<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
- Hoe je risico's beschrijft
- Hoe je risico's beoordeelt
- Wat het verschil is tussen een risico en een kans

Daarnaast zetten we op een rijtje welke risico's kunnen ontstaan als duurzame toegankelijkheid niet geborgd is. En welke kansen er kunnen liggen als duurzame toegankelijkheid wél geborgd wordt.

➢ <link>Lijst risico's en kansen op het gebied van duurzame toegankelijkheid

<kop> Definitie van 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)

- **Onzekerheid**
  Binnen overheidsorganisaties is het niet altijd 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.

- **Gevolgen**
  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.

- **Doelen**
  Overheidsorganisaties hebben doelen die ze willen bereiken. Ze organiseren het werk zodanig dat ze de doelen halen. Door in te spelen op onzekerheden die doelen kunnen bedreigen, kun je als organisatie jezelf verbeteren en doelen 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.

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

Doordat *(bron)*	**Wordt het waarschijnlijker dat** *(gebeurtenis)*	**Met als gevolg dat** *(implicatie)*
de procedure voor digitaal vernietigen niet wordt uitgevoerd	te vernietigen gegevens in vakapplicatie X te lang bewaard worden	de 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	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> 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.

<kop>Wat is het verschil tussen een risico en een kans?
Als de implicaties van een bepaalde gebeurtenis negatief zijn, dan hebben we het over een **risico**. Als de implicaties positief zijn, dan hebben we het over een **kans**. Je kunt dezelfde situatie vaak beschrijven in de vorm van een risico én in de vorm van een kans. Vergelijk:

- Doordat we **niet tijdig vernietigen** wordt het **waarschijnlijker** dat we overheidsinformatie onnodig bewaren, met als gevolg dat de kosten **toenemen**
- Doordat we **wel tijdig vernietigen** wordt het **minder waarschijnlijk** dat we overheidsinformatie onnodig bewaren, met als gevolg dat de kosten **afnemen**.

<subpagina>Risico's en kansen op het gebied van duurzame toegankelijkheid

Deze handreiking richt zich op de mogelijke risico's én kansen rondom duurzame toegankelijkheid van overheidsinformatie. Als de duurzame toegankelijkheid van overheidsinformatie niet voldoende geborgd is, kan dat negatieve gevolgen hebben. En andersom: het kan *positieve* gevolgen hebben wanneer je overheidsinformatie *wél* duurzaam toegankelijk maakt. In de lijst hieronder zetten we deze kansen en risico's op een rijtje.

Type	**Risico's** *Als duurzame toegankelijkheid van overheidsinformatie* ***onvoldoende*** *geborgd is, dan …*	**Kansen** *Als duurzame toegankelijkheid van overheidsinformatie geborgd is, dan …*
Besluitvorming	… kunnen door het ontbreken van duidelijk metagegevensbeheer bestuurders geen goed onderbouwde besluiten nemen.	… kan de overheidsorganisatie duidelijker aantonen wat ze besluit omdat de overheidsinformatie betrouwbaar en goed te interpreteren is.
Kosten en milieubelasting	… kunnen door het niet tijdig vernietigen van overheidsinformatie de opslagkosten toenemen. En daarmee de belasting voor het milieu die met deze opslag gemoeid is.	… wordt er bijvoorbeeld door het ontdubbelen van gegevens, tijdige vernietiging bespaard op kosten voor opslag en het verminderen van de klimaatlast.
Tijdverlies en moreel medewerkers	…kunnen door het ontbreken van een goede zoekfunctie medewerkers onnodig veel tijd kwijt raken aan het uitvoeren van taken. Dit heeft een negatief effect op het werkplezier.	… is de medewerker minder tijd kwijt aan het uitvoeren van zijn taken omdat overheidsinformatie makkelijk te vinden is. Dit bevordert het werkplezier.
Reconstructie	… wordt het door het ontbreken van betrouwbare en interpreteerbare overheidsinformatie moeilijker om verantwoording af te leggen over het handelen	… stelt het de overheidsorganisatie in staat om transparant te zijn over haar eigen handelen. Ze stelt overheidsinformatie beschikbaar aan degenen die er recht op hebben of maakt deze actief openbaar op basis van de Woo .
Naleving informatie-wetgeving	… is de organisatie door het ontbreken van (onder andere) goed toegangsbeheer minder in staat om tegemoet te komen aan de vereisten die vanuit informatiewetgeving zoals de BIO gesteld worden	… door onder andere tijdig te vernietigen en te zorgen voor betrouwbare informatie voldoet de overheidsorganisatie aan wet- en regelgeving als de AVG en BIO.
Naleving overige wetgeving	… is de organisatie minder in staat om te voldoen aan vereisten die vanuit sectorale wetgeving gesteld worden	… is de organisatie in staat om makkelijker te voldoen aan vereisten die vanuit sectorale wetgeving gesteld worden
Dienstverlening	… kan door het niet tijdig vinden van overheidsinformatie de dienstverlening aan de burger in de knel komen.	… kan de overheidsorganisatie met betrouwbare overheidsinformatie goede dienstverlening leveren.

Type	**Risico's** *Als duurzame toegankelijkheid van overheidsinformatie* ***onvoldoende*** *geborgd is, dan …*	**Kansen** *Als duurzame toegankelijkheid van overheidsinformatie geborgd is, dan …*
Vertrouwen bij burgers en ketenpartners	… kan door onbetrouwbare overheidsinformatie beschikbaar te stellen aan burgers en ketenpartners het vertrouwen bij de burgers en ketenpartners worden geschaad	… kan de overheidsorganisatie onder andere verantwoording afleggen richting de burger en andere belanghebbenden. … is er vertrouwen binnen een ketensamenwerking omdat er gebruik wordt gemaakt van dezelfde (bron)informatie

Deze lijst is afgeleid van module 1 van het DUTO-raamwerk. Ze sluiten ook aan op de methodiek 'Basis Beveiligingsniveau (BBN)' die in het kader van de Baseline Informatiebeveiliging Overheid (BIO) is ontwikkeld. Deze lijst kun je gebruiken als hulpmiddel bij het <link>stappenplan en de <link>quickscan.

Tip: Maak de generieke gevolgen in de lijst specifiek voor de context van jouw organisatie. Benoem bijvoorbeeld *welke* sectorale wetgeving alleen nageleefd kan worden als informatiebeheer op orde is.