Afbeelding met Lettertype, tekst, schermopname, Graphics

Automatisch gegenereerde beschrijving

Leveranciersrisicomanagement  
proces

Voorbeelddocument

Versie: Februari 2025

Afbeelding met Kleurrijkheid, Graphics, blauw, patroon

Automatisch gegenereerde beschrijving

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

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je met het maken van een eigen leveranciersrisicomanagementproces. 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.

Afbeelding met biljartbal, symbool, cirkel

Automatisch gegenereerde beschrijving

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*](mailto: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](#_Toc191478108)

[2 Processtappen 5](#_Toc191478109)

[2.1 Oriëntatie 5](#_Toc191478110)

[2.2 Selectie en inkoop 6](#_Toc191478111)

[2.3 Implementatie 7](#_Toc191478112)

[2.4 Beheer en optimalisatie 7](#_Toc191478113)

[2.5 Uitfasering 8](#_Toc191478114)

[3 Procesrollen en verantwoordelijkheden 9](#_Toc191478115)

# Inleiding

Het proces voor leveranciersrisicomanagement is bedoeld om risico's van leveranciers op een gestructureerde manier effectief te beheren en te controleren. Deze procesbeschrijving beschrijft hoe het leveranciersrisicomanagementproces wordt uitgevoerd binnen <vul naam organisatie in>. Dit proces sluit aan bij het leveranciersrisicomanagementbeleid van <vul naam organisatie in> dat is vastgesteld in het IBP-beleid.

# Processtappen

***Toelichting***

* *Let op: Deze procesbeschrijving maakt gebruik van algemene stappen voor leveranciersmanagement. Als jouw organisatie al een eigen leveranciersmanagementproces heeft, voeg je de risicomanagementstappen uit deze procesbeschrijving toe aan je eigen leveranciersmanagementproces.*

Het proces voor leveranciersrisicomanagement is aan de hand van de generieke leveranciersmanagementstappen opgesteld en beperkt zich tot het managen van risico’s. Dit proces onderscheidt vijf nauw samenhangende stappen die binnen <vul naam organisatie in> samen zorgen voor een gestructureerde en veilige samenwerking met leveranciers. 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. De volgende stappen zijn gehanteerd:

1. Oriëntatie
2. Selectie en inkoop
3. Implementatie
4. Beheer en optimalisatie
5. Uitfasering

Hieronder lichten we elke stap toe.

## Oriëntatie

***Toelichting***

* *Let op: De uitwerking van deze stap beperkt zich tot het risicomanagement van leveranciers.*
* *Dit proces gaat ervan uit dat je de deelprojecten Classificatie van systemen en Beveiligingseisen en maatregelen vastleggen in securitybaselines al hebt uitgevoerd. Daarmee heb je een BIV-classificatiemethode en een securitybaseline geïmplementeerd. Heb je dit nog niet gedaan? Ga voor deze deelprojecten dan naar fase 1 en 2 van het Groeipad.*
* *Leveranciers die aan het privacy-convenant voldoen hebben al een BIV-classificatie uitgevoerd op hun systemen. Dit is echter de interpretatie van de leverancier. Zorg dat je altijd zelf het BIV-classificatieproces doorloopt.*

De stappen binnen de oriëntatiefase bestaan uit het opstellen van wensen en eisen voor het te contracteren product, waarna vervolgens een BIV-classificatie wordt uitgevoerd. Er volgt dan een marktonderzoek om potentiële leveranciers te identificeren.

De oriëntatiefase bestaat uit een aantal taken:

A. Wensen- en eisenlijst opstellen   
Stel wensen en eisen op voor het te contracteren product.

B. BIV-classificatie uitvoeren   
Voer een BIV-classificatie uit op basis van de eisen uit stap A of herzie de oude BIV-classificatie van het te vervangen systeem.

C. Maatregelen uit securitybaseline nagaan

Ga na welke maatregelen uit de securitybaseline van toepassing zijn op de ICT die moet worden ingekocht.

D. Marktonderzoek uitvoeren

Voer marktonderzoek uit om potentiële leveranciers te identificeren en een longlist op te stellen. Onderzoek welke leveranciers de ICT zouden kunnen leveren, en in hoeverre die aan de eisen kunnen voldoen.

## Selectie en inkoop

***Toelichting***

* *Let op: De uitwerking van deze stap beperkt zich tot risicomanagement van leveranciers.*
* *Op basis van de uitgevoerde BIV-classificatie in combinatie met de securitybaseline, volgt een lijst met maatregelen die dienen te worden toegevoegd aan de aanbestedingseisen. Bepaal zelf of er maatregelen ontbreken die wel dienen te worden meegenomen bij de aanbestedingseisen. Denk hierbij aan AVG-verplichtingen en het verwijderen en vernietigen van data.*

In deze fase bepaalt <vul naam organisatie in> welke producten of diensten nodig zijn en welke leveranciers deze kunnen leveren. Er wordt een selectieproces doorlopen waarbij de potentiële leveranciers worden beoordeeld op basis van criteria, zoals kwaliteit, prijs, betrouwbaarheid en risico's. Dit gebeurt aan de hand van de volgende taken:

A. Programma van eisen opstellen

Stel een programma van eisen op waarin minimaal de maatregelen die volgen uit de BIV-classificatie zijn opgenomen. Bepaal of boven op de maatregelen die volgen uit de BIV-classificatie de volgende onderwerpen van toepassing zijn en voeg deze toe aan het programma van eisen:

* Financiële stabiliteit en continuïteit van de leverancier;
* Naleving van wet- en regelgeving en bestaande kaders (bijv. AVG, ISO27001);
* Privacy-statement van de leverancier;
* <Vul aan met onderwerpen die standaard onderdeel moeten uitmaken van het programma van eisen>.

B. Leveranciers vergelijken

Vergelijk leveranciers op basis van het programma van eisen en controleer of ze de noodzakelijke maatregelen kunnen nemen zoals opgesteld in stap A.

C. Keuzes documenteren

Als we een leverancier kiezen die niet aan alle maatregelen kan voldoen, dan documenteren we deze keuze en besluiten of we dit risico accepteren of zelf aanvullende maatregelen nemen. <Pas deze tekst aan zodat duidelijk is wie de verantwoordelijkheid heeft om de risico’s te accepteren of aanvullende maatregelen te nemen>. Leg de uiteindelijke lijst met maatregelen inclusief de uitzonderingen vast.

D. Eisen contractueel vastleggen

Neem de eisen op in de opdrachtovereenkomst en eventueel de Service Level Agreement (SLA). <Pas aan indien er een andere contractvorm is die de organisatie hanteert waar deze eisen in opgenomen kunnen worden>. Laat het contract indien mogelijk toetsen door een jurist, of werk met een gestandaardiseerd contractmodel.

## Implementatie

***Toelichting***

* *Let op: De uitwerking van deze stap beperkt zich tot het risicomanagement van leveranciers.*

De implementatiefase richt zich op het integreren van het product in het bestaande ICT-landschap, waarbij wordt gewaarborgd dat dit gebeurt volgens de gemaakte afspraken. Tijdens deze stap beoordelen we in hoeverre de leverancier voldoet aan de overeengekomen eisen en worden eventuele afwijkingen gesignaleerd. Dit gebeurt aan de hand van de volgende taken:

A. Monitoren leverancier   
Monitor of de leverancier zich aan de gemaakte afspraken houdt door prestaties te volgen.

B. Afwijkingen vastleggen

Leg afwijkingen vast en bespreek deze met de leverancier om tijdig corrigerende maatregelen te nemen.

## Beheer en optimalisatie

***Toelichting***

* *Let op: De uitwerking van deze stap beperkt zich tot het risicomanagement van leveranciers.*
* *Na implementatie van het systeem, gaan we ervan uit dat dit is opgenomen in je configuratiemanagementdatabase (CMDB) en dat een systeemeigenaar is toegekend zoals beschreven in het configuratiemanagementproces. Dit doe je in het deelproject Classificatie van systemen in fase 1 van het Groeipad. Heb je dit nog niet gedaan? Doe dit dan eerst.*
* *Heb je beperkte tijd voor het voeren van leveranciersgesprekken (taak 2.4 A)? Prioriteer dan leveranciers van hoge-risicosystemen, omdat verstoringen hier een grote impact hebben op de continuïteit van onderwijsprocessen en het functioneren van de organisatie.*

De beheer- en optimalisatiefase richt zich op het waarborgen van de kwaliteit en op de naleving van afspraken met leveranciers. Tijdens deze fase wordt gecontroleerd of de leverancier blijft voldoen aan de vastgestelde eisen, worden prestaties geëvalueerd en worden afwijkingen of risico’s vroegtijdig gesignaleerd. Indien nodig kunnen verbeteringen of aanpassingen worden doorgevoerd om de dienstverlening te optimaliseren. Dit gebeurt aan de hand van de volgende taken:

A. Gesprekken met leveranciers voeren   
De systeemeigenaar is verantwoordelijk voor het voeren van gesprekken met de leveranciers, waarin minimaal de afgesproken eisen uit stap 2.2 D worden besproken. Indien zich informatiebeveiligingsincidenten hebben voorgedaan, bespreek hoe de leverancier hiermee is omgegaan.

B. Gespreksresultaten documenteren

Documenteer de resultaten van de leveranciersgesprekken in gespreksverslagen. Neem hierin minimaal op:

* bevindingen, zoals afwijkingen van beveiligingseisen of afspraken;
* afspraken voor verbeteringen;
* geplande acties en termijnen.

C. Verbeterafspraken maken

Als de leverancier niet voldoet aan de gemaakte afspraken uit taak 2.2 D worden verbeterafspraken gemaakt. Deze afspraken worden toegevoegd aan de gespreksverslagen.

## Uitfasering

***Toelichting***

* *Let op: De uitwerking van deze stap beperkt zich tot het risicomanagement van leveranciers.*

De uitfaseringsfase richt zich op het gecontroleerd beëindigen van de samenwerking met een leverancier en het veilig afsluiten van systemen. Dit kan nodig zijn bij het aflopen van een contract, de overstap naar een andere leverancier, of onverwachte situaties als contractbreuk of beveiligingsrisico’s. Met deze stap wordt gezorgd voor naleving van wettelijke eisen – zoals de AVG – en het beperken van schaduw-ICT of het voorkomen van verlies van cruciale data. Een goed voorbereide beëindiging voorkomt problemen en zorgt voor een gecontroleerde overgang. Dit gebeurt aan de hand van de volgende taak:

A. Afspraken maken over dataverwijdering en -vernietiging

Maak afspraken over dataverwijdering en het verbreken van verbindingen. Zorg ervoor dat de leverancier geen toegang meer heeft tot interne systemen en data. Controleer of alle gevoelige informatie en bedrijfsgegevens correct zijn overgedragen of vernietigd.

# Procesrollen en verantwoordelijkheden

***Toelichting***

* *Hier geef je aan welke rollen zijn betrokken bij het leveranciersrisicomanagementproces.*
* *Bij kleine besturen kunnen meerdere rollen bij dezelfde persoon worden belegd. Voor het operationeel beheren van de maatregelen en risico’s kun je de IBP'er, security officer of privacy officer om hulp vragen.*

De volgende rollen zijn binnen <vul naam organisatie in> betrokken bij het leveranciersrisicomanagementproces.

|  |  |
| --- | --- |
| **Rol** | **Verantwoordelijkheden** |
| **Eerste lijn** | |
| Bestuur, directie, schoolleiding | * Goedkeuren en vaststellen van het leveranciersrisicomanagementproces. * <Vul aan met verantwoordelijkheden.> |
| Verantwoordelijke voor inkoop | * Opstellen en beheren van contractuele afspraken. * <Vul aan met verantwoordelijkheden.> |
| Systeemeigenaar | * Monitoren of leverancier zich aan de gemaakte afspraken houdt door middel van leveranciersgesprekken. * Escaleren van incidenten of afwijkingen naar de IBP’er. * Opstellen van rapportages op basis van leveranciersgesprekken. * <Vul aan met verantwoordelijkheden.> |
| **Tweede lijn** | |
| Proceseigenaar | * Ontwikkelen en beheren van het leveranciersrisicomanagementproces. * Toezien op naleving van het proces en escaleren van afwijkingen. * Periodiek evalueren van het proces en verbeteringen doorvoeren. * <Vul aan met verantwoordelijkheden.> |
| IBP’er, security officer of privacy officer | * Ondersteunen bij het vaststellen van mitigerende maatregelen of het accepteren van het risico wanneer een leverancier niet volledig kan voldoen aan de maatregelen die zijn opgenomen in het programma van eisen. * Inhoudelijk ondersteunen bij gesprekken met leveranciers over de contractueel vastgelegde maatregelen. * <Vul aan met verantwoordelijkheden.> |