

Risicomanagementproces

Voorbeelddocument

Versie: Januari 2025



**Let op: verwijder deze pagina voor gebruik**

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je met het maken van een eigen risicomanagementproces. 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 de procesbeschrijving definitief maakt.
* Deze procesbeschrijving gaat ervan uit dat taken, rollen en functies die nodig zijn om het proces 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***

* *Geef hier aan wie het document vaststelt. Dat kan bijvoorbeeld de proceseigenaar zijn, maar ook het bestuur.*
* *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](#_Toc189073399)

[2 Processtappen 5](#_Toc189073400)

[2.1 Identificatie 5](#_Toc189073401)

[2.2 Analyse 6](#_Toc189073402)

[2.3 Beheersing 6](#_Toc189073403)

[2.4 Monitoring & Rapportage 7](#_Toc189073404)

[3 Rollen en verantwoordelijkheden 8](#_Toc189073405)

[Bijlage A 10](#_Toc189073406)

[Impacttabel 10](#_Toc189073407)

[Kanstabel 11](#_Toc189073408)

# Inleiding

Het risicomanagementproces is bedoeld om risico’s op een gestructureerde manier te identificeren, analyseren en beheersen, waarbij risico’s en maatregelen worden gekoppeld aan eigenaren en de status van de risico’s wordt bijgehouden en gerapporteerd. Deze procesbeschrijving beschrijft hoe het risicomanagementproces wordt uitgevoerd binnen <vul naam organisatie in>. Dit proces sluit aan bij het risicomanagementbeleid van <vul naam organisatie in>.

# Processtappen

Het risicomanagementproces bestaat uit 4 stappen die er samen voor zorgen dat risico’s binnen <vul naam organisatie in> goed beheerd worden. Aan de hand van dit proces krijgen we als organisatie inzicht in welke risico’s we lopen en kunnen we beoordelen wat deze risico’s mogelijk voor ons betekenen. Op basis van deze kennis kunnen we een gedegen afweging maken over de beste beheersstrategie. Het risicomanagementproces bestaat uit de volgende 4 processtappen:

* Identificatie
* Analyse
* Beheersing
* Monitoring & Rapportage

Hieronder lichten we elke stap toe.

## Identificatie

***Toelichting***

*Je geeft bij deze stap onder andere aan welke bronnen worden gebruikt om de risico’s die de organisatie loopt in kaart te brengen. Er kan worden gebruikgemaakt van:*

* *Het procesoverzicht van de organisatie;*
* *Het applicatieoverzicht van de organisatie;*
* *De uitgevoerde businessimpactanalyses (zie deelproject Businesscontinuïteit);*
* *Het dreigingsbeeld funderend onderwijs.*

Het identificeren van risico’s valt uiteen in een aantal taken:

A. Periodiek risico’s identificeren

Bepaal <vul in met welke interval> welke risico’s <vul naam organisatie in> loopt. Dit gebeurt op basis van:

* <Som de bronnen op die je hiervoor gebruikt>

Vinden er grote wijzigingen plaats binnen <vul naam organisatie in>? Dan moeten de bijbehorende risico’s ook worden geïdentificeerd. Het kan zijn dat dit buiten de periodieke identificatie moet gebeuren.

B. Geïdentificeerde risico’s opnemen in risicoregister

Neem geïdentificeerde risico’s altijd op in het risicoregister.

C. Risico-eigenaar aanwijzen

Na de opname in het risicoregister wordt het risico gekoppeld aan een risico-eigenaar.

## 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

Na het identificeren van de risico’s, analyseren we wat de impact van elk risico is en wat de kans is dat dit risico zich voordoet binnen onze school. Dit doen we met de zogeheten kans-impact-analyse, waarbij de impact en de kans samen de hoogte van een risico bepalen. Op basis van de hoogte van het risico kiezen we vervolgens een beheerstrategie.

In bijlage A van deze procesbeschrijving zijn de Kans en Impact scoringstabellen opgenomen.

## Beheersing

***Toelichting***

*Bij deze stap geef je aan hoe je omgaat met het beheersen van risico’s. Werk je met risicobereidheid? Pas dan de tekst over het accepteren van risico’s zo aan dat de risicobereidheid wordt meegenomen.*

Na analyse van het risico maakt de risico-eigenaar een keuze over hoe er met het risico wordt omgegaan. Dat gebeurt aan de hand van de volgende taken:

A. Bepaal de beheersstrategie

Er zijn 4 mogelijkheden voor het beheersen van een risico:

* Vermijden: het aanpassen van het proces of omgeving, zodat het risico niet meer bestaat.
* Mitigeren (verminderen): het nemen van maatregelen om het risico te beperken.
* Overdragen: het beperken van de gevolgen van een risico door middel van verzekeren of het delen van de negatieve gevolgen van een risico met een andere organisatie.
* Accepteren: kun je een risico niet vermijden, mitigeren of overdragen? Of zijn de kosten hiervoor groter dan de baten? Dan kun je ervoor kiezen het risico te accepteren.

B. Maak een beheerskeuze

De risico-eigenaar maakt een beheerskeuze en legt deze vast in het risicoregister. Kiest de eigenaar voor het vermijden, mitigeren of overdragen van het risico? Dan wordt er een beheersmaatregel bepaald.

C. Wijs een actiehouder aan

Voor elke beheersmaatregel wijst de risico-eigenaar een actiehouder aan. Deze actiehouder is verantwoordelijk voor de implementatie van de beheersmaatregel en legt periodiek verantwoording af aan de risico-eigenaar over de status van de beheersmaatregel. De beheersmaatregelen en de actiehouders van deze maatregelen worden altijd geregistreerd in het risicoregister.

Wordt er gekozen voor het accepteren van een risico? Dan moet de risico-eigenaar hierover rapporteren naar het bestuur. In de volgende processtap beschrijven we hoe dat gaat.

## Monitoring & Rapportage

**Toelichting**

* *Beschrijf hoe risico-eigenaren monitoren of de genomen maatregelen effectief zijn.*
* *Neem op hoe vaak per jaar deze rapportage plaatsvindt en in welke vorm.*

De risico-eigenaren zijn verantwoordelijk voor de monitoring van de effectiviteit van de maatregelen die de actiehouders hebben geïmplementeerd. De actiehouders houden in het risicoregister de status van beheersmaatregelen bij, zodat dit inzichtelijk is voor de risico-eigenaren. Aan de hand van <geef aan welke vorm de rapportage heeft> rapporteren de risico-eigenaren jaarlijks <aantal keer> aan het schoolbestuur over de effectiviteit van de genomen maatregelen.

# 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 | * Het identificeren van risico’s.
* Aanwijzen van een risico-eigenaar.
* De verdere verantwoordelijkheden komen bij de risico-eigenaar te liggen.
* <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.
* <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.
* <Vul aan met verantwoordelijkheden>.
 |
| IBP’er, CISO, security officer, privacy officer | * Inhoudelijke ondersteuning bij het bepalen van informatiebeveiligings- en privacyrisico’s en de beheerskeuze.
* Ongevraagd advies aan het bestuur en de risico- eigenaren over de volledigheid van het risicoregister en de voortgang van maatregelen.
* <Vul aan met verantwoordelijkheden>.
 |
| **Derde lijn** |
| Functionaris gegevensbescherming | * Bepaal of deze rol een functie heeft binnen dit proces.
* <Zo ja, vul aan met verantwoordelijkheden>.
 |
| Interne audit | * Bepaal of deze rol een functie heeft binnen dit proces.
* <Zo ja, vul aan met verantwoordelijkheden>.
 |

# Bijlage A

## Impacttabel

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **1 - Laag** | **2 - Basis** | **3 - Gemiddeld** | **4 - Gevoelig** | **5 - Kritiek** |
| Reputatie | --- | Negatieve berichtgeving in lokale media en losse uitingen op sociale media. | Verlies van vertrouwen voor korte termijn door beperkte groep stakeholders. Negatieve nationale berichtgeving of aanhoudende negatieve lokale berichtgeving, commotie op sociale media. | Geschonden vertrouwen van (groepen) stakeholders. Aanhoudende negatieve nationale berichtgeving, grote commotie op sociale media. | Verlies van vertrouwen voor lange termijn door stakeholders. Internationale negatieve berichtgeving, met grote kans op toekomstige negatieve berichtgeving. |
| Onderwijs | Beperkte storing binnen een onderwijsactiviteit. | Hooguit verstoring van een aantal activiteiten binnen een domein of dienst tot 1 uur. | Verstoring van een deel van het onderwijs (binnen een domein of dienst) voor meerdere uren. | Verstoringen van een groot deel van het onderwijs, 1 tot 2 dagen uitval. | Merendeel van het onderwijs wordt onmogelijk voor meer dan 2 dagen. |
| Onderwijscertificatie | --- | Kritische vragen over onderwijscertificatie. | Extra toezicht op onderwijscertificatie. | Beperking van onderwijscertificatie. | Verlies van onderwijscertificatie. |
| Financieel | Directe schade ligt tussen 0 en €10.000. | Directe schade ligt tussen €10.000 en €50.000. | Directe schade ligt tussen €50.000 en €250.000. | Directe schade ligt tussen €250.000 en €1.000.000. | Directe schade is groter dan €1.000.000. |
| Compliance – AVG | Beperkte hoeveelheid persoonsgegevens van enkele betrokkenen, geen bijzondere persoonsgegevens. | Kleine hoeveelheid betrokkenen, geen bijzondere persoonsgegevens. | Persoonsgegevens van een redelijke hoeveelheid betrokkenen of bijzondere gegevens van een klein aantal betrokkenen. | Persoonsgegevens van een grote hoeveelheid betrokkenen of bijzondere gegevens van een redelijk aantal betrokkenen. | Persoonsgegevens van een zeer grootschalige hoeveelheid betrokkenen of bijzondere persoonsgegevens van een groot aantal betrokkenen. |

## Kanstabel

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **1 – Zeer onwaarschijnlijk** | **2 - Onwaarschijnlijk** | **3 - Mogelijk** | **4 - Waarschijnlijk** | **5 - Vrijwel zeker** |
| Kwalitatief | Niet aangetoond dat dit plaatsvindt. Zeer specifieke omstandigheden voor nodig. Komt vrijwel niet voor dat het in de praktijk misgaat. | Is voorgekomen, vaak specifieke omstandigheden voor nodig. Gaat in de praktijk niet vaak mis. | Is meerdere keren voorgekomen in de praktijk. | De kans dat dit in de (nabije) toekomst misgaat is reëel, omdat er bv. al een werkend concept-misbruik-scenario bestaat. | Er zijn concrete aanwijzingen dat dit in de praktijk plaatsvindt of misgaat. |
| Kwantitatief op basis van frequentie | **1x per 20 jaar** | **1x per 5 jaar** | **1x per jaar** | **Maandelijks** | **Wekelijks** |
| Kwantitatief op basis van % kans | **< 2%** | **2 – < 10%** | **10 – 25%** | **25 – 50%** | **> 50%** |