

Risicomanagementbeleid

Voorbeelddocument

Versie: Januari 2025



**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.



Dit template is opgesteld door Kennisnet en verschijnt onder de licentie [*Creative Commons Naamsvermelding 4.0 Nederland*](https://creativecommons.org/licenses/by/4.0/legalcode.nl).

**Vragen?**

Heb je vragen over dit voorbeelddocument? Kijk voor meer informatie op [*normenkaderibp.kennisnet.nl/groeipad*](file:///Users/jhgerrits/Documents/1.%20Kennisnet%20voorbeeldocumenten/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 5](#_Toc189075560)

[1.1 Doel 5](#_Toc189075561)

[1.2 Reikwijde 5](#_Toc189075562)

[2 Governance 6](#_Toc189075563)

[2.1 De eerste lijn 6](#_Toc189075564)

[2.2 De tweede lijn 7](#_Toc189075565)

[2.3 De derde lijn 8](#_Toc189075566)

[3 Risicomanagementproces 8](#_Toc189075567)

[3.1 Identificatie 8](#_Toc189075568)

[3.2 Analyse 9](#_Toc189075569)

[3.3 Beheersing 9](#_Toc189075570)

[3.4 Monitoring en rapportage 9](#_Toc189075571)

[4 Monitoring en herziening beleid en proces 10](#_Toc189075572)

[4.1 Monitoring 10](#_Toc189075573)

[4.2 Herziening 10](#_Toc189075574)

# 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.*

Als instelling die zich inzet voor een veilige werk- en leeromgeving, erkennen we het belang van het identificeren, analyseren en beheersen van potentiële risico's die de continuïteit van activiteiten en de reputatie van <vul naam organisatie in> kunnen beïnvloeden. 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>.

## 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.

## 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.

# 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.



## 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.

## 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. 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.

## 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>.

# Risicomanagementproces

Het risicomanagementproces bestaat uit een aantal stappen die er samen voor zorgen dat de risico’s binnen <vul naam organisatie in> worden beheerd. Het risicomanagementproces bestaat uit 4 stappen. Hier lichten we toe hoe we deze stappen precies uitvoeren. .



## Identificatie

***Toelichting***

*In deze paragraaf bepaal je wie verantwoordelijk is voor het registreren en identificeren van risico’s en wie de eigenaar is.*

* *Let op: de risico-eigenaar moet kunnen besluiten over mitigerende maatregelen en dus hoog genoeg gepositioneerd zijn binnen de organisatie.*
* *Bepaal hier ook hoe je wilt omgaan met het eigenaarschap van risico’s die voor meerdere scholen binnen het bestuur gelden en waar het eigenaarschap daarvan het best kan worden belegd.*

Om ervoor te zorgen dat risico’s worden beheerd, moeten ze in kaart zijn gebracht. Risico’s die zijn geïdentificeerd, kun je ook niet beheren. En dat kan leiden tot het verstoren van de organisatiedoelstellingen, waaronder het geven van onderwijs. De eerste lijn is verantwoordelijk voor het identificeren van risico’s die mogelijk een negatieve impact hebben op de doelstellingen van het betreffende organisatieonderdeel. Het schoolbestuur en de verschillende locaties die eronder vallen hebben gezamenlijk de verantwoordelijkheid voor het identificeren van risico’s die betrekking hebben op de gehele organisatie. De verantwoordelijkheid voor het registreren van risico’s is belegd in de eerste lijn. Ook het risico-eigenaarschap is belegd in de eerste lijn.

## Analyse

***Toelichting***

* *Geef hier aan welke risicoanalysemethodiek je gebruikt voor de analyse van risico’s.*
* *Bepaal of de organisatie werkt met bruto/netto-risico’s.*

De kans en impact van een risico worden aan de hand van periodieke risicoanalyses bepaald. Wij gebruiken hiervoor de kans-impactanalyse:

* Kans en impact worden gebruikt om de grootte van een risico te bepalen.
* De kans dat een risico zich voordoet en de impact die dat risico heeft op de organisatie worden op een <vul in wat voor schaal gebruikt wordt> gescoord.

## Beheersing

***Toelichting***

* *Na analyse van het risico, maakt de risico-eigenaar een keuze over hoe er met het risico wordt omgegaan. Dit is de beheerskeuze.*
* *Je kunt hier ook iets opnemen over de risicoacceptatiegraad. Grotere organisaties werken met grotere hoeveelheden risico’s. Er kan dan worden gewerkt met een risicoacceptatiegraad. Dit betekent dat risico’s die onder de acceptatiegraad vallen automatisch worden geaccepteerd. Vul in dit beleid nog niet de acceptatiegraad in, maar bepaal wel wie er verantwoordelijk is voor het vastleggen hiervan. De risicoacceptatiegraad wordt vastgelegd in de risicomanagementprocesbeschrijving.*

De risico-eigenaren maken de beheerskeuzes. Elke beheersmaatregel krijgt een actiehouder. Die is verantwoordelijk voor de implementatie van de beheersmaatregel.

## Monitoring en rapportage

***Toelichting***

* *Beschrijf hier hoe de risico-eigenaren aan het schoolbestuur rapporteren over de status van de risico’s en de beheersmaatregelen. Neem minimaal op hoe vaak per jaar deze rapportage plaatsvindt.*
* *Zorg na het ontvangen van de rapportage voor een terugkoppeling vanuit het schoolbestuur aan de risico-eigenaren.*

De risico-eigenaren monitoren of beheersmaatregelen effectief zijn en rapporteren hierover <aangeven hoe vaak per jaar> aan het schoolbestuur.

# Monitoring en herziening beleid en proces

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

## 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 monitort 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. Ook rapporteert de proceseigenaar aan de hand van <beschrijf hoe deze verantwoording gerapporteerd wordt>.

## 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.*

De proceseigenaar evalueert het risicomanagementbeleid en het risicomanagementproces, en stelt waar nodig verbeteringen voor. Hierbij worden <beschrijf wie er betrokken dienen te worden bij eventuele wijzigingsvoorstellen> betrokken. Het schoolbestuur moet dit risicomanagementbeleid na <vul in welke interval> jaar formeel herzien en vaststellen.