# <Pagina> Stappenplan risicobeoordeling

*<Intro> Deze module**beschrijft een methode voor risicobeoordeling in vorm van een stappenplan. Ook gaat de module in op de hulpmiddelen die daarbij gebruikt kunnen worden.*

Deze module beschrijft een werkwijze voor risicobeoordeling aan de hand van een stappenplan. Ruwweg bestaat deze werkwijze uit drie fases:

* Een **voorbereiding**, die leidt tot een plan van aanpak
* De **uitvoering** van de risicobeoordeling, die leidt tot conclusies over welke risico’s bestaan en hoe ernstig die zijn
* De afrondende fase waarin over de conclusies **gecommuniceerd** wordt met managers zodat die prioriteiten kunnen stellen en daaraan acties kunnen verbinden.



# <subpagina>Stap 1: Bereid je voor

*<intro>Hoe begin je met risicobeoordeling? Wat moet je geregeld hebben? Kortom: hoe bereid je je voor?*

Een goed begin is het halve werk. Het opstellen van een duidelijk en concreet plan van aanpak helpt bij het krijgen van draagvlak en een opdracht voor risicobeoordeling. En door de juiste collega’s actief te betrekken bij het proces van risicobeoordeling, leg je de basis voor meer bewustwording en vergroot je de kans dat de resultaten van een risicobeoordeling ook doorvertaald worden naar acties.

|  |  |
| --- | --- |
| Actie | Geef antwoord op de volgende vragen |
| Onderzoek de context | Wat is er binnen je organisatie geregeld op het gebied van risicobeoordeling? |
| Bepaal het niveau | Richt je je op een bedrijfsproces of op een individuele applicatie daarbinnen? |
| Bepaal het onderwerp | Waar ga je naar kijken? Naar welke processen en/of applicaties? |
| Stel een team samen | Wie gaat het doen?  |

Houd goed bij welke keuzes je maakt bij het opstellen van een plan van aanpak risicobeoordeling. En leg vast wat je bij het uitvoeren van de beoordeling allemaal vaststelt. Dit kan ook gebruikt worden in rapportage achteraf en bij verantwoording richting auditors of toezichthouders.

## <uitklapmenu>Onderzoek de context

Om een risicobeoordeling goed uit te voeren, is het waardevol om aan te sluiten bij wat er binnen jouw organisatie geregeld is op het gebied van risicobeoordeling. Zo bereik je betere resultaten. Hetzelfde geldt voor aansluiten op wat binnen jouw organisatie geprioriteerd wordt.

Onderzoek wat er al georganiseerd wordt op het gebied van risicobeoordeling. Stel daarbij de volgende vragen:

* Welk beleid is er op het gebied van risicobeoordeling?
* Zijn er risicoprofielen en beheerregimes vastgesteld?
* Zijn de rollen en verantwoordelijkheden hierbij duidelijk en wordt dit ook zo uitgevoerd?
* Is er een PDCA-cyclus voor risicobeoordeling ingericht?
* Welke risicobeoordelingen worden er al uitgevoerd in jouw organisatie? Is er al een auditproces waarbij je kunt aansluiten?
* Zijn er al auditrapporten of andere rapporten gepubliceerd waarin cruciale processen en/of risico’s van de organisatie worden benoemd?
* Wat wordt er georganiseerd op het gebied van risicobeoordeling door de andere I-domeinen (privacy, informatiebeveiliging en openbaarmaking)?
* Maakt je organisatie gebruik van *tooling* voor Governance, Risk Management and Compliance (GRC) om risicobeoordeling te kunnen uit voeren en vast te leggen?

Als deze zaken niet zijn belegd voor je organisatie, en er dus geen bestaande benadering is rondom risicobeoordeling, dan is een *ad hoc* traject risicobeoordeling mogelijk. Zo’n op zichzelf staand traject kan leiden tot nuttige inzichten. Maar voor organisaties die niet kiezen voor een systematische werkwijze op het gebied van risicomanagement, ontstaat het risico dat ze belangrijke risico’s over het hoofd zien. Wanneer je dus vaststelt dat je niet aan kunt sluiten bij een bestaande werkwijze omdat die niet bestaat, is het goed om ook dát risico te benoemen en aan besluitvoerders mee te geven.

### <kop>Never let a good crisis go to waste

Bij het plannen van een traject voor risicobeoordeling neem je niet de alleen formele zaken mee die hierboven genoemd zijn. Je kijkt ook naar lopende zaken die zorgen voor reuring binnen een organisatie. Een aankomende reorganisatie kan bijvoorbeeld aanleiding zijn om eens tegen het licht te houden welke risico’s er binnen bedrijfsprocessen aanwezig zijn voor wat betreft duurzame toegankelijkheid. Datzelfde geldt voor incidenten zoals een data-lek of een kritisch inspectierapport. Eventuele negatieve aandacht die daaruit voortkomt, kan ertoe leiden dat je organisatie meer dan voorheen wil weten welke risico’s er bestaan op het gebied van informatiebeheer.

## <uitklapmenu>Kijk je naar een proces of naar een applicatie?

Het is goed om van te voren scherp te hebben, wat precies het onderwerp van je risicobeoordeling wordt. Je kunt hierbij kiezen voor een bestaand **bedrijfsproces**. In dat geval heeft de risicobeoordeling betrekking op de manier waarop dit bedrijfsproces ondersteund wordt door duurzaam toegankelijke overheidsinformatie. Je brengt dus in kaart op welke manieren het bedrijfsproces kwetsbaar is als overheidsinformatie *niet* duurzaam toegankelijk is.

Een **tweede optie** is om een **specifieke applicatie** te beoordelen. Dat kan gaan om een bestaande applicatie die een belangrijke rol speelt binnen een of meerdere bedrijfsprocessen. In dit geval beoordeel je of duurzame toegankelijkheid van overheidsinformatie door deze applicatie voldoende ondersteund wordt. En wat de negatieve uitkomsten kunnen zijn, als dat niet zo is. Een risicobeoordeling van dit type kan relevant zijn om te bepalen of een applicatie nog mee kan (met eventuele aanpassingen), of aan vervanging toe is.

Een **derde optie** is het **beoordelen van een nieuwe applicatie** die nog niet is aanbesteed of ingericht. In dat geval sluiten informatieprofessionals aan bij het treffen van passende maatregelen bij het inrichten van een nieuwe applicatie. De risicobeoordeling brengt in kaart of verschillende opties voor inrichting in voldoende mate zorg dragen voor duurzame toegankelijkheid. Bij een aanbesteding worden keuzes gemaakt, de risicobeoordeling laat zien welke risico’s iedere keuze met zich meebrengt. Zo kun je een afgewogen besluit nemen.

## <uitklapmenu> Welke processen en applicaties neem je mee?

Binnen je organisatie worden meerdere bedrijfsprocessen uitgevoerd en die processen worden ondersteund door meerdere applicaties die zorgdragen voor duurzame toegankelijkheid van overheidsinformatie. Vaak gaat het om tientallen processen en honderden applicaties. Bij het uitvoeren van risicobeoordeling richt je je in beginsel op de belangrijkste processen en de meest wezenlijke applicaties. Deze processen en applicaties zijn de steunpilaren van de organisatie en het is van cruciaal belang om risico’s op het gebied van duurzame toegankelijkheid daarbinnen in beeld te hebben en zoveel mogelijk te mitigeren.

Het helpt hierbij om te beschikken over een zo volledig mogelijk overzicht van de informatiehuishouding binnen jouw organisatie. Het hebben van een overzicht (eventueel op basis van architectuur) is [een randvoorwaarde (RVW08)](https://www.nationaalarchief.nl/archiveren/kennisbank/randvoorwaarden-generiek-deel) binnen het DUTO-raamwerk.

De volgende factoren bepalen mede of het gaat om een kritiek bedrijfsproces dan wel een kritieke applicatie:

* Er worden [bijzondere persoonsgegevens](https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacy-en-persoonsgegevens/wat-zijn-persoonsgegevens#bijzondere-persoonsgegevens)beheerd en gebruikt;
* Er wordt informatie beheerd en gebruikt die vaak nodig is om informatievragen te beantwoorden en aan Woo-verzoeken te voldoen;
* Er wordt informatie beheerd en gebruikt die op grond van de Woo [actief openbaar](https://www.informatiehuishouding.nl/projecten/actieve-openbaarmaking-overheidsinformatie/documenten/publicaties/2024/10/22/handreiking-openbaar-maken-doe-je-zo---conceptversie) gemaakt moet worden;
* Er wordt informatie in beheerd en gebruikt die van *hoge waarde* is, bijvoorbeeld omdat die *jarenlang nodig is voor bedrijfsprocessen en/of blijvend te bewaren* is;
* Het gaat om informatie die dusdanig gevoelig of vertrouwelijk is, dat een *datalek* een onacceptabel groot is;
* Het gaat om een proces of een applicatie waarvan *de impact van uitval* onacceptabel groot is

## <uitklapmenu>Stel een team samen

Wanneer je de scope van de risicobeoordeling hebt bepaald, en je een helder beeld hebt van de context waarbinnen je opereert, kun je zorgen dat de juiste collega’s aanhaken bij de risicobeoordeling die je in de planning hebt. Je trekt hierbij samen op met:

* Collega’s met verantwoordelijkheid voor specifieke bedrijfsprocessen of applicaties
* Collega’s uit andere i-domeinen
* Externe collega’s die een rol spelen binnen organisatie-overstijgende processen

Risicobeoordeling is een teamsport. Het doel van risicobeoordeling met een focus op duurzame toegankelijkheid is om bedrijfsonderdelen te helpen bij hun werk. De risicobeoordeling brengt in kaart welke risico’s bestaan als de informatie waar ze mee werken niet duurzaam toegankelijk is. Het maakt inzichtelijk voor collega’s hoe informatiebeheer hun werk beïnvloedt, en helpt ze om hierin keuzes te maken en prioriteiten te stellen.

Hetzelfde geldt voor andere i-domeinen (specialisten op gebied van privacy, informatiebeveiliging en openbaarmaking onder de Woo). Duurzame toegankelijkheid van overheidsinformatie is ook van belang voor deze domeinen.

# <subpagina>Stap 2: Voer de risicobeoordeling uit

*<intro>Nadat je scope, context en criteria hebt bepaald, volgt stap 2 binnen deze module. Dat is het uitvoeren van de risicobeoordeling zelf.*

Het uitvoeren van de risicobeoordeling is de hoofdmoot van het proces. In deze fase breng je in kaart welke risico’s kunnen bestaan, analyseer je of deze risico’s daadwerkelijk aanwezig zijn, en beoordeel je hoe ernstig de risico’s zijn.

## <uitklapmenu>Identificeren

Als overheidsinformatie niet duurzaam toegankelijk is, brengt dat verschillende soorten risico’s met zich mee. Binnen deze handreiking maken we onderscheid tussen risico’s op het gebied van legitimiteit, efficiëntie, en meerwaarde voor de samenleving. Deze categorieën zijn afgeleid uit [module 1 van het DUTO-raamwerk](https://www.nationaalarchief.nl/archiveren/kennisbank/module-1-de-waarde-van-de-duurzame-toegankelijkheid). Ze sluiten ook aan op de methodiek ‘Basis Beveiligingsniveau (BBN)’ die in het kader van [de Baseline Informatiebeveiliging Overheid (BIO)](https://www.bio-overheid.nl/) is ontwikkeld.

| **Type** | **Risico***Als overheidsinformatie niet duurzaam toegankelijk is, dan …* |
| --- | --- |
| Besluitvorming | … kunnen bestuurders geen goed onderbouwde besluiten nemen |
| Kosten | … nemen de kosten voor informatiebeheer en bedrijfsvoering toe |
| Milieubelasting | … neemt de milieubelasting die met data-opslag gemoeid is toe. |
| Tijdverlies | … zijn medewerkers relatief meer tijd kwijt aan dezelfde taken |
| Moreel medewerkers | … neemt het werkplezier af  |
| Reconstructie | … wordt het moeilijker om intern en extern verantwoording af te leggen  |
| Naleving informatiewetgeving | … is de organisatie minder in staat om tegemoet te komen aan de vereisten die vanuit informatiewetgeving gesteld worden |
| Naleving overige wetgeving | … is de organisatie minder in staat om te voldoen aan vereisten die vanuit sectorale wetgeving gesteld worden |
| Dienstverlening | … wordt het minder waarschijnlijk dat de organisatie doelstellingen behaalt op het gebied van dienstverlening aan het publiek  |
| Vertrouwen bij het publiek | … neemt de kans toe dat het imago van de organisatie schade oploopt en dat het vertrouwen bij het publiek neemt |
| Vertrouwen bij partners | … neemt de kans toe dat partners (bijvoorbeeld: ketenpartijen) vertrouwen verliezen in onze organisatie |

Dit is een generieke lijst. Pas deze lijst aan, zodat deze risicotypes goed aansluiten bij jouw organisatie, bijvoorbeeld door te benoemen *welke* sectorale wetgeving alleen nageleefd kan worden als informatiebeheer op orde is. En door expliciet te maken welke relaties van jouw organisatie rusten op goed informatiebeheer. Je kunt ook besluiten om aan bepaalde risico’s een hogere weging toe te kennen.

Zorg verder dat de zaken waaraan jouw organisatie veel waarde hecht, ook meegenomen worden. Dit kan aan de hand van zogenoemde kroonjuwelen: thema’s die bij management van de organisatie leven en die bijdragen aan missie en visie van de organisatie.

* Als er zorg bestaat over imagoschade, benoem dat dan, en laat krantenkopjes zien om negatieve berichtgeving te illustreren.
* Als milieu speelt, zet dan in op de milieubelasting van data-opslag die toeneemt naarmate er niet of te laat vernietigd wordt.
* Illustreer de impact van gebrekkig informatiebeheer op de bedrijfsvoering met termen zoals ‘infobesitas’ en [‘dementerende overheid’](https://www.inspectie-oe.nl/publicaties/publicatie/2021/02/09/een-dementerende-overheid-2.0).

Verbind deze kroonjuwelen met het belang van duurzame toegankelijkheid. En benoem de risico’s die gebrekkig informatiebeheer kan vormen voor deze kroonjuwelen.

Betrek de betrokken afdelingen bij het bepalen van risico’s. Waar loop je tegenaan? Ik kan niets vinden? Voer deze gesprekken samen met de proceseigenaren, zodat zij direct betrokken worden.

### <kop>Risico’s per DUTO-proces

Om duurzame toegankelijkheid te borgen binnen een bedrijfsproces, moet informatiebeheer ingericht worden aan de hand van de vijf [DUTO-processen](https://www.nationaalarchief.nl/archiveren/kennisbank/duto-processenmodel): registreren, vernietigen, bewaren, migreren, ter beschikking stellen. DUTO-processen worden ingericht door invulling te geven aan [randvoorwaarden](https://www.nationaalarchief.nl/archiveren/kennisbank/randvoorwaarden-generiek-deel) (op de organisatielaag) en door [DUTO-functies](https://www.nationaalarchief.nl/archiveren/kennisbank/duto-functiemodel) in te richten binnen de applicatielaag.

Per DUTO-proces breng je de risico’s in kaart die ontstaan als dat proces niet of onvoldoende ingericht is. Alle DUTO-processen moeten ingevuld worden, maar in specifieke situaties kun je er voor kiezen om bij de risicobeoordeling aan een of twee DUTO-processen meer aandacht te besteden dan aan de anderen.

Bijvoorbeeld:

* Je onderzoekt in het bijzonder het vermogen om tijdig te **vernietigen** wanneer het gaat om een bedrijfsproces waarbinnen datalekken als zeer ernstig beschouwd worden.
* Je richt je extra op **bewaren** en **migreren** naar mate het gaat om bedrijfsprocessen waarin overheidsinformatie jarenlang beheerd en gebruikt wordt. In dat geval is het aannemelijk dat de informatie langer meegaat dan de applicaties en bestandsformaten die op het moment van de risicobeoordeling in gebruik zijn.

Onderstaande tabel werkt dit uit voor het DUTO-proces Registreren. Niet alle risicotypes komen terug bij ieder DUTO-proces.

|  |  |
| --- | --- |
| **Type** | **Risico***Als het DUTO-proces registreren dit bedrijfsproces niet/onvoldoende ondersteunt, dan …* |
| Besluitvorming | … wordt essentiële informatie niet meegenomen bij belangrijke besluiten |
| Tijdverlies | … zijn gebruikers langer op zoek naar informatie die ze nodig hebben, bijvoorbeeld omdat de juiste metagegevens niet zijn toegekend |
| Reconstructie | … neemt het risico toe dat besluitvorming naderhand niet gereconstrueerd kan worden |
| Naleving overige wetgeving | … neemt de kans toe dat bepaalde procedures niet goed gevolgd kunnen worden, met juridische consequenties |
| Dienstverlening | … neemt de kans toe dat lopende zaken niet goed afgehandeld worden |
| Vertrouwen bij het publiek | … kan het vertrouwen bij het publiek daaronder leiden, bijvoorbeeld omdat burgers gevraagd wordt om dezelfde informatie meerdere malen aan te leveren. |

## <uitklapmenu> Analyseren

Om te beoordelen of DUTO-processen binnen een bedrijfsproces gerealiseerd worden, ga je na of de randvoorwaarden aanwezig zijn. En je bepaalt of de benodigde DUTO-functionaliteit is ingericht binnen de applicaties die een bedrijfsproces ondersteunen. Je pelt de organisatie af als een ui, van algemeen (concern-breed) naar specifieke (individuele applicaties).

* Organisatiebreed: Wat is er al geregeld aan **generieke randvoorwaarden** voor duurzame toegankelijkheid? Als er bijvoorbeeld geen vastgestelde selectielijst is die actief geïmplementeerd wordt ([RVW13 binnen het DUTO-raamwerk](https://www.nationaalarchief.nl/archiveren/kennisbank/randvoorwaarden-generiek-deel)), dan vormt dat een risico voor de gehele organisatie.
* Bedrijfsproces: Worden **DUTO-processen** ondersteund, en zijn randvoorwaarden ook hier geborgd (naast generieke randvoorwaarden zijn er specifieke randvoorwaarden opgesteld voor individuele DUTO-processen)
* Binnen applicaties: Wordt de benodigde **DUTO-functionaliteit** gerealiseerd?

Als je risicobeoordeling zich primair richt op een specifieke applicatie, dan zul je meer aandacht besteden aan DUTO-functies en minder aan randvoorwaarden.

### <kop>Detailniveau

Bij de analyse van applicaties kun je kiezen voor een hoog-over benadering, waarbij je een paar relatief simpele vragen beantwoordt. Bijvoorbeeld:

* Kan deze applicatie **vernietigen**?
* Is er een **procedure** voor vernietigen (inclusief beleid voor backups)?

Of voor een meer gedetailleerde analyse, waarbij je diezelfde vraag opbreekt in meerdere vragen aan de hand van DUTO-functies die de DUTO-processen ondersteunen (voor het DUTO-proces vernietigen zijn dat er zes). Zijn deze aanwezig?

* Is **metagegevensbeheer** gerealiseerd binnen deze applicatie?
* Is **toegangsbeheer** gerealiseerd binnen deze applicatie?
* Is **validatie** gerealiseerd binnen deze applicatie?
* Is **verantwoording** gerealiseerd binnen deze applicatie?
* Is **vernietiging** gerealiseerd binnen deze applicatie?
* Is **zoeken** gerealiseerd binnen deze applicatie?

Voor het hoogste detailniveau kun je een selectie maken uit de modeleisen die voor de DUTO-processen zijn opgesteld. Voor het DUTO-proces Vernietigen dat we hier als voorbeeld gebruiken, zijn er in totaal [negentien modeleisen](https://www.nationaalarchief.nl/archiveren/kennisbank/modeleisen-vernietigen).

Tip: neem bij het beoordelen van applicaties niet alleen mee of deze *op het moment van de risicobeoordeling* bepaalde DUTO-functionaliteit bieden, maar ook of ze dat in de toekomst zullen blijven doen. Als duidelijk is dat een applicatie op voorzienbare tijd haar *end of life* zal bereiken, dan heeft dat implicaties voor de borging van DUTO binnen je organisatie. In dit geval is het van belang om na te gaan of de juiste voorzieningen zijn getroffen op het gebied van het DUTO-proces Migreren. En om te zorgen dat je betrokken wordt bij het aanbesteden en inrichten van een nieuwe applicatie.

## <uitklapmenu>Evalueren

De resultaten van de analyse laten zien welke risico’s bestaan. Nu is het nodig om conclusies te trekken: hoe ernstig zijn de risico’s? Om te kunnen prioriteren, is het nuttig om risico’s te ordenen (bijvoorbeeld: hoog, middel, laag). Stel criteria op om objectief te bepalen welk niveau van toepassing is. Dit draagt bij aan consistentie en zorgt dat verschillende analisten in dezelfde situatie tot dezelfde conclusie komen.

|  |
| --- |
| Dit onderdeel van het proces is nog niet nader uitgewerkt |

# <subpagina>Stap 3: Communiceren en implementeren

<intro>De conclusies van de risicobeoordeling laten zien welke risico’s bestaan en hoe ernstig ze zijn. De laatste stap van het proces is om deze conclusies te delen. En te zorgen dat er waar nodig actie wordt ondernomen.

De kern is dat er advies gegeven wordt aan management welke risico’s er bestaan binnen bedrijfsprocessen of applicaties, hoe ernstig deze risico’s zijn, en welke oplossingen er bestaan.

* Breng risico’s en de gevolgen zo concreet mogelijk in kaart. Wat levert het op, wat kost het, hoeveel tijd en medewerkers ben je kwijt?
* Spreek hierbij niet alleen in negatieve zin over risico’s, maar ook over positieve uitkomsten. Bijvoorbeeld: ‘we kunnen geld besparen’ in plaats van ‘we zijn nu veel geld kwijt’
* Beschrijf scenario’s en bied opties, inclusief ‘niets doen’. Een bewuste keuze om een risico te accepteren is iets heel anders dan een risico voort laten bestaan omdat niet bekend is dat het überhaupt bestaat.
* Identificeer *quick wins*: relatief eenvoudige en betaalbare oplossingen die zonder veel inzet grote risico’s weg kunnen nemen voor de organisatie.

|  |
| --- |
| Dit onderdeel van het proces is nog niet nader uitgewerkt |