

Normenkader
Informatiebeveiliging en Privacy
voor het onderwijs

Risicomanagementproces

Voorbeelddocument

Versie: September 2026



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 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](#).

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

- 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
2	Processtappen	5
2.1	Identificatie	5
2.2	Analyse	6
2.3	Beheersing.....	7
2.4	Monitoring & Rapportage	8
3	Rollen en verantwoordelijkheden	9
Bijlage A.....		12
	Impacttabel	12
	Kanstabel.....	13

1 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>.

2 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

Wanneer je de stappen uit het risicomanagementproces uitvoert is vastgelegd in het risicomanagementbeleid. Het uitvoeren van de periodieke risicoanalyse, actuele dreigingen of grote organisatieveranderingen kunnen allemaal redenen zijn om het proces te doorlopen. Hieronder lichten we elke stap toe.

2.1 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 business impactanalyses (zie deelproject Businesscontinuïteit);*
- *Het dreigingsbeeld funderend onderwijs.*

Om ervoor te zorgen dat risico's worden beheerd, moeten ze in kaart zijn gebracht. Risico's die zijn geïdentificeerd, kun je immers ook niet beheersen. En dat kan leiden tot het verstoren van de organisatiedoelstellingen en het primaire proces: 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 hun 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.

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

A. Dreigingen analyseren

Binnen deze stap worden de verschillende dreigingen die van toepassing kunnen zijn op de informatie, applicaties of processen van de organisatie in kaart gebracht. Hierbij kan gebruikgemaakt worden van het *Dreigingsbeeld Funderend Onderwijs* van Kennisnet. Voor actuele dreigingen wordt beoordeeld in hoeverre deze voor risico's kunnen zorgen en vormen de basis voor het daadwerkelijk identificeren van van de risico's in stap B.

B. Risico's identificeren

De risico-identificatie volgt op de dreigingsanalyse, waarin de potentiële dreigingen en kwetsbaarheden zijn geanalyseerd die mogelijk impact kunnen hebben op de organisatie. Op basis van deze analyse worden de risico's geïdentificeerd die impact kunnen hebben op processen, informatievoorzieningen en onderwijskwaliteit. De volgende inzichten in de organisatie worden hiervoor gebruikt.

- **Het procesoverzicht van de organisatie:** Het procesoverzicht kan gebruikt worden om binnen de processen specifiek naar de procesrisico's op zoek te gaan.
- **Het applicatieoverzicht van de organisatie:** Het applicatieoverzicht kan bijvoorbeeld gebruikt worden om te kijken of er type applicaties zijn die voor specifieke risico's zorgen.
- **De uitgevoerde business impactanalyses:** Deze analyses geven een goed inzicht in waar mogelijk de grootste risico's liggen binnen de processen.

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. De risico-eigenaar is verantwoordelijk voor het uitvoeren van de volgende stappen binnen het risicomanagementproces. In de praktijk komt het vaak voor dat alle stappen binnen dit proces worden doorlopen in een risicoanalyse sessie.

2.2 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

Na de identificatie worden risico's geanalyseerd om vast te stellen welke prioriteit zij krijgen binnen het risicomanagementproces. Deze analyse wordt jaarlijks uitgevoerd. Zijn er relevante ontwikkelingen of vinden er incidenten plaats? Dan kunnen er aanvullende of tussentijdse analyses plaatsvinden. Tijdens de analyse wordt voor ieder risico zowel de **kans** als de **impact** ingeschat aan de hand van de kans- en impacttabel zoals weergegeven in *bijlage B: Impacttabel* en *bijlage C: Kanstabel*.

- 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. Deze risicowaarde kan worden geplot op de heatmap in *bijlage A: Risicobereidheidsniveau's en -tabellen*. Afhankelijk van de risicowaarde wordt het risico ingedeeld in één van de onderstaande categorieën. Uit de categorie volgt een bijbehorende actie of gevolg:

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.

2.3 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 de risicoanalyse volgt de risicobeheersing om te bepalen of risico's acceptabel zijn of dat er aanvullende maatregelen nodig zijn om risico's tot een acceptabel niveau te verlagen. Houd hierbij rekening met het vooraf vastgestelde risicocriteria, zoals de risicobereidheid.

Risico-eigenaren stellen samen met ondersteunende functies zoals de IBP'er passende beheersmaatregelen vast. Zij bepalen welke acties nodig zijn om het risico te vermijden, te mitigeren, over te dragen of bewust te accepteren, afhankelijk van de aard en ernst van het risico

A. Bepaal de beheerskeuze

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.

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. Bij het accepteren van het risico dient dit vastgelegd te worden met motivatie in het risicoregister.

B. Wijs een actiehouders aan

Voor elke beheersmaatregel wijst de risico-eigenaar een actiehouders aan. Deze actiehouders 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.

2.4 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 status van de risico's en de voortgang/effectiviteit van de genomen maatregelen. De tweede lijn analyseert de rapportage, beoordeelt de werking van de maatregelen en kan hierover advies geven aan het bestuur.

3 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 actiehouders

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

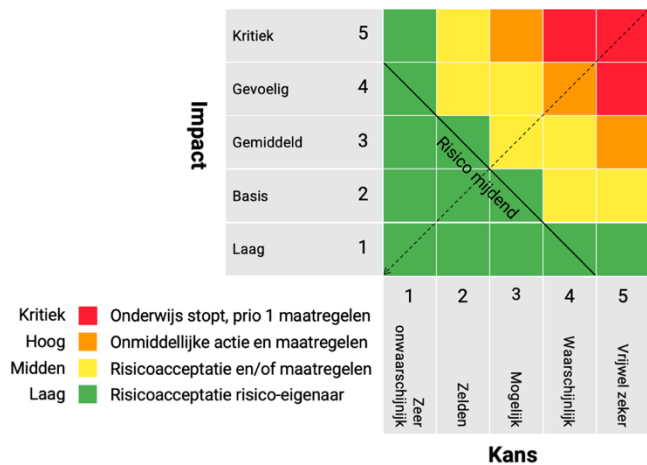
Rol	Verantwoordelijkheden
Eerste lijn	
Bestuur, directie, schoolleiding	• Risicobereidheid vastleggen. • Het identificeren van risico's. • Aanwijzen van een risico-eigenaar. • Monitoringsrapport inzien. • <Vul aan met verantwoordelijkheden>.
Risico-eigenaar	• Analyseren van risico's. • Maken van een 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>.
Actiehouders	• 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>.

Bijlage A: Risicobereidheidsniveau's en -tabellen

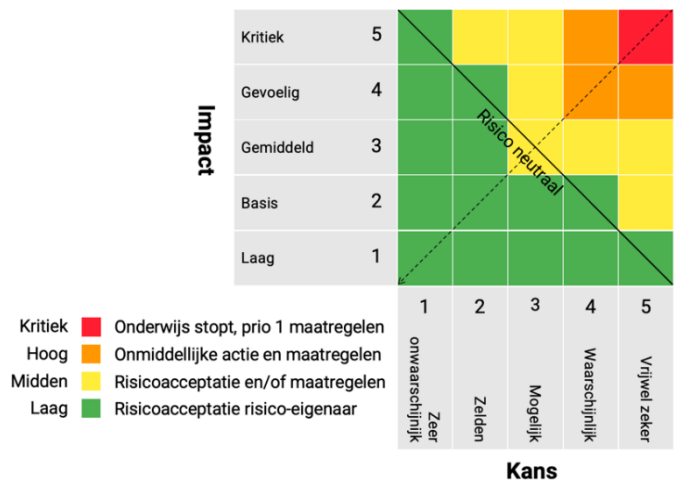
C.1 Risicomijdend

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.



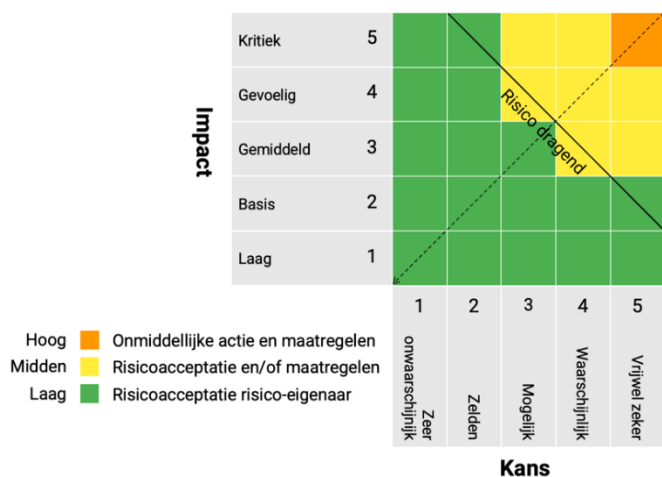
C.2 Risico-neutraal

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.



Bijlage B | 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.

Bijlage C | 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%