Normenkader
Informatiebeveiliging en Privacy
voor het onderwijs

Risicomanagementbeleid

Voorbeelddocument

Versie: September 2026

Let op: verwijder deze pagina voor gebruik

Over dit voorbeelddocument

Dit voorbeelddocument helpt je met het maken van een eigen risicomanagementbeleid. Elke school en elk schoolbestuur is anders. Pas het proces daarom aan aan jouw eigen situatie.

Aanpassen van dit voorbeelddocument

Let bij het aanpassen van het document op het volgende:

- Bij hoofdstukken en paragrafen zijn soms toelichtingen geplaatst. Verwijder deze voordat je het beleid definitief maakt.
- Dit beleid gaat ervan uit dat taken, rollen en functies die nodig zijn om het beleid uit te voeren bij de juiste personen belegd zijn. Is dit niet zo? Ga dan eerst naar fase 1 van het Groeipad.
- Geel gearceerde teksten moet je vervangen door eigen tekst.

Totstandkoming

Dit voorbeelddocument is samengesteld door Kennisnet. Binnen het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken.

Sommige rechten voorbehouden

Hoewel aan dit document de uiterste zorg is besteed, aanvaardt Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden. Ook aanvaardt Kennisnet geen enkele aansprakelijkheid voor schade van welke aard dan ook, ontstaan uit het (onjuiste) gebruik van dit document.

Vragen?

Heb je vragen over dit voorbeelddocument? Kijk voor meer informatie op *normenkaderibp.kennisnet.nl/groeipad* of stuur een mail naar *ibp@kennisnet.nl.*

Documentgeschiedenis

Toelichting

- *Vul in wie het beleid vaststelt.*
- *Geef aan of het document openbaar, vertrouwelijk of geheim is en wie het in die gevallen mogen zien.*

Revisies

Versie	Datum	Auteur	Review

Vaststelling

Naam	Functie	Versie	Datum

Documentclassificatie

Classificatie	Beschrijving
Openbaar	Dit document mag zonder beperkingen worden gedeeld
Vertrouwelijk	Dit document mag worden gedeeld met medewerkers van <naam schoolbestuur en eventuele andere organisaties>.
Geheim	Dit document is exclusief bestemd voor de volgende personen: <bijv. leden MT>.

Inhoudsopgave

1 Inleiding

Toelichting

- *In dit hoofdstuk geef je aan wat de doelen van het risicomanagementbeleid zijn. De hiervoor geformuleerde doelen zijn voorbeelden. Pas ze aan aan je eigen organisatie.*
- *Binnen dit hoofdstuk bepaal je ook de reikwijdte van het risicomanagementbeleid. Om te voldoen aan het normenkader moeten in elk geval de risicogebieden informatiebeveiliging, privacy en fysieke beveiliging zijn opgenomen. Heb je al een risicomanagementbeleid in je organisatie? Dan kun je ervoor kiezen om voorgaande risicogebieden daarin op te nemen. Heb je nog geen risicomanagementbeleid? Overleg dan met bijvoorbeeld je controller of je ook risicogebieden als financiën in dit beleid opneemt. Geef in dit hoofdstuk duidelijk aan op welke risicogebieden dit beleid betrekking heeft.*

Risicomanagement is het regelmatig identificeren, beoordelen en mitigeren van risico's in relatie tot de doelstellingen van de organisatie. Als instelling die zich inzet voor een veilige werk- en leeromgeving, erkennen we het belang van risicomanagement om de continuïteit van activiteiten te garanderen en de reputatie van <vul naam organisatie in> te beschermen. Door regelmatig risicoanalyses te herhalen, blijven onze beveiligingsmaatregelen goed aansluiten op actuele dreigingen en risico's.

Dit risicomanagementbeleid is nodig voor het effectief beheren van risico's. Door risico's proactief aan te pakken, proberen we negatieve gevolgen te minimaliseren en bij te dragen aan de doelstellingen die <vul naam organisatie in> nastreeft. Dit beleidsstuk vormt de basis voor de risico-organisatie binnen <vul naam organisatie in>.

1.1 Doel

Met een risicomanagementbeleid identificeer, analyseer en beheers je risico's die de continuïteit van activiteiten en de reputatie van <vul naam organisatie in> kunnen beïnvloeden. Door risico's proactief aan te pakken, help je met het creëren van een veilige leer- en werkomgeving, en ben je voorbereid op mogelijke verstoringen. Risicomanagement helpt ons daardoor met het:

- proactief identificeren van risico's en bepalen welke van invloed zijn op de doelstellingen;
- bevorderen van een cultuur van risicobewustzijn en -verantwoordelijkheid binnen de school, waarin alle leerlingen en medewerkers bijdragen aan het identificeren en beheren van risico's;
- ontwikkelen van effectieve strategieën en maatregelen om risico's te beheersen en te verminderen;
- waarborgen van de betrokkenheid van belanghebbenden door effectieve communicatie en rapportage over risico's en risicobeheersactiviteiten;
- aanpassen aan veranderende omstandigheden en nieuwe risico's.
- voldoen aan relevante wet- en regelgeving en normen met betrekking tot risicomanagement.

1.2 Reikwijde

Het risicomanagementbeleid is van toepassing op alle medewerkers, leerlingen en bezoekers van <vul naam organisatie in>. Dit beleid is van toepassing op de volgende risicogebieden:

- Informatiebeveiliging
- Privacy
- Fysieke beveiliging
- <Vul andere risicogebieden aan>

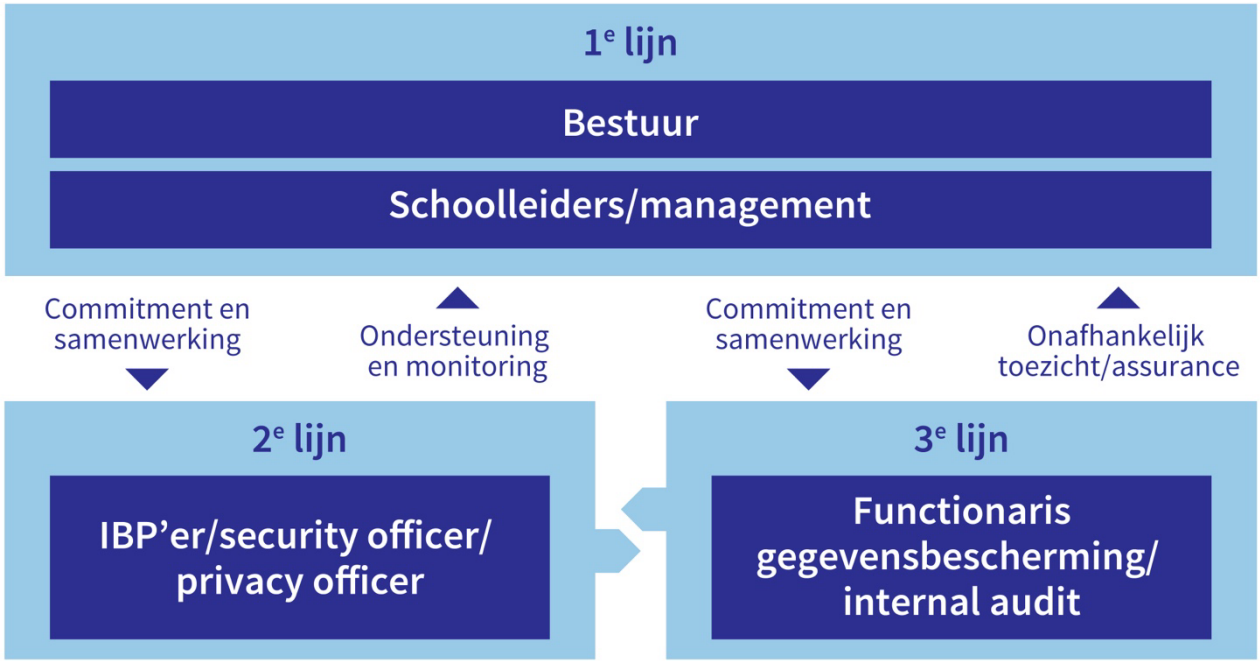
Het risicomanagementbeleid beperkt zich tot het beschrijven van de risicomanagementaanpak. In de risicomanagementprocesbeschrijving is uitgewerkt welke stappen je doorloopt bij het identificeren, analyseren en beheersen van risico's.

2 Governance

Toelichting

- *In dit hoofdstuk geef je aan hoe de governance van risicomanagement binnen de school is georganiseerd. Wie zorgt ervoor dat het beleid op de juiste manier wordt uitgevoerd?*
- *In dit voorbeelddocument maken we gebruik van het Three Lines Model. Dit organisatiemodel helpt om de governance van risicomanagement op een gestructureerde manier te organiseren. Je kunt uiteraard gebruikmaken van een andere manier om risicomanagement te organiseren.*

Risicomanagement bij <vul naam organisatie in> is ingericht aan de hand van het Three Lines model (3L-model). Het 3L-model is een leidraad bij het inrichten van de governance van een organisatie.



2.1 De eerste lijn

Toelichting

- *Beschrijf hier uit welke rollen de eerste lijn bestaat. Op een school kunnen dat teamleiders, coördinatoren, schoolleiders, conrectors of het hoofd bedrijfsvoering zijn.*

Het 3L-model heeft als uitgangspunt dat het management verantwoordelijk is voor processen, informatie en systemen van de organisatie, de risico's die hieruit voortvloeien en het nemen van de juiste maatregelen om de risico's te verkleinen. Het management vormt daarom de eerste lijn. Het risico-eigenaarschap is altijd belegd binnen de eerste lijn. Het schoolbestuur is eindverantwoordelijk voor risicomanagement.

2.2 De tweede lijn

Toelichting

- *Hier geef je aan wie de proceseigenaar risicomanagement is.*
- *Leg hier vast of de proceseigenaar risicomanagement of het schoolbestuur de procesbeschrijving risicomanagement moet vaststellen.*
- *Heeft jouw organisatie geen IBP'er of een vergelijkbare rol in dienst? Dan kan het proceseigenaarschap ook bij een bestuurder of schoolleider worden belegd. Let op: er is wel inhoudelijke kennis nodig om dit proces op een juiste manier te ondersteunen. Externe training over dit onderwerp kan daarom raadzaam zijn.*

Naast de eerste lijn moet er een rol zijn die de eerste lijn ondersteunt, adviseert en coördineert en die bewaakt of het management de verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. Het proceseigenaarschap van risicomanagement valt in de tweede lijn en is belegd bij <vul functietitel in>. De proceseigenaar kan om ondersteuning vragen bij de IBP'er/ CISO. De proceseigenaar van risicomanagement is verantwoordelijk voor het opstellen en beheren van het beleid en het risicomanagementproces en toetst de toepassing ervan. De proceseigenaar heeft geen beslissingsbevoegdheid en is niet verantwoordelijk voor risico's. Bij het proceseigenaarschap behoren de volgende verantwoordelijkheden:

- **Beleids- en procesbeheer**: de proceseigenaar is verantwoordelijk voor de ontwikkeling van het risicomanagementbeleid en het proces. Het gaat hierbij nadrukkelijk om de verantwoordelijkheid voor het *ontwikkelen* van het beleid en proces en niet om de verantwoordelijkheid voor het *implementeren* van het beleid en het proces. Die verantwoordelijkheid ligt bij het schoolbestuur als eindverantwoordelijke voor risicomanagement. Het schoolbestuur heeft de bevoegdheid om het risicomanagementbeleid formeel goed te keuren en te wijzigen. <Vul functietitel in> heeft de bevoegdheid om het risicomanagementproces formeel goed te keuren.
- **Faciliteren van de eerste lijn**: de proceseigenaar faciliteert de eerste lijn met behulp van templates, training, methodieken en andere ondersteuning.

- **Toetsing toepassing van beleid**: de proceseigenaar legt verantwoording af aan het schoolbestuur over het functioneren van het risicomanagementproces en het toepassen van het beleid door de eerste lijn.

2.3 De derde lijn

Toelichting

- *Hier geef je aan wie verantwoordelijk is voor het onafhankelijk toetsen van de samenwerking tussen en het functioneren van de eerste en tweede lijn. Denk aan een interne auditor of de Functionaris Gegevensbescherming.*

De derde lijn controleert of de eerste en tweede lijn soepel samenwerken en goed functioneren. De derde lijn is onafhankelijk, beoordeelt of de interne risicobeheersing van het schoolbestuur goed is ingericht en suggereert waar nodig verbeteringen. Binnen onze organisatie wordt de derde lijn gevormd door <vul functietitel in>.

2.4 Rollen en verantwoordelijkheden

Toelichting

- *Hier geef je aan welke rollen zijn betrokken bij het risicomanagementproces.*
- *Bij kleinere organisaties zal het bestuur zelf vaak risico-eigenaar zijn en voor het operationeel beheren van de risico's de IBP'er/CISO om hulp vragen.*
- *Een functie uit de eerste of de tweede lijn kan worden aangewezen als actiehouder*

De volgende rollen zijn binnen <naam schoolbestuur> betrokken bij het risicomanagementproces.

Rol	Verantwoordelijkheden
Eerste lijn	
Bestuur, directie, schoolleiding	• Risicobereidheid vastleggen. • Het identificeren van risico's. • Aanwijzen van een risico-eigenaar. • Monitoringsrapport inzien. • <Vul aan met verantwoordelijkheden>.
Risico-eigenaar	• Analyseren van risico's. • Maken van een beheerskeuze. • Verantwoording afleggen aan het bestuur over de status van de risico's en beheersmaatregelen.

	• Verantwoording afleggen aan de tweede lijn (IBP'er, Security Officer, Privacy Officer) over de status van de risico's en beheersmaatregelen. • <Vul aan met verantwoordelijkheden>.
Actiehouder	• Implementeren van de maatregel. • Verantwoording afleggen aan de risico-eigenaar. • <Vul aan met verantwoordelijkheden>.
Tweede lijn	
Proceseigenaar risicomanagement	• Zorgen voor ondersteuning van de eerste lijn met een risicomanagement-procesbeschrijving, training over het gebruik van deze procesbeschrijving en het risicoregister. • Opstellen en beheren van het risicoregister: zorg dragen dat de risico's eenduidig zijn verwoord en dat er geen dubbelingen in staan. • Bewaakt of het risicomanagement adequaat wordt uitgevoerd volgens afgesproken standaarden. • <Vul aan met verantwoordelijkheden>.
IBP'er, CISO, security officer, privacy officer	• Inhoudelijke ondersteuning bij het bepalen van informatiebeveiligings- en privacyrisico's en de beheerskeuze. • Geeft ongevraagd advies aan het bestuur en de risico-eigenaren over de volledigheid van het risicoregister, de voortgang van maatregelen en de naleving van het risicomanagementbeleid. • <Vul aan met verantwoordelijkheden>.
Derde lijn	
Functionaris gegevensbescherming	• Toetst onafhankelijk of privacyrisico's en beheersmaatregelen correct en volledig zijn geïdentificeerd en beoordeeld en rapporteert deze bevindingen gevraagd en ongevraagd aan het bestuur. • <Zo ja, vul aan met verantwoordelijkheden>.
Interne audit	• Bepaal of deze rol een functie heeft binnen dit proces. • <Zo ja, vul aan met verantwoordelijkheden>.

3 Risicomanagementkader

In dit hoofdstuk wordt het kader gesteld voor het toepassen van risicomanagement.

3.1 Risicobereidheid

Toelichting

Op basis van je strategische keuzes bepaal je hoeveel risico's de organisatie wil accepteren. Binnen de risicobereidheid maak je een keuze uit de risicoprofielen. Op basis van deze risicoprofielen ga je risico's anders beoordelen, mitigeren en herzien.

Het bestuur is eindverantwoordelijk voor risicomanagement en zorgt ervoor dat het in lijn is met de strategische doelen van de organisatie. Hierbij is het van belang om een passende risicobereidheid te hanteren. Zo blijven risico's beheersbaar en breng je de continuïteit en doelstellingen van de organisatie niet in gevaar. Er kan gekozen worden uit de volgende profielen:

Risicomijdend | werkdruk: *verzwaren*

- Beperken van zo veel mogelijk risico's.
- Zie passende heatmap in *bijlage A*

Risico-neutraal | werkdruk: *in balans*

- Het neutraal omgaan met risico's: kritieke tot ongewenste risico's beperken.
- Zie passende heatmap in *bijlage A*

Risicodragend | werkdruk: *verlichten*

- Alleen de kritieke en onacceptabele risico's beperken.
- Zie passende heatmap in *bijlage A*

<naam bestuur> heeft een risicobereidheid bepaald met als uitgangspunt **risico** <**dragend/neutraal/mijdend**>.

3.2 Analyse

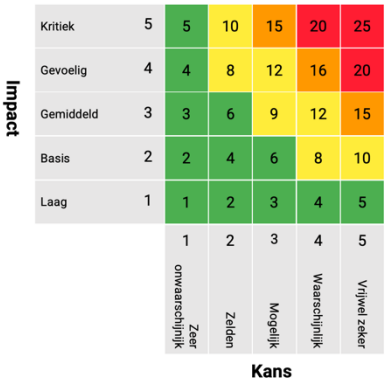
Toelichting

Bij het analyseren van risico's gaan we ervan uit dat er wordt gebruikgemaakt van de kans-impact-matrix. Gebruik je een andere methode voor het analyseren van risico's? Pas dan de omschrijving hieronder en in bijlage A aan.

A. Risico's analyseren

Risico's worden, aansluitend op de identificatie, genalayseerd om vast te stellen welke prioriteit zij krijgen binnen het risicomanagementproces. De analyse wordt jaarlijks uitgevoerd via een gestructureerde risicoanalyse, met de mogelijkheid tot aanvullende of tussentijdse analyses bij relevante ontwikkelingen of incidenten, waarbij voor ieder risico zowel de **kans** als de **impact** wordt ingeschat aan de hand van de kans- en impacttabel zoals weergegeven in *bijlage A: Kans- en Impacttabel*.

De kans geeft aan hoe waarschijnlijk het is dat het risico zich voordoet. De impact beschrijft de mogelijke gevolgen voor de organisatie als het risico optreedt. Beide worden op een schaal van 1 (laag/zeer onwaarschijnlijk) tot 5 (kritiek/vrijwel zeker) gescoord en met elkaar vermenigvuldigd. De uitkomst van de kans × impact resulteert in een risicowaarde tussen 1 en 25, die kan worden geplot op de heatmap zoals weergegeven in het figuur hiernaast en wordt vastgelegd in het risicoregister.



Figuur 1: Heatmap risicomanagement (bijlage A1)

Afhankelijk van de risicowaarde wordt het risico ingedeeld in één van de onderstaande categorieën, die elk richting geven aan de verdere behandeling en opvolging:

Risicoclassificatie	Gevolg of te nemen actie
Kritiek	Onderwijs stopt, hoge prioriteit maatregelen treffen
Hoog	Onmiddellijke actie en maatregelen vereist
Midden	Bestuur stelt risicoacceptatie en/of maatregelen vast
Laag	Acceptabel risico door risico-eigenaar

Tabel 1: Risicoclassificatietabel

Deze classificatie maakt het mogelijk om risico's objectief te prioriteren. De analyse wordt vastgelegd in het [risicoregister of link naar risicoregister opnemen], inclusief de onderbouwing, risico-eigenaar, te treffen of al getroffen maatregelen en de planning van de maatregelen die nog getroffen moeten worden.

3.3 Classificatie, beoordeling en acceptatie

<naam bestuur> hanteert de volgende systematiek voor het behandelen van risico's. Hiermee kunnen we risico's op een gestructureerde en transparante manier beoordelen en - waar nodig - gemotiveerd accepteren.

- <naam bestuur> classificeert risico's op basis van een 5 × 5 schaal model en volgens de definities van de impact- en kanstabellen.
- <naam bestuur> maakt gebruik van bruto en netto risicowaardes. Bruto houdt in dat er geen maatregelen getroffen worden op het moment van identificeren. Netto houdt in dat er maatregelen zijn getroffen of getroffen gaan worden en daarmee de risicowaarde minimaal wordt verlaagd tot een acceptabel niveau.
- <naam bestuur> laat (rest)risico's beoordelen door inhoudelijke experts. Dit zijn de professionals die in lijn 2 van het 3L-model vallen. De risico-eigenaar bevindt zich in de eerste lijn en is eventueel gemandateerd door bestuur.

3.4 Beheersingsstrategieën

Om geïdentificeerde risico's te beheersen maakt <naam bestuur> gebruik van 4 risico-beheersingsstrategieën. Deze worden toegepast op basis van de gehanteerde risicobereidheid. De strategieën zijn gericht op het beperken, verleggen of accepteren van risico's binnen de vastgestelde kaders.

- **Vermijden**: bepaalde activiteiten stopzetten of aanpassen om het risico te vermijden.
- **Mitigeren**: er worden beheersmaatregelen ingevoerd om het risico te verlagen tot een acceptabel niveau.
- **Overdragen**: het risico wordt overgedragen aan een (externe IT-) leverancier of verzekeraar.
- **Accepteren**: het risico valt binnen de acceptatiewaardes en volgt waar nodig het risico-acceptatieproces.

3.5 Risicoacceptatieschema

Toelichting

Je kan er als organisatie voor kiezen om af te wijken van de onderstaande risico-acceptatie profielen. Zorg dat minimaal vastgelegd is wie de risico's mag accepteren. Dit kan bijvoorbeeld ook altijd het bestuur zijn en is afhankelijk van de structuur van je organisatie.

Vanwege de vastgestelde risicobereidheid van <naam bestuur> is het volgende risico-acceptatieschema van kracht <*Behoud de beoogde risicobereidheid een en verwijder de overige opties:*>

Mijdend	
Risicowaarde **1 t/m 6**	Risico-eigenaar mag het risico accepteren.
Risicowaarde **7 t/m 12**	Enkel het bestuur mag het risico accepteren.
Risicowaarde **13 t/m 25**	Mag absoluut niet geaccepteerd worden.

Neutraal	
Risicowaarde **1 t/m 8**	Risico-eigenaar mag het risico accepteren.
Risicowaarde **9 t/m 15**	Enkel het bestuur mag het risico accepteren.
Risicowaarde **16 t/m 25**	Mag absoluut niet geaccepteerd worden.

Dragend	
Risicowaarde **1 t/m 10**	Risico-eigenaar mag het risico accepteren.
Risicowaarde **11 t/m 20**	Enkel het bestuur mag het risico accepteren.

Risicowaarde **21 t/m 25**	Mag absoluut niet geaccepteerd worden.

3.6 Onderhoud van risico's

Toelichting

Je kunt ervoor kiezen om risico's te herzien op basis van de classificatie of om een standaard termijn voor het herzien van alle risico's te kiezen. De keuze die je hierin maakt is afhankelijk van de structuur en capaciteit van je organisatie.

Zowel de risicoanalyse als dit beleid moeten minstens eens per 2 jaar worden herzien. <naam bestuur> hanteert daarbij de volgende cycli voor monitoring en herbeoordeling van geïdentificeerde risico's:

Risicoclassificatie	***Risico-onderhoudscyclus***
Kritiek	Maandelijks (1 maand)
Hoog	Halfjaarlijks (6 maanden)
Midden	Jaarlijks (12 maanden)
Laag	Tweejaarlijks (24 maanden)

3.7 Communicatie van risico's

Toelichting

Bepaal op welke manier je als organisatie wil communiceren over risico's. Je kunt dit doen op basis van het classificatieniveau. Zo is het in het voorbeeld hieronder uitgewerkt. Je kunt er ook voor kiezen om over alle risico's in één keer te communiceren. Leg ook vast op welke manier deze communicatie plaatsvindt.

<naam bestuur> communiceert over risico's op een wijze die aansluit bij de gekozen beheersstrategie en de rol van betrokken partijen. Risico's die betrekking hebben op de bescherming van persoonsgegevens wordt de FG geraadpleegd volgens het 3L-model. Onderstaande toelichting beschrijft per risicoclassificatie met wie je moet communiceren en of je verplicht bent om te communiceren.

Risicoclassificatie	**Risico-communicatie**
Kritiek	Verplicht te rapporteren aan bestuur en belanghebbenden
Hoog	Verplicht te rapporteren aan bestuur en belanghebbenden
Midden	Verplicht te rapporteren aan bestuur en belanghebbenden

Laag	Niet verplicht om te communiceren

Communicatie van de risico's is gebaseerd op het uitgangspunt van de behandelingsstrategie:

- **Vermijden**: communiceer het uitgangspunt om het risico te vermijden met de desbetreffende risico-eigenaar.
- **Mitigeren**: overweeg het risico mee te nemen in het bewustwordingsplan.
- **Overdragen**: communiceer het risico met de partij waaraan wordt overgedragen.
- **Accepteren**: communicatie vindt plaats met minimaal de inhoudelijke expert(s) en, conform het acceptatieschema, met de relevante belanghebbenden.

3.8 Aanleiding voor een risicoanalyse

Om risico's te beheersen, moeten deze eerst inzichtelijk gemaakt worden. Risico's worden inzichtelijk gemaakt door middel van een risicoanalyse. Er zijn verschillende aanleidingen om een risicoanalyse te starten of te herzien:

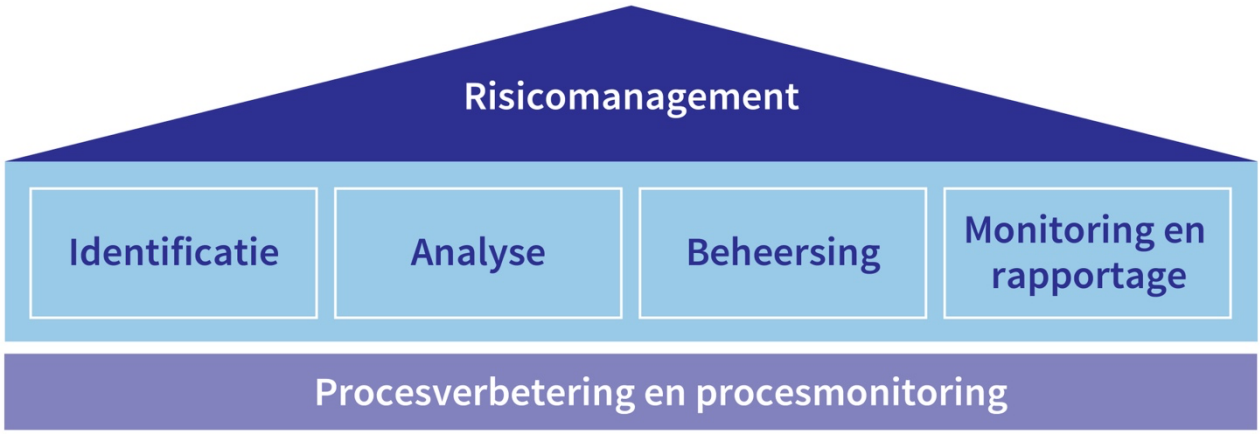
- Bij invoering van een nieuw proces of werkwijze voor de verwerking van informatie.
- Bij een significante wijziging in een bestaand proces, werkwijze, ketensamenstelling of infrastructuur.
- Bij een verandering in relevante wet- en regelgeving die tot strengere beveiligingseisen leiden.
- Bij een verhoging van de BIV-classificatie van het bedrijfsmiddel.
- Bij een incident dat aanleiding geeft om risico's te heroverwegen.
- Bij het verstrijken van de geldigheidsduur van een risicoanalyse (twee jaar).
- Bij een mogelijke verandering in het dreigingslandschap. Het is de verantwoordelijkheid van de CISO/IBP'er om de organisatie hierover te informeren.

3.9 Structuur Risicomanagementproces

Toelichting

Let op: binnen dit beleid is rekening gehouden met netto en bruto risico's. Beoordeel zelf aan de hand van de bestaande werkwijze of je met netto en brute risico's wilt gaan werken.

Het risicomanagementproces bestaat uit een aantal opeenvolgende stappen. Elke stap vervult een specifieke functie binnen het beheersen van (privacy)risico's en wordt in dit document afzonderlijk toegelicht:



Er wordt <tweejaarlijks/jaarlijks> of bij een van de aanleidingen uit paragraaf *3.7 Aanleiding voor een risicoanalyse* een risicoanalyse uitgevoerd. Je doorloopt dan minimaal de eerste 3 stappen van het risicomanagementproces:

- **Identificatie**: Hierbij worden de processen geïnventariseerd en per onderdeel geanalyseerd welke dreigingen van toepassing zijn. Deze dreigingen worden als input gebruikt voor het risicomanagement. Op basis van de dreigingen worden risico's geïdentificeerd. Hiervoor kunnen methodieken als MAPGOOD, RAVIB of het MITRE ATT&CK-framework worden gebruikt.
- **Analyse:** Elk risico wordt beoordeeld op kans en impact. Dit leidt tot een risicowaarde. Deze beoordeling wordt vastgelegd in het risicoregister, inclusief risicoclassificatie en risico-eigenaar.
- **Beheersing:** Voor elk risico wordt een beheerstrategie gekozen en uitgevoerd. Bij risicoacceptatie wordt het risico formeel geaccepteerd. Na het nemen van de juiste maatregelen mowr het netto risico ingevuld te worden.
- **Monitoring en rapportage:** Risico's en beheersmaatregelen worden continu bewaakt en periodiek herbeoordeeld. Zie *3.5 Onderhoud van risico's*. De resultaten hiervan worden gerapporteerd volgens 3.5 en 3.6.

De proces-eigenaar van het risicomanagementproces monitort of het proces volgens de afspraken wordt uitgevoerd en kan proceswijzigingen voorstellen als dat nodig is.

4 Monitoring en herziening beleid en proces

Zowel het risicomanagementbeleid als het risicomanagementproces worden periodiek geëvalueerd en eventueel herzien.

4.1 Monitoring

Toelichting

- *Beschrijf hier hoe vaak per jaar de proceseigenaar verantwoording aflegt aan het schoolbestuur over het functioneren van het risicomanagementproces.*
- *Beschrijf hoe deze verantwoording wordt gerapporteerd.*

De proceseigenaar evalueert of de organisatie het risicomanagementbeleid en het risicomanagementproces volgt. En legt <beschrijf hoe vaak per jaar> verantwoording af aan het schoolbestuur over het functioneren van het risicomanagementbeleid en het proces. De verantwoording wordt gerapporteerd via een <schriftelijke evaluatierapportage>, waarin bevindingen en aanbevelingen worden opgenomen. De evaluatie kan gebaseerd worden op:

- Resultaten uit interne audits of controles.
- Inzichten uit incidenten of afwijkingen.
- Bevindingen uit gesprekken met risico-eigenaren en andere betrokkenen.
- Ontwikkelingen of (grote en/of kritieke) wijzigingen binnen de organisatie of de sector.

4.2 Herziening

Toelichting

- *Beschrijf wie er worden betrokken bij eventuele wijzigingsvoorstellen.*
- *Je kunt ervoor kiezen om de formele herziening van de risicomanagementprocesbeschrijving niet periodiek in te plannen, maar om gedurende de uitvoering waar nodig verbeteringen door te voeren. Kies je hiervoor? Geef dit dan hier aan.*

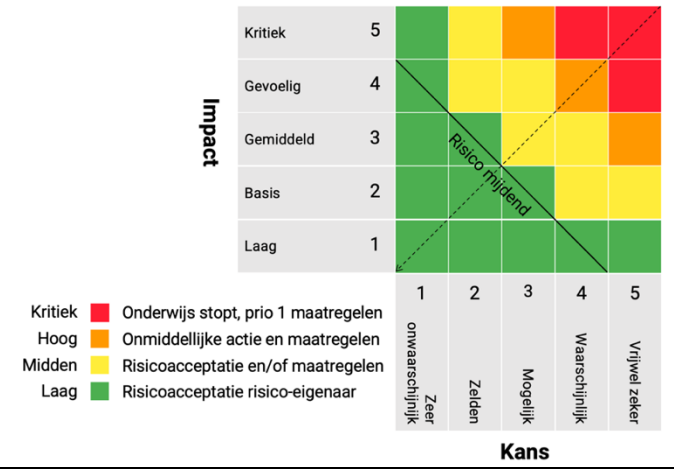
Op basis van de tweejaarlijkse evaluatie stelt <de proceseigenaar> waar nodig concrete verbeteringen en aanpassingen voor voor het risicomanagementbeleid en -proces. Deze aanpassingen kunnen gericht zijn op inhoudelijke verbeteringen, procesoptimalisatie of het verduidelijken van verantwoordelijkheden. Bij het opstellen van wijzigingsvoorstellen worden relevante betrokkenen geraadpleegd, zoals <de CISO, IBP'er, FG, risico-eigenaren en bestuur/directie/schoolleiding>.

Het bestuur beoordeelt en herziet het beleid en stelt het minimaal eens per twee jaar formeel vast. Zo blijft het effectief aansluiten bij de actuele situatie en organisatiebehoeften. Tussentijdse herziening kan plaatsvinden bij ingrijpende wijzigingen, zoals nieuwe wet- en regelgeving, organisatorische veranderingen of structurele knelpunten in de uitvoering van het beleid.

Bijlage A: Risicobereidheidsniveau's en -tabellen

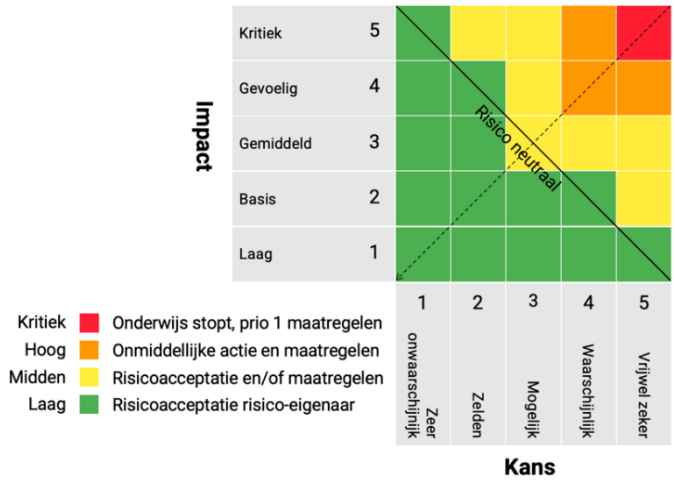
C.1 Risicomijdend

Het bestuur streeft ernaar om zo veel mogelijk risico's te vermijden en dus 'in control' te zijn over deze risico's. Dit versterkt procedures en richtlijnen en verhoogt de professionaliteit. Dit kan in sommige gevallen leiden tot extra werkdruk. Er worden beheersmaatregelen genomen, ook voor relatief kleine risico's.



C.2 Risico-neutraal

Het bestuur stelt zich pragmatisch op bij de risico afweging. Risico's worden beoordeeld en geaccepteerd zolang deze binnen het aanvaardbare kader blijven. Er worden beheersmaatregelen getroffen voor midden-, hoge en kritieke risico's, met een evenwichtige benadering waarbij de risicobeheersing gepaard gaat met de werkbaarheid. Maatregelen zijn doelgericht, proportioneel en gericht op de onderwijsprocessen.



C.3 Risicodragend

Het bestuur accepteert de risico's zolang deze niet onder de grens van midden- of hoge risico's vallen. Risico's worden bewust aanvaard als onderdeel van goed functionerend en adaptief onderwijs. Er is sprake van een doordachte houding: niet elk risico hoeft vooraf volledig beheerst te worden, zolang er vertrouwen is in het vermogen om adequaat te reageren als zich een situatie voordoet.