

Handleiding risicobeoordeling vastleggen

Registeren van risico's in TrustBound GRC na de risicobeoordeling volgens de methode in de SURF Toolkit.

Auteur(s): SURF
Versie: 1.0
Datum: 30 juni 2026

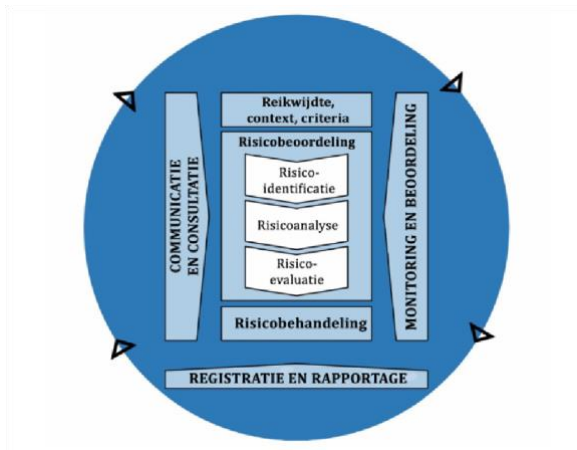
Deze publicatie is gelicenseerd onder een Creative Commons Naamsvermelding 4.0 Internationaal.

Inhoudsopgave

1	Inleiding	3
2	Vorbereiding, context	4
3	Risico-identificatie	6
4	Risico-analyse	8
4.1	Kans en impact: heatmap ontwerpen	8
4.2	Analyse vastleggen	10
5	Risico-evaluatie	11

1 Inleiding

Deze handleiding is onderdeel van de [toolkit risicobeoordeling](#) en neemt je mee in hoe je de uitkomsten van de stappen van risicobeoordeling vastlegt in het TrustBound GRC platform. Met 'risicobeoordeling' bedoelen wij hier een onderdeel van het risicomanagement proces uit het risicomanagement framework zoals beschreven in de ISO 31000 norm. De risicobeoordeling bestaat uit drie stappen: risico-identificatie, risicoanalyse en risico-evaluatie.



Figuur 1 Risicomanagement proces volgens ISO31000

Echter, voordat je een risicobeoordeling kunt uitvoeren, moet eerst duidelijk worden beschreven wat precies wordt beoordeeld. Pas daarna kunnen risico's worden geïdentificeerd, geanalyseerd en geëvalueerd. De [SURF toolkit risicobeoordeling](#) en de SURF training IT risicobeoordeling leggen uit hoe dit proces wordt uitgevoerd.

Deze handleiding richt zich uitsluitend op het vastleggen van de uitkomsten in TrustBound GRC. De volgorde van de stappen waarmee je informatie vastlegt in TrustBound GRC komt niet altijd overeen met de volgorde waarin je in de praktijk de informatie verzamelt. Let dus op: je proces wordt dus niet gestuurd door de tool en je gaat de tool pas gebruiken als je informatie hebt verzameld.

Werk je in de praktijk met het [Template Risicoregister](#)? De risicobeoordeling haalt informatie op die helpt bij het invullen van de kolommen D,E, G-L, N, S, en U van dat template. Deze handleiding laat zien hoe die informatie in het TrustBound GRC platform kan worden ingevoerd.

Keuzes voor maatregelen die risico's behandelen zijn de stap ná de risicobeoordeling en vormen geen onderdeel van de toolkit of van deze handleiding.

2 Voorbereiding, context

Voordat je met een risicobeoordeling aan de slag gaat, verzamel je informatie om het object van de risicobeoordeling goed te leren kennen. Wat is het doel, proces of object dat je gaat beoordelen, wat wil je beschermen? Je kunt een risicobeoordeling doen over doelstellingen, een proces of informatieverzameling, of over netwerk- en informatiesystemen. Zodra de scope duidelijk is, kun je die vastleggen in TrustBound GRC.

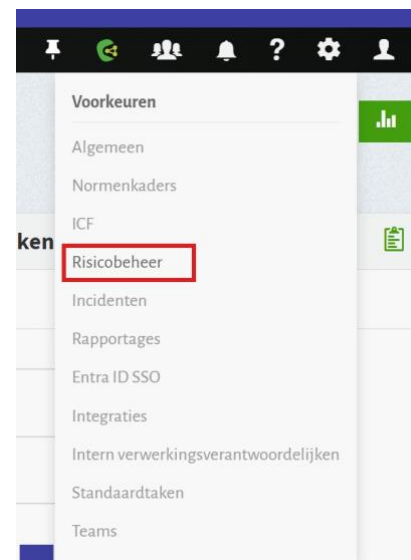
Functioneel Beheer van risico's in TrustBound

Een functioneel beheerder kan in TrustBound de voorkeuren rond risicobeheer configureren.

Mocht je deze optie niet zien als beheerder, stuur dan een bericht naar support@trustbound.com. Het is een optie die de servicedesk van TrustBound kan activeren voor jouw omgeving. Vraag naar het activeren van de **configuratiemogelijkheden voor Risicobeheer**.

Via **Voorkeuren => Risicobeheer** zijn de volgende configuratiemogelijkheden beschikbaar:

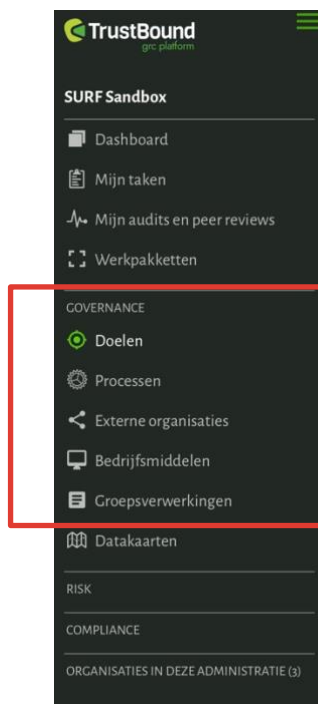
- Risicosoorten: standaard staan Kans en Risico actief. Deze kunnen naar wens verder worden aangevuld. De risicosoort *Kans* wordt in deze handleiding verder niet toegelicht.
- Risicomatrix: standaard is een 5-puntsschaal actief. Mocht je een andere indeling willen gebruiken, dan kan je die hier toevoegen. Let op: Stel de risicomatrix bij voorkeur éénmalig vast. Latere wijzigingen kunnen invloed hebben op reeds vastgelegde risico's



Registreren in TrustBound:

Ga naar de module Governance:

Handleiding risicobeoordeling vastleggen



1. Maak een nieuw doel, proces of asset (bedrijfsmiddel) aan. Dit is nodig omdat risico's altijd zijn gekoppeld aan een doelstelling of een te beschermen belang zoals een proces of asset (iets dat je wilt
2. Geef het doel, proces of asset (bedrijfsmiddel) een eigenaar. Dat is ook de eigenaar van het risico.
3. Klik op toevoegen.
4. Ga naar lijstweergave op het scherm om te controleren dat je onderwerp voor de risicobeoordeling goed is opgeslagen.

3 Risico-identificatie

Het doel van de risico-identificatie is risico's te vinden, te herkennen en te beschrijven. 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.

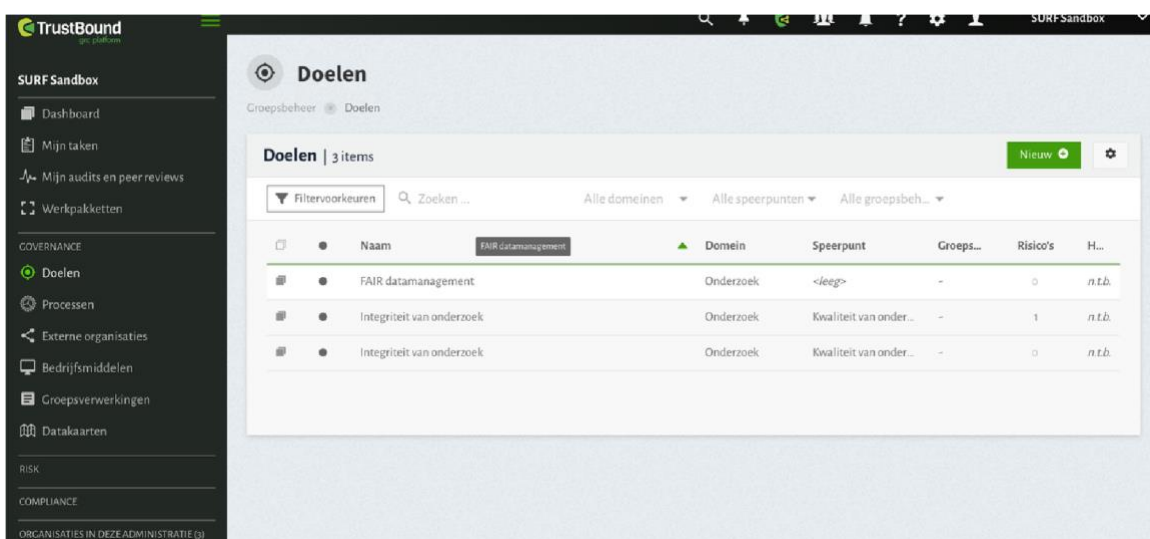
Geïdentificeerde risico's beschrijf je bij voorkeur in één zin: een **dreiging** manifesteert zich of maakt succesvol misbruik van een **kwetsbaarheid**, waardoor een **impact** ontstaat.

Als de dreigingen, kwetsbaarheden en impacten beschreven zijn, kun je die vastleggen in TrustBound GRC. Maar let op: in het proces zul je de stappen risico-identificatie, risico-analyse en risico evaluatie in de praktijk vaak iteratief doorlopen. Daarom is het soms handiger om eerst de volledige risicobeoordeling te hebben uitgevoerd voordat je je verslag en notities gaat vertalen naar het TrustBound platform.

Registreren in TrustBound GRC:

Ga naar de module Governance.

Vanuit de lijst weergave op het scherm kies je het doel, proces of asset (bedrijfsmiddel) dat je gaat beoordelen. In onderstaand voorbeeld kijken we naar met de lijst met doelen.



Klik op een doel naar keuze, dan krijg je het volgende scherm.

Handleiding risicobeoordeling vastleggen

FAIR datamanagement

Groepsbeheer • Doelen • FAIR datamanagement

FAIR datamanagement Bewerken

Gegevens • Taken • Risico's • Beheersmaatre... • Bijlagen

Beschikbaarheid op decentraal niveau

■ Dit doel heeft betrekking op de hele organisatie, centraal en decentraal.

Dienst 1
Faculteit 1
Faculteit 2

Naam van het doel	FAIR datamanagement
Status / Versie / Gewijzigd	Concept versie 0.1 17 april (Nicole van Deursen)
Domein	Onderzoek
Groepsbeheerder	Niet opgegeven
Eigenaar	Nicole van Deursen
Omschrijving van het doel	fdfdf bla bla

4. Klik op tabblad Risico's.

5. Klik op de groene knop: Nieuw risico.

6. Vul de velden in.

- Voer een of meerdere dreigingen in. Op dit moment is dit een keuzelijst met standaard dreigingen. Gebruikers kunnen aan Trustbound vragen om een standaardlijst in te voeren. Je kunt dus zelf kiezen wat jouw standaarddreigingen zijn, bijvoorbeeld op basis van SURF dreigingsbeeld, MAPGOOD, ISO 27005, RAVIB, Mitre of een zelf samengestelde lijst.
- Beschrijf kwetsbaarheden die van toepassing zijn in het veld 'oorzaken'. Op dit moment is dit de beste plek om zwakke plekken van je onderwerp van risicobeoordeling te benoemen. Dit gaat over zwakke plekken in processen, mensen of technologie. Maar het zou ook over de fysieke omgeving en bewaking/beveiliging kunnen gaan.
- Geef inschatting van mogelijke impacten in het veld 'gevolgen'. Er kunnen meerdere impacten van toepassing zijn.
- De velden Classificatie en Categorie beheer je zelf en zijn aanpasbaar, je kan dit in de dashboards gebruiken om te filteren op de risico's.

7. Klik op toepassen en sluiten.

Risico toevoegen

Dreiging
Geen dreigingen geselecteerd.

Soort risico
☐ Operationeel risico
 ☐ Strategisch risico
 ☐ Tactisch risico

Titel
Titel voor risico:

Groepseigenaar
Nicole van Deursen

Classificatie
Geen items geselecteerd

Categorie(en)
Geen items geselecteerd

Beschrijving 0/2000

Oorzaken 0/2000

Gevolgen 0/2000

Annuleren Toepassen Toepassen + sluiten

4 Risico-analyse

Het doel van de risico-analyse is 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.

4.1 Kans en impact: heatmap ontwerpen

In je [instellingsbeleid](#) heb je al vastgelegd hoe je waardes geeft aan kans en impact.

Waarde geven aan Kans (Dreiging én kwetsbaarheid)

5	Zeër waarschijnlijk: de dreigingsactor heeft sterke intentie, beschikt over de benodigde capaciteit en dergelijke activiteiten zijn eerder waargenomen. De mens, het proces of de technologie is kwetsbaar voor deze dreiging.
4	Waarschijnlijk: het is waarschijnlijk dat de actor effect veroorzaakt doordat er een <i>gematigde dreiging</i> uitgaat naar een <i>hoge kwetsbaarheid</i> , of een <i>hoge dreiging</i> naar een <i>beperkte kwetsbaarheid</i> .
3	Mogelijk: het is mogelijk dat de actor effect veroorzaakt doordat er een <i>gematigde dreiging</i> uitgaat naar een <i>gematigde kwetsbaarheid</i> .
2	Onwaarschijnlijk: het is onwaarschijnlijk dat de actor effect veroorzaakt doordat er een <i>beperkte dreiging</i> uitgaat naar <i>gematigde kwetsbaarheid</i> , of een <i>gematigde dreiging</i> naar een <i>beperkte kwetsbaarheid</i> .
1	Zeër onwaarschijnlijk: het is zeer onwaarschijnlijk dat de actor effect veroorzaakt doordat deze een <i>beperkte dreiging</i> vormt en het doelwit ook <i>beperkt kwetsbaar</i> is.

Waarde geven aan Impact

5. Catastrofaal	• De impact is direct en immens. Alle aangesloten onderwijsinstellingen kampen met serieuze problemen en dat raakt ook nationale belangen. En/of het heeft dood tot gevolg.
4. Kritiek	• De impact is groot. De geraakte organisatie functioneert niet meer, en zal er niet of nauwelijks meer van kunnen herstellen. Ook diens partners worden dus geraakt. En/of het heeft zwaar letsel tot gevolg.
3. Aanzienlijk	• Het geraakte systeem of proces functioneert niet meer en moet hersteld worden, met flinke reputatieschade en financiële en/of juridische gevolgen. En/of heeft het tot onveilige situaties geleid.
2. Significant	• Het geraakte systeem of proces functioneert tijdelijk niet naar behoren door uitval van beschikbaarheid, integriteit en/of vertrouwelijkheid. De consequenties voor de organisatie zijn te overzien.
1. Beperkt	• Er wordt niet of nauwelijks hinder ondervonden door de gebeurtenis en het kan volledig hersteld worden met beperkte middelen.

Wanneer je gebruik maakt van heatmaps om kans en impactschalen te visualiseren, kun je deze ook in TrustBound vastleggen.

Registreren in TrustBound:

Ga naar 'voorkeuren' (dat is het tandwiel in de balk aan de bovenkant).

Klik op het tabblad 'risicomatrixen'. Standaard is er een 5x5 matrix beschikbaar. Indien nodig kun je een nieuwe risicomatrix aanmaken. Je kunt hier kiezen of je een matrix wil maken per bepaald type risico, of eentje voor alle soorten risico's. Kies voor opslaan en bewerken.

Handleiding risicobeoordeling vastleggen

Nieuwe risicomatrix

Groepsbeheer » Voorkeuren » Risicobeheer » Nieuwe risicomatrix

Algemeen Normenkaders ICF **Risicobeheer** Incidenten ...

Nieuwe risicomatrix

Naam van de risicomatrix*

SURF toolkit

Risicosoorten ⓘ

Operationeel risico, Strategisch risico, Tactisch risico

Daarna kun je invullen of je een 5x5 matrix wil of iets anders.

Risicomatrix bewerken

Publiceren ↗ ⋮

Naam van de risicomatrix*

SURF toolkit

Risicosoorten ⓘ

Operationeel risico, Tactisch risico, Strategisch risico

X-as label

Kans

Y-as label

Impact

Matrix

5	-	-	-	-	-		
4	-	-	-	-	-		
3	-	-	-	-	-		
2	-	-	-	-	-		

Blootstellingsniveaus

+

Aantal X-as waarden (cellen)

5 x ▾

Aantal Y-as waarden (cellen)

5 x ▾

Matrix cel

Klik op een cel in de matrix om deze te bewerken.

Annuleren

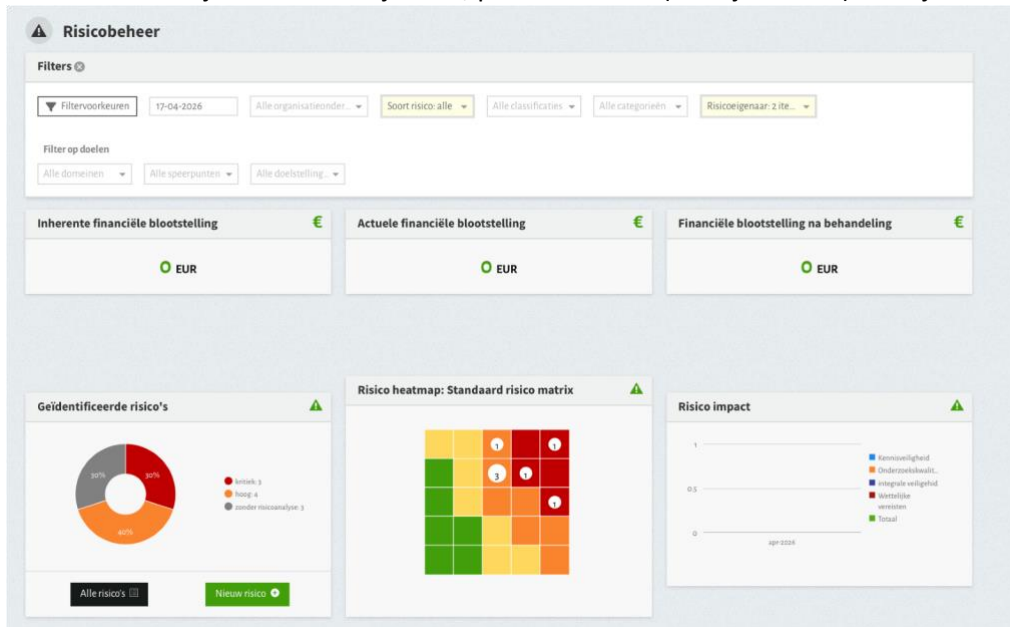
Toepassen Toepassen + sluiten

Klik op publiceren rechtsboven.

4.2 Analyse vastleggen

Ga naar module RISK en kies voor Risicobeheer.

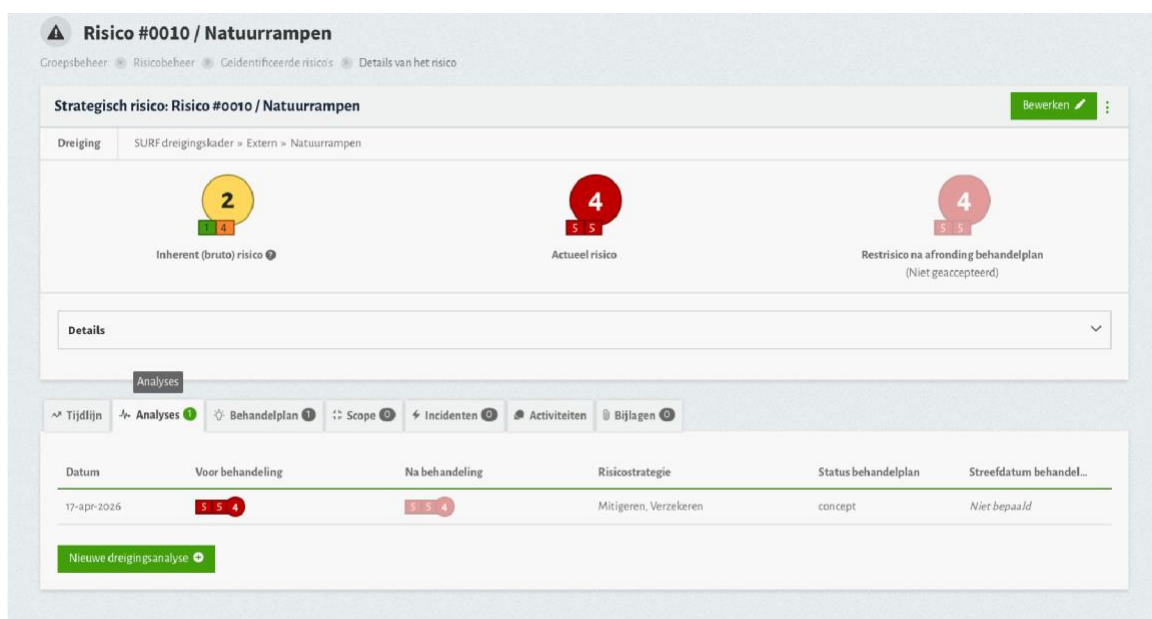
Via de filters kun je zoeken naar je doel, proces of asset (bedrijfsmiddel) waar je mee bezig was.



Klik op het zwarte vakje: 'alle risico's'.

Zoek daar het risico dat je eerder hebt aangemaakt.

Klik op het tabblad analyses en maak een nieuwe dreigingsanalyse aan. Wat in het TrustBound platform 'dreigingsanalyse' wordt genoemd, heet in de SURF Toolkit de 'risico-analyse'.



Let op! Dit is een test- en trainingsomgeving. Wijzigingen worden niet overgenomen in Productie.

Actueel risico Risicobehandeling Restrisiko

De beginwaarden voor Kans x Impact en de risicobehandeling zijn overgenomen uit de laatste dreigingsanalyse, d.d. 17 april 2026.

Datum van deze dreigingsanalyse ?
20-04-2026

Kans ?
Waarschijnlijk

Impact ?
Groot

Impact

Kans

Toelichting op de gekozen waarde voor Kans 0/2000

Toelichting op de gekozen waarde voor Impact 0/2000

Annuleren Opslaan

5 Risico-evaluatie

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.

Handleiding risicobeoordeling vastleggen

Registreren in TrustBound:

Zoek je risico weer op en kies voor het tabblad 'behandelplan'.

Risico #0010 / Natuurrampen

Groepsbeheer • Risicobeheer • Geïdentificeerde risico's • Details van het risico

Strategisch risico: Risico #0010 / Natuurrampen Bewerken

Dreiging: SURF dreigingskader » Extern » Natuurrampen

2

Inherent (bruto) risico

4

Actueel risico

4

Restrisico na afronding behandelplan
(Niet geaccepteerd)

Details

Eigenaar Nicole van Deursen	Beschrijving dfsdf
Infrastructuur componenten Niet opgegeven	Oorzaken vul hier de zwakke plekken in
Classificatie Niet opgegeven	Gevolgen beschrijf hier impacten
Categorie(en) Niet opgegeven	

~ Tijdlijn ~ Analyses 1 ~ **Behandelplan** ~ Scope ~ Incidenten ~ Activiteiten ~ Bijlagen

Concept — Aangeboden ter beoordeling — Bezig — Afgerond

Risicostrategie: **Mitigeren, Verzekeren**
Dit is de gekozen risicostrategie uit de laatste dreigingsanalyse. [Klik hier om te bewerken.](#)

	MRT '26	APR '26	MEI '26	JUN '26	JUL '26	AUG '26	SEP
BC.05-VWN Crisismanagement SURFAUDIT IB TOETSINGSKADER (NBA)*							

Vandaag

Onder 'risicostrategie' kies je welke optie jouw organisatie heeft gekozen voor dit risico. Klik op opslaan. De overige velden zijn niet van toepassing op de stappen in de risicobeoordeling.

Handleiding risicobeoordeling vastleggen

Let op! Dit is een test- en trainingsomgeving. Wijzigingen worden niet overgenomen in Productie.

Inherent (bruto) risico Actueel risico **Risicobehandeling** Restrisico

Dit is de eerste dreigingsanalyse voor dit risico; daarom kunt u naast het actuele risico ook het inherente (bruto) risico opgeven.

Risicostrategie ?

Mitigeren x Verzekeren x

Accepteren
Mitigeren
Overdragen
Vermijden
Verzekeren

Normen-/toetsingskader

Kies een normen-/toetsingskader

Beheersmaatregelen selecteren

Selecteer een normen-/toetsingskader om maatregelen te selecteren.

Verwijderen Annuleren Opslaan