

<pagina>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. Hoe groot deze zijn en wat de gevolgen hiervan kunnen zijn. Risicobeoordelingen (dus ook DUTO-risicobeoordeling) zijn activiteiten die onderdeel vormen van een breder geheel: risicomanagement.

Deze module werkt aan de hand van **vijf randvoorwaarden** uit wat organisaties moeten regelen om risicomanagement organisatorisch te borgen.

- <link> Organisatorische borging van risicomanagement

Eerst gaat de module in op de volgende vragen:

- Wat is het verschil tussen DUTO-risicobeoordeling en risicomanagement?
- Wat zijn de voordelen van risicomanagement?
- Wat is de rol van het verantwoordelijk management binnen risicomanagement?

<kop> DUTO-risicobeoordeling en risicomanagement

Om een relatie te kunnen leggen tussen DUTO-risicobeoordeling en risicomanagement, maken we gebruik van de volgende definities:

- Met **risicomanagement** bedoelen we de gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot risico's (NEN-ISO 31000:2019, 3.2).
- Een **risicobeoordeling** is een methode die zorgt voor inzicht in welke risico's er bestaan, hoe groot deze risico's zijn en welke maatregelen genomen kunnen worden.
- Een **DUTO-risicobeoordeling** is een risicobeoordeling met een specifieke focus op risico's die ontstaan wanneer overheidsinformatie niet duurzaam toegankelijk is.

Om zelf een DUTO-risicobeoordeling uit te voeren, kun je de <link>Quickscan gebruiken. Of het uitgebreidere <link>stappenplan DUTO-risicobeoordeling.

<kop> Voordelen van risicomanagement

Deugdelijk ingericht risicomanagement op het gebied van informatiebeheer heeft drie voordelen:

- Het maakt het makkelijker om DUTO-risicobeoordeling uit te voeren. Met name het <link>Stappenplan gaat ervanuit dat organisaties randvoorwaarden rondom risicomanagement hebben ingevuld.
- Het zorgt ervoor dat de resultaten van een DUTO-risicobeoordeling opgenomen worden in het besluitvormingsproces. Zodat de bevindingen uit een risicobeoordeling leiden tot weloverwogen besluiten waarmee risico's beheersbaar worden gemaakt.
- Het draagt bij aan het verwezenlijken van de doelstellingen van de organisatie (of onderdelen daarvan).

<kop> De rol van het verantwoordelijk management

Het verantwoordelijk management is op **twee momenten** aan zet:

1. Bij het inrichten van het proces rondom risicomanagement.

Wat er geregeld moet worden op dit gebied lees je op de pagina over <link> de organisatorische borging van risicomanagement

2. Op het moment dat een DUTO-risicobeoordeling is uitgevoerd en geleid heeft tot een risicorapportage.

Het verantwoordelijk management moet dan als risico-eigenaar besluiten te nemen over de inzichten uit de DUTO-risicobeoordeling. En sturen op concrete acties met benodigde mensen en middelen.

<subpagina>Organisatorische randvoorwaarden voor risicomanagement

Om DUTO-risicobeoordeling mogelijk te maken, moeten organisaties een aantal zaken goed te regelen op het gebied van risicomanagement. Er zijn vijf randvoorwaarden voor het effectief uitvoeren van risicobeoordeling. De tabel hieronder zet ze kort op een rijtje.

Randvoorwaarde	Toelichting
Besluitvormingsprocessen	Er is beleid vastgesteld voor het risicomanagement en het is verankerd in de organisatie. Dit beleid vertaalt zich onder andere door het beschikbaar stellen van mensen en middelen voor het uitvoeren van een risicobeoordeling. Verantwoordelijkheden zijn duidelijk belegd. Ook het uitwerken van nadere procedures en criteria voor risicobeoordeling horen hierbij.
Cyclisch werken	Het risicomanagement wordt uitgevoerd in zich herhalende patronen, zoals een PDCA-cyclus waar risicobeoordelingen een onderdeel van vormen.
Integrale benadering	Trek samen op met andere bedrijfsonderdelen met een vergelijkbaar takenpakket. Voor risicomanagement op het gebied van informatiebeheer betekent dat samenwerking met andere I-domeinen (privacy, informatiebeveiliging, gegevensmanagement en openbaarmaking).
Overzicht	Zorg dat je de structuur van de organisatie en de inrichting van bedrijfsprocessen goed in beeld hebt. Voor risicomanagement op het gebied van informatiebeheer betekent dit dat je een overzicht hebt van de processen, applicaties en informatie in de organisatie. Dit overzicht biedt inzicht in hoe de processen worden ondersteund met applicaties, wie daar verantwoordelijk voor is en waar de overheidsinformatie zich bevindt.

Randvoorwaarde	Toelichting
Commitment	Er is commitment binnen de organisatie voor DUTO-risicobeoordeling. Commitment is voor een groot deel gedragsmatig. Dat blijkt bijvoorbeeld uit dat er regelmatig betrokkenheid wordt uitgesproken door de verschillende managementslagen voor het risicomanagement. Maar ook door constructieve samenwerking tussen proceseigenaren en informatieprofessionals bij uitvoeren van risicobeoordeling met een gedeeld beeld van de bedoeling en noodzaak.

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.

<kop>Uitwerking van organisatorische randvoorwaarden voor risicomanagement <uitklapmenu>Besluitvormingsprocessen

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

Denk hierbij aan:

Beleid over:	Toelichting
Te hanteren normen, richtlijnen en modellen	Een voorbeeld is het vaststellen van een metagegevensschema zoals MDTO. Een organisatie kan ook in beleid vastleggen dat informatiesystemen <i>by design</i> worden ingericht conform het DUTO-raamwerk en dat het maken van een risicobeoordeling daar een steevast onderdeel van is.
Handelswijze rondom het risicomanagement	Het is duidelijk hoe de organisatie risicomanagement ziet en hoe dit wordt uitgevoerd in de organisatie.
Risicocriteria	Het is duidelijk hoeveel risico en welk soort risico de organisatie mag nemen ten opzichte van de doelstellingen van een organisatie en hoe deze afgewogen worden. In het stappenplan DUTO-risicobeoordeling kun je zien hoe de risico's gewogen kunnen worden<Link stap 6 van het stappenplan>.

Beleid over:	Toelichting
Benodigde middelen	Risicomanagement kan alleen effectief worden uitgevoerd als wordt geïnvesteerd in kennis en kunde. Bijvoorbeeld door te investeren in opleiding van medewerkers of het werven van specialisten. Daarnaast moeten organisatieonderdelen die risicomanagement uitvoeren ook over geschikte hulpmiddelen kunnen beschikken, bijvoorbeeld om resultaten te kunnen vastleggen, monitoren en rapporteren.
Bevoegdheden, verantwoordelijkheden en verantwoordingsplicht	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 bij wie de risico's thuishoren. De risico-eigenaar (meestal een proceseigenaar) kan besluiten over de passende maatregelen met betrekking tot de risico's.

<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 cyclisch te werken met zichzelf herhalende stappen, wordt continu gewerkt aan het verminderen of wegnemen 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, gegevensmanagement en openbaarmaking. Door risicobeoordeling voor duurzame toegankelijkheid te integreren met initiatieven van andere informatiedomeinen, 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. Bovendien kan het nemen van passende maatregelen ook positieve gevolgen hebben voor deze domeinen. Bijvoorbeeld als er risico's bestaan op gebied van toegangsbeheer of op zoeken en vinden, kan het nemen van passende maatregelen positieve gevolgen hebben voor meerdere domeinen tegelijkertijd.

Integraal werken houdt onder andere in dat:

- **Onderzoeksvragen op elkaar worden afgestemd**

Er is onderlinge afstemming tussen aanverwante 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 informatiedomeinen gelijksoortige of tegenstrijdige vragen krijgt. Het verkrijgen van een integraal beeld heeft ook voordelen voor de i-domeinen. Denk bijvoorbeeld aan risico's die een organisatie kan lopen als het DUTO-proces vernietigen niet goed is ingericht, kan dat ook risico's op leveren 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.

- **Er een gezamenlijke risicobeoordeling wordt uitgevoerd**

De lijnorganisatie wordt minder belast als de verwante 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.

- **Duidelijk is wie waarvoor verantwoordelijk is**

Als je de belanghebbenden in beeld hebt, kun je gericht onderzoek doen. En aanwijzen wie verantwoordelijk is voor het oppakken van de actiepunten die voortkomen uit een risicobeoordeling. Dat kan door in de voorbereiding een RACI-tabel op stellen waar instaat wie betrokken is en wat hun rol is

<uitklapmenu>Overzicht

Er is een overzicht van processen, wettelijke context, informatiestromen en -systemen, gehanteerde standaarden en hun samenhang, bijvoorbeeld een architectuuroverzicht. Dit is een van de <link naar RVW08 DUTO-raamwerk>randvoorwaarden die in het DUTO-raamwerk zijn opgenomen voor organisatorische borging van duurzame toegankelijkheid.

Het overzicht maakt duidelijk welke processen er zijn, over welke informatie de organisatie beschikt, waar deze zich bevindt en wie daarvoor verantwoordelijk is. Het overzicht helpt bij het <link stappenplan stap 1> bepalen van de scope voor de risicobeoordeling en <link stappenplan stap 3>het maken van het plan van aanpak.

<uitklapmenu>Commitment

Risicomanagement is effectief als de verschillende lagen van de organisatie blijken dat ze dit een belangrijk onderwerp.

Commitment door:	Toelichting
Management	De inbedding van risicomanagement in de organisatie is erbij gebaat wanneer het belang herhaaldelijk door de hoogste managementlagen wordt onderschreven. Daarbij wordt ook naar de organisatie gecommuniceerd wat de bedoeling is van het risicomanagement en hoe zich dat verhoudt tot de doelstellingen van de organisatie. Top-down-sturing kan een impuls geven aan risicomanagement in een organisatie. Wanneer het leiderschap in een organisatie regelmatig het belang van risicomanagement benadrukt, bevordert dit de aandacht voor het onderwerp.

Commitment door:	Toelichting
Proceseigenaar	De proceseigenaar kan bijdragen aan commitment door binnen het organisatieonderdeel dat verantwoordelijk is voor de uitvoer van het bedrijfsproces, te communiceren over de bedoeling van de risicobeoordeling en hoe dat bijdraagt aan de doelstellingen van het bedrijfsproces.
Informatieprofessional	De informatieprofessional kan bijdragen aan commitment door een constructieve gesprekspartner te zijn van de business. De informatieprofessional moet in staat zijn om de meerwaarde van een DUTO-risicobeoordeling uit te leggen op een manier die aansluit bij behoeften en zorgen van de proceseigenaar. Door mee te denken over effectieve oplossingen om de risico's te beheersen en kansen te benutten, wordt risicobeoordeling meer dan een 'moetje'. Het levert de proceseigenaar concreet iets op.