# <pagina>Stappenplan DUTO-risicobeoordeling

Het **stappenplan DUTO-risicobeoordeling** is bedoeld voor organisaties die op zoek zijn naar een gedetailleerde en systematische risicobeoordeling. En die op het gebied van risicomanagement al processen ingericht hebben. In de module <link> DUTO-risicobeoordeling en risicomanagement staat beschreven welke processen dat zijn.

Het stappenplan leidt tot een risicorapportage die het verantwoordelijk management kan gebruiken om acties op het gebied van informatiebeheer te plannen, prioriteren, uit te laten voeren en daarop te sturen.

Er is ook een lichte variant van het stappenplan: de <link>quickscan. Deze is geschikt voor organisaties die snel en globaal inzicht willen krijgen in de belangrijkste risico’s die ze lopen op het gebied van informatiebeheer.

## <kop>Stappenplan

Het stappenplan bestaat uit de volgende stappen:

|  |  |
| --- | --- |
| Stap | Toelichting |
| 1. Bepaal het onderwerp van de risicobeoordeling
 | Beschrijf concreet en duidelijk wat het onderwerp van de risicobeoordeling is. Maak aan de hand van het onderwerp en aanpak een **vragenlijst**.  |
| 1. Onderzoek de context
 | Verken de omgeving waarin de risicobeoordeling plaatsvindt. Zodat je duidelijk hebt wie je kunt betrekken en welke informatiebronnen je kunt gebruiken bij de risicobeoordeling.  |
| 1. Maak een plan van aanpak
 | Leg concreet vast hoe je de DUTO-risicobeoordeling uit gaat voeren in het **plan van aanpak.** |
| 1. Breng de risico’s in kaart
 | Ga op onderzoek uit om mogelijke risico’s in kaart te brengen. Je voert aan de hand van de vragenlijst gesprekken met belanghebbenden.  |
| 1. Beschrijf de risico’s
 | Analyseer en beschrijf concreet welke risico’s er voor jouw organisatie met betrekking tot het onderwerp van de risicobeoordeling bestaan. |
| 1. Beoordeel de risico’s
 | Beoordeel aan de hand van **scores** de risico’s voor jouw organisatie. |
| 1. Maak een risicorapportage
 | Leg de conclusies van de risicobeoordeling en advies voor mogelijke maatregelen vast in een **risicorapportage**. |

Deze stappen sluiten op hoofdlijnen aan bij NEN-ISO 18128:2024. Zie de lijst veelgestelde vragen voor een <link> gedetailleerde uitwerking hiervan.

# <subpagina> Stap 1: Bepaal het onderwerp van de risicobeoordeling

Een DUTO-risicobeoordeling begin je niet zomaar. Je sluit bijvoorbeeld aan op een bestaande jaarlijkse cyclus van risicobeoordeling. Maar het kan ook zijn dat je binnen en buiten de organisatie signalen ontvangt dat er geen tijdige vernietiging van overheidsinformatie plaatsvindt of dat overheidsinformatie moeilijk te vinden is. Ook heb je als informatiespecialist vaak al een goed globaal beeld van risico’s op het gebied van duurzame toegankelijkheid in de organisatie. Jouw kennis en ervaring helpen om concreet en duidelijk te beschrijven waar je de risicobeoordeling op wilt richten. Door het onderwerp van de DUTO-risicobeoordeling duidelijk te beschrijven, wordt deze effectiever.

Zorg er bij het bepalen van het onderwerp voor dat:

* je verbinding legt met ontwikkelingen die binnen jouw organisatie spelen. Zoals het uitvoeren van (nieuwe) wet-en regelgeving, het aanschaffen, bouwen of herinrichten van een applicatie, een reorganisatie en opgave om efficiënter en effectiever te werken;
* je (voor zover mogelijk) zorgt voor samenhang met andere informatiedomeinen zoals privacy en informatiebeveiliging. Dit voorkomt dubbel werk en conflicten.

## <kop>Keuze voor aanpak in de breedte, diepte of thematisch

Wanneer je het onderwerp hebt bepaald, besluit je hoe het onderwerp van de risicobeoordeling wilt benaderen: breed, diep of thematisch.

|  |  |  |
| --- | --- | --- |
| **Aanpak**  | **Nadruk op**  | **Voorbeelden**  |
| Breed  | Hoe worden meerdere [**DUTO-processen**](https://www.nationaalarchief.nl/archiveren/kennisbank/duto-processenmodel) uitgevoerd in meerdere bedrijfsprocessen en ondersteunende applicaties.  | In het kader van de jaarlijkse concern-brede cyclus risicobeoordeling wil je ook weten welke risico’s er op het gebied van informatiebeheer bestaan. Daarom voer je een brede DUTO-risicobeoordeling uit die voor bedrijfsprocessen door de hele organisatie in kaart brengt of er risico’s verbonden zijn aan de manier waarop de DUTO-processen binnen die bedrijfsprocessen zijn ingericht.  |
| Diep  | Hoe worden meerdere [**DUTO-proces**](https://www.nationaalarchief.nl/archiveren/kennisbank/duto-processenmodel)**sen of functies** binnen één specifiek bedrijfsproces en ondersteunende applicaties geborgd? | Er wordt een nieuwe applicatie aangeschaft voor personeelsbeheer. Je wilt inzicht krijgen in welke modeleisen je meegeeft aan deze nieuwe applicatie. Je kijkt daarbij ook naar hoe eisen in huidige applicatie worden uitgevoerd.  |
| Thematisch | Focus op één **specifiek DUTO-proces**, **DUTO-functie, of randvoorwaarde** binnen meerdere bedrijfsprocessen en ondersteunende applicaties. | Je vermoedt al enige tijd dat er binnen de organisatie geen tijdige vernietiging plaatsvindt. Je selecteert een aantal bedrijfskritische processen en ondersteunende applicaties. Daarbinnen onderzoek je functionaliteit en procedures rondom Vernietigen, aan de hand van het [DUTO-proces Vernietigen](https://www.nationaalarchief.nl/archiveren/kennisbank/module-5-duto-proces-vernietigen) |

## <uitklapmenu>Het maken van een vragenlijst

Maak aan de hand van de aanpak en de modules uit het DUTO-raamwerk een vragenlijst. Deze dient als basis voor stap 4.

Bij het maken van de vragenlijst houd je rekening met de volgende aandachtspunten:

* De vragenlijst in de <link>quickscan is een nuttig beginpunt, zeker voor een brede risicobeoordeling;
* Maak een vragenlijst samen met specialisten op het gebied van informatiebeveiliging en privacy;
* Stel ja/nee vragen en vraag vervolgens door. Zo zorg je dat je scherp krijgt hoe dingen ingericht zijn en welke keuzes daarbij gemaakt zijn.

## <kop>Voorbeelden van vragenlijsten per aanpak

## <uitklapmenu>Breed

In het kader van de jaarlijkse concern-brede cyclus risicobeoordeling wil je ook weten welke risico’s er op het gebied van informatiebeheer bestaan. Daarom voer je een brede DUTO-risicobeoordeling uit die voor bedrijfsprocessen door de hele organisatie in kaart brengt of er risico’s verbonden zijn aan de manier waarop de DUTO-processen binnen die bedrijfsprocessen zijn ingericht.

Je neemt de <link>vragenlijst uit de quickscan als uitgangspunt en werkt deze nader uit.

## <uitklapmenu> Diep

Er wordt een nieuwe applicatie aangeschaft voor personeelsbeheer. Je wilt inzicht krijgen in welke modeleisen je meegeeft aan deze nieuwe applicatie. De vragen zijn dan gericht op:

* Hoe worden de verschillende eisen nu uitgevoerd in de huidige applicatie? Wat kan er beter?
* Wat zijn risico’s als we bepaalde eisen niet meenemen?

## <uitklapmenu> Thematisch

Je vermoedt al enige tijd dat er binnen de organisatie geen tijdige vernietiging plaatsvindt. Je selecteert een aantal bedrijfskritische processen en ondersteunende applicaties. Daarbinnen onderzoek je functionaliteit en procedures rondom Vernietigen, aan de hand van het [DUTO-proces Vernietigen](https://www.nationaalarchief.nl/archiveren/kennisbank/module-5-duto-proces-vernietigen). Per applicatie wil je weten of het mogelijk is te vernietigen. Je doet dit aan de hand van vragen rondom de zes DUTO-functies die het DUTO-proces vernietigen ondersteunen.

* Is **metagegevensbeheer** gerealiseerd binnen deze applicatie?

Ja, hoe wordt dit gedaan? Nee, wat is de reden dat het niet binnen deze applicatie is gerealiseerd.

* 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 <link>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).

Daarnaast besteed je aandacht aan de specifieke randvoorwaarden van dit proces.

* Is er een **procedure** voor vernietigen (inclusief beleid voor back-ups)?
* Vindt vernietiging volgens deze procedure plaats?

# <subpagina>Stap 2: Onderzoek de context

Nadat je hebt bepaald wat het onderwerp is van de risicobeoordeling, richt je je op de omgeving waarin de risicobeoordeling plaats gaat vinden. De informatie die je hier ophaalt, gebruik je om een plan van aanpak te maken en om de risico’s in kaart te brengen. Ook kun je de vragenlijst verder verfijnen met inzichten die je in deze stap hebt opgedaan.

Jouw onderzoek van de context richt zich op:

1. wie je minimaal nodig hebt om de risicobeoordeling uit te kunnen voeren.

Het kan daarbij gaan om:

* Collega’s met verantwoordelijkheid voor specifieke bedrijfsprocessen en applicaties.
* Collega’s uit andere informatie-domeinen zoals informatiebeveiliging, privacy en informatiearchitecten. Duurzame toegankelijkheid van overheidsinformatie is immers ook van belang voor deze domeinen. Ook kunnen zij kennis delen over o.a. het informatielandschap en welke bedrijfskritische processen er zijn.
* Externe collega’s die een rol spelen binnen organisatie-overstijgende ketenprocessen. Zie de <link> Handreiking Archiveren in de informatieketen voor meer informatie over zulke processen
1. welke interne en externe omgevingsfactoren (met name op het gebied van informatiebeheer) van invloed kunnen zijn op de risicobeoordeling. Te denken valt bijvoorbeeld aan weinig sturing op het gebied van informatiebeheer. Maar ook aan wat er binnen de organisatie leeft. Waar ligt het bestuur wakker van?
2. wat er al aan informatie bekend is:
* Inzicht in het informatielandschap van de organisatie.
* Bestaande methode voor risicobeoordeling binnen de organisatie
* Bestaande risicocriteria - welke risico’s is men bereid te nemen wil nemen en welke niet?
* Bestaande formats voor plannen van aanpak en risicorapportages
* Eerdere risicobeoordelingen die anderen op dit gebied hebben uitgevoerd of gerelateerd zijn hieraan.
* Eerdere maatregelen die zijn genomen om risico’s aan te pakken.

Maak hierbij gebruik van informatiebronnen als:

* een team dat zich bezighoudt met kwaliteitsmanagement en/of planning en control waarbij je algemene risicocriteria kunt opvragen en andere hulpvragen kunt stellen.
* Inspectie en auditrapporten
* Financiële rapporten
* Uitkomsten van kwaliteitsonderzoeken op het gebied van informatiebeveiliging ([BIO](https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/bio-en-ensia/baseline-informatiebeveiliging-overheid/)) en privacy ([DPIA](https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia)).
* Rapporten van informatie-architecten en businessanalisten die inrichtingskeuzes voor een applicatie beschrijven. Deze bevatten vaak risico-afwegingen.

Pas zonodig de vragenlijst aan.

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

Stel een kernteam samen of sluit aan bij een bestaand team. Vanuit het kernteam werk je samen met andere betrokkenen. Maak een plan van aanpak voor de DUTO-risicobeoordeling waarin je concreet vastlegt hoe je de DUTO-risicobeoordeling uit gaat voeren. Gebruik hiervoor bij voorkeur een bestaand format.

Neem minimaal de volgende onderdelen op in het plan:

* De aanleiding voor de risicobeoordeling?
* De reikwijdte van de risicobeoordeling
* De werkwijze die je gaat gebruiken
* De betrokken partijen en andere belanghebbenden
* Benodigde hulpmiddelen, tijdspad en geld
* Factoren die risicobeoordeling kunnen belemmeren

Het plan van aanpak 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. 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: Breng de risico’s in kaart

De voorgaande stappen waren gericht op het voorbereiden van de daadwerkelijke risicobeoordeling. De volgende stappen gaan over de uitvoering van de risicobeoordeling. De eerste stap hierin is op onderzoek uitgaan om risico’s in kaart te brengen.

De risico’s breng je in de kaart door de volgende acties:

* Voer aan de hand van de vragenlijst die je in stap 1 hebt opgesteld gesprekken met direct betrokkenen. Zoals proceseigenaren, vakinhoudelijke experts als business-analisten en informatiearchitecten.
* Vraag daarbij steeds door. Als je vraagt of een bepaalde functionaliteit ingevuld is, en het antwoord is ‘nee’: Wat is daar de oorzaak van? Welke afweging is er gemaakt? Is er een alternatief? Vraag ook door als het antwoord ‘ja’ is: Hoe is het precies geregeld? Welke keuzes zijn er gemaakt? Is er actief beheer?
* Besteed in de gesprekken ook aandacht aan de obstakels die ervaren worden bij de uitvoering van taken op het gebied van informatiebeheer.
* Gebruik eerdere onderzoeksresultaten te gebruiken (zie stap 2). Toets deze bij gesprekspartners te toetsen: Kloppen deze resultaten nog? Zo niet, wat is er veranderd?
* Besteed niet alleen aandacht DUTO-functionaliteiten die op dit moment ingericht zijn. Maar ook of ze dat in de toekomst zullen blijven doen. Als duidelijk is dat een applicatie op voorzienbare tijd wordt uitgefaseerd, dan heeft dat gevolgen voor de duurzame toegankelijkheid. Ga in dat geval na of de juiste voorzieningen zijn getroffen op het gebied van het <link>DUTO-proces Migreren. En zorg dat je betrokken wordt bij het aanbesteden en inrichten van een nieuwe applicatie.
* Leg de verschillende bevindingen zorgvuldig vast.

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

Door de gesprekken te voeren heb je informatie verzameld over mogelijke risico’s. In deze stap analyseer en beschrijf je de risico’s. Je geeft aan:

* wat er zich mogelijk voor kan doen (gebeurtenis),
* waardoor dit kan gebeuren (oorzaak)
* wat dat betekent voor de organisatie (gevolg).

Voor meer uitleg bij deze drie elementen van risico, zie de module <link>Wat is een risico?

Aandachtspunten bij het beschrijven van een risico zijn:

* Eén gebeurtenis kan verschillende oorzaken en gevolgen hebben.
* De <link>module ‘Wat is een risico’ bevat een algemene lijst met gevolgen die zich voor kunnen doen als overheidsinformatie niet duurzaam toegankelijk is. Gebruik deze lijst als startpunt en pas hem 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 wanneer duurzame toegankelijkheid van overheidsinformatie goed geregeld is.
* Sluit aan bij bestaande analyses uit informatiebronnen als auditrapporten
* Sluit bij de gevolgen ook aan bij de doelstellingen, de waarden van de organisatie.
* Maak een lijst van veel voorkomende oorzaken en gevolgen. Die kun je bij een latere DUTO-risicobeoordeling als kunt gebruiken

## <kop> Overzichtstabel risicobeoordeling – beschrijving risico’s

Gebruik een tabel om de risico’s overzichtelijk bij elkaar te brengen. Hieronder staat een voorbeeld.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Oorzaak** | **Mogelijke gebeurtenissen** | **Gevolgen** |
| 1 | De functie maskering wordt niet ondersteund binnen een bedrijfskritische applicatie  | * onbevoegden hebben toegang tot gevoelige gegevens
 | * Onrechtmatig handelen
* Juridische en financiële claims
 |
| 2 | Er zijn geen duidelijke afspraken gemaakt over welke metagegevens we gebruiken  | * medewerkers zijn onnodig veel tijd kwijt aan het vinden van informatie.
* overheidsinformatie is moeilijk te interpreteren.
 | * Hogere kosten
* Afnemend werkplezier
* Slechte dienstverlening
 |
| 3 | Er is geen procedure voor het borgen van het registratieproces | * onbetrouwbare gegevens worden geregistreerd
 | * Onrechtmatige besluiten
 |

Deze tabel breid je in de volgende stappen uit met een risicoscore en met mogelijke maatregelen. Je kunt deze overzichtstabel opnemen als bijlage in de risicorapportage. Hiervoor is een sjabloon beschikbaar.

<link naar download>Sjabloon overzichtstabel risicobeoordeling

# <subpagina> Stap 6: Beoordeel de risico’s

Nadat je de verschillende risico’s hebt beschreven, ga je de verschillende risico’s beoordelen. 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 beoordelen 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 schaal van 1-4:

|  |  |
| --- | --- |
| **Kansscore** | **Impactscores** |
| 1 – Zeer laag2 – Laag3 – Middel4 – Hoog | 1 - Klein 2 - Middel 3 - Groot 4 - Ernstig |

Door de kans score en de impactscore met elkaar te vermenigvuldigen, krijg je de risicoscore.

|  |  |
| --- | --- |
|  | **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 |

De risicoscores kun je groeperen en kwalificeren van laag tot extreem.

|  |  |
| --- | --- |
| **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 voeg je toe aan de overzichtstabel.

## <kop> Overzichtstabel risicobeoordeling – risicoscores

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Risico** | **Kans** | **Impact** | **Score** | **Kwalificatie** |
| 1. | Doordat de functie maskering niet ondersteund wordt binnen bedrijfskritische applicatie X bestaat de kans dat onbevoegden toegang hebben tot gevoelige gegevens, met als gevolg onrechtmatig handelen, juridische en financiële claims | 3(Middel) | 4(Ernstig) | 12 | Extreem risico  |
| 2. | Doordat er geen duidelijke afspraken gemaakt zijn over welke metagegevens we gebruiken, zijn medewerkers onnodig veel tijd kwijt aan het vinden van informatie, met als gevolg hogere kosten en afnemend werkplezier  | 4(Hoog) | 2 (Middel) | 8 | Hoog risico |

## <uitklapmenu> Het bepalen van maatregelen

Nadat je de risico’s hebt beoordeeld, bepaal je of en welke maatregelen nodig zijn om met risico’s om te gaan. En welke dat zijn. Op hoofdlijnen heb je de volgende opties:

* Verkleinen – je verkleint het risico door maatregelen die de impact van een gebeurtenis verminderen of die de kans op een gebeurtenis terugbrengen (of zelfs: die een gebeurtenis geheel voorkomen)
* Overdragen – je neemt maatregelen die het risico bij een andere partij beleggen.
* Accepteren – je kiest ervoor om vooralsnog geen maatregelen te nemen. En om juist gunstige kansen te benutten.

Wees pragmatisch bij de maatregelen die je voorstelt:

* Ga voor laaghangend fruit: relatief eenvoudige en betaalbare oplossingen die zonder veel inzet grote risico’s weg kunnen nemen voor de organisatie.
* Zet in op integrale oplossingsrichtingen die ook voor de overige I-domeinen van toepassing zijn.
* Sluit daarbij aan op [passende maatregelen](https://www.nationaalarchief.nl/archiveren/kennisbank/module-passende-maatregelen-voor-duurzame-toegankelijkheid) op het gebied van duurzame toegankelijkheid.
* Bij een management dat het verminderen van kosten prioriteert, kun je ook gebruik maken van een kosten-baten analyse. Je geeft bij de verschillende maatregelen aan wat de te verwachten kosten en voordelen zijn. Tenslotte vergelijk je de verschillende maatregelen op kosten en baten. Op basis daarvan kun je een gericht advies geven aan het management. De baten kunnen uitgedrukt worden in financiële of kwalitatieve opbrengsten.

Let op: een aantal geringe risico’s kun je in deze tabel weglaten op basis van de risicocriteria die in de organisatie zijn afgesproken. Bijvoorbeeld: score onder de 5 beschouwt de organisatie als acceptabel. Er zijn dan geen maatregelen nodig.

De maatregelen voeg je toe aan de overzichtstabel. Geef ook een prioritering aan.

## <kop> Overzichtstabel risicobeoordeling – maatregelen

|  |  |  |  |
| --- | --- | --- | --- |
| **Risico** | **Kwalificatie**  | **Maatregel**  | **Prioriteit**  |
| 1. | Extreem  | Verminder dit risico door zo spoedig mogelijk de functie maskering met de bijbehorende eisen in te richten binnen applicatie X.  | Hoog  |
| 2. | Hoog  | Doe een verdiepingsonderzoek naar wat er al geregeld is aan metagegevens en welke metagegevens toegevoegd moeten worden. Onderzoek of deze metagegevens met terugwerkende kracht automatisch kunnen worden toegevoegd.  | Hoog |

# <subpagina> Stap 7: Maak een risicorapportage

Sluit de DUTO-risicobeoordeling af met een risicorapportage en een advies. De kern van de risicorapportage is dat je met de risicorapportage inzicht geeft aan het verantwoordelijk management over welke risico’s er bestaan, hoe ernstig deze ’zijn, hoe ze aangepakt kunnen worden. Maak daarbij duidelijk dat het management voor de vervolgstappen verantwoordelijk is.

Neem in de risicorapportage minimaal het volgende op.

* Het onderwerp van de risicobeoordeling (zie stap 1)
* De beschrijving van het onderzoeksproces inclusief gespreksverslag (stap 4)
* Concrete beschrijving van risico’s en de gevolgen (stap 5). Benoem hierbij in het bijzonder gevolgen die relevant zijn voor de missie van je organisatie. Als er zorg bestaat over imagoschade, benadruk dat dan in gevolgen en laat krantenkopjes zien om negatieve berichtgeving te illustreren. Als de organisatie duurzaamheid hoog in het vaandel, zet dan bijvoorbeeld in op de milieubelasting van dataopslag die toeneemt naarmate er niet of te laat vernietigd wordt.

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’.

* Advies bestaande uit aanbevelingen voor passende maatregelen met prioritering (stap 6). Maak voor zover mogelijk gebruik van een bestaand format.

Leg tot slot de risicorapportage voor aan het verantwoordelijk management. Deze moeten dan reageren en besluiten welke maatregelen ze uit willen laten voeren. In de module <link> DUTO-risicobeoordeling en risicomanagement wordt de rol van het verantwoordelijk management verder beschreven.

De managementreactie is een integraal onderdeel van de risicorapportage als apart hoofdstuk of bijlage. De managementreactie voeg je sowieso toe aan de overzichtstabel. Hiermee ben je transparant over de vervolgstappen. Dit zorgt dat management op daarop actief kan sturen.

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. De acties die ondernomen worden, kunnen immers van belang zijn voor de volgende risicobeoordeling. Zo ontstaat een patroon waarbij inzicht in risico’s actueel blijft en bij het nemen van maatregelen voortgebouwd kan worden op eerdere maatregelen.