# <titel>DUTO-risicobeoordeling als onderdeel van risicomanagement

Deze handreiking richt zich op DUTO-risicobeoordeling. Dat is het concrete proces waarbij informatieprofessionals bepalen welke risico’s er voor een organisatie bestaan op het gebied van informatiebeheer. En hoe ernstig deze risico’s zijn. Of het nu gaat om risico’s op het vlak van informatiebeheer of op andere vlakken: regelmatige risicobeoordeling is onderdeel van een breder beleid dat zorgt dat risicomanagement binnen een organisatie belegd is.

Deze module bevat:

* <link>Uitleg over de plaats die DUTO-risicobeoordeling binnen risicomanagement inneemt
* <link>Aanwijzingen voor beslissers en managers die betrokken zijn bij het inrichten van processen op het gebied van risicomanagement
* <link>Aanwijzingen voor beslissers en managers die een risicorapportage hebben ontvangen en op basis daarvan tot actie moeten overgaan

Wil je weten hoe je daadwerkelijk een DUTO-risicobeoordeling uitvoert, ga dan naar het<link>stappenplan.

# <subpagina>Risicomanagement

**DUTO-risicobeoordeling** is een belangrijk onderdeel van risicomanagement. Het genereert de input die het mogelijk maakt om risico’s te herkennen en daarop te acteren. Dit maakt het mogelijk om efficiënter te presteren, in te kunnen spelen op veranderingen, en toe te werken naar de strategische doelstellingen van de organisatie.

Met **risicomanagement** bedoelen we de gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot risico's (NEN-IS0 31000:2019, 3.2). Dat houdt onder meer in dat bij besluitvormingsprocessen rekening gehouden wordt met bestaande risico’s. Alle risico’s wegnemen kan niet, managen kan wel.

Een visuele weergave van de plek die risicobeoordeling inneemt binnen het bredere kader van risicomanagement, wordt voor deze plek nog voorbereid

**<kop>Managers en beslissers aan zet**

Managers en beslissers zijn op **twee momenten** aan zet:

* bij het *inrichten* van het proces. Om te zorgen dat een DUTO-risicobeoordeling waardevolle en bruikbare inzichten op kan leveren;
* op het moment dat een DUTO-risicobeoordeling uitgevoerd is en geleid heeft tot een *risicorapportage*. Op dat moment is het nodig om de inzichten uit die risicobeoordeling door te vertalen naar concrete plannen.

We noemen <link naar subpagina ‘Organisatorische borging’>vijf belangrijke zaken die binnen een organisatie op orde moeten zijn om DUTO-risicobeoordeling goed tot zijn recht te laten komen;

We bieden <link naar subpagina ‘Overgaan tot actie’> aandachtspunten en advies om te zorgen dat de conclusies uit een risicorapportage ook worden doorvertaald naar concrete acties.

# <subpagina>Vooraf: organisatorische borging van DUTO-risicobeoordeling

Om DUTO-risicobeoordeling mogelijk te maken is het nodig om binnen een organisatie een aantal zaken goed te regelen. Dit zijn randvoorwaarden voor het effectief uitvoeren van risicobeoordeling.

|  |  |
| --- | --- |
| **Randvoorwaarde** | **Toelichting** |
| Commitment | Er is commitment binnen de organisatie voor het DUTO-risicomanagement. Dat blijkt er bijvoorbeeld uit dat er regelmatig betrokkenheid wordt uitgesproken. |
| Besluitvormingsprocessen | Er is beleid vastgesteld voor het risicomanagement en het is verankerd in de organisatie. Dit beleid vertaalt zich door in het beschikbaar stellen van mensen en middelen voor het uitvoeren van risicobeoordeling. |
| Cyclisch werken | Het risicomanagement wordt uitgevoerd in zich herhalende patronen. |
| Integrale benadering | Er zijn initiatieven op het gebied van risicomanagement bij andere I-domeinen (privacy, informatiebeveiliging en openbaarmaking) |
| Overzicht over applicaties en processen | Er is een overzicht van de processen, applicaties en de daarmee samenhangende overheidsinformatie in de organisatie. Met dit overzicht kun je inzicht krijgen in welke processen door welke applicaties worden ondersteund en waar overheidsinformatie zich bevindt. Dit helpt bij het bepalen van de reikwijdte van de DUTO-risicobeoordeling. |

Deze randvoorwaarden zijn afgeleid van NEN-ISO 31000:2019. In de <link>Veelgestelde vragen lichten we nader toe hoe deze en andere normen binnen deze handreiking doorvertaald worden naar de context van informatiebeheer bij de Nederlandse overheid.

## <uitklapmenu>Commitment

Het risicomanagement in een organisatie moet op strategisch niveau zijn ingebed. Het hoger management moet zich bewust zijn van het belang van risicomanagement en de rol die daarin voor hen is weggelegd. De inbedding van risicomanagement in organisatie is erbij gebaat wanneer het belang herhaaldelijk door de hoogste managementlagen wordt onderschreven en daaraan gevolg wordt gegeven door het tonen van betrokkenheid.

Dit draagt bij aan de adoptie van risicomanagement in de organisatie. Top-down-sturing kan een impuls geven aan risicomanagement in een organisatie. Wanneer het leiderschap in een organisatie regelmatig het belang benadrukt van risicomanagement, bevordert de aandacht voor het onderwerp.

## <uitklapmenu>Besluitvormingsprocessen

De besluitvormingsprocessen betreffen zowel de besluiten die nodig zijn voor het inrichten van het risicomanagement voor duurzame toegankelijkheid, als het integreren van het risicomanagement in de governance, afspraken en structuren van de organisatie. Het risicomanagement moet niet losstaan van bedrijfsactiviteiten die organisatie uitvoert.

Denk hierbij aan:

* Het **vaststellen en verankeren van beleid** ten behoeve van het risicomanagement. Heldere beleidskeuzes geven richting aan hoe het risicomanagement in de organisatie vorm gegeven moet worden en maken duidelijk welke uitgangspunten daarbij gelden.
* De **benodigde middelen** voor het risicomanagement. Risicomanagement kan alleen effectief worden uitgevoerd als wordt geïnvesteerd in kennis en kunde. Dat kan bijvoorbeeld door te investeren in opleiding van medewerkers of het werven van specialisten. Daarnaast moeten organisatieonderdelen die risicomanagement uitvoeren ook over geschikte tooling kunnen beschikken, bijvoorbeeld om resultaten te kunnen vastleggen, monitoren en rapporteren.
* Het **vastleggen van bevoegdheden, verantwoordelijkheden en verantwoording**. Om risicomanagement te kunnen uitvoeren, moet het duidelijk zijn wie verantwoordelijk is voor de uitvoer daarvan en welke bevoegdheden daarbij horen. Voor onderzoekers die informatiesystemen onderzoeken, moet duidelijk zijn wie verantwoordelijk is voor de informatie in een bedrijfsproces en kan besluiten over de maatregelen om risico’s te managen.De integrale werkwijze kan bevorderd worden als de verschillende I-domeinen ook dicht bij elkaar zitten in de organisatiestructuur, bijvoorbeeld als ze deel uit maken van dezelfde afdeling.

## <uitklapmenu>Cyclisch werken

Het risicomanagement wordt uitgevoerd in zich herhalende patronen. Dit heeft meestal de vorm van PDCA-cyclus (Plan, Do, Check en Act): het maken van een plan, het uitvoeren van het plan, het evalueren van de resultaten en het uitvoeren van de aanpassingen om de verbeteringen te bewerkstelligen.

Dit heeft de volgende voordelen:

* **Actueel beeld van risico’s:** Door het werken in een PDCA-cyclus , wordt het DUTO-risicomanagement een doorlopend proces, met als gevolg dat het overzicht van risico’s actueel blijft.
* **Cumulatieve verbetering:** Door kort-cyclisch te werken met zichzelf herhalende stappen, wordt continu gewerkt aan het mitigeren van risico’s. Het eindresultaat van één cyclus biedt een nieuwe en betere uitgangspositie voor de start van de volgende cyclus. Het resultaat is doorlopende vermindering van risico’s.
* **Procesoptimalisatie:** Organisaties die kort-cyclisch werken, kunnen snel inspelen op veranderende omstandigheden.

## <uitklapmenu>Integrale benadering

Het versterkt de impact van een DUTO-risicobeoordeling als informatieprofessionals samenwerken met de andere i-domeinen: privacybescherming, informatiebeveiliging, en gegevensmanagement. Door risicobeoordeling voor duurzame toegankelijkheid te integreren met initiatieven van andere i-domeinen, kan het effect worden vergroot en een hogere efficiëntie worden bereikt. Daarbij wordt ook de lijnorganisatie ontlast, omdat de uitvraag door de verschillende domeinen gecoördineerd plaatsvindt.

Integraal te werken houd onder andere de volgende acties in:

* **Stem onderzoeksvragen op elkaar af**

Onderlinge afstemming tussen aanverwante i-domeinen, zoals met privacy en informatiebeveiliging over onderzoeksvragen die gesteld worden bij de inventarisatie van de risico’s. Daarmee kan worden voorkomen dat een organisatieonderdeel vanuit verschillende i-domeinen gelijksoortige of tegenstrijdige vragen krijgt. Het verkrijgen van een integraal beeld heeft ook voordelen voor de i-domeinen. Denk bijvoorbeeld aan risico’s die gelopen worden als het DUTO-proces vernietigen niet goed is ingericht, dat levert ook risico’s op voor de bescherming van persoonsgegevens. En risico’s gerelateerd aan een DUTO-functie als toegangsbeheer zijn ook vanuit het perspectief van informatiebeveiliging relevant. Een holistische aanpak helpt om maatregelen op elkaar af te stemmen;

* **Voer gezamenlijk onderzoek uit**

De lijnorganisatie wordt minder belast als de verwante i-domeinen onderzoeksvragen waar mogelijk bundelen. Het kan ook een goed idee zijn om gezamenlijk het gesprek met proceseigenaren te voeren over risico’s. Dit help voorkomen dat proceseigenaren zich overvallen voelen door een opeenvolging van onderzoeken vanuit verschillende vakgebieden.

* **Stel een RACI tabel op**

Door in de voorbereiding een RACI-tabel (of vergelijkbare methodiek) op stellen, wordt duidelijk welke belanghebbenden er zijn en wat hun relatie is tot het risicomanagement. Door de belangen van de stakeholders in kaart te hebben kan gerichter onderzoek gedaan worden en aangewezen worden wie verantwoordelijk is voor het oppakken van de actiepunten die voortkomen uit een risico-rapportage.

## <uitklapmenu>Overzicht

Er is overzicht van processen, wettelijke context, informatiestromen en -systemen, gehanteerde standaarden en hun samenhang, bijvoorbeeld een architectuuroverzicht. Zie ook de <link naar RVW08 DUTO-raamwerk>randvoorwaarde in het DUTO-raamwerk.

Het overzicht maakt duidelijk welke processen er zijn, over welke informatie de organisatie beschikt, waar deze zich bevindt en wie daarvoor verantwoordelijk is. Een architectuuroverzicht geeft daarbij ook een beeld van de wetgeving en kaders die richting geven aan de werkprocessen. Het overzicht helpt bij het bepalen van de scope voor de risicobeoordeling en het maken van het plan van aanpak.

# <subpagina>Achteraf: overgaan tot actie

Het uitvoeren van de risicobeoordeling resulteert in een eindrapportage met in ieder geval de bevindingen conclusies. Op basis hiervan kan het management weloverwogen besluiten nemen. Zo kan het management besluiten om:

* Niets te doen; de bestaande situatie blijft gehandhaafd
* Een dieper gaande analyse te laten uitvoeren op bepaalde risico’s om beter inzicht te krijgen
* Maatregelen uitvoeren om risico’s weg te nemen of te verkleinen.

Tevens is de eindrapportage voor managers een hulpmiddel om aan auditors en toezichthouders inzichtelijk te maken dat ze in het kader van risicomanagement systematische risicobeoordeling uitvoeren aan de hand van een formele methodiek.

Het management is nu aan zet om mogelijke maatregelen te treffen met betrekking tot de risico’s. Het is mogelijk dat de eindrapportage ook al een advies bevat aan het management over de te nemen maatregelen. De keuze om dit advies wel of niet te geven kan gemaakt, worden bij het opstellen van het plan van aanpak.

Aandachtspunten voor het management bij het nemen van maatregelen zijn:

* Vaak wordt afweging gedaan op kosten, inspanningen ten opzichte van de mogelijke voordelen. Echter het wel of geen maatregelen treffen met betrekking tot risico is niet alleen kwestie van geld. Ook kwalitatieve baten zoals het perspectief van compliance met wet- en regelgeving, dienstverlening aan burgers, doelstellingen van de organisatie en afspraken met ketenpartners dienen bij de besluitvorming meegenomen te worden
* In plaats van te focussen op nadelige gevolgen, kunnen door wegnemen van risico’s ook kansen ontstaan
* In het geval van integrale behandeling met andere I-domeinen zoals privacy en informatiebeveiliging, kan het nemen van passende maatregelen ook positieve gevolgen hebben voor deze I-domeinen. Bijvoorbeeld als er risico bestaat op gebied van toegangsbeheer (dit verder uitwerken) of op zoeken en vinden (openbaarheid) Voorbeeld bedenken waarbij passende maatregel voordelen oplevert voor meerdere domeinen.
* Wanneer passende maatregelen worden getroffen, betekent dit niet het einde van risicobeoordeling. Hierop moet ook gestuurd worden. Soms leveren maatregelen andere resultaten op dan verwacht of kunnen er nieuwe risico’s ontstaan. Nog verbinding maken met verantwoordelijkheid management in relatie tot risicomanagement?
* Bij het opstellen van een actieplan om maatregelen te treffen worden ook de medewerkers betrokken die expertise hebben op het gebied van DUTO en daarover kunnen adviseren.

Er zijn twee hulpmiddelen die kunnen helpen bij het ontwikkelen van een actieplan naar aanleiding van een risicobeoordeling

## <uitklapmenu>De “wat is aanvaardbaar” methode

Deze methode is ook wel bekend als de As low as reasonably practicable (ALARP) methode. Deze methode kan worden gebruikt om te beslissen of een bepaald risico aanvaardbaar is of niet en of hierop maatregelen getroffen moeten worden. Deze methode gaat uit van het principe dat het risiconiveau wordt teruggebracht tot een laag, redelijkerwijs niveau.

De risico’s worden geordend op aanvaardbaarheid:

* onaanvaardbaar, wanneer het risico alleen in buitengewone omstandigheden kan worden gerechtvaardigd;
* aanvaardbaar, waarbij het risico verder moet worden beperkt als dit redelijkerwijs haalbaar is;
* algemeen aanvaardbaar (tussen ondraaglijk en aanvaardbaar), waar het risico zo laag is dat verdere risicoreductie hoeft niet te worden overwogen.

## <uitklapmenu>Kosten-baten analyse

Hierbij identificeer je verschillende maatregelen die je wilt treffen om een risico te verkleinen of weg te nemen. Je geeft daarbij de te verwachte kosten en voordelen aan.

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.