico identificatie. Voor beginners kan dit moeilijk zijn. Een sjabloon kan dan helpen:

- *Sjabloon:* Het risico dat [specifieke dreiging] kan leiden tot [specifiek proces gevolg], waardoor [bedrijfsmiddel] wordt aangetast door [kwetsbaarheid], met als [strategisch gevolg].
- *Bijvoorbeeld:* Het risico dat een phishing-aanval kan leiden tot ongeautoriseerde toegang tot klantgegevens, waardoor vertrouwelijke informatie wordt aangetast door menselijke fouten, met als gevolg een datalek/afbreukrisico/vragen van burgers en verantwoording naar de raad.

Relatie met ISO 27005: Risico-identificatie is een kernstap. De transparantie van deze stap versterkt interne communicatie en maakt periodieke review mogelijk bij proceswijzigingen.

8.6. Stap 5 – Waardeer risico's (kans × impact)

Gebruik de vastgestelde 5 puntsschaal van de IBD voor kans en **impact (LINK)**. Waardeer de risico's als groep, timebox de discussie per risico en bepaal wie eventueel de beslissende stem heeft:

- Kans: hoe vaak kan dit gebeuren?
- Impact: wat gebeurt er als het gebeurt?
- Risicoscore = Kans × Impact

Kans (1-5)	Impact (1-5)	Risico

Sorteer risico's op score binnen hun canvasblok. Leg deze kans en impact waardering vast in de spreadsheet template bij het betreffende risico wat al vastgelegd was. Het resultaat kan vervolgens gebruikt worden om de hoogste risico's later weer te geven in de PRMG-sheet (zie bijlage). De PRMG-sheet moet gezien worden als communicatiemiddel naar het management waar de hoogste risico's kunnen worden opgenomen in één overzicht.

Relatie met ISO 27005: Risicoanalyse is input voor beoordeling. Monitoring van kans/impact wijzigingen hoort in beheerprocessen opgenomen te worden. De waardering moet herzien worden bij incidenten of bij signalen van veranderde dreigingen of wijziging van wetgeving, gemeentebeleid, het proces of de onderliggende informatiesystemen.

8.7. Stap 6 – Behandel risico's volgens ISO 27005

Vergelijk de risicoscores van de "C" cyberrisico's met de vastgestelde risicobereidheid, gebruik hiervoor de risicotabel in de spreadsheet met kans- en impacttabellen. Voor risico's die erboven uitstijgen, kies je een risicobehandelstrategie uit ISO 27005:

- Vermijden: Activiteit stoppen of aanpassen zodat risico verdwijnt
- Verminderen/mitigeren: Kans of impact verlagen met maatregelen
- Overdragen: Risico verleggen naar derden (bijv. verzekeren, uitbesteden)
- Accepteren: (Rest)risico expliciet accepteren en registreren

Voor elk risico waarvoor vermindering gekozen wordt:

- Noteer maatregelen op post-its, met een verwijzing naar een norm indien mogelijk;
- Label als O (organisatorisch), P (personeel), F (fysiek), T (technisch);
- Herwaardeer risico na maatregelen: is restrisico acceptabel, en leg deze keuze vast.

Zie het stroomschema van de risicobehandelstrategie eerder in dit document.

Relatie met ISO 27005: De keuze van behandelmethode vereist communicatie met management en verantwoordelijken. Review vindt plaats op basis van effectiviteit van maatregelen en herbeoordeling van restrisico's.

8.8. Stap 7 – GAP-analyse en actieplan tegen BIO2-maatregelen

Controleer welke maatregelen reeds zijn geïmplementeerd conform BIO2. Gebruik de maatregelenlijst:

- Wat is al aanwezig?
- Wat ontbreekt?
- Wat moet worden ingepland?
- Wijs een actiehouder toe en een plandatum

Doel: Voorkom dubbel werk en richt je op noodzakelijke aanvullende maatregelen.

Relatie met ISO 27005: GAP-analyse is een vorm van monitoring. Doorlopende evaluatie van maatregelen is een essentieel onderdeel van het review-proces.

8.9. Stap 8 – Maak de resultaten concreet

Verzamel en digitaliseer de resultaten:

- Ingevuld BMC-sjabloon(procesoverzicht), zie bijlage.
- Risicoregister spreadsheet met risico-omschrijving, kans, impact, score, MAPGOOD-tag, BIV-tag, risico-eigenaar. Zie bijlage
- Maatregelenoverzicht (inclusief GAP-status), [zie link](#).
- Ingepulde PRMG-sjabloon, zie bijlage.
- Actielijst met verantwoordelijken en implementatie plandata

Deze resultaten vormen input voor het gemeentelijk risicoregister, risicoacceptatieovereenkomsten en de ISMS-documentatie en voor het informatiebeveiligingsplan.

Relatie met ISO 27005: Documentatie maakt communicatie mogelijk met toezichhouders en auditors. Monitoring van de uitvoering van acties is onderdeel van de PDCA-cyclus.

8.10. Bijlagen en hulpmiddelen en links:

Blanco BMC-sjabloon (printbaar of digitaal) (link naar PPT template))

Blanco PRMG-sjabloon (link naar PPT template)

Kans- en impacttabel en risicomatrix (5 puntsschaal)

Risicoregisteremplate (Excel) (Link)

[BIO2-maatregelenlijst uit de GAP analyse](#)

9. De MAPGOOD-methode

De MAPGOOD-methode is beschreven in het kennisproduct de “diepgaande risicoanalyse methode”, hier wordt nog uitgegaan van een 3 puntsschaal, passend bij de BBN-indeling van de BIO 1.04. De 3 puntsschaal geeft niet voldoende ruimte om risico's goed te waarderen waardoor men vaak op “hoog” zou uitkomen. Zie diepgaande risicoanalyse ([link](#)).

10. Hoe zit het met de relatie tussen de ISO27005 aanpak en andere risicomanagement standaarden.

Voor gemeentelijke CISO's en controllers is het belangrijk om inzicht te hebben in hoe verschillende risicomanagementstandaarden zich tot elkaar verhouden. In het bijzonder is het relevant om de verschillen en overeenkomsten te begrijpen tussen COSO ERM, ISO 31000 en ISO 27005. Deze drie kaders bieden elk hun eigen benadering van risicomanagement, waarbij ze deels overlappen maar ook verschillende doelen en toepassingsgebieden hebben.

COSO ERM (Enterprise Risk Management) is een breed strategisch raamwerk dat organisaties helpt om risico's te beheren in het licht van hun missie, strategie en doelstellingen. Het legt sterk de nadruk op governance, cultuur, prestaties en integratie van risicomanagement in besluitvorming. Voor controllers binnen gemeenten biedt COSO een manier om risicomanagement te koppelen aan prestatie-indicatoren en beleidsdoelen. COSO bevat componenten als doelstellingenbepaling, risico-identificatie, risicobeoordeling, risicobehandeling, informatie & communicatie en monitoring. COSO ERM wordt ook gebruikt door controllers.

ISO 31000 is een internationaal erkende norm die richtlijnen biedt voor risicomanagement in brede zin. Het is sectoronafhankelijk en toepasbaar op zowel strategisch als operationeel niveau. ISO 31000 bestaat uit drie hoofdelementen: principes (waaronder systematisch, gestructureerd en op maat), een organisatorisch kader (waaronder leiderschap, integratie in beleid en processen), en het proces zelf (van contextbepaling tot evaluatie en monitoring). Het is een praktisch hanteerbaar model voor controllers die risicomanagement gemeentebreed willen positioneren.

ISO 27005 daarentegen is specifiek gericht op informatiebeveiligingsrisico's en sluit aan op het Information Security Management System (ISMS) zoals beschreven in ISO 27001. Deze norm helpt proceseigenaren en CISO's bij het in kaart brengen, analyseren en behandelen van risico's rondom de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. ISO 27005 beschrijft een gestructureerd proces dat begint bij het vaststellen van de context, gevolgd door risico-identificatie, risicoanalyse, risicobeoordeling,

risicobehandeling, acceptatie en evaluatie. Deze standaard is afgeleid van de ISO 31000 en heeft daarmee veel overeenkomsten.

Hoewel de focus verschilt, zijn er duidelijke overeenkomsten tussen de drie kaders. Alle drie hanteren zij een cyclisch procesmodel, waarin continue verbetering centraal staat. Ook delen ze de basisstappen van risicomanagement: het bepalen van de context, identificeren van risico's, analyseren van risico's, evalueren en behandelen. Verder benadrukken alle kaders het belang van managementbetrokkenheid en communicatie.

De belangrijkste verschillen zitten in de reikwijdte en doelgroep. COSO richt zich op het integreren van risicomanagement in de gehele organisatie en op strategisch niveau. ISO 31000 biedt een generiek kader dat geschikt is voor allerlei typen risico's en organisaties. ISO 27005 daarentegen is specifiek gericht op informatiebeveiliging en biedt veel meer detail in de uitvoering van het risicomanagementproces binnen het ISMS. Een relevante vraag voor de praktijk is of een aanpak volgens ISO 27005 ook voldoet aan de eisen of uitgangspunten van COSO. Het antwoord daarop is bevestigend, mits ISO 27005 wordt ingebed in een bredere context van organisatiebrede risicosturing. ISO 27005 kan dan worden beschouwd als een domeinspecifieke invulling van het risicoproces zoals COSO dat beschrijft. Voor de gemeentelijke controller biedt dit aanknopingspunten om informatiebeveiligingsrisico's te verbinden met bredere strategische en financiële risico's. Voor de proceseigenaar/CISO is het een manier om zijn of haar werk aan te laten sluiten op gemeentelijke beleidsdoelen en governance.

In de praktijk betekent dit dat de controller en proceseigenaar en de CISO elkaar moeten opzoeken. Waar de controller vanuit COSO en ISO 31000 toeziet op integrale risicosturing, levert de proceseigenaar ondersteund door de CISO via ISO 27005 inhoudelijke input op het gebied van informatiebeveiliging. Zo ontstaat een samenhangend beeld van risico's en maatregelen binnen de gemeentelijke organisatie.

Belangrijk is wel dat de aanpak van ISO 27005 wordt gekoppeld aan het gemeentebrede risicoprofiel.

Dit vraagt om:

- Heldere afstemming over risicobereidheid en -acceptatie;
- Structurele uitwisseling tussen CISO, controller en proceseigenaren;
- Inbedding van informatiebeveiligingsrisico's in het gemeentelijk risicoregister.

Wanneer deze koppeling gemaakt wordt, kunnen de drie kaders elkaar versterken in plaats van overlappen of concurreren. COSO biedt dan het kader, ISO 31000 de praktische vertaling en ISO 27005 de diepgang op het vlak van informatiebeveiliging. Een belangrijke aanvullende overweging is de relatie tussen risicobereidheid en het gemeentelijk weerstandsvermogen. Risicobereidheid bepaalt in feite welk type en welke omvang van risico's de gemeente bereid is te accepteren, terwijl het weerstandsvermogen aangeeft in hoeverre de gemeente financieel in staat is om onverwachte risico's op te vangen. Deze twee moeten in balans zijn: een hoge risicobereidheid zonder voldoende weerstandsvermogen kan leiden tot bestuurlijke en financiële problemen. Wanneer de omvang of impact van een risico groter is dan het beschikbare weerstandsvermogen, of wanneer aanvullende middelen nodig zijn om een risico te mitigeren, is het van belang dat dit onderwerp wordt voorgelegd aan het college en mogelijk aan de gemeenteraad. De

gemeenteraad heeft immers het budgetrecht en moet instemmen met extra middelen of herprioritering van bestaand beleid. Voor de controller betekent dit dat risicomanagement ook altijd in relatie moet staan tot de financiële beleidskaders en de planning & control-cyclus van de gemeente.

11. Van risicoanalyse naar structureel risicomanagement binnen het ISMS

Na het uitvoeren van risicoanalyses met behulp van methoden zoals MAPGOOD en het Business Model Canvas (BMC) en (PRMG), is er vaak al veel in beeld: risico's, beheersmaatregelen, betrokken actoren en een eerste planning. Maar dat is pas het begin. Een effectief ISMS – zoals vereist door ISO 27001 – vraagt om structurele borging van deze inzichten in beleid, processen en besluitvorming. Hieronder staan acht essentiële stappen om risicoanalyse te vertalen naar volwassen risicomanagement, ingebed in de PDCA-cyclus én in de gemeentelijke planning- en controlcyclus. Zie hiervoor ook onze handreiking [ISMS](#) en de handreiking [ISMS-procesimplementatie](#)

11.1. Vertaling naar beleid en doelstellingen

Bron: ISO 27001: §5.2, §6.2

Na het in kaart brengen van risico's is het belangrijk om deze te koppelen aan het informatiebeveiligingsbeleid en aan concrete doelstellingen. ISO 27001 vereist dat doelstellingen gebaseerd zijn op risico's en in lijn zijn met het beleid. Dit creëert richting, prioritering en meetbaarheid voor de organisatie.

Acties:

- Herijk het informatiebeveiligingsbeleid op basis van actuele risico's.
- Stel concrete, meetbare beveiligingsdoelen op (bijv. reductie van risico's binnen 6 maanden).
- Laat deze doelstellingen vaststellen door het management en opnemen in jaarplannen.

11.2. Vastleggen in risicoregister en maatregelregister

Bron: ISO 27001: §6.1.2, §6.1.3, §8.2

De geïdentificeerde risico's en maatregelen moeten structureel worden vastgelegd. Dit gebeurt in een risicoregister (voor risico's) en een maatregelregister (voor beheersacties). Deze vormen het hart van het ISMS en zorgen voor consistentie, opvolging en verantwoording.

Acties:

- Registreer per risico: omschrijving, kans, impact, totaalrisico, verantwoordelijke, status.
- Leg maatregelen vast met implementatiedatum en uitvoeringsverantwoordelijke.
- Koppel risico's aan processen, systemen of organisatieonderdelen.

11.3. Monitoring en rapportage (Check-fase)

Bron: ISO 27001: §9.1, §8.2

Informatiebeveiliging vereist continu inzicht: wordt er voortgang geboekt, zijn risico's voldoende onder controle, zijn maatregelen effectief? Monitoring is essentieel om tijdig bij te sturen en hoort bij de 'Check' in de Plan-Do-Check-Act-cyclus.

Acties:

- Rapporteer periodiek (bijv. per kwartaal) over risico's en maatregeluitvoering.
- Bespreek voortgang in reguliere overleggen (MT, proceseigenaren, CISO-overleggen).
- Zet kritieke risico's of uitblijvende acties op de escalatieagenda.

11.4. Integratie in de Planning & Control-cyclus

Bron: ISO 27001: §6.1.3, §5.1, §7.1

Risicobeheersing vraagt soms om extra inzet, budget of bestuurlijke keuzes. Door risico's en maatregelen te koppelen aan de reguliere gemeentelijke planning- en controlcyclus ontstaat structurele aandacht en bestuurbaarheid.

Acties:

- Neem relevante maatregelen op in jaarplannen en begrotingen.
- Maak middelen vrij via reguliere P&C-processen (bijv. voor awareness, ICT-maatregelen).
- Verwerk risico-informatie in managementrapportages en jaarverantwoording.

11.5. Evaluatie via interne audit en management review

Bron: ISO 27001: §9.2, §9.3 | NIS2/Cbw: bestuurlijke verantwoordelijkheid voor toezicht en risicobeheersing

Het ISMS moet periodiek worden geëvalueerd op effectiviteit. Interne audits toetsen de werking van maatregelen en processen. De jaarlijkse management review beoordeelt of het ISMS als geheel nog doeltreffend en geschikt is. Onder ISO 27001 ligt deze verantwoordelijkheid bij de top van de organisatie. Onder NIS2 en Cbw ligt die formele verantwoordelijkheid expliciet bij het bestuur: in het geval van gemeenten is dat het college van B&W.

De gemeentesecretaris en de CISO vervullen een cruciale rol in de voorbereiding en inhoudelijke onderbouwing van deze evaluatie, maar kunnen niet de formele eindverantwoordelijkheid dragen. Bestuurlijke besluitvorming over het ISMS moet aantoonbaar en traceerbaar zijn.

Acties:

Voer jaarlijks een interne audit uit op werking van het ISMS, inclusief de opvolging van risico's en uitvoering van maatregelen.

Laat de gemeentesecretaris en de CISO een management review opstellen met o.a.:

- de belangrijkste risico's en hun status;
- incidenten en trends;
- voortgang van maatregelen;
- auditbevindingen en verbeterpunten.

Leg de management review voor aan het college van B&W voor bestuurlijke bespreking en besluitvorming.

Leg besluiten vast (bijv. in collegevoorstellen, verslagen, of als bijlage bij de begrotingscyclus).

11.6. Continue verbetering (Act-fase)

Bron: ISO 27001: §10.1, §10.2

Risico's veranderen voortdurend door technologische, organisatorische en maatschappelijke ontwikkelingen. Een goed werkend ISMS past zich continu aan, leert van ervaringen en blijft in beweging.

Acties:

- Actualiseer risicoanalyses bij significante wijzigingen in processen, systemen of wetgeving.
- Evalueer incidenten en oefenscenario's en verwerk 'lessons learned'.
- Pas procedures, werkafspraken en beleid aan waar nodig.

11.7. Risicoacceptatie, escalatie en waiver-procedure

Bron: ISO 27001: §6.1.3 d, §5.1, §10.1

Niet alle risico's kunnen of willen meteen worden aangepakt. Soms ontbreken middelen, is het politiek gevoelig, of is het risico dermate groot dat het de bevoegdheid van een proceseigenaar overstijgt. Om te voorkomen dat deze situaties stilvallen, is een formele besluitstructuur nodig.

Acties:

- Richt een waiver-procedure in waarbij tijdelijke afwijking van maatregelen mogelijk is onder strikte voorwaarden (tijdelijkheid, evaluatiemoment, besluit door MT of directie).
- Stel een escalatieproces in voor risico's boven een bepaalde drempelwaarde.
- Registreer risico's met "geen actie" expliciet in het register, met motivering.

11.8. Koppeling met andere cybersecurity- en beheerprocessen

Bron: ISO 27001: §6.1.3, §8.2, §9.1, Annex A.5-A.18

Risicoanalyses zijn geen op zichzelfstaande instrumenten. Ze moeten gevoed worden door andere processen zoals incident management, change management, bedrijfscontinuïteit en leveranciersbeheer. Deze koppelingen maken het ISMS robuust, responsief en verbonden met de realiteit.

Acties:

- Koppel incident management aan het ISMS: incidenten kunnen nieuwe risico's opleveren.
- Koppel change management: grote wijzigingen vragen om risico-inschatting vooraf.
- Stem risicobeheersing af op BIA's en bedrijfscontinuïteitsmaatregelen.
- Veranker risico-eisen in aanbestedingen, SLA's en leveranciersbeoordelingen.

11.9. Rollen en verantwoordelijkheden

CISO:

- Coördineert het ISMS en bewaakt de integrale aanpak van risicomangement.
- Beheert het risicoregister en bewaakt opvolging van maatregelen.
- Adviseert en ondersteunt proceseigenaren en management.
- Bereidt de management review inhoudelijk voor en adviseert over risico's en prioriteiten.

Proceseigenaar:

- Is eindverantwoordelijk voor de risico's binnen zijn of haar proces.
- Voert risicoanalyses uit
- Neemt maatregelen of laat deze uitvoeren.
- Rapporteert over voortgang en obstakels richting CISO of lijnmanagement.

Gemeentesecretaris / directeur bedrijfsvoering:

- Heeft een coördinerende en adviserende rol op het niveau van de ambtelijke top.
- Zorgt ervoor dat het ISMS als proces wordt uitgevoerd binnen de organisatie.
- Bereidt samen met de CISO de management review voor en agendeert deze bij het college van B&W.
- Fungeert als verbindingspunt tussen ambtelijke organisatie en bestuurlijke besluitvorming.

College van B&W (bestuur):

- Is formeel verantwoordelijk voor de informatiebeveiliging van de gemeente, zoals vereist onder NIS2 en Cbw.
- Accordeert de inhoud en uitkomsten van de management review.
- Neemt besluiten over noodzakelijke beleidswijzigingen, prioriteiten en inzet van middelen op basis van de uitkomsten.
-

Concerncontroller:

- Adviseert over de financiële haalbaarheid en beheersbaarheid van voorgestelde risico-beheersmaatregelen.
- Toetst of risico's, maatregelen en rest-risico's aansluiten bij het risicoprofiel en de risicobereidheid van de organisatie.
- Waarborgt de integratie van het risicomanagementproces met de planning- en controlcyclus, inclusief begroting, jaarverslag en audit-activiteiten.
- Draagt bij aan de management review vanuit financieel-strategisch perspectief.
- Ziet toe op consistent gebruik van risicobeoordelingscriteria binnen de organisatie en adviseert over acceptatiegrenzen.

12. Bijlage: Definities en kaders voor risicomanagement in gemeentelijke context

Effectief risicomanagement begint bij een gedeeld begrip van kernbegrippen en methodieken. In de context van een gemeente betekent dit dat we risico's benaderen op strategisch (organisatie), tactisch (proces) en operationeel (systeem) niveau. Hiervoor gebruiken we beproefde instrumenten zoals MAPGOOD, het Business Model Canvas (BMC) en het Proces Risico Model Gemeente (PRMG). Deze combinatie helpt om risico's integraal te benaderen, vanuit inhoud, techniek én organisatieverantwoordelijkheid.

12.1. Dreiging

Een dreiging is een mogelijke gebeurtenis die de doelstellingen van een gemeente negatief kan beïnvloeden, bijvoorbeeld door schade aan beschikbaarheid, integriteit of vertrouwelijkheid van informatie of versterking van dienstverlening.

12.2. Kwetsbaarheid

Een kwetsbaarheid is een zwakke plek in de organisatie, techniek of het gedrag van mensen, waardoor een dreiging zich makkelijker kan manifesteren. Bijvoorbeeld: onvoldoende logging, verouderde systemen of een gebrek aan bewustzijn.

12.3. Actor

Een actor is een persoon of groepering die — al dan niet bewust — bijdraagt aan een incident. Dat kan bijvoorbeeld een kwaadwillende hacker zijn, maar ook een interne medewerker die onbedoeld een fout maakt of regels niet goed begrijpt. Ook natuurlijke oorzaken zoals een overstroming kunnen actoren zijn.

12.4. Risico

Een risico is de combinatie van een dreiging, een kwetsbaarheid, de kans dat het gebeurt en de verwachte impact. Een risico is gekoppeld aan een mogelijk incident dat zich zou kunnen voordoen binnen een proces, systeem of organisatieonderdeel.

12.5. Incident

Een incident is de daadwerkelijke manifestatie van een risico. Een dreiging is werkelijkheid geworden en heeft geleid tot schade of versterking.

13. Methodieken in samenhang

13.1. Business Model Canvas (BMC)

Het BMC brengt de opbouw van een proces, dienst of organisatieonderdeel visueel in kaart via negen bouwstenen, zoals kernpartners, kernactiviteiten en waardepropositie. Binnen gemeenten is dit model geschikt om processen strategisch te positioneren, inzicht te krijgen in de ketensamenwerking en afhankelijkheden in kaart te brengen.

13.2. Proces Risico Model Gemeente (PRMG).

Het PRMG is een risicodenkkader dat direct gekoppeld is aan het BMC. Voor elk BMC-aspect worden risico's geïdentificeerd en uitgewerkt, bijvoorbeeld: "Wat zijn de risico's voor onze kernpartners?" of "Welke risico's spelen er rond de waardepropositie?". Deze methode is bij uitstek geschikt voor **gezamenlijke sessies met stakeholders**, omdat het gestructureerde gesprekken stimuleert en expliciet maakt wie waarvoor verantwoordelijk is. Het PRMG helpt om risico's systematisch te verzamelen en vormt een brug tussen strategisch inzicht en operationele beheersmaatregelen. Het voordeel van de PRMG-aanpak is dat de proceseigenaar niet alleen cyberrisico's vindt (alhoewel je ook alleen daar op zou kunnen focussen) maar tevens ook algemene proces risico's vindt.

13.3. MAPGOOD

MAPGOOD staat voor Mensen, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving en Diensten. Het model helpt gemeenten om risico's te analyseren over de volle breedte van een proces of informatiesysteem, en is bruikbaar op operationeel en tactisch niveau. Het model kan eerst gebruikt worden om het informatiesysteem te beschrijven in alle facetten, vervolgens kan bij die facetten gezocht worden naar risico's met de voorbeeld lijsten die in de aanpak zitten. Het dwingt tot het stellen van gerichte vragen per aspect, en maakt blinde vlekken zichtbaar. Deze aanpak is door de IBD al uitgegeven als de [diepgaande risicoanalyse](#).

14. Bijlage risicomatrix

Zie IBD-website, [BIO2 kans en impact tabellen](#).



Kijk voor meer informatie op:
www.informatiebeveiligingsdienst.nl

Nassaulaan 12

2514 JS Den Haag

CERT: 070 204 55 11 (9:00 – 17:00 ma – vr)

CERT 24x7: Piketnummer (instructies via voicemail)

info@IBDGemeenten.nl / incident@IBDGemeenten.nl