# <pagina>Wat is een risico?

Het beoordelen van risico’s, in het bijzonder op het gebied van informatiebeheer, staat centraal in deze handreiking. Voordat je start met een DUTO-risicobeoordeling, is het belangrijk te weten wat onder de term risico wordt verstaan.

Deze module gaat over:

* Wat een risico is en
* Hoe je deze beschrijft
* Welke implicaties en kansen risico’s kunnen hebben
* Hoe je risico’s beoordeelt

## <kop> Wat is een risico?

In deze handreiking gebruiken we de volgende definitie voor ‘risico’: **Risico is het gevolg van onzekerheid op het behalen van je doelen.** Deze definitie is afgeleid uit NEN-ISO norm 31000 (Risicomanagement – Richtlijnen)

Binnen overheidsorganisaties is er altijd een mate van **onzekerheid** aanwezig. Het is niet zeker dat zaken precies zo lopen als je had verwacht. Door te erkennen dat deze onzekerheid er is, kun je ook maatregelen treffen om je hierop voor te bereiden en passend te reageren.

Als zaken anders lopen dan gepland kan dit **gevolgen** hebben voor de organisatiedoelen. Soms kan dit positief zijn doordat een aanpassing in het proces leidt tot een betere dienstverlening richting de burger, tevreden klanten en meer vertrouwen. Maar het kan ook leiden tot financiële schade voor een organisatie.

Overheidsorganisaties hebben **doelstellingen** die ze willen bereiken. Het werk wordt zodanig georganiseerd dat deze doelstellingen worden gehaald. Door in te spelen op onzekerheden die doelstellingen kunnen bedreigen, kun je als organisatie jezelf verbeteren en doelstellingen blijven behalen.

## <kop> Hoe beschrijf je een risico?

Nu we weten wat een risico is, kunnen we deze beschrijven. Een goede risicobeschrijving bevat de volgende onderdelen:

1. De **bron van het risico** is een feit waardoor het risico ontstaat.
2. Een mogelijke **gebeurtenis** die voortkomt uit de bron van het risico.
3. De **implicaties** van die gebeurtenis voor de doelstellingen van de overheidsorganisatie.

Aan de hand van deze elementen kun je een risico beschrijven in de vorm van een drietrapsraket:

|  |  |  |
| --- | --- | --- |
| **Doordat** *(bron risico)* | **Bestaat de kans dat** *(gebeurtenis)* | **Met als gevolg** *(implicatie)* |
| de procedure voor digitaal vernietigen niet wordt uitgevoerd | te vernietigen gegevens in vakapplicatie X te lang bewaard worden. | dat organisatie niet rechtmatig handelt en juridische claims kan verwachten.  |
| in het migratieproces alleen de actuele gegevens van applicatie A naar B worden gemigreerd  | de overige gegevens niet of versnipperd worden beheerd.  | dat overheidsinformatie niet of nauwelijks in samenhang gevonden kan worden.  |
| er binnen werkproces X geen duidelijke afspraken zijn over het gebruik van metagegevens  | overheidsinformatie binnen werkproces X niet te vinden of te interpreteren is. | dat dienstverlening aan de burger kan verslechteren. |

Een goede, concrete risicobeschrijving helpt bij het maken van weloverwogen keuzes over welke maatregelen te treffen. Daarom maak je zoveel mogelijk duidelijk waarop het risico betrekking heeft binnen het informatiesysteem. Bijvoorbeeld een specifiek bedrijfsproces of een applicatie daarbinnen.

## <kop> Implicaties en kansen

Deze handreiking richt zich op de mogelijke risico’s rondom duurzame toegankelijkheid van overheidsinformatie. Als de duurzame toegankelijkheid van overheidsinformatie niet voldoende in de overheidsorganisatie geborgd is, heeft dat verschillende implicaties. Binnen deze handreiking maken we onderscheid tussen gevolgen op het gebied van:

* Publieke waarde (meerwaarde voor samenleving)
* Legitimiteit (voldoen aan wet- en regelgeving)
* Organisatie (effectieve en efficiënte uitvoering van taken)

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. De categorieën zijn verwerkt in onderstaande lijst. De gevolgen, kansen en mogelijkheden zijn algemeen beschreven. Maak deze specifiek voor jouw organisatie. Bijvoorbeeld door te benoemen *welke* sectorale wetgeving alleen nageleefd kan worden als informatiebeheer op orde is. En wat er leeft binnen de organisatie.

| **Soort risico** | **Gevolgen** *Als duurzame toegankelijke overheidsinformatie* ***onvoldoende*** *geborgd is, dan …* |
| --- | --- |
| Besluitvorming | … kunnen door het ontbreken van duidelijk [metagegevensbeheer](https://www.nationaalarchief.nl/archiveren/kennisbank/randvoorwaarden-generiek-deel) bestuurders geen goed onderbouwde besluiten nemen. |
| Kosten en milieubelasting  | … kunnen door het [niet tijdig vernietigen](https://www.nationaalarchief.nl/archiveren/kennisbank/module-5-duto-proces-vernietigen) van overheidsinformatie de opslagkosten toenemen. En daarmee de belasting voor het milieu die met deze opslag gemoeid is.  |
| Tijdverlies en moreel medewerkers | …kunnen door het ontbreken van een goede [zoekfunctie](https://www.nationaalarchief.nl/archiveren/kennisbank/duto-functiemodel) medewerkers onnodig veel tijd kwijt raken aan het uitvoeren van taken. Dit heeft een negatief effect op het werkplezier.  |
| Reconstructie | … wordt het door het ontbreken van [betrouwbare en interpreteerbare overheidsinformatie](https://www.nationaalarchief.nl/archiveren/kennisbank/module-2-de-duto-kenmerken) moeilijker om verantwoording af te leggen over het handelen |
| Naleving informatie-wetgeving | … is de organisatie door het ontbreken van (onder andere) goed [toegangsbeheer](https://www.nationaalarchief.nl/archiveren/kennisbank/randvoorwaarden-generiek-deel) minder in staat om tegemoet te komen aan de vereisten die vanuit informatiewetgeving zoals de BIO gesteld worden |
| Naleving overige wetgeving | … is de organisatie minder in staat om te voldoen aan vereisten die vanuit sectorale wetgeving gesteld worden  |
| Dienstverlening | … kan door het [niet tijdig vinden](https://www.nationaalarchief.nl/archiveren/kennisbank/module-2-de-duto-kenmerken) van overheidsinformatie de dienstverlening aan de burger in de knel komen.  |
| Vertrouwen bij burgers en ketenpartners  | … kan door onbetrouwbare overheidsinformatie beschikbaar te stellen aan burgers en ketenpartners de kans toenemen dat het vertrouwen bij de burgers en ketenpartners wordt geschaad |

Daarnaast kun je ook duidelijk maken wat de kansen en mogelijkheden zijn wanneer duurzame toegankelijkheid goed geregeld is:

| **Soort risico** | **Kansen en mogelijkheden** *Als duurzame toegankelijke overheidsinformatie* ***voldoende*** *geborgd is, dan …* |
| --- | --- |
| Besluitvorming | … kan de overheidsorganisatie duidelijker aantonen wat ze besluit omdat de overheidsinformatie [betrouwbaar en goed te interpreteren](https://www.nationaalarchief.nl/archiveren/kennisbank/module-2-de-duto-kenmerken) is. |
| Kosten en milieubelasting  | … wordt er bijvoorbeeld door het ontdubbelen van gegevens, tijdige vernietiging bespaard op kosten voor opslag en het [verminderen van de klimaatlast.](https://www.nationaalarchief.nl/archiveren/kennisbank/organisatie#collapse-141736)  |
| Tijdverlies en moreel medewerkers | … is de medewerker minder tijd kwijt aan het uitvoeren van zijn taken omdat overheidsinformatie makkelijk te [vinden](https://www.nationaalarchief.nl/archiveren/kennisbank/module-2-de-duto-kenmerken) is. Dit bevordert het werkplezier.  |
| Reconstructie | … stelt het de overheidsorganisatie in staat om transparant te zijn over haar eigen handelen. Ze stelt overheidsinformatie [beschikbaar](https://www.nationaalarchief.nl/archiveren/kennisbank/module-2-de-duto-kenmerken) aan degenen die er recht op hebben of maakt deze actief openbaar op basis van de Woo . |
| Naleving informatie- wetgeving | … door onder andere tijdig te vernietigen en te zorgen voor betrouwbare informatie voldoet de overheidsorganisatie aan wet-en regelgeving als [de AVG en BIO](https://www.nationaalarchief.nl/archiveren/kennisbank/legitimiteit#collapse-141730).  |
| Naleving overige wetgeving | … is de organisatie in staat om makkelijker te voldoen aan vereisten die vanuit [sectorale wetgeving](https://www.nationaalarchief.nl/archiveren/kennisbank/legitimiteit#collapse-141730) gesteld worden |
| Dienstverlening | … kan de overheidsorganisatie met betrouwbare overheidsinformatie [goede dienstverlening](https://www.nationaalarchief.nl/archiveren/kennisbank/publieke-waarde#collapse-141721) leveren.  |
| Vertrouwen bij burgers en ketenpartners  | … kan de overheidsorganisatie onder andere [verantwoording](https://www.nationaalarchief.nl/archiveren/kennisbank/legitimiteit#collapse-141730) afleggen richting de burger en andere belanghebbenden. … is er vertrouwen binnen een [ketensamenwerking](https://www.nationaalarchief.nl/archiveren/kennisbank/organisatie#collapse-141735) omdat er gebruik wordt gemaakt van dezelfde (bron)informatie  |

Deze lijsten kunnen gebruikt worden in de stappen 4 en 5 van het stappenplan DUTO- risicobeoordeling.

## <kop>Hoe beoordeel je een risico?

Nadat je de risico’s hebt beschreven, wil je ook inzichtelijk maken hoe groot of klein een risico is voor jouw organisatie. Wat zijn de aard en omvang van de gevolgen? De handreiking hanteert een veel gebruikte scoringsmethode waarbij de **kans (K)** dat een gebeurtenis plaatsvindt, wordt gekoppeld aan de **impact (I)** die dat kan hebben. Door de kans score en impact score met elkaar te vermenigvuldigen, ontstaat een risicoscore. Je kunt aan de hand van hoogte van de score bepalen of er sprake is van een laag risico of een extreem risico en alles ertussen in.

In het <link naar stap 6>stappenplan wordt deze methode nader uitgewerkt.