Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# Hoe breng ik mijn te beschermen belangen in kaart?

Een aantal concrete eerste stappen

# Inleiding

Deze publicatie biedt praktische handvatten die je kunt gebruiken om de 'te beschermen belangen' (TBB's) van jouw organisatie in kaart te brengen. Wanneer je jouw te beschermen belangen in kaart hebt gebracht kun je deze vervolgens gebruiken om bijvoorbeeld een risicoanalyse uit te voeren.

## Doelgroep

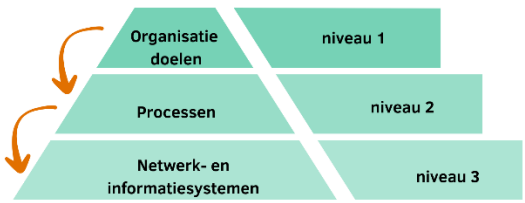
Dit kennisproduct richt zich op personen die werkzaam zijn op tactisch niveau van organisaties die willen beginnen met het in kaart brengen van hun te beschermen belangen.

## Deze publicatie is tot stand gekomen met bijdragen van:

Directie CIO Rijk, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Digital Trust Center, Bluebird & Hawk B.V., CISO-Office, Ministerie van Infrastructuur en Waterstaat, PBLQ

## Wat is een te beschermen belang?

Een organisatie heeft haar eigen organisatie doelstellingen. De organisatie heeft er belang bij dat deze doelstellingen worden behaald (niveau 1). Om deze doelstellingen te realiseren wordt er informatie verwerkt, en zijn er processen ingericht (niveau 2). Deze processen worden ondersteund door netwerk- en informatiesystemen (niveau 3). Te beschermen belangen hebben betrekking op alle onderstaande niveaus.




Iedere organisatie heeft haar eigen unieke te beschermen belangen.

Deze publicatie helpt je om een eerste (ruwe) lijst van jou te beschermen belangen op procesniveau samen te stellen. Het NCSC adviseert om te starten met het in kaart brengen van jouw organisatiedoelstellingen (niveau 1), om vervolgens de processen in kaart te brengen (niveau 2).

Een voorbeeld van een te beschermen belang op niveau 2 is: *de mogelijkheid om ten behoeve van het proces voorraadbeheer tijdig nieuwe voorraden te kunnen bestellen.*

## NIS2

Artikel 21, lid 1 van de NIS2-richtlijn verplicht entiteiten passende en evenredige technische, operationele en organisatorische maatregelen te nemen, afgestemd op de risico's die zich voordoen. Dit kennisproduct helpt je om de eerste stappen te zetten om deze risico's in kaart te brengen.

In het kader van de NIS2-richtlijn verwijst een te beschermen belang naar netwerk- en informatiesystemen die essentieel zijn voor de beschikbaarheid, veiligheid en integriteit van processen. Denk hierbij aan:

**Informatiebeveiliging:** de bescherming van vertrouwelijke informatie tegen ongeautoriseerde toegang, wijziging of vernietiging

**Operationele continuiteit:** netwerk- en informatiesystemen die bij uitval de primaire dienstverlening van de organisatie verstoren.

# 1. Randvoorwaarden scheppen en opdracht formuleren

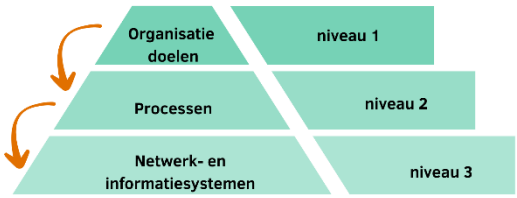
Voordat je aan de slag gaat met het in kaart brengen van jouw te beschermen belangen is het belangrijk om de juiste randvoorwaarden te scheppen. In deze stap schrijf je een beknopt plan van aanpak. Dit plan helpt je om draagvlak bij collega's te creëren en is het uitgangspunt om mandaat te verkrijgen van het bestuur van jouw organisatie.

## Bepaal de definitie van een TBB voor jouw organisatie

Voordat je de TBB's van jouw organisatie in kaart kunt gaan brengen, is het belangrijk dat je scherp hebt wat dit omvat. Jouw definitie van een TBB beschrijf je in een plan van aanpak. Dit helpt bij het inventariseren van TBB's en het voeren van de dialoog over hoe belangrijk een bepaalde TBB is ten opzichte van een andere TBB.

Het NCSC adviseert om TBB's te bezien in de eerdergenoemde abstractieniveaus:

- **Niveau 1: organisatiedoelstellingen**
- **Niveau 2: processen** die ondersteunend zijn aan deze organisatiedoelen.
- **Niveau 3: netwerk- en informatiesystemen** die deze deze processen faciliteren en informatieverwerking mogelijkmaken.




### Concretiseren van de organisatiedoelen

Elke organisatie heeft haar eigen specifieke doelstellingen. Aan deze doelstelling kleven diverse belangen. Denk hierbij aan financiële-, juridische-, reputatie- en veiligheidsbelangen. Om de organisatiedoelen te kunnen (blijven) realiseren moeten deze risico's voldoende worden beperkt.

Begin met het concretiseren van de doelstelling(en) van jouw organisatie en definieer op hoofdlijnen welke categorieën belangen hiermee gemoeid gaan. In bijlage 1 is een inspiratielijst bijgevoegd die je kunt gebruiken als startpunt.

*Voorbeeld: mijn organisatie is een commerciële dienstverlener gericht op het maken van winst. De belangrijkste belangencategorieën zijn financieel, reputatie en juridisch.*

### Essentiële processen definiëren

Vervolgens bepaal je welke organisatieprocessen essentieel zijn ten aanzien van de hierboven genoemde categorieën van belangen.

*Voorbeeld: voor een commerciële dienstverlener is de continuïteit van het verkoopproces en het bijhouden van klantgegevens essentieel om de organisatiedoelstellingen te bereiken.*

### NIS2

**Kritieke netwerk en informatiesystemen bepalen**

NIS2 richt zich slechts op netwerk- en informatiesystemen (niveau 3). Na het definiëren van essentiële informatie en processen kan worden bepaald wat de meest kritieke netwerk en informatiesystemen zijn.

Het NCSC adviseert organisaties die nog aan het begin staan van het krijgen van zicht op hun TBB's om deze stap nog niet te zetten en eerst haar TBB's op het niveau van processen (niveau 2) in kaart te brengen.

## Hoe bepaal ik de waarde van een TBB?

Naast zicht op essentiële processen moet je deze ook waarderen en prioriteren. De aanpak hiervoor beschrijf je ook in het plan van aanpak.

### TBB-waardering: een draaiknop, geen schakelaar

Bij het waarderen van TBB's adviseert het NCSC om een 5-punts schaal aan te houden. Zo kun je TBB's waarderen (en prioriteren) zonder deze mogelijk onterecht als *geen* TBB te classificeren (later in de publicatie wordt hier verder op ingegaan).

Een voorbeeld van een 5-punts schaal is:

- **Zeer groot belang**
- **Groot belang**
- **Matig belang**
- **Beperkt belang**
- **Geen belang**

Voorbeeld van een waardering:

- Beperkt belang: *wanneer onbevoegden toegang krijgen tot bepaalde informatie, heeft dit tijdelijke (uren) en beperkte nadelige gevolgen voor de organisatie.*

- Zeer groot belang: *wanneer onbevoegden toegang krijgen tot bepaalde informatie, komt het voortbestaan van de organisatie in direct gevaar.*

### Procesvoorstel

Nadat je een definitie hebt bepaald van een TBB voor jouw organisatie (dit mag nog ruw zijn), is het belangrijk om in het plan de verschillende processtappen in volgorde te beschrijven. In jouw procesvoorstel zou bijvoorbeeld kunnen staan dat je:

1. Verschillende stakeholders in kaart gaat brengen.
2. Een eerste inventarisatie gaat maken van aan informatie die reeds aanwezig is op het gebied van organisatiedoelstellingen en processen (Zie bijlage 1 voor voorbeelden).
3. Dialooggespreken en/of een workshop met collega's gaat organiseren waarin je belangen inventariseert en met elkaar prioriteert.
4. De resultaten in een referentietabel gaat samenvatten (zie hoofdstuk 3).
5. Deze referentietabel aan het bestuur als oplevert en eventuele vervolgstappen toelicht en toetst.

### Een ruw resultaat is goed genoeg

*'Perfect is the enemy of good enough.'*

Voor organisaties die nog geen of beperkt zicht hebben op hun te beschermen belangen adviseert het NCSC om in deze eerste inventarisatie de doelen niet te hoog te stellen. Een eerste ruwe lijst met TBB's die beperkt zijn onderbouwd, gewaardeerd in een referentie tabel, is in deze eerste stap een prima resultaat en een goede basis voor verdere iteraties.

## 2. Mandaat en draagvlak

In de vorige stap heb je de randvoorwaarden geschept om de te beschermen belangen van jouw organisatie in kaart te brengen. De volgende stap in dit proces is om mandaat te verkrijgen bij het bestuur van jouw organisatie.

### Mandaat verkrijgen

Om mandaat te verkrijgen van het bestuur van jouw organisatie ga je in gesprek. In dit gesprek kun je het procesvoorstel dat je geschreven hebt ter besluitvorming aanbieden bij het bestuur van jouw organisatie.

### NIS2 en het bestuur

De NIS2 verplicht het bestuur van een entiteit om genomen maatregelen voor het beheer van cyberbeveiligingsrisico's goed te keuren en toe te zien op de uitvoering hiervan.[1] Het bestuur is ook verplicht om een opleiding te volgen op het gebied van cybersecurity en deze toonbaar actueel te houden. Tevens kan het bestuur onder de NIS2 hoofdelijk aansprakelijk gesteld worden bij overtreding.

[1] NIS2, artikel 20, lid 1

### Hoe overtuig ik het bestuur?

Zorg dat je dezelfde taal spreekt als het bestuur van jouw organisatie. Probeer zo veel als mogelijk technische termen te vermijden en ga het gesprek op strategisch niveau aan. Leg uit waarom je de TBB's binnen jouw organisatie in kaart wil brengen en waarom dit belangrijk is. Probeer jouw uitleg simpel te houden en bij de kern van je voorstel te blijven.

### Gesprek met het bestuur

Tijdens het gesprek met het bestuur van jouw organisatie kun je bijvoorbeeld de volgende vragen stellen om meer beeld te krijgen bij de visie van het bestuur:

- Wat zijn de huidige en langetermijn doelen van onze organisatie?
- Welke zaken zijn kritiek voor ons bij het realiseren van deze doelen en onze bedrijfsvoering?
- Hoe stuur je op deze kritieke zaken?
- Voor welke belangrijke uitdagingen staat de organisatie?
- Wat zijn de belangrijkste kernwaarden van onze organisatie?
- Hoe wil je omgaan met zowel de kansen als bedreigingen van nieuwe technologieën en trends bij het realiseren van de organisatiedoelen?

Wanneer je in kaart hebt gebracht wat de doelen van jouw organisatie zijn kun je deze vervolgens als hulpmiddel gebruiken bij stap 3 om processen identificeren die cruciaal zijn voor de dienstverlening binnen jouw organisatie.

In samenspraak met het bestuur van jouw organisatie kun je relevante stakeholders identificeren die je moet spreken om een beeld te krijgen van de primaire processen binnen je organisatie. Voorbeelden van stakeholders zijn:

- Informatie-eigenaren
- Lijnmanagement
- Proceseigenaren
- Chief Information Office (CIO)
- Externe stakeholders zoals toeleveranciers

Zorg er tenslotte voor dat je overeenstemming bereikt over het geplande resultaat van jouw opdracht. De eerste stap zou een ruwe lijst met te beschermen belangen op procesniveau kunnen zijn. Deze kunnen dan op een later moment aangescherpt en verder geprioriteerd worden. Maak een keuze op basis van het volwassenheids- en ambitieniveau van jouw organisatie.

### Betrekken stakeholders

Na het verkrijgen van mandaat van het bestuur van jouw organisatie kun je de belangrijkste stakeholders gaan informeren. In deze gesprekken kunt je het doel van de opdracht toelichten en het proces uitleggen. Het is belangrijk dat je in deze fase benoemt wat je van de stakeholders verlangt en dat de wederzijdse verwachtingen duidelijk zijn.

## 3. TBB's in kaart brengen

In de voorgaande stappen heb je de voorbereidingen getroffen en mandaat verkregen. Het is nu tijd om echt aan de slag te gaan!

In deze stap ga je de TBB's van jouw organisatie in kaart brengen en vervolgens waarderen en prioriteren. Deze resultaaten verwerk je in een referentietabel.

### Inventariseren

Wanneer je de TBB's van jouw organisatie in kaart gaat brengen is het nuttig om éérst te inventariseren welke informatie er al beschikbaar is. Dit houdt in dat je praat met stakeholders binnen verschillende afdelingen, zoals bijvoorbeeld een inkoopafdeling.

Binnen deze afdelingen kun je veelal waardevolle informatie vinden over eerder geïdentificeerd risico's en eventuele TBB's.

Voorbeelden van waardevolle informatie die kunnen verwijzen naar TBB's bij een inkoopafdeling zijn:

1. Leveranciersinformatie zoals contracten, service level agreements en compliancestandaarden.
2. Risicoanalyses die zijn gemaakt voorafgaand aan het inkopen van een dienst of product.
3. Evaluaties van bestaande diensten waarin potentiele risico's worden genoemd.

Dergelijke informatie helpt je een eerste beeld te krijgen van de TBB's van jouw organisatie. Deze informatie kun je gebruiken als input tijdens het inventariseren van jouw TBB's. Samen met stakeholders binnen de organisatie ga je de dialoog aan om de TBB's verder te inventariseren, concretiseren en prioriteren.

## Dialoog

### Voorbereiding

Om de dialoog effectief te laten verlopen moet je ervoor zorgen dat de juiste mensen aan tafel zitten. In de vorige stappen heb je gesproken met verschillende stakeholders binnen de organisatie. Op basis van deze informatie kunt je een afweging maken welke mensen binnen jouw organisatie moeten deelnemen aan de dialoog.

### Werkvorm

Bepaal aan de hand van het type organisatie en het ambitieniveau wat een goede werkvorm is om binnen de organisatie de dialoog over TBB's aan te gaan. Het NCSC adviseert om één of meerdere workshops te organiseren met vijf tot maximaal acht deelnemers.

De ervaring leert dat bij grotere groepen dit ten koste van de kwaliteit van de dialoog gaat. Een alternatief is om meerdere 1-op-1 gesprekken te voeren. Het nadeel hiervan is dat je meer tijd kwijt bent en geen gebruik kan maken van de dynamiek van een groep met verschillende perspectieven.

### Referentietabel opstellen

Aan de hand van de inventarisatie maak je een eerste versie van een *referentietabel*. Een referentietabel is een tabel waarin je de TBB's van jouw organisatie kunt categoriseren en prioriteren. In bijlage 2 vind je een voorbeeld van een referentietabel.

Het NCSC adviseert de volgende eigenschappen:

- Een verticale y-as met daarin de 5 punts indeling als in de afbeelding/bijlage. Hier kun je de TBB's prioriteren van *zeer groot belang* tot *geen belang*.

- Een horizontale x-as met daarin de categorieën die aan het licht gekomen zijn gekomen tijdens de eerste inventarisatie. Voorbeelden van deze categorieen zijn: reputatie, financiele, juridische en veiligheidsbelangen. (een uitgebreide lijst van voorbeelden vind je in bijlage 1 van deze publicatie).

| | Financieel | Reputatie | Juridisch | Veiligheid |
|---|---|---|---|---|
| Zeer groot belang | | | | |
| Groot belang | | | | |
| Matig belang | | | | |
| Beperkt belang | | | | |
| Geen belang | | | | |

### Voorbereiden van de gesprekspartners

Voor een effectieve workshop of dialoog neem je bij start de deelnemers eerst mee in jouw plannen en het doel van de workshop. Denk bijvoorbeeld aan de onderstaande zaken:

- **Het beoogde resultaat:** na deze workshop hebben we een eerste ruwe lijst van TBB's op procesniveau.
- Het voorwerk dat je al hebt gedaan waarbij je stilstaat bij de **processtappen** die je doorlopen hebt met dit initiatief en het **mandaat** dat je hebt gekregen.
- De **definitie van een TBB** waarin je de verschillende abstractieniveau's uitlegt als in hoofdstuk 1.
- Dat je wil redeneren vanuit de **organisatie doelstellingen** en vanuit daar de TBB's op procesniveau wil bepalen.
- Je legt de werking van de **referentietabel** uit.

### De dialoog

Nadat je de partners hebt meegenomen in de doelen van de workshop en ieder aan de hand van jouw uitleg dezelfde taal spreekt kun je de dialoog starten. Werk hierbij van breed naar smal. Een voorbeeld van de invulling van de workshop is:

1. De deelnemers (zonder te veel sturing) zelfstandig laten nadenken over:
    a. Eventueel ontbrekende belangen categorieen op de x-as van de referentietabel
    b. De ontbrekende te beschermen belangen in de tabel

2. Vervolgens vraag je de deelnemers kort hun bevindingen toe te lichten en vangt deze inzichten op een whiteboard of flipover. De praktijk leert dat deelnemers vaak tot vergelijkbare inzichten komen. In samenwerking met de deelnemers ga je deze bevindingen clusteren.
3. Je gaat een groepsbrede dialoog aan over de verschillende inzichten en probeert hier conclussies uit te trekken.
4. Nadat je de ontbrekende categorieën heeft toegevoegd aan de referentietabel ga je met elkaar de door de groep genoemde processen waarderen en invullen in de referentietabel.

### Gezamenlijk conclusies trekken

Aan het einde van de workshop kun je gezamenlijk kijken naar de opbrengst. Bepaal of eventuele vervolggesprekken nodig zijn en met wie deze dan gevoerd moeten worden.

**Let op!**

In deze fase is het normaal als het resultaat op verschillende vlakken nog onvolledig is. Het zijn immers ruwe inschattingen. Zie de workshop als een eerste stap in een langere reis met als einddoel het professioneel beheren van TBB's.

## Resultaat

Na de workshop verwerk je de opbrengst in een nieuwe versie van de referentietabel. Eventueel maak je een verslag van de workshop of de gesprekken die je hebt gevoerd.

### Presenteer het resultaat aan het bestuur

Als laatste stap presenteer je het resultaat aan het bestuur. Je gaat de dialoog aan met het bestuur over de (ruwe) lijst met TBB's. Daarbij kun je bijvoorbeeld toelichten dat:

- Dit voor het bestuur, gelet op haar rol als risicoeigenaar, een waardevol overzicht is om vervolgstappen te bepalen met als doel om meer grip te krijgen op de te beschermen belangen en potentiele risico's.
- De referentietabel met TBB's slechts een eerste aanzet is en je graag gezamenlijk wil nadenken over een vervolgopdracht waarin je enkele kritische punten (naar de inschatting van het bestuur) uit de tabel zal uitwerken en concretiseren.
- De waardering en prioritering van de TBB's in de referentietabel niet vaststaat, en dat het bestuur deze eerst (voorlopig) moet valideren.
- Je de referentietabel in een volgende stap uit zou willen breiden naar het abstractieniveau van informatie systemen en netwerken (niveau 3) en wil waarderen en prioriteren met behulp van de eerder ingevulde referentietabel.
- Je dit niet ziet als eenmalige actie maar je graag het mandaat zou krijgen om deze referentietabel periodiek te onderhouden en zo actueel te houden.

# 4. Vooruitblik: vervolgstappen

Wanneer je de bovenstaande stappen hebt gevolgd ben je in het bezit van een (ruwe) lijst met TBB's van jouw organisatie op procesniveau.

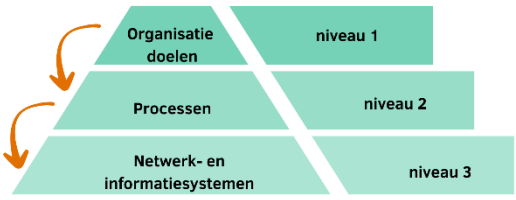
In dit hoofdstuk staan beknopt een aantal vervolgstappen die je kunt ondernemen.

## Niveau 3 verder uitwerken

In deze publicatie heb je de organisatiedoelen en de daaraan gerelateerde processen in kaart gebracht en deze vervolgens gewaardeerd in een referentietabel.

De volgende stap is om deze tabel uit te werken naar het niveau van netwerk- en informatiesystemen.

Daarbij begin je bij de zeer grote belangen en werkt vanuit daar omlaag in de tabel. Je maakt in deze stap een eerste overzicht van kritieke elementen binnen digitale infrastructuur in relatie tot de te beschermen belangen op procesniveau. In een toekomstige publicatie zal het NCSC hier dieper op in gaan.




## Eigenaarschap

Incidenten op het vlak van gevoelige informatie kunnen een grote impact hebben op de organisatiedoelen. Daarom is het noodzakelijk om deze risico's te beheersen.

Om informatie goed te kunnen beheren is het belangrijk dat alle informatie een 'eigenaar' heeft. De lijst met TBB's kan helpen om binnen de geïdentificeerde categorieën een eigenaar aan te wijzen.

De factsheet "risico's beheersen: de waarde van informatie als uitgangspunt" biedt handvatten om grip te krijgen op de beheersing van risico's bij het werken met informatie.

## Actueel houden

Het in kaart brengen van de TBB's van jouw organisatie is geen eenmalige exercitie. Zaken zoals veranderde bedrijfsdoelstellingen, nieuwe wetgeving of risico's kunnen ervoor zorgen dat jouw TBB's veranderen.

Richt in samenspraak met het bestuur een proces en/of beleid in, waarin je afspreekt hoe het overzicht van TBB's actueel gehouden kan worden. Je kunt bijvoorbeeld vaststellen dat de referentietabel elke X aantal maanden herzien moet worden.

### NIS2 en risicoanalyse

De NIS2 stelt verplicht dat entiteiten passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen te beperken. Om tot passende en evenredige maatregelen te komen voer je een risicoanalyse uit.[2]

## Risicoanalyse

Door de TBB's van jouw organisatie in kaart te brengen krijg je beter zicht op de risico's die de organisatie loopt. De TBB's van jouw organisatie kun je gebruiken als input voor een risicoanalyse.

Het NCSC heeft diverse publicaties die je kunnen helpen bij het uitvoeren van een risicoanalyse. Zo moet je bij een risicoanalyse:

de specifieke dreigingen per TBB in kaart te brengen, zie:

- *Hoe breng ik mijn rechtstreekse leveranciers in kaart?*
- *Hoe breng ik mijn dreigingen in kaart?*

zicht krijgen op de huidige digitale weerbaarheid van uw organisatie, zie:

- *Hoe krijg ik grip op mijn security controls?*
- *Basismaatregelen cybersecurity*

Op basis van een risicoanalyse kun je vervolgens bepalen wat de juiste maatregelen zijn om deze belangen te beschermen.

[2] Eén van de verplichte maatregelen is beleid over risicoanalyse- en beveiliging van informatiesystemen.

## Bijlage 1: Inspiratielijst

In deze bijlage vind je een inspiratielijst met categorieën en daaronder enkele voorbeelden van processen of informatie die ondersteunend is aan deze processen. Deze kun je gebruiken om te bepalen of jouw organisatie ten aanzien van deze voorbeelden belangen heeft op het gebied van de beschikbaarheid, vertrouwlijkheid en integriteit van deze belangen.

**Financiële belangen**

- Integriteit van financiële gegevens
- Beschikbaarheid van budgetten en prognoses
- Vertrouwelijkheid van salarisadministratie
- Vertrouwelijkheid van bankgegevens en transacties

**Juridische belangen**

- Vertrouwelijkheid van contracten en overeenkomsten
- Integriteit van compliance-documentatie
- Vertrouwelijkheid van juridische correspondentie
- Vertrouwelijkheid van intellectuele eigendomsrechten

**Veiligheidsbelangen**

- Integriteit van beveiligingsprocedures en -protocollen
- Integriteit van toegangscontrole-informatie
- Beschikbaarheid van Incidentresponsplannen
- Beschikbaarheid van fysieke beveiliging van locaties

**Operationele belangen**

- Beschikbaarheid van productieprocessen en -systemen
- Vertrouwelijkheid van logistieke gegevens
- Beschikbaarheid van supply chain-informatie
- Integriteit van onderhoudsdocumentatie

**Reputatiebelangen**

- Vertrouwelijkheid van marketingstrategieën
- Integriteit van persberichten en communicatieplannen
- Vertrouwelijkheid van klanttevredenheidsrapporten
- Beschikbaarheid van social media-accounts en inhoud

**Personeelsbelangen**

- Vertrouwelijkheid van personeelsdossiers
- Integriteit van medische gegevens
- Beschikbaarheid van trainings- en ontwikkelingsplannen
- Vertrouwelijkheid van correspondentie met werknemers

**Strategische belangen**

- Vertrouwelijkheid van bedrijfsstrategieën en -plannen
- Vertrouwelijkheid van fusie- en overnameplannen
- Integriteit van marktanalyses en concurrentie-informatie
- Beschikbaarheid van innovatie- en ontwikkelingsprojecten

**Klantbelangen**

- Vertrouwelijkheid van klantgegevens
- Integriteit van verkooprapporten
- Vertrouwelijkheid van klantcommunicatie en correspondentie
- Beschikbaarheid van loyaliteitsprogramma's en klantprofielen

**Innovatiebelangen**

- Beschikbaarheid van onderzoeks- en ontwikkelingsprojecten
- Vertrouwelijkheid van prototypen en blauwdrukken
- Integriteit van octrooien en handelsmerken
- Beschikbaarheid van innovatielabs en testomgevingen

**Omgevingsbelangen**

- Integriteit van milieu- en duurzaamheidsrapporten
- Integriteit van compliance met milieuwetgeving
- Beschikbaarheid van afvalverwerkingsprocedures

**Leveranciers**- en **partnerbelangen**

- Vertrouwelijkheid van leverancierscontracten en SLA's
- Vertrouwelijkheid van partner- en alliantieovereenkomsten
- Integriteit van gezamenlijke projectdocumentatie
- Vertrouwelijkheid van communicatie met leveranciers en partners

**Product gerelateerde belangen**

- Vertrouwelijkheid van productontwerpen en specificaties
- Vertrouwelijkheid van productieplannen en -documentatie
- Integriteit van kwaliteitscontrole- en testgegevens
- Vertrouwelijkheid van distributie- en verkoopstrategieën

**Gegevensbeschermingsbelangen**

- Integriteit van privacybeleid en AVG-compliance
- Beschikbaarheid van registraties en -rapportages
- Integriteit van toestemmingsdocumentatie van klanten en gebruikers

**Noodplannings- en continuïteitsbelangen**

- Beschikbaarheid van bedrijfscontinuïteitsplannen
- Beschikbaarheid van noodherstelprocedures
- Beschikbaarheid van evacuatieplannen en veiligheidsprocedures
- Beschikbaarheid van communicatieplannen voor noodgevallen

**Ethiek- en compliance belangen**

- Integriteit van gedragscodes en ethische richtlijnen
- Vertrouwelijkheid van compliance-audits en rapportages
- Vertrouwelijkheid van Interne onderzoeksrapporten
- Vertrouwelijkheid van klokkenluidersmeldingen

**Communicatiebelangen**

- Beschikbaarheid van interne en externe communicatieprotocollen
- Vertrouwelijkheid van PR-strategieën en mediacontacten
- Beschikbaarheid van crisiscommunicatieplannen

# Bijlage 2: Referentietabel

| | Financieel | Reputatie | Juridisch | Veiligheid |
|---|---|---|---|---|
| **Zeer groot belang** | | | | |
| **Groot belang** | | | | |
| **Matig belang** | | | | |
| **Beperkt belang** | | | | |
| **Geen belang** | | | | |

**Uitgave**
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

**Meer informatie**
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

Juli 2024