# <pagina>Wat is een risico?

Het begrip risico staat centraal in deze handreiking. Voor managers werken we uit wat organisaties op orde moeten hebben om risicomanagement goed in te richten en onderdeel te maken van de manier waarop zij sturen en besluiten nemen. Het uitvoeren van een DUTO-risicobeoordeling is daar een essentieel onderdeel van – zo krijg je in beeld welke risico’s bestaan op het gebied van informatiebeheer. En hoe ernstig die zijn. Het stappenplan DUTO-risicobeoordeling vormt een concrete methodiek om zo’n risicobeoordeling uit te voeren.

Voordat je start met het (laten) uitvoeren van een DUTO-risicobeoordeling, is het belangrijk te weten wat onder de term risico wordt verstaan.

Deze module beschrijft:

* de term risico
* het verschil tussen risico’s, effecten en uitkomsten
* hoe je risico’s beschrijft en meet

## <kop>Definitie

In deze handreiking hanteren we de volgende **definitie van risico**:

Het effect van onzekerheid op het behalen van doelstellingen.

Bron: NEN-ISO 31000:2018+C11:2019 (Richtlijnen Risicomanagement)

De definitie bevat drie belangrijke onderdelen:

|  |  |
| --- | --- |
| **Onzekerheid** | Overheidsorganisaties kunnen er niet van uitgaan dat altijd alles loopt zoals verwacht. Aangename en onaangename verrassingen liggen op de loer. Wanneer je erkent dat deze onzekerheid bestaat, kun je ook maatregelen treffen om onverwachte omstandigheden tijdig waar te nemen en passend daarmee om te gaan.  |
| **Effect**  | Als zaken anders lopen dan verwacht, kan dit positieve en negatieve effecten hebben voor de belangen en doelstellingen van een overheidsorganisatie. In het positieve geval kan het kansen en mogelijkheden bieden voor een overheidsorganisatie.  |
| **Doelstellingen** | Overheidsorganisaties formuleren doelstellingen voor zichzelf. Deze worden vaak gekoppeld aan de strategie om deze te bereiken.  |

Voorbeelden van doelstellingen zijn:

* In 2026 is het Nationaal Archief zichtbaar en erkend als expertisecentrum op het gebied van duurzame toegankelijkheid.
* Het [Rijksbrede programma Open Overheid](https://www.open-overheid.nl/over-open-overheid#:~:text=Het%20Rijksbrede%20programma%20Open%20Overheid,goed%20functioneren%20van%20de%20overheid.) heeft zich tot doel gesteld om de openheid van de Rijksoverheid te vergroten en haar informatiehuishouding en -voorziening te verbeteren
* Een van de doelstellingen van de [VNG](https://vng.nl/rubrieken/over-de-vng#:~:text=Het%20doel%20van%20de%20VNG,maatschappelijke%20opgaven%20centraal%20te%20stellen.) is om de krachten van gemeenten te bundelen en gezamenlijk op te treden in het belang van de lokale overheid en haar inwoners.
* Het doel van overheidsorganisatie X is om goede dienstverlening te bieden en klanttevredenheid te vergroten.

## <kop>Hoe beschrijf je een risico?

Bij het beschrijven van een risico zorg je ervoor dat deze zo concreet, beknopt mogelijk is en aansluiten bij de organisatiedoelen. Duidelijke risicobeschrijvingen helpen o.a. bij bewustwording van risico’s en bij het maken van weloverwogen keuzes door de overheidsorganisatie.

Een goede risicobeschrijving bevat de volgende onderdelen:

1. Het bevat de **gebeurtenis.** Dit kan een gebeurtenis zijn die je nu constateert, waarvan nu sprake is en/of een gebeurtenis waarvan je verwacht of denkt dat deze in de toekomst kan gebeuren.
2. **Waarop** heeft de gebeurtenis **betrekking**? De gebeurtenis kan bijvoorbeeld betrekking hebben op organisatieonderdelen, applicaties en informatiesystemen.
3. De **bron van het risico** is waardoor het risico wordt veroorzaakt. Er kunnen meerdere bronnen zijn die afzonderlijk of in combinatie kunnen leiden tot risico’s.
4. De **gevolgen** van een gebeurtenis kunnen implicaties hebben voor de doelstellingen van de overheidsorganisatie. Je kunt een gevolg kwantitatief (in geld) en kwalitatief beschrijven. Ook kunnen verschillende gevolgen elkaar versterken.

**Voorbeelden van risicobeschrijving**

Doordat de toegangsbeheer op personeelsdossiers niet is geregeld (**bron**) is er afgelopen week een cyberaanval uitgevoerd (geconstateerde **gebeurtenis**) op gevoelige persoonsgegevens in het personeelssysteem (heeft **betrekking** op) met als gevolg financiële en reputatieschade voor de organisatie (**gevolg**)

Doordat de procedure voor digitaal vernietigen niet wordt uitgevoerd (**bron**) worden te vernietigen gegevens in vakapplicatie X mogelijk te lang bewaard (mogelijke **gebeurtenis** en **betrekking** op) met juridische schade/claims als **gevolg**.

## <kop>Hoe meet je een risico?

Door risico’s te meten, krijg je inzicht hoe groot de risico’s zijn voor de organisatie.

Aan de hand van duidelijke risicobeschrijvingen kun je risico’s meten. Je geeft dan een bepaalde score aan de risico’s op basis van de **kans** dat een gebeurtenis zich voordoet, en de **impact** die dan ontstaat. Zo kun je onderscheid maken tussen lage risico’s en hoge of zelfs extreme risico’s.

Deze methode gebruik je bij het uitvoeren van een DUTO-risicobeoordeling. In het <link naar stap 5>stappenplan wordt deze methode nader uitgewerkt.