<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, te 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**.
2. 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.
3. Maak een plan van aanpak	Leg concreet vast hoe je de DUTO-risicobeoordeling uit gaat voeren in het **plan van aanpak.**
4. Voer het gesprek	Voer aan de hand van de vragenlijst gesprekken met deskundigen.
5. Beschrijf de risico's	Analyseer en beschrijf concreet welke risico's er voor jouw organisatie met betrekking tot het onderwerp van de risicobeoordeling bestaan.
6. Beoordeel de risico's	Beoordeel aan de hand van **scores** de risico's voor jouw organisatie.
7. Maak een risicorapportage	Leg de conclusies van de risicobeoordeling en advies voor mogelijke oplossingen 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.

Het stappenplan DUTO-risicobeoordeling leidt tot het maken en bespreken van de risicorapportage. Daarna houd je de vinger aan de pols bij het implementeren van de aanbevelingen uit de risicorapportage. Wat dit inhoudt, lees je in <link> op de pagina Nazorg.

<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.

<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. In alle gevallen maak je gebruik van onderdelen van het DUTO-raamwerk:

- In module 3 van het DUTO-raamwerk worden de **DUTO-processen** en de bijbehorende **DUTO-functies** gedefinieerd.
- Daarnaast benoemen we de **randvoorwaarden** die nodig zijn om alle DUTO-processen goed in te richten.
- Modules 4 tot en met 8 van het DUTO-raamwerk bevatten **modeleisen** voor ieder DUTO-proces.

Hoe je de DUTO-processen, functies, randvoorwaarden en modeleisen in de praktijk gebruikt, kun je lezen in <link>de gebruiksaanwijzing bij het ontwerpstelsel.

Aanpak	**Nadruk op**	**Voorbeelden**
Breed	Hoe worden meerdere **DUTO-processen** 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-processen 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 gebruikt om mee te geven aan deze nieuwe applicatie. Je kijkt daarbij ook naar hoe modeleisen in de huidige applicatie worden uitgevoerd.
Thematisch	Focus op één **specifiek DUTO-proces**, **DUTO-functie, of randvoorwaarde** binnen meerdere bedrijfsprocessen en ondersteunende applicaties.	Je weet dat er al enige tijd geen tijdige vernietiging plaatsvindt. Je selecteert een aantal processen en ondersteunende applicaties. Daarbinnen onderzoek je functionaliteit en procedures rondom vernietiging aan de hand van het <link>DUTO-proces Vernietigen.

Tip: In sommige gevallen is het nuttig om de risicobeoordeling specifiek te richten op een aantal bedrijfskritische processen. De <link>module Quickscan bevat een lijst met criteria die gebruikt kan worden om te bepalen welke processen bedrijfskritisch zijn.

<kop>Maak een vragenlijst
Maak aan de hand van de aanpak en de modules uit het DUTO-raamwerk een vragenlijst. Stel ja/nee vragen en bouw daarop voort met aanvullende verdiepingsvragen. Zo zorg je dat je scherp krijgt hoe dingen ingericht zijn en welke keuzes daarbij gemaakt zijn. De <link>vragenlijst uit de Quickscan DUTO-risicobeoordeling is een startpunt. Bij deze vragenlijst is ook een <link> lijst met verdiepingsvragen beschikbaar.

<kop>Vragenlijsten per aanpak
<uitklapmenu> Breed
Bij een **brede risicobenadering** stel je vragen over de invulling van informatiebeheer door de hele organisatie heen. Je richt je zowel op organisatorische randvoorwaarden als op de invulling van DUTO-functionaliteit binnen applicaties die processen ondersteunen.

Je neemt de <link>vragenlijst uit de quickscan als uitgangspunt en werkt deze nader uit. Werk daarbij samen met specialisten op het gebied van informatiebeveiliging en privacy . Of gebruik bestaande vragenlijsten en voeg daaraan vragen over informatiebeheer toe. Leg daarbij de verbinding met ontwikkelingen die binnen jouw organisatie spelen. Denk aan:

- het uitvoeren van (nieuwe) wet- en regelgeving,
- het aanschaffen, bouwen of herinrichten van een applicatie
- een reorganisatie
- een opgave om efficiënter en effectiever te werken

Tip: Bekijk of er in de cyclus bij de voorgaande jaren vragen zijn gesteld waar je op terug wilt komen, bijvoorbeeld om voortgang te kunnen signaleren. Je kunt ook eerdere onderzoeksresultaten gebruiken (zie stap 2). Toets deze bij gesprekspartners: Kloppen deze resultaten nog? Zo niet, wat is er veranderd?

<uitklapmenu> Diep
Bij een **diepe risicobeoordeling** stel je meer gedetailleerde vragen over hoe DUTO-functionaliteit precies geborgd is binnen de applicaties die een bepaald proces ondersteunen.

Je neemt de <link>vragenlijst uit de Quickscan DUTO-risicobeoordeling als uitgangspunt en werkt deze nader uit. Bijvoorbeeld door gedetailleerde vragen toe te voegen over de invulling van bepaalde randvoorwaarden. En over de implementatie van specifieke DUTO-functionaliteit aan de hand van de modeleisen uit het DUTO-raamwerk.

<uitklapmenu> Thematisch
Bij een **thematische risicobeoordeling** kijk je naar een specifiek aspect van informatiebeheer. Bijvoorbeeld de organisatiebrede invulling van een randvoorwaarde uit het DUTO-raamwerk. Of de implementatie van een specifiek DUTO-proces binnen meerdere processen.

Voor de applicaties die de geselecteerde processen ondersteunen wil je steeds 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?
- 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 <link>negentien modeleisen. 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?

Ook bij een thematische risicobeoordeling is het belangrijk om steeds door te vragen. De <link>Quickscan DUTO-risicobeoordeling bevat een lijst met verdiepingsvragen.

<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 in stap 3 een plan van aanpak te maken. Ook kun je door onderzoek een eerste idee krijgen van mogelijke risico's. Met de inzichten die je in deze stap krijgt, kun je zo nodig de vragenlijst verder verfijnen.

Het vooronderzoek richt zich op:	**Denk daarbij aan:**
Welke collega's je nodig hebt om de risicobeoordeling uit te kunnen voeren.	• **Proceseigenaren** die verantwoordelijk zijn voor specifieke bedrijfsprocessen en applicaties. • **Collega's uit andere informatie-domeinen** zoals informatiebeveiliging, privacy en informatiearchitecten. • **Externe collega's** die een rol spelen binnen organisatie-overstijgende <link>ketenprocessen.
Welke interne en externe factoren van invloed kunnen zijn op de risicobeoordeling	• de **wettelijke context** waarin de organisatie opereert. • de **sturing** op informatiebeheer binnen de organisatie. • **zorgpunten** bij het verantwoordelijk management • **verwachtingen vanuit de samenleving** ten aanzien van het functioneren van de organisatie
Welke hulpmiddelen er binnen de organisatie al beschikbaar zijn:	• **Beleid** voor duurzame toegankelijkheid • Een **overzicht** van overheidsinformatie • Een **kwaliteitssysteem** • Bestaande **methode voor risicobeoordeling** • Bestaande **risicocriteria** • Bestaande **formats** voor plannen van aanpak en risicorapportages • **Eerdere risicobeoordelingen** die anderen op dit gebied of een gerelateerd gebied hebben uitgevoerd. • **Eerdere maatregelen** die zijn genomen om risico's aan te pakken.

Maak bij het vooronderzoek gebruik van informatiebronnen zoals:

- Inspectie en auditrapporten
- Financiële rapporten
- Uitkomsten van kwaliteitsonderzoeken op het gebied van informatiebeveiliging (BIO) en privacy (DPIA).

- Instrumenten zoals een (informatie)architectuur, documentair structuurplan, zaaktypecatalogus, verwerkingsregister of een ordeningsstructuur
- Rapporten van informatie-architecten en businessanalisten die inrichtingskeuzes voor een applicatie beschrijven. Denk bijvoorbeeld aan een requirementsanalyse. Dergelijke rapporten bevatten vaak risico-afwegingen.

Als er een team is dat zich bezighoudt met kwaliteitsmanagement en/of planning en control, benader dat team dan om algemene risicocriteria op te vragen en andere hulpvragen te stellen.

<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: Voer het gesprek

De voorgaande stappen waren gericht op het voorbereiden van de daadwerkelijke risicobeoordeling. In deze stap ga je met de vragenlijst de organisatie in. Je voert gesprekken met proceseigenaren en eventueel vakinhoudelijke experts zoals business-analisten en informatiearchitecten.

De volgende aandachtspunten helpen je om de effectiviteit van de vraaggesprekken te vergroten:

- **Plan altijd een gesprek in**. Je kunt de vragenlijst van te voren opsturen ter voorbereiding, maar plan altijd een gesprek in met de proceseigenaar om de vragenlijst samen door te lopen. Door aan de hand van de vragenlijst in gesprek te gaan, voorkom je dat vragen verkeerd worden geïnterpreteerd. Je vergroot zo bovendien de zichtbaarheid van informatiebeheer.
- **Wees duidelijk over het doel van de risicobeoordeling**. Risicobeoordeling is geen vorm van toezicht. Het doel van een risicobeoordeling is om de lijnorganisatie *in control* te brengen op het gebied van duurzame toegankelijkheid.

De rol van de informatieprofessional is om te ontzorgen en mee te denken over mogelijke concrete oplossingen.

- **Wees een constructieve gesprekspartner**. Zorg dat je de meerwaarde van DUTO en DUTO-risicobeoordeling uitlegt op een manier die aansluit bij de behoeften en zorgen die er bij de gesprekpartners zijn. Besteed daarbij ook aandacht aan obstakels die ervaren worden bij de uitvoering van taken op het gebied van informatiebeheer.
- **Documenteer je waarnemingen.** Maak een verslag van het gesprek en deel dit met de betrokkenen, zodat zij zaken nog kunnen aanvullen en bevestigen. Dit helpt om stap 3 uit te kunnen voeren.
- **Vraag altijd door.** Zo krijg je een scherper beeld van wat er speelt en kun je een beter advies formuleren. De Quickscan DUTO-risicobeoordeling bevat een <link>lijst met verdiepingsvragen die je kunt gebruiken om het gesprek aan te gaan.

<subpagina> Stap 5: Beschrijf de risico's

Door de gesprekken te voeren heb je informatie verzameld. In deze stap analyseer je samen met het kernteam de antwoorden. Je beschrijft hierbij concreet de risico's en kansen door aan te geven:

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.

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

Tip: De module 'Wat is een risico' bevat een <link>algemene lijst met gevolgen die zich voor kunnen doen als overheidsinformatie niet duurzaam toegankelijk is. Gebruik deze lijst als startpunt en pas hem zodat hij goed aansluit bij jouw organisatie. Ter inspiratie kun je ook de voorbeelden van mogelijke risico's uit de <link>vragenlijst bij de Quickscan DUTO-risicobeoordeling gebruiken.

Aandachtspunten bij het beschrijven van een risico zijn:

- Eén gebeurtenis kan verschillende oorzaken en gevolgen hebben.
- Risico's en kansen kunnen met elkaar samenhangen: een risico op organisatieniveau kan bijvoorbeeld invloed hebben op de risico's in een bedrijfsproces. Een risico bij het proces registratie kan weer doorwerken in andere processen zoals bewaren.

Bij het beschrijven van de gevolgen is het raadzaam om de connectie te zoeken met thema's die relevant zijn voor jouw organisatie, bijvoorbeeld:

- Als je bij een gemeente werkt waar het college zich sterk maakt voor duurzaamheid dan kun je de nadruk leggen op de milieubelasting van dataopslag.
- Bij organisaties die sterk in de publieke belangstelling staan, kun je de nadruk leggen op de imagoschade die kan ontstaan wanneer ze wet- en regelgeving niet naleven
- Wanneer je organisatie genoodzaakt is te bezuinigen, kun je inzetten op de kansen die er zijn om geld te besparen

<kop> Overzichtstabel risicobeoordeling – beschrijving risico's
Gebruik een tabel om de risico's overzichtelijk bij elkaar te brengen. Hieronder staat een voorbeeld waarin de <link>onderdelen van een risicobeschrijving zijn benoemd:

Doordat *(bron)*		**Wordt het waarschijnlijker dat** *(gebeurtenis)*	**Met als gevolg dat** *(implicatie)*
1	De functie maskering niet ondersteund wordt binnen een bedrijfskritische applicatie	… onbevoegden toegang krijgen tot gevoelige gegevens	• Onrechtmatig handelen • Juridische en financiële claims
2	Er geen duidelijke afspraken zijn gemaakt over welke metagegevens we gebruiken	… medewerkers onnodig tijd kwijt zijn aan het vinden van informatie	• Hogere kosten • Afnemend werkplezier • Slechte dienstverlening
3	Er geen procedure is 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 ze beoordelen. Een van de meest gebruikte methoden is het geven van een bepaalde score aan de risico's. Deze methode wordt ook gebruikt door risicobeoordeling op het gebied van informatiebeveiliging en privacy. Door risico's te beoordelen kun je ze met elkaar vergelijken en in de loop van de tijd bepalen of risico's toe- of afnemen.

De risicoscores zijn een indicatie. Ze vormen een aanvulling op wat je eigenlijk al wist. En drukken je intuïtie cijfermatig uit.

<kop>Kwantificeer de risico's
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 laag	1 - Klein
2 – Laag	2 - Middel
3 – Middel	3 - Groot
4 – Hoog	4 - Ernstig

Door de kansscore en de impactscore met elkaar te vermenigvuldigen, krijg je de risicoscore. Je kunt de scores inzichtelijk maken door ze met kleuren te illustreren.

		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 van 6 of 9	Hoog risico
Score van 12 of 16	Extreem risico

Tip: Maak organisatiebrede afspraken over hoe je scores toewijst aan een risico. En stel risicocriteria vast: welke risicoscore is voor je organisatie acceptabel, en welke *niet*. Zie ook de pagina: <link>Organisatorische randvoorwaarden voor risicomanagement.

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 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

<kop>Formuleer oplossingen

Nadat je de risico's hebt beoordeeld, bepaal je of en welke oplossingen nodig zijn om met risico's om te gaan. En welke dat zijn.

Op hoofdlijnen je de volgende opties om met risico's om te gaan:

- **Verkleinen** – je verkleint het risico door oplossingen die de impact van een gebeurtenis verminderen of die de kans op een gebeurtenis terugbrengen (of zelfs: die een gebeurtenis geheel voorkomen)
- **Overdragen** – je belegt de verantwoordelijkheid bij een andere partij, bijvoorbeeld wanneer de oplossing organisatiebreed uitgevoerd moet worden.
- **Accepteren** – je kiest ervoor om vooralsnog de risico's te accepteren.

Stel pragmatische oplossingen voor. Hiermee sluit je aan bij het idee uit de nieuwe Archiefwet en -regelgeving dat organisaties <link naar FAQ>*passende* maatregelen moeten treffen op het gebied van duurzame toegankelijkheid.

- Houd rekening met **haalbaarheid**. De haalbaarheid (technisch, organisatorisch en financieel) kun je toetsen met specialisten zoals business-analisten. Aan de hand daarvan kun je de oplossingen prioriteren.
- 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 informatiedomeinen van toepassing zijn.

De oplossingen voeg je toe aan de overzichtstabel. Geef ook een prioritering aan. En benoem wie de **risico-eigenaar** is. Deze persoon is verantwoordelijk voor het uitvoeren van oplossingen.

<kop> Overzichtstabel risicobeoordeling – maatregelen

Risico	Kwalificatie	Oplossing	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

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 lager dan 6 beschouwt de organisatie als acceptabel. Er zijn dan geen acties nodig.

<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, en 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 (<link>stap 1)
- Een **beschrijving van het onderzoeksproces** inclusief vooronderzoek (<link>stap 2), betrokken collega's (<link>stap 3) en gespreksverslagen (<link>stap 4)
- Concrete **beschrijving van risico's** (<link>stap 5).
- **Aanbevelingen** voor mogelijke oplossingen met prioritering (<link>stap 6).

Let op: Plaats in de rapportage de nadruk op de risico's die jij hebt geconstateerd op basis van het gesprek. Focus niet op de antwoorden op de ja/nee vragen uit de vragenlijst. Die antwoorden creëren al snel een vals gevoel van veiligheid. Als bijvoorbeeld 10 van de 12 vragen met een 'ja' worden beantwoord, dan is 83% positief

beantwoord. Dat roept bij een proceseigenaar geen gevoel van urgentie op. Terwijl achter de vragen die met een 'nee' zijn beantwoord ernstige risico's verscholen kunnen gaan. En bij vragen die aanvankelijk met een 'ja' worden beantwoord, kunnen de verdiepingsvragen aan het licht brengen dat er ook daar nog risico's weggenomen kunnen worden.

Tips:
- Maak voor zover mogelijk gebruik van een bestaand format voor een risicorapportage.
- Sluit aan bij bestaande analyses uit informatiebronnen zoals auditrapporten
- Focus op kansen in plaats van negatieve uitkomsten: 'we kunnen geld besparen' in plaats van 'we zijn nu veel geld kwijt'.

<Kop>Bespreek de risicorapportage
Leg de risicorapportage tot slot in een gesprek voor aan het verantwoordelijke management en andere betrokkenen. Zorg dat je scherp hebt wie de risico-eigenaar is. Het kan bijvoorbeeld gaan om een organisatiebreed risico dat onder de verantwoordelijkheid van de directie valt. Of om een applicatie-specifiek risico dat een actie vereist van de proceseigenaar. Maak dat onderscheid tussen organisatie- en procesgebonden ook duidelijk in de rapportage. Een proceseigenaar is niet verantwoordelijk voor organisatiebrede risico's, al kan die misschien wel een rol spelen bij het bespreekbaar maken daarvan.

De risico-eigenaren besluiten uiteindelijk welke oplossingen uitgevoerd worden. Denk met de risico-eigenaren mee en toon begrip voor hun positie. Zo laat je zien dat je als informatieprofessional een serieuze gesprekspartner bent die begrijpt dat er keuzes gemaakt moeten worden.

Tip: In de module <link> DUTO-risicobeoordeling en risicomanagement wordt de rol van het verantwoordelijk management verder beschreven.

De risico-eigenaren geven hun commentaar op de risicorapportage in de vorm van een **managementreactie**. Deze voeg je als apart hoofdstuk of bijlage toe aan de risicorapportage. De managementreactie neem je ook op in de overzichtstabel. Hiermee is duidelijk wat de vervolgstappen zijn. Hierop kan het verantwoordelijk management actief sturen.

<subpagina> Nazorg

Na het maken van een risicorapportage is jouw rol niet uitgespeeld. Integendeel, je biedt nazorg. Dit houdt in dat:

- je **proactief helpt** om de afgesproken acties uit te voeren;
- je **controleert** of het beoogde resultaat is bereikt;
- je **monitort**: je let op factoren binnen en buiten de organisatie die van invloed kunnen zijn op bestaande risico's of de kans op nieuwe risico's vergroten. Denk aan (nieuwe) wet- en regelgeving, het aanschaffen, bouwen of herinrichten van een applicatie en een reorganisatie. Door regelmatig te monitoren, krijg je inzicht in actuele risico's en kun je anticiperen op nieuwe risico's maar ook positieve kansen benutten;
- je **initiatief neemt** om te starten met een nieuwe risicobeoordeling, waarbij je eerdere ervaringen en leermomenten meeneemt.

Kortom, door met de risico-eigenaren mee te blijven denken en te werken, levert de DUTO-risicobeoordeling concrete resultaten op voor duurzaam toegankelijk informatiebeheer binnen de organisatie en helpt het om <link>risicomanagement binnen de organisatie verder te ontwikkelen.