# <pagina>Stappenplan DUTO-risicobeoordeling

Voor overheidsorganisaties is het belangrijk om regelmatig in kaart te brengen welke risico’s er bestaan op het gebied van informatiebeheer. En hoe ernstig deze risico’s zijn. Met een DUTO-risicobeoordeling brengen organisaties in kaart welke risico’s bestaan als de overheidsinformatie waar je mee werkt niet duurzaam toegankelijk is. Alleen zo kunnen ze goed prioriteren en efficiënte plannen maken op het gebied van informatiebeheer. DUTO-risicobeoordeling maakt voor management en andere stakeholders inzichtelijk hoe informatiebeheer hun werk en belanghebbenden beïnvloedt en helpt hen om keuzes te maken en prioriteiten te stellen.

## <kop>Stappenplan

Dit stappenplan geeft praktische handvatten bij het plannen en uitvoeren van een DUTO-risicobeoordeling. Het is bedoeld voor informatieprofessionals en andere tactische adviseurs.

Het stappenplan helpt je bij:

* Een vooronderzoek uitvoeren en de scope bepalen. Met als resultaat een **plan van aanpak**.
* Een DUTO-risicobeoordeling uitvoeren. Met als resultaat een **risicorapportage.**

Beslissers en managers kunnen een risicorapportage gebruiken om te prioriteren en plannen te maken op het gebied van informatiebeheer. De module <link> DUTO-risicobeoordeling en risicomanagement geeft aandachtspunten voor beslissers en managers als ze op basis van een risicorapportage tot actie overgaan.

Onderstaande tabel geeft een samenvatting van het stappenplan:

|  |  |
| --- | --- |
| Stap | Toelichting |
| 1. Onderzoek de context | Ga na wat er binnen je organisatie al geregeld is op het gebied van risicomanagement en sluit daarbij in het uitvoeren van de risicobeoordeling zoveel mogelijk op aan. |
| 1. Bepaal de scope | Bepaal de processen en applicaties die je meeneemt in de DUTO-risicobeoordeling. En op welk detailniveau je de risicobeoordeling uit gaat voeren. |
| 1. Maak een plan van aanpak | Leg concreet vast hoe je de DUTO- risicobeoordeling uit gaat voeren in het **plan van aanpak.** |
| 1. Inventariseer de risico’s | Inventariseer welke risico’s er voor jouw organisaties binnen de scope bestaan. |
| 1. Meet de risico’s | Meet hoe groot de risico’s voor jouw organisatie zijn. |
| 1. Maak een risicorapportage | Leg de conclusies van de risicometing vast in een **risicorapportage**. |

## <kop> DUTO-risicobeoordeling als onderdeel van een cyclus

Dit stappenplan gaat uit van een DUTO-risicobeoordeling die onderdeel uitmaakt van een regelmatige, structurele cyclus.

Vaak is de aanleiding voor een DUTO-risicobeoordeling dat er een jaarlijkse cyclus bestaat als onderdeel waarvan risico’s regelmatig beoordeeld worden. De module <link>DUTO-risicobeoordeling en risicomanagement gaat nader in op het inrichten van zo’n cyclus.

Soms is er een andere, aparte aanleiding. Dan kan het gaan om:

* **externe ontwikkelingen** die jouw overheidsorganisatie raken, zoals een verandering in takenpakket, het uitvoeren van nieuwe wet- en regelgeving, of een reorganisatie;
* een **aanbesteding** van nieuwe applicaties of een grondige aanpassing van bestaande applicaties;
* een **incident** zoals een datalek, een parlementaire enquête, een inspectieonderzoek en negatieve publiciteit.

In deze gevallen is een *ad hoc DUTO-risicobeoordeling* waardevol. Ook daarbij kun je dit stappenplan gebruiken. Wel zul je sommige stappen net wat anders invullen. Bij de stappen waar dat aan de orde is, geven we dat apart aan.

# <subpagina>Stap 1: 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 risicomanagement en risicobeoordeling. Zo bereik je betere resultaten.

Onderzoek wat er al georganiseerd wordt op het gebied van risicomanagement en risicobeoordeling. De volgende vijf randvoorwaarden voor het uitvoeren van een risicobeoordeling moeten ingevuld zijn:

* Commitment
* Besluitvormingsprocessen
* Cyclisch werken
* Integrale benadering
* Overzicht over applicaties en processen

De <link>module ‘Risicobeoordeling als onderdeel van risicomanagement’ werkt deze randvoorwaarden nader uit.

## <kop>Wat als de vijf randvoorwaarden niet of gedeeltelijk ingevuld zijn?

Als één of twee randvoorwaarden binnen jouw organisatie niet of beperkt zijn ingevuld, onderneem dan zelf actie, zoals:

* Maak een start met het in kaart brengen van in ieder geval bedrijfskritische processen en applicaties. Het bepalen van bedrijfskritische processen en applicaties doe je bij voorkeur samen met privacy-en informatiebeveiliging specialisten. Zie ook <link> Hoe bepaal ik of het bedrijfsproces en applicatie kritisch zijn?
* Voor het invullen van bepaalde randvoorwaarden is *het management* aan zet.

Het genereren van betrokkenheid, het opstellen van beleid, en het organiseren van een besluitvormingsproces op basis van een terugkerende cyclus zijn daar voorbeelden van.

* Beïnvloed het commitment van management door DUTO-risicobeoordeling te verbinden aan de zaken waaraan jouw organisatie veel waarde hecht. Dit kan aan de hand van zogenaamde kroonjuwelen: thema’s die bij management van de organisatie leven en die bijdragen aan missie en visie van de organisatie.

Als meer dan twee randvoorwaarden niet of beperkt zijn ingevuld binnen jouw organisatie, dan kan de DUTO-risicobeoordeling minder impact hebben.

Als over de hele breedte invulling van alle randvoorwaarden ontbreekt, dan maak je bij het invullen van het stappenplan andere keuzes. Geef in de risicorapportage van de DUTO-risicobeoordeling duidelijk aan welke randvoorwaarden nog niet (voldoende) ingevuld zijn. Het doel van de DUTO-risicobeoordeling is dan om risico’s op het gebied van informatiebeheer in kaart te brengen én om binnen je organisatie het gesprek aan te gaan over hoe er op informatiebeheer gestuurd wordt.

Onderstaande tabel geeft voorbeelden hoe je een beperkte of volledig ontbrekende invulling van randvoorwaarden aanpakt:

|  |  |
| --- | --- |
| **Situatie** | **Aanpak** |
| Er is geen cyclus | Wanneer je vaststelt dat je niet kunt aansluiten bij een bestaande cyclus omdat deze niet bestaat, is het goed om dit bij het management te benoemen. Stem af met het management om een op zich zelf staand traject DUTO-risicobeoordeling te starten als een soort van pilot om cyclisch werken te starten. De inzichten die hieruit voortkomen kunnen de organisatie helpen om risicomanagement en risicobeoordeling gestructureerd in de organisatie in te bedden. |
| Er is geen integrale benadering | Organiseer zelf samenwerking met specialisten van andere informatiedomeinen zoals privacy, informatiebeveiliging en openbaarheid (Woo). Of sluit aan bij andere bestaande trajecten of cycli zoals de jaarplancyclus of kwaliteitstoetsen. Maak daarbij ook gebruik van bevindingen die gedaan zijn door bijvoorbeeld een toezichthouder informatiebeheer en privacy. |

## <kop>Hoe bepaal ik of het bedrijfsproces en applicatie kritisch zijn?

Gebruik de volgende factoren om te bepalen of een bedrijfsproces of een applicatie kritisch is:

* 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 hierom informatie die wezenlijk is om rechten en plichten van individuele burgers te traceren
* Het gaat om informatie rondom publieke verantwoording over de bestuurlijke besluitvorming
* Het gaat om grootschalige gegevensverzamelingen
* 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.

# <subpagina>Stap 2: Bepaal de scope

Het bepalen van de scope hangt nauw samen met de aanleiding voor de DUTO-risicobeoordeling:

* Bij de structurele, jaarlijkse risicomanagement cyclus ligt de focus vaak op <link>bedrijfskritische processen en applicaties.
* Bij de ad hoc DUTO-risicobeoordeling ligt de focus vaak op de aanleiding voor deze benadering. Bijvoorbeeld een datalek.

Als je de scope hebt bepaald, kies dan het bijbehorende aanpak: in de breedte, diepte of thematisch.

|  |  |  |
| --- | --- | --- |
| **Aanpak** | **Niveau** | **Voorbeeld** |
| Breed –  Horizontale benadering | Niveau van elkaar samenhangende **bestaande** bedrijfsprocessen en ondersteunende applicaties  Je brengt de kwetsbaarheden van huidige informatiesystemen in kaart. Zijn de DUTO-processen en de daarbij behorende functies voldoende verankerd in de informatiesystemen om risico’s op het gebied van duurzame toegankelijkheid te voorkomen. | DUTO-risicobeoordeling richt zich op het vormgeven van de DUTO-processen bewaren en vernietigen binnen het ketenproces Omgevingswet en de daarbij ondersteunende applicaties. |
| Diep – Onderzoek op detail | Niveau van één bestaand of nieuw bedrijfsproces en ondersteunende applicatie(s). Hierbij gaat het om **ad hoc DUTO-risicobeoordeling.**  **Bestaand**  Een DUTO-risicobeoordeling van dit type is relevant om te bepalen of een applicatie nog mee kan (met eventuele aanpassingen), of aan vervanging toe is.  **Nieuw**:  Ad hoc DUTO-risicobeoordeling van bijvoorbeeld een nieuwe applicatie die nog niet is aanbesteed of ingericht. Deze risicobeoordeling brengt in kaart of verschillende opties voor inrichting in voldoende mate zorg dragen voor duurzame toegankelijkheid. | Ad hoc DUTO-risicobeoordeling richt zich op het proces het beheren van personeelsgegevens binnen bestaand personeelsbeheersysteem X.  Ad hoc DUTO-risicobeoordeling richt zich op aanschaf van een nieuwe applicatie ter ondersteuning van (nieuw) beleidsvormend proces. |
| Thematisch – Focus op een specifiek DUTO-proces, DUTO-functie, of randvoorwaarde | Thematische DUTO-risicobeoordeling kan zich richten op één of meerdere huidige bedrijfsprocessen en daarbij behorende applicaties. | Hoe is de functie metagegevensbeheer vormgegeven binnen het huidige informatielandschap? |

## <uitklapmenu>Stel een team samen

Je hebt de scope van de DUTO- risicobeoordeling bepaald en een helder beeld van de context waarbinnen je opereert.

Maak afspraken zodat de juiste collega’s aanhaken bij de DUTO-risicobeoordeling.

Is er op het gebied van randvoorwaarden al veel geregeld, dan kun je aansluiten bij een bestaand team. Zorg er in ieder geval voor dat je samenwerkt met, in volgorde van belang:

1. Collega’s met verantwoordelijkheid voor specifieke bedrijfsprocessen en applicaties.
2. Collega’s uit andere i-domeinen zoals informatiebeveiliging. Immers duurzame toegankelijkheid van overheidsinformatie is ook van belang voor deze domeinen.
3. Externe collega’s die een rol spelen binnen <link naar Handreiking Archiveren in de informatieketen> organisatie-overstijgende keten- processen

# <subpagina> Stap 3: Maak een plan van aanpak

Maak een plan van aanpak voor de DUTO-risicobeoordeling. Leg concreet vast hoe je de DUTO-risicobeoordeling uit gaat voeren.

Neem daarom minimaal de volgende onderdelen op in het plan:

* Waarom deze risicobeoordeling? (aanleiding)
* Waarop richt je de risicobeoordeling? (reikwijdte)
* Hoe ga je dit doen? (welke werkwijze, welke stappen neem je?)
* Met wie? (wie zijn er bij betrokken, met wie communiceer je en van wie haal je kennis en wat zijn de rollen en verantwoordelijkheden?)
* Waarmee (benodigde hulpmiddelen, tijdspad en geld)
* Wat zijn factoren die risicobeoordeling kunnen belemmeren? (denk aan het niet op orde hebben van <link>organisatorische randvoorwaarden op het gebied van risicomanagement)
* Of het gaat om een pure risicobeoordeling of om een adviestraject waarbij je ook aanbevelingen doet en oplossingsrichtingen in kaart brengt.

Het plan van aanpak kun je zien als een vorm van een projectplan. Het maakt de gemaakte afspraken duidelijk aan het team. Welke keuzes er gemaakt zijn en waarom. Ook maak je het management door middel van het plan duidelijk wat je precies gaat doen en wat je daarvoor aan tijd, geld, mensen nodig hebt. Zo weet het management wat te verwachten. Dit draagt bij aan commitment vanuit het management. Aan de hand van het plan van aanpak kan bovendien door alle betrokkenen de voortgang bewaakt worden en zo nodig kan er bijgestuurd worden.

Na het voltooien van het plan van aanpak en de goedkeuring van het management hierop, ga je daadwerkelijk aan de slag met de uitvoering van de risicobeoordeling.

# <subpagina> Stap 4: Inventariseer de risico’s

Inventariseer samen met het team de risico’s die binnen de scope en bijbehorend niveau van aanpak vallen. Je inventariseert de risico’s door bijvoorbeeld:

* Gesprekken te voeren met direct betrokkenen zoals proceseigenaren en medewerkers. Waar lopen zij tegenaan, welke obstakels zien zij bij de uitvoering van hun taken en welke behoeften?
* Gebruik te maken van informatiebronnen als eerdere onderzoeksresultaten.

Stel minimaal de volgende vragen om de risico’s te inventariseren, binnen de vastgestelde aanpak en scope:

* 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 heeft dit gevolgen 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 de DUTO- risicobeoordeling zich primair richt op een specifieke applicatie (diepte-aanpak), dan zul je meer aandacht besteden aan DUTO-functies en minder aan randvoorwaarden.

**Voorbeeld**:

Je hebt in het plan van aanpak bij scope en niveau van aanpak aangegeven dat je vanwege een datalek in applicatie X een diepteaanpak hierop wil uitvoeren. Uit eerste gesprekken blijkt dat het datalek o.a. is veroorzaakt door het niet tijdig vernietigen van overheidsinformatie. Je besluit om in het bijzonder het DUTO-proces vernietigen binnen applicatie X verder te onderzoeken.

Je stelt dan vragen als:

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

Als je verder de diepte in gaat, breek je dezelfde vraag op in meerdere vragen. Dit doe je 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?

Naast de functies kun je ook op detailniveau 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).

Je komt daarmee steeds dieper bij de risicobron (zie ook aandachtspunten).

**Aandachtspunten**

1. Voer de inventarisatie uit met de onderdelen zoals deze in de <link>module “Wat is risico?” staan:

* Gebeurtenis,
* Waarop heeft de gebeurtenis betrekking?
* De bron van het risico
* De gevolgen

Dit helpt je bij de volgende stap waarin je de risico’s gaat meten.

1. Leg de verschillende bevindingen zorgvuldig vast. Deze vormen onderdeel van de risicorapportage en dienen als verantwoording over de gehanteerde werkwijze.
2. Maak een lijst van veelvoorkomende oorzaken en gevolgen zodat je deze bij een latere DUTO-risicobeoordeling als leidraad kunt gebruiken.
3. 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. *Zie ook diepte-aanpak bij bepaal de scope.*

## <kop> Hulpmiddel generieke lijst van gevolgen

Als de duurzame toegankelijkheid van overheidsinformatie niet voldoende in de overheidsorganisatie geborgd is, heeft dat verschillende gevolgen.

Binnen deze handreiking maken we onderscheid tussen gevolgen op het gebied van:

* Publieke waarde (meerwaarde voor samenleving)
* Legitimiteit (voldoen 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.

Dit heeft geleid tot een generieke lijst van gevolgen:

| **Soort risico** | **Gevolgen**  *Als (aspecten van) duurzame toegankelijke overheidsinformatie onvoldoende geborgd 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 wat de kansen en mogelijkheden zijn binnen de informatieketen wanneer duurzame toegankelijkheid van overheidsinformatie goed geregeld is. Je kunt ook besluiten om aan bepaalde gevolgen een hogere weging toe te kennen. Bijvoorbeeld door de gevolgen voor de zogenaamde kroonjuwelen extra te benadrukken:

1. Als er zorg bestaat over imagoschade, benadruk dat dan in gevolgen en laat krantenkopjes zien om negatieve berichtgeving te illustreren.
2. Als de organisatie duurzaamheid als missie heeft, zet dan in op de milieubelasting van data-opslag die toeneemt naarmate er niet of te laat vernietigd wordt.
3. 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).

De generieke lijst kan op verschillende niveau’s gebruikt worden. Onderstaande tabel werkt dit uit voor thematische aanpak die in het bijzonder kijkt naar de invulling van het <link naar DUTO-raamwerk, module 4>DUTO-proces Registreren.

**Let op**: Niet alle risicotypes komen terug bij ieder DUTO-proces.

|  |  |
| --- | --- |
| **Type** | **Gevolgen**  *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. |

# <subpagina> Stap 5: Meet de risico’s

Er zijn verschillende manieren om risico’s te meten. Een van de meest gebruikte methoden is het geven van een bepaalde score aan de risico’s. Deze methodiek wordt ook gebruikt door risicobeoordeling op het gebied van informatiebeveiliging en privacy. Denk aan een DPIA (Data Protection Impact Assessment). Door risico’s te meten kun je ze met elkaar vergelijken en ook in de loop van de tijd bepalen of risico’s toe- of afnemen.

De risicoscoringsmethode bestaat uit:

* Gebeurtenis
* Kansscore (**K**)
* Impactscore (**I**)
* Totale score: **K**ans x **I**mpact

Kans en impact kunnen gescoord worden op een ordinale schaal van 1-4, als volgt:

|  |  |
| --- | --- |
| **Kansscore** | **Impactscores** |
| 1 – Zeer laag  2 – Laag  3 – Middel  4 – Hoog | 1 - Klein  2 - Middel  3 - Groot  4 - Ernstig |

Door de kansscore en de impactscore met elkaar te vermenigvuldigen, krijg je de risicoscore. De risicoscores kun je groeperen en kwalificeren van laag tot extreem.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **Impactscore (I)** | | | |
| 1 (Klein) | 2 (Middel) | 3 (Groot) | 4 (Ernstig) |
| **Kansscore (K)** | 1 (Zeer laag) | 1x1=1 | 1x2=2 | 1x3=3 | 1x4=4 |
| 2 (Laag) | 2x1=2 | 2x2=4 | 2x3=6 | 2x4=8 |
| 3 (Middel) | 3x1=3 | 3x2=6 | 3x3=9 | 3x4=12 |
| 4 (Hoog) | 4x1=4 | 4x2=8 | 4x3=12 | 4x4=16 |

|  |  |  |
| --- | --- | --- |
|  | **Risicoscore** | **Kwalificatie** |
|  | Score van 1 of 2 | Laag risico |
|  | Score van 3 of 4 | Middelmatig risico |
|  | Score tussen 5 en 11 | Hoog risico |
|  | Score van 12 of hoger | Extreem risico |

De resultaten van de meting geef je in een tabel weer die als bijlage op kunt nemen in de eindrapportage:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risicogebeurtenis** | **Kans (K)** | **Impact (I)** | **Risico (KxI)** | **Kwalificatie** |
| Te vernietigen gegevens in vakapplicatie X worden te lang bewaard | 4 (Hoog) | 3 (Groot) | 12 | **Extreem risico** |
| Cyberaanval op persoonsgegevens in het personeelssysteem | 2 (Laag) | 4 (Ernstig) | 8 | **Groot risico** |
| Gegevens van sensors verzameld in de publieke ruimte worden niet voorzien van alle benodigde metagegevens | 2 (Laag) | 2 (Middel) | 4 | **Middelmatig risico** |

# <subpagina> Stap 6: Maak een risicorapportage

Sluit de DUTO- risicobeoordeling af met een risicorapportage. De kern van de risicorapportage is dat je met de risicorapportage inzicht geeft aan het management over welke risico’s er bestaan binnen bedrijfsprocessen en applicaties, hoe ernstig deze risico’s zijn, indien met advies: welke oplossingen er bestaan.

Neem in de risicorapportage minimaal het volgende op:

* De context waarin de risicobeoordeling heeft plaats gevonden.

Let op: als je ad hoc risicobeoordeling hebt uitgevoerd, dan heeft dat impact op de rapportage. Hetzelfde geldt als de randvoorwaarden niet of nauwelijks zijn ingevuld. Deze onderwerpen benoem je dan zeker in de risico rapportage.

* De uitkomsten van de inventarisatie en meting
* Concrete beschrijving van risico’s en de gevolgen. Tip: Spreek 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’

**Risicorapportage plus advies**

Als je in het plan van aanpak formeel vastgelegd hebt dat de risicobeoordeling een adviestraject is waarbij je ook aanbevelingen doet en oplossingsrichtingen in kaart brengt, neem dan ook het volgende op:

* Scenario’s en opties, inclusief ‘niets doen’.
* *Quick wins oftewel laaghangend fruit*: relatief eenvoudige en betaalbare oplossingen die zonder veel inzet grote risico’s weg kunnen nemen voor de organisatie.
* Integrale oplossingsrichtingen die ook voor de overige I-domeinen van toepassing zijn.
* Sluit daarbij aan op passende maatregelen op het gebied van duurzame toegankelijkheid: [Overwegingen bij implementatie](https://www.nationaalarchief.nl/archiveren/kennisbank/overwegingen-generiek-deel) en [Module Passende maatregelen voor duurzame toegankelijkheid](https://www.nationaalarchief.nl/archiveren/kennisbank/module-passende-maatregelen-voor-duurzame-toegankelijkheid)

Leg tot slot de risicorapportage voor aan het verantwoordelijk management. Deze is dan aan zet om in actie te komen. Wat ze daarbij moeten doen, staat in de module <link>DUTO-risicobeoordeling als onderdeel van risicomanagement. Om duurzaam toegankelijk informatiebeheer verder in de organisatie tot stand te brengen is het belangrijk dat je ook bij vervolgstappen betrokken bent of ten minste weet wat de vervolgstappen zijn.