

SURF

Handreiking bij toolkit risicobeoordeling



Deze handreiking is beschikbaar onder de licentie Creative Commons Naamsvermelding 4.0 Internationaal.



Oktober 2024

Toolkit risicobeoordeling

Doel van de handreiking

Deze handreiking is onderdeel van de toolkit risicobeoordeling. De handreiking geeft een inleiding op risicobeoordeling en samen met de andere onderdelen van de toolkit helpt het instellingen op weg om zelf een risicobeoordeling te faciliteren.

Eis uit het SURFaudit toetsingskader

Een risicobeoordeling is een stap uit het risicomanagementproces. Het staat als volgt beschreven in het SURFaudit toetsingskader, onder RM02:

Instellingen voeren risicobeoordelingen uit om actuele risicoprofielen met betrekking tot bedrijfsdoelstellingen te bepalen. De waarschijnlijkheid en impact van alle geïdentificeerde risico's worden regelmatig beoordeeld, met behulp van kwalitatieve en kwantitatieve methoden. De waarschijnlijkheid en impact van inherente en restrisico's worden bepaald per categorie, op portefeuillebasis.

Onderdelen van de toolkit

De toolkit bestaat uit een handreiking, printbare kaartjes, een excel bestand en een powerpoint presentatie voor de workshop.



| Inleiding

ISO 31000 en ISO 27005

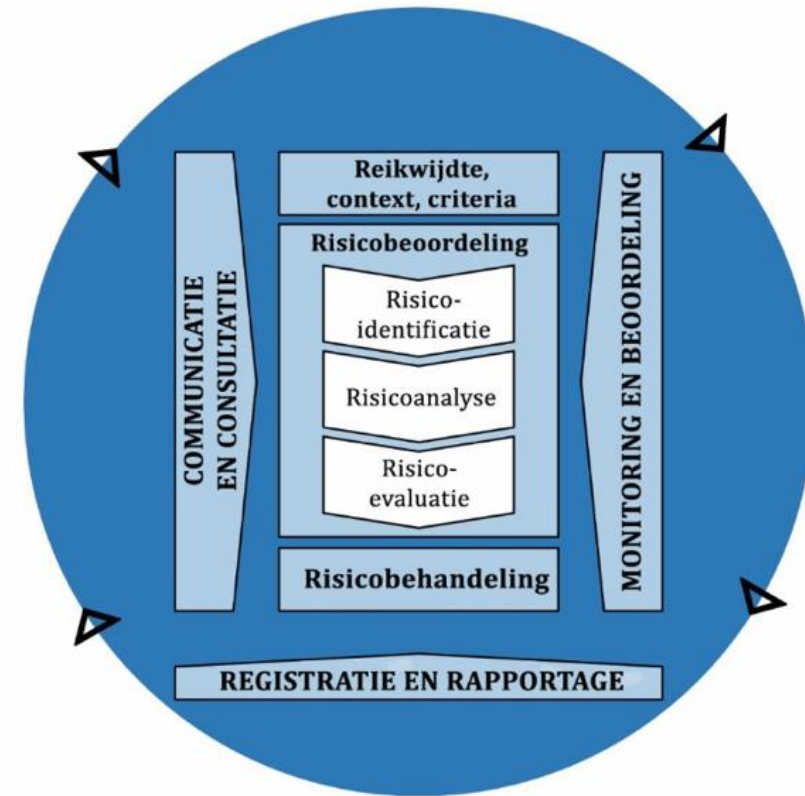
Een risicobeoordeling is een stap binnen het risicomanagementproces.

In de ISO 31000 standaard voor risicomanagement bestaat een risicobeoordeling uit 3 stappen: risico-identificatie, risicoanalyse en risico-evaluatie.

In deze handreiking worden de drie stappen toegelicht en specifiek gemaakt voor informatierisico's.

Het nemen van risicobeperkende maatregelen (de risicobehandeling) is de stap die na een risicobeoordeling volgt en wordt niet behandeld in deze handreiking.

De ISO 27005 is een uitwerking van de ISO 31000 specifiek voor het beheersen van informatiebeveiligingsrisico's. Naar beide normen wordt in deze handreiking regelmatig verwezen.



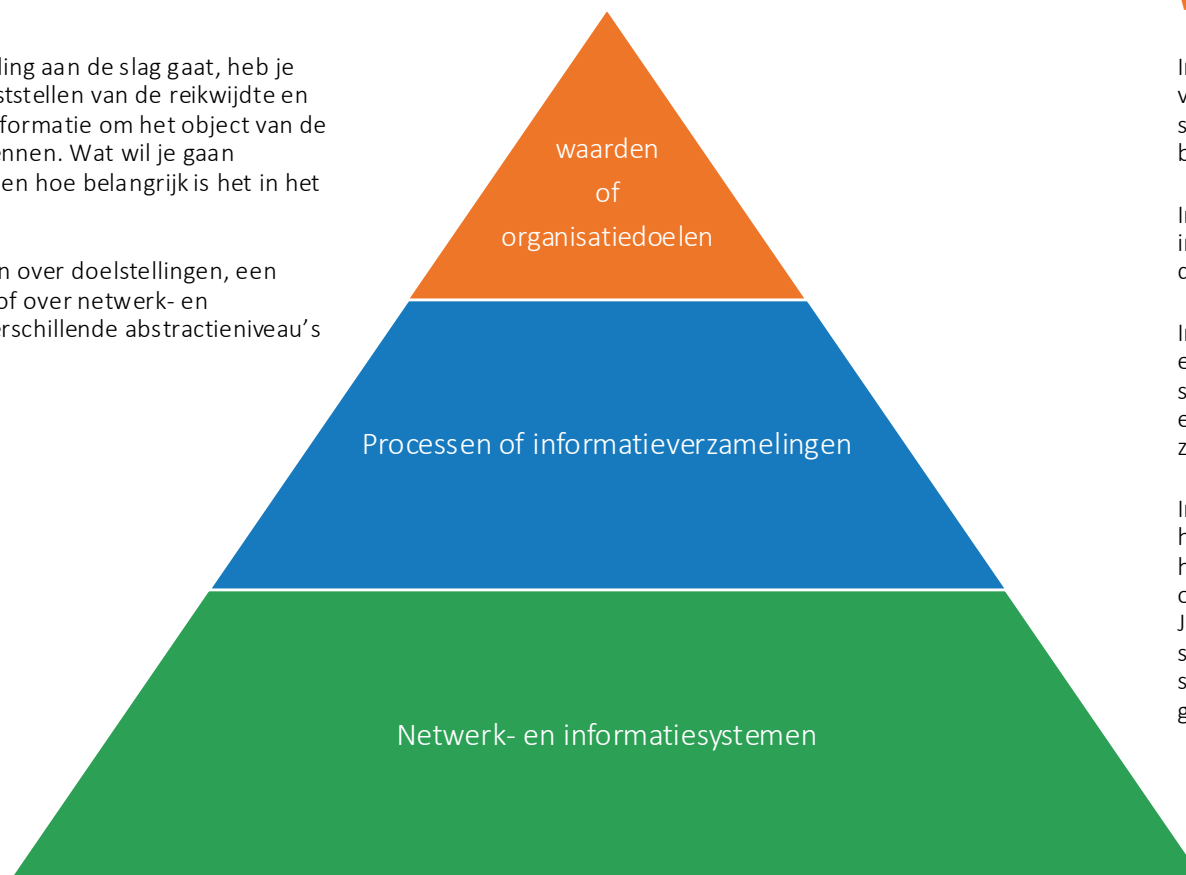
Risicomanagementproces volgens ISO NEN 31000:2018+C11:2019

| Voorbereiding

Reikwijdte en context

Voordat je met een risicobeoordeling aan de slag gaat, heb je eerst de stap ervoor gezet: het vaststellen van de reikwijdte en context. In die stap verzamel je informatie om het object van de risicobeoordeling goed te leren kennen. Wat wil je gaan beschermen, wie beslist daarover en hoe belangrijk is het in het grotere geheel van de instelling?

Je kunt een risicobeoordeling doen over doelstellingen, een proces of informatieverzameling, of over netwerk- en informatiesystemen. Er zijn dus verschillende abstractieniveaus denkbaar.



Abstractieniveaus van hetgeen je wilt beschermen en gaat beoordelen tijdens het risicobeoordelingsproces

Wat wil je beschermen?

In de voorbereiding zet je op een rij aan welke doelstellingen het object van beoordeling een bijdrage moet leveren. Hiervoor kun je de strategische plannen van de instelling of afdeling erbij pakken en naar de bedrijfsimpactanalyse (BIA) of de enterprise architectuur kijken.

In documentatie van de BIA staat hoe belangrijk processen zijn voor de instelling. Uit de BIA volgt een opsomming van activiteiten en processen die prioriteit hebben tijdens een verstoring.

In een enterprise architectuur staat niet alleen hoe informatie, applicaties en technologie samenhangen, maar ook de bedrijfsprocessen, functionele structuur, stakeholders, en strategie en principes van de organisatie. Een enterprise architectuur biedt dus ook steun bij organisatievraagstukken zoals risicomanagement.

Indien jouw organisatie geen (volledige) BIA of enterprise architectuur heeft, en dat ook niet snel kan opleveren, dan kun je met de eigenaar van het te beoordelen object (dat is de persoon die verantwoordelijkheid over het object moet afleggen aan de bestuurders) zelf de scope in kaart brengen. Je verzamelt zoveel mogelijk relevante informatie, bijvoorbeeld uit strategische jaarplannen of functionele eisen. Ook als je een systeemcomponent gaat beoordelen is het belangrijk te weten aan welke grotere doelstelling dat systeem bijdraagt.

| Organiseer een workshop

Wie doet de risicobeoordeling?

Nadat de voorbereiding is afgerond, de doelstellingen van je object bekend zijn, en relevante kennis is verzameld kan je de risicobeoordeling gaan organiseren. Idealiter zijn daarbij de eigenaar en experts aanwezig.

Eigenaar

Om iets goed te kunnen beschermen, moet het een eigenaar hebben. Bij voorkeur is dat een expliciete eigenaar. Lijnmanagers in primaire processen zijn de aangewezen personen om eigenaar te zijn. Zij geven dagelijkse leiding aan de organisatie, op de plekken waar het direct impact heeft als informatie niet betrouwbaar of beschikbaar is.

Idealiter wordt de uitvoering van een risicobeoordeling georganiseerd door de eigenaar zelf. Die is immers verantwoordelijk voor het identificeren van risico's. Bovendien ben je dan als informatiebeveiligers één van de expert-gesprekspartners aan tafel en hoeft je niet alle lasten op je eigen schouders te dragen. De eigenaar is idealiter ook zelf bij de sessies aanwezig om de om risico's te begrijpen, de risicobereidheid in te brengen, en te beslissen.

Hulptroepen

Bij informatiebeveiliging kijk je naar informatierisico's. Toch hangen informatierisico's nauw samen met andere risicocategorieën zoals financiën, compliance, privacy, bedrijfscontinuïteit of fysieke veiligheid. Een incident in het ene gebied kan namelijk een gevolg hebben voor een ander gebied. Bekende voorbeelden hiervan zijn wanneer ransomware ook een datalek is of als bij een inbraak in een gebouw ICT apparatuur wordt gestolen.

Dit soort gebeurtenissen kunnen veel geld kosten. Om die inschatting van kosten goed te kunnen maken heb je hulp van je collega's van financiën nodig en van de eigenaar van je object. Hetzelfde geldt voor de wisselwerking met andere vakgebieden zoals fysieke veiligheid, innovatie, internationalisering, inkoop, ICT, personeelszaken, juridische zaken of kennisveiligheid.

Pogingen om een risicobeoordeling in een silo te doen met alleen een focus op informatiebeveiliging zijn voorbestemd om onvolledig te zijn en kost ook heel veel energie. Die beperking zou je kunnen accepteren en bij je communicatie over risico's een disclaimer opnemen. Maar beter is het om zoveel mogelijk interdisciplinair te samenwerken.

Welke methode kies je?

In de ISO 31000 bestaat de risicobeoordeling uit drie stappen: risico-identificatie, risicoanalyse en risico-evaluatie. Waar het kortgezegd om gaat is het in woorden en waarden beschrijven van risico's en aangeven hoe belangrijk die risico's zijn.

Er bestaat een enorme hoeveelheid aan methoden om dit te doen. Hoe maak je nu een keuze voor een aanpak die past bij jouw object, ervaring en organisatie? Veel bekende methoden volgen niet letterlijk de bovengenoemde stappen en ze houden ook geen rekening met een interdisciplinaire aanpak. Ook deze handreiking is weer een van de vele manieren om een risicobeoordeling aan te pakken. Er is geen goed of slecht in deze: Informeer jezelf en kies vooral een aanpak die past bij jou en je omgeving.

Bij risicobeoordeling hoeft je echt niet altijd eerst te kiezen voor een formele methode. Het kan een prima start zijn om te beginnen op basis van gezond verstand en met wat je tot je beschikking hebt. Klein beginnen, hoe simpel ook, is altijd beter dan helemaal niets doen. Al doende leert men. Brainstormen, mindmaps maken, w-vragen stellen: allemaal goede eerste stappen als je geen andere middelen hebt. Ook hoeft je je in je organisatie niet te beperken tot één enkele methode. De resultaten van risicobeoordelingen uit verschillende methoden kun je vergelijken met behulp van taxonomieën. Wat wel belangrijk is, is dat je de resultaten documenteert.

Stap 1: Risico-identificatie

Doel

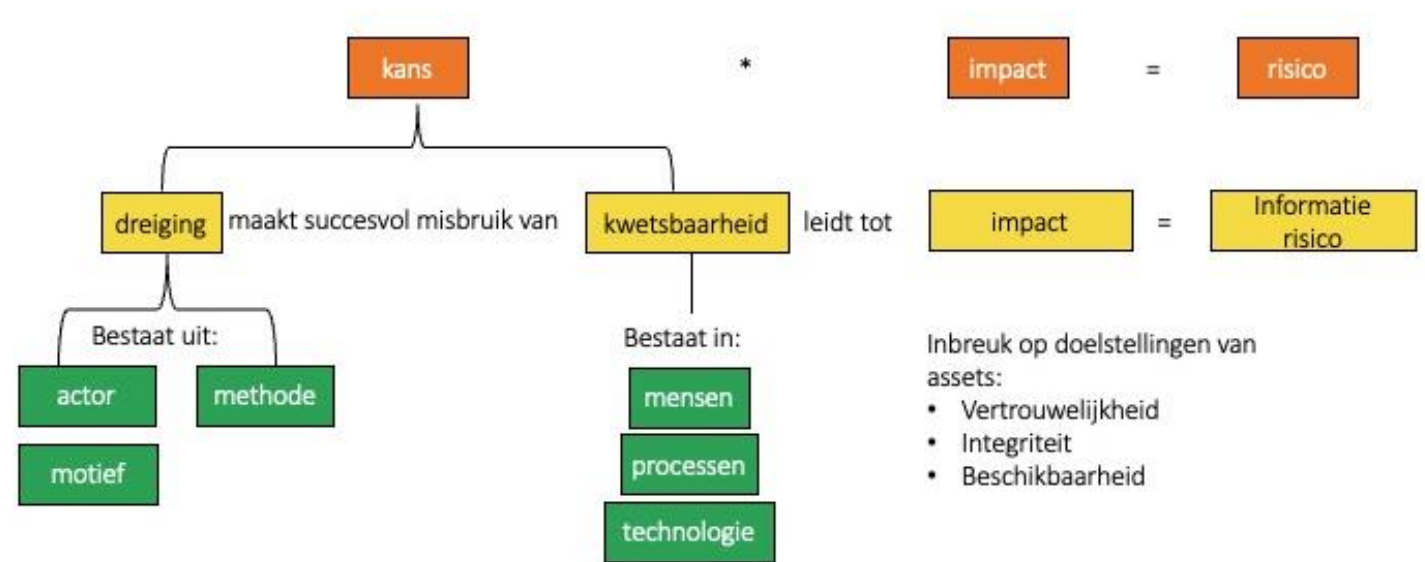
Het doel van de risico-identificatie is risico's te vinden, herkennen en beschrijven die verhinderen om de doelstellingen te bereiken. Daarbij is het belangrijk om niet te proberen reeds bekende problemen te beschrijven, maar juist te kijken naar indicatoren van opkomende risico's, dreigingen, aannames en overtuigingen.

Ter inspiratie kun wel kijken naar bekende informatie (incidenten overzicht uit het verleden, de privacy impact assessment, rapportages van crisisoefeningen, audits, relevante softwarekwetsbaarheden, rapporten over soortgelijke objecten), maar laat dit een inspiratie zijn. Probeer de vertaling te maken naar veranderingen in de omgeving. Dit kan een aanstaande reorganisatie zijn waardoor processen en mensen gaan veranderen. Het kan ook gaan over de verwachtingen die er zijn door nieuwe technologie of veranderende geopolitieke verhoudingen.

Termen

De termen risico's en dreigingen worden in de praktijk vaak door elkaar gebruikt. Zij zijn echter niet hetzelfde. Een risico is een scenario dat uit een aantal variabelen bestaat, waaronder dreigingen (actoren, hun motieven en methoden), kwetsbaarheden (in processen, menselijk handelen en technologie) en mogelijke vormen van impact of schade.

De opbouw van een risicoscenario



Een **dreiging** is vaak extern aan een organisatie en nauw verbonden met tegenstanders die de organisatie schade zouden kunnen berokkenen. Deze actoren hebben motieven en methoden (tactiek, technieken en procedures). Wij kunnen huidige dreigingen observeren en proberen toekomstige dreigingen te voorspellen. Maar intern in de organisatie bestaan ook dreigingen door medewerkers die onbedoeld fouten maken of moedwillig schade berokkenen. Andere dreigingen kunnen voortkomen uit de natuur (overstroming) of geopolitiek (oorlog, spionage).

Bij **impact** gaat het om schade aan de informatiedoelstellingen vertrouwelijkheid, integriteit en beschikbaarheid van het onderwerp van de risicobeoordeling. Impact kan ook doorwerken op andere doelstellingen of risicogebieden zoals intellectueel eigendom, privacy, compliance of reputatie.

Kwetsbaarheden zijn alle zwakke plekken in mensen, processen en de technologie. Processen kunnen onhandig zijn ontworpen of zelfs ontbreken. Mensen staan onder druk en kunnen vergissingen maken of hebben te weinig kennis om een informatiesysteem goed te gebruiken. De technologie kan slecht ontworpen zijn of later gevonden software kwetsbaarheden bevatten.

Scenarios

Bij het beschrijven van risico's neem je alle variabelen mee in scenario's. Bovenstaande illustratie laat zien hoe je een risicobeschrijving kan opbouwen.

Stap 2: Risicoanalyse

Kans en impact

In deze stap ga je een waarde geven aan het beschreven risicoscenario. Je kijkt dan naar de waarschijnlijkheid van optreden van een scenario en de ernst van de mogelijke impact.

Bij dreigingen kun je bijvoorbeeld een waarde geven aan de professionaliteit van de actor of je geeft een waarde aan de sterkte van het motief. Bij kwetsbaarheden neem je ook in beschouwing hoe doeltreffend bestaande beheersmaatregelen zijn. Als je veel data ter beschikking hebt kun je kwantitatief te werk gaan. Veel beginnende teams starten met kwalitatieve beoordelingen.

In de ISO 27005, bijlage A, staan tabellen die daarbij kunnen helpen. Je kunt ook je eigen schalen opstellen.

Heatmaps

Heatmaps zijn populair om verslag te leggen van de risicoanalyse. Onder risicoprofessionals is soms kritiek op de inhoudelijke waarde van heatmaps. Als het je helpt om de urgentie van een probleem over te brengen kan een heatmap handig zijn. Maak er echter geen doel van om het te maken, het is een middel om resultaten te communiceren.

Perceptie en groepsdenken

De risicoanalyse kan worden beïnvloed door meningsverschillen, vooroordelen, percepties van risico en oordelen. Een mogelijke manier om daarmee om te gaan is het volgen van de Delphi methode.

Delphi methode

In deze methode leg je het risicoscenario voor aan een groep respondenten. Deze vullen de waardering in, met een beschrijving van hun motivatie waarom ze dat denken. Je verzamelt de resultaten en berekent een gemiddelde.

Daarna vindt er terugkoppeling plaats naar de hele groep. Zij kunnen dan het gemiddelde zien, maar ook de uitschieters en de motivatie van de andere participanten. Het idee is dat deelnemers hun score kunnen aanpassen nadat ze de argumenten van de anderen hebben gezien. Na die tweede ronde kan er nog een derde ronde komen. Het doel is om te komen tot een grote mate van consensus.

Het is goed mogelijk deze methode online te gebruiken. Bijvoorbeeld door een groep op een Bulletin Board bijdragen te laten plaatsen over een onderwerp. Een gespreksleider zorgt ervoor dat samenvattingen gemaakt worden en de discussie in voornoemde fasen gedurende een aantal dagen of zelfs weken plaats vindt. Voordeel is dat de discussie zo gevoerd wordt op het moment en de plek dat het participanten goed uitkomt. Een ander voordeel van deze aanpak is dat gedurende het proces de documentatie groeit, waardoor je een verslaglegging hebt hoe een waardering tot stand is gekomen en welke overwegingen zijn meegenomen.



| Stap 3: Risico-evaluatie

Besluitvorming

De risico-evaluatie bereidt de besluitvorming door de eigenaar voor. De resultaten van de risicoanalyse worden op een rij gezet om te bepalen waar aanvullende actie vereist is. Dit kan leiden tot een besluit om:

- verder niets te doen;
- na te denken over opties voor risicobehandeling;
- verdere analyse uit te voeren om beter inzicht in het risico te hebben;
- bestaande beheersmaatregelen te handhaven;
- doelstellingen te herzien.

Hiermee zijn de 3 stappen van de risicobeoordeling afgerond.

kroonjuweel	Scenario	Kans	Impact	risicobereidheid	Geadviseerde actie:	toelichting
1	1	Waarschijnlijk -4-	Minimaal -1-	hoog	Accepteren	Situatie monitoren en indien wet- en regelgeving verandert opnieuw risicobeoordeling uitvoeren.
1	2	Zeer waarschijnlijk -5-	Kritiek -4-	laag	Mitigeren	Zo snel mogelijk beoordelen welke maatregelen nodig zijn en projectplan opstellen.
2	3	Mogelijk -3-	Minimaal -1-	hoog	Accepteren	Situatie monitoren.
2	4	Waarschijnlijk -4-	Catastrofaal -5-	laag	Mitigeren	Zo snel mogelijk beoordelen welke maatregelen nodig zijn en projectplan opstellen.

Voorbeeld van een risico-evaluatie uitkomst

Tot slot

Onzekerheid

Een van de moeilijkste elementen van risicomanagement is het accepteren dat subjectiviteit niet is uit te sluiten. Hoeveel informatie je ook verzamelt en hoe sterk je methode ook is, het blijft een inschatting gebaseerd op de ervaring van dat moment.

De essentie van risicomanagement is het kunnen nemen van een beslissing met die onzekerheid in het achterhoofd.

Gelukkig is het geen eenmalige exercitie! Natuurlijk kijk je meerdere keren per jaar terug naar je uitkomsten om deze te actualiseren. Hierdoor werk je ook aan het omgaan met onzekerheden.



Meer lezen?

Te beschermen belangen:

[Hoe breng ik mijn te beschermen belangen in kaart?](#)

Methodes:

[ENISA Risk management toolbox](#)

Dreigingen:

www.surf.nl/cyberdreigingsbeeld

Risico scenario's:

[ISACA: how to write risk scenario's](#)

Delphi:

[De Delphi methode nader bekeken](#)