Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Hoe breng ik mijn technische te beschermen belangen in kaart?

Een aantal concrete *next* steps

Deze publicatie biedt handvaten die je kunt gebruiken om de 'te beschermen belangen' (TBB's) van jouw organisatie op technisch abstractieniveau in kaart te brengen. Wanneer je jouw te beschermen belangen in kaart hebt gebracht kun je deze vervolgens gebruiken om bijvoorbeeld een risicoanalyse of Business Impact Analyse (BIA) uit te voeren.

Doelgroep

Dit kennisproduct richt zich op personen die werkzaam zijn op het tactisch niveau van organisaties die de *volgende* stap willen zetten 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, Ministerie van Defensie, PBLQ.

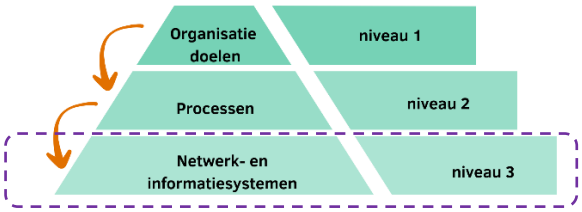
Reeks: hoe breng ik mijn TBB's in kaart?

Dit product is het tweede deel in de reeks *hoe breng ik mijn te beschermen belangen in kaart*.

Staat jouw organisatie aan het begin van het in kaart brengen van haar TBB's? Start dan met de stappen in de eerste publicatie; *hoe breng ik mijn te beschermen belangen in kaart: first steps*.

Terugblik: de eerste stappen

Iedere organisatie heeft haar eigen 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.



Stappenplan

De eerste publicatie heeft je geholpen om een eerste (ruwe) lijst van de TBB's van jouw organisatie op procesniveau (niveau 2) samen te stellen. Dit doe je door de volgende stappen te doorlopen:

1. Randvoorwaarden scheppen en opdracht formuleren
2. Mandaat krijgen en draagvlak creeëren
3. TBB's in kaart brengen door middel van dialoog / workshop met relevante stakeholders
4. TBB's prioriteren in een referentietabel

Na het doorlopen van bovenstaande stappen heb je een (ruwe) lijst van de TBB's van jouw organisatie op procesniveau. Bij voorkeur heb je deze geprioriteerd in een referentietabel als in de bijlage van de eerste publicatie.

Uitkomst van dit product

Dit tweede deel helpt je in drie stappen om jouw te beschermen belangen op het niveau van netwerk- en informatiesystemen in kaart te brengen (niveau 3). Na het doorlopen van de stappen heb je een lijst met de TBB's van jouw organisatie op het niveau van netwerk- en informatiesystemen.

Let op! Deze TBB's hebben niet alleen betrekking op de netwerk- en informatiesystemen zelf, maar kunnen bijvoorbeeld ook betrekking hebben op het gebied van fysieke veiligheid van de systemen of het personeel dat met deze systemen werkt.

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. Kies een proces

In deze stap kies je op basis van de waardering in de referentietabel één proces uit om verder te onderzoeken.

Wanneer je jouw TBB's op het abstractieniveau van netwerk- en informatiesystemen in kaart wil gaan brengen is het belangrijk om het overzicht te behouden. Begin niet met alle processen tegelijk, maar start met de focus op één proces.

Je bent in het bezit van een (ruwe) lijst met TBB's van jouw organisatie op procesniveau. Wanneer je de stappen in de eerste publicatie hebt gevolgd heb je deze geprioriteerd op een 5-punts schaal.

Een voorbeeld van een 5-punts schaal is:

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

Aan de hand van deze 5-puntsschaal kies je één van de processen die je het hoogst geprioriteerd hebt. Dit proces is immers aangemerkt als het meest belangrijke proces binnen de organisatie.

Voorbeeld: "*Uitbetalen personeel*"

Organisatie X heeft de stappen in de eerste publicatie doorlopen en heeft een geprioriteerde referentietabel met de TBB's van de organisatie op procesniveau. Het proces "*uitbetalen personeel*" is op de 5-puntsschaal aangewezen als "*Zeer groot belang*". De organisatie kiest er voor om met dit proces aan de slag te gaan.

	Financieel	Reputatie	Juridisch	Veiligheid
Zeer groot belang	- Inkoopproces - Facturatieproces - Bestelproces	- Uitbetalen personeel - Bestelproces - Klantenserviceproces	- Uitbetalen personeel	
Groot belang	- Uitbetalen personeel - Voorraadbeheer	- Facturatieproces	- Bestelproces	
Matig belang	- Klantenserviceproces	- Inkoopproces - Voorraadbeheer	- Facturatieproces	- Uitbetalen persone
Beperkt belang			- Voorraadbeheer - Klantenserviceproces	- Inkoopproces - Facturatieproces - Voorraadbeheer - Bestelproces
Geen belang				- Klantenserviceproc

2. Onderzoek het proces

In deze stap onderzoek je uit welke substappen het proces bestaat. Zie dit als een 'quickscan' van het proces. Vervolgens breng je het proces visueel in kaart door middel van een flowchart.

Wat weet je al van dit proces?

Een goede eerste stap is om te onderzoeken of er al zicht is op het proces binnen de organisatie zelf. De ervaring leert dat er vaak al meer is vastgelegd dan je denkt. Denk bijvoorbeeld aan het betrekken van de financiële afdeling voor het proces *inkoop*.

Procesdecompositie

Betrek de belangrijkste stakeholders bij jouw onderzoek. Deze stakeholders kunnen je helpen bij het in kaart brengen van het gekozen proces. Voorbeelden van stakeholders zijn:

- Systeemeigenaren
- Producteigenaren
- Proceseigenaren
- Informatie-eigenaren
- IT-beheerders

Met de verschillende stakeholder(s) knip/deel je het proces op in verschillende sub/deelstappen, ook wel processtappen genoemd. Aan het eind van dit hoofdstuk vind je een concreet voorbeeld van een procesdecompositie.

De processtappen schrijf je uit in een zogenoemde 'flowchart' of stroomdiagram. Een flowchart is een schematische voorstelling van een proces. Door het proces visueel in kaart te brengen maak je het makkelijker om in een later stadium de stap te maken naar het technische abstractieniveau.

In de bijlage van deze publicatie is een template van een flowchart opgenomen. Je kunt deze zelf aanpassen of uitbreiden aan de hand van jouw gekozen proces.

Kerninformatie achterhalen per processtap

Bedenk van tevoren welke kerninformatie je van deze processtappen zou willen weten.

Voorbeelden hiervan zijn:

Documentatie:

- Welke documentatie is er beschikbaar?
- Zijn er werkinstructies voor medewerkers die inzicht kunnen geven?

Informatie en gegevens:

- Welke specifieke gegevens worden verwerkt? Bijvoorbeeld:salarisgegevens,belasting-informatie en/of bankgegevens)
- Welke informatiestromen gaan er allemaal rond in deze processtap? Bijvoorbeeld:
    - mutaties in salarisgegevens (salarisverhoging, in dienst / uit dienst),
    - salarisbatch digitaal naar bank verzenden,
    - aangifte loonheffing via het salarispakket naar de belastingdienst versturen.

Input

- Wat is de input die de processtap nodig heeft? (meestal de output van de vorige processtap)
- Welke informatiebronnen worden er gebruikt?

Verwerking:

- Wat is de toegevoegde waarde van deze processtap in het proces?
- Wat heb ik na deze stap wat ik hiervoor niet had?

Uitvoer:

- Wat is de concrete output van deze processtap?

Incidenten:

- Welke veelvoorkomende incidenten treden er op en hoe worden ze opgelost?
- Zijn er historische gegevens beschikbaar? (hoe vaak?, op welk vlak?)
- Zijn er incidentrapportages beschikbaar?

Betrokken rollen:

- Welke medewerkers of afdelingen zijn betrokken bij elke stap?
- Wie is verantwoordelijk voor elke stap en wat als deze persoon niet beschikbaar is? (back-up)
- Wat zijn de procedures voor het escaleren van problemen?
- Wat is de rol van en afspraken met een toeleverancier (meer informatie vind je in deze publicatie).

Controlepunten:

- Welke controles zijn er om fouten te voorkomen of te detecteren?
- Welke kwaliteitscontroles zijn er om de nauwkeurigheid te waarborgen?
- Hoe wordt er feedback verzameld en verwerkt?
- Hoe vaak worden (interne) audits uitgevoerd en wat zijn de bevindingen?

'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 de doelen niet te hoog te stellen. Een eerste ruwe lijst met processtappen en beperkte kerninformatie is in deze eerste stap een prima resultaat en een goede basis voor verdere iteraties.

Voorbeeld: "*Uitbetalen personeel*"

Organisatie X onderzoekt het proces "uitbetalen personeel".

Verschillende stakeholders zoals de financiële afdeling, personeelszaken/HR, en de IT-afdeling worden betrokken.

In een workshop doorlopen/werken zij gezamenlijk de procesdecompositie uit. Zij komen tot de volgende processtappen:

1. Verzamelen van gegevens
2. Berekenen van salarissen
3. Salaris goedkeuring
4. Uitbetaling
5. Rapportage en documentatie
6. Feedback en correcties.

Vervolgens gaat men aan de slag met het achterhalen van kerninformatie.

Voor de processtap "*Berekenen van salarissen*" concludeert men onder andere dat deze stap afhankelijk is van een **integer overzicht van gewerkte uren** die in de voorgaande stap "*verzamelen van gegevens*" wordt opgemaakt. Verder komt men tot de conclusie dat er in het verleden wel eens fouten zijn ontstaan in deze berekening die pas na uitbetaling aan het licht komen.

De bovenstaande inzichten vormen de basis voor de volgende stap: "*operationaliseren en waarderen*".

3. Operationaliseren en waarderen

In de vorige stap heb je het proces onderzocht, opgeknipt in processtappen en gevisualiseerd in een flowchart. Nu ga je samen met een informatiemanager, (netwerk)architect of IT-beheerder per processtap de technische procesafhankelijkheden in kaart brengen.

Operationaliseren en de technische procesafhankelijkheden in kaart brengen

Samen met de informatiemanager, (netwerk)architect of IT-beheerder ga je het gekozen proces ontleden. Per processtap ga je na welk netwerk- en/of informatiesysteem dit proces mogelijk maakt of ondersteund.

Vragen die je kunt stellen zijn:

Systemen: Wat is er op technologisch vlak nodig om het proces in stand te houden?

- Welke onderdelen en/of objecten ondersteunen dit proces?
- Wanneer kan het proces niet meer doorlopen?
- Welke systemen en software zijn er onderliggend aan dit proces?

Databronnen: Waar komen de gegevens vandaan?

- Bijvoorbeeld: HR-systemen of tijdregistratiesystemen

Dataopslag:

- Waar en hoe worden de ingevoerde gegevens opgeslagen? (data at rest)
- Back-up en herstel: Wat zijn de systemen voor back-up en herstel van gegevens?

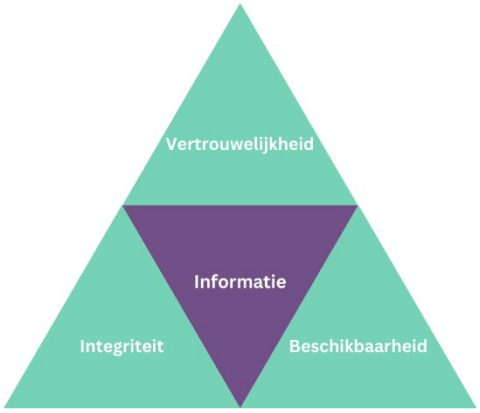
Datatransport:

- Waar en hoe worden gegevens in de infrastructuur verstuurd? (data in transit)

Benoem de belangrijkste systemen, objecten, locaties etc. per proces. Focus je dus *niet* alleen op de netwerk- en informatiesystemen zelf, maar ook op de locatie en de mensen die met deze systemen werken. Je kan hier denken aan fysieke toegangsbeveiliging, of het personeel dat administrator-rechten heeft op de geïdentificeerde systemen.

Waarderen

Je hebt nu een beeld van de netwerk- en informatiesystemen die de gekozen TBB op procesniveau ondersteunen. Aan de hand van de zogenoemde BIV-classificatie ga je deze onderdelen / objecten waarderen.



BIV-driehoek

BIV staat voor beschikbaarheid, integriteit en vertrouwelijkheid:

- **Beschikbaaarheid** (continuiteit): is de informatie of het systeem toegangelijk en bruikbaar wanneer dit nodig is?
- **Integriteit** (betrouwbaarheid): in hoeverre moet mijn informatie juist en volledig zijn en moet ik maatregelen nemen tegen ongeautoriseerde wijzigingen?

- **Vertrouwelijkheid** (exclusiviteit): is de informatie of het systeem beschermd tegen openbaarmaking of ongeautoriseerde toegang?

Om de geïdentificeerde onderdelen te waarderen adviseert het NCSC om een 5-punts score toe te kennen aan de geïdentificeerde objecten. Een voorbeeld van een 5-punts score is:

- Niveau 0: geen
- Niveau 1: laag
- Niveau 2: midden
- Niveau 3: hoog
- Niveau 4: zeer hoog

Eerst bepaal je hoe cruciaal de **beschikbaarheid** van de informatie is, bijvoorbeeld: moet deze 24/7 toegankelijk zijn? Vervolgens kijk je naar de **integriteit**: hoe ernstig is het als deze informatie onbedoeld wijzigt? Als laatste beoordeel je deze op **vertrouwelijkheid**: wat zijn de gevolgen als deze informatie openbaar gemaakt wordt of door ongeautoriseerde wordt ingezien? De informatie in de eerder opgestelde referentietabel (zie de publicatie: "*hoe breng ik mijn te beschermen belangen in kaart: first steps*", die hier te vinden is) kunt u gebruiken bij het scoren.

Dit proces herhaal je bij elk geïdentificeerd systeem. Vervolgens verwerk je dit in een nieuwe tabel voor de BIV-scores. Een template voor een dergelijke tabel is te vinden in de bijlage van dit product.

Elk object of systeem heeft nu een BIV-score toegekend gekregen. Je hebt nu de objecten en/of systemen in de processtap geoperationaliseerd en gewaardeerd.

Voorbeeld: "*Uitbetalen personeel*"

Organisatie X onderzoekt de processtap *berekenen van salarissen*.

Bij de voorgaande stap *Onderzoek het proces* kwam men tot de conclusie dat de organisatie afhankelijk is van een **integer overzicht van gewerkte uren.** De organisatie gaat vervolgens onderzoeken welke middelen er worden gebruikt om tot dit overzicht te komen.

Operationaliseren:

Men komt tot de conclusie dat het overzicht van gewerkte uren in een **Excelbestand** op de **file server** wordt geplaatst. De financiële afdeling uploadt dit bestand in de **salarisadministratie software** die als cloudoplossing wordt gebruikt.

Waarderen:

Bij het waarderen komt men tot de conclusie dat:
- De ***beschikbaarheid*** van onder andere de **salarisadministratie software *zeer hoog*** is maar wel slechts in één week van de maand.

- Omdat salarissen nog altijd uitbetaald kunnen worden wanneer de ***vertrouwelijkheid*** van het **Excelbestand** of de gegevens in de **salarisadministratie software** geschaad zou worden besluit men dit te waarderen als ***midden***.

- De ***integriteit*** is ***zeer hoog*** voor zowel het **Excelbestand** als de gegevens in de **salarisadministratie software.** Eén van de redenen hiervoor is dat geld dat overgemaakt wordt naar onjuiste rekeningnummers moeilijk te corrigeren is en dat daardoor de medewerkers niet tijdig hun salaris ontvangen.

Zie hieronder een illustratief voorbeeld van een ingevulde tabel:

	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Niveau 4: zeer hoog	*Salarisadministratie software*	*Salarisadministratie software* *Excelbestand* *File server*	
Niveau 3: hoog	*File server* *Excelbestand*		
Niveau 2: midden			*Salarisadministratie software* *Excelbestand* *File server*
Niveau 1: laag			
Niveau 0: geen			

4. Herhalen

In deze stap herhaal je stap 3 om uiteindelijk het gehele proces in kaart te brengen. Vervolgens kun je, wanneer gewenst, meerdere processen in kaart brengen en op zoek gaan naar trends of patronen.

Je hebt voor één processtap jouw TBB's op technisch abstractieniveau (niveau 3) in kaart gebracht. Herhaal dit tot je het gekozen proces geheel in kaart hebt gebracht.

Om de opgehaalde informatie te verwerken en te structureren kan je gebruik maken van bijvoorbeeld een visuele procesanalyse (*ook wel Brown paper sessie genoemd*). Hierbij wordt een groot vel papier of whiteboard in combinatie met post-its gebruikt om processen in kaart te brengen en te analyseren. Het verwerken van de verzamelde informatie in een Exceldocument of processoftware is een prima alternatief.

Hoeveel processen je in kaart wil brengen en het detailniveau daarvan hangt af van de volwassenheid en het ambitieniveau van jouw organisatie. Wanneer jouw organisatie nog aan de start staat met het in kaart brengen van haar TBB's is een ruw resultaat een goede basis voor verdere iteraties op een later moment.

Hoe meer processen je in kaart brengt, hoe makkelijker het wordt om de resultaten te vergelijken. Je kunt dan bijvoorbeeld trends ontdekken. Wanneer je méérdere processen in kaart hebt gebracht kun je de resultaten vergelijken en jezelf de volgende vragen stellen:

- Welke trends of patronen zie ik?
- Welke netwerk- en/of informatiesystemen komen het meeste voor?
- Waar zit de bottleneck?
- Welke netwerk- en/of informatiesystemen hebben bij falen de grootste impact op de bedrijfsdoelstellingen?
- Hoe afhankelijk is de organisatie van de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van deze systemen?

Voorbeeld: "*Uitbetalen personeel*"

Organisatie X concludeert dat verschillende kritische organisatieprocessen volledig afhankelijk zijn van de beschikbaarheid, integriteit en vertrouwelijkheid van de file server die binnen de organisatie wordt gebruikt. Een van de voorbeelden is het proces "*uitbetalen personeel*", omdat het Excel-bestand waarin de gewerkte uren worden bijgehouden is opgeslagen op de file server bij de processtap "*berekenen van salarissen*".

5. Vervolgstappen

Wanneer je de bovenstaande stappen hebt gevolgd ben je in het bezit van een lijst met TBB's van jouw organisatie op technisch abstractieniveau. In dit hoofdstuk staan beknopt een aantal vervolgstappen die je kunt ondernemen.

Input voor risicoanalyse of Business Impact Analyse (BIA)

Uiteindelijk wil je dat jouw organisatie alle risico's in kaart brengt en een passend niveau van weerbaarheid ontwikkelt. Door het uitvoeren van een risicoanalyse en/of BIA kun je vaststellen wat er nodig is om dit te realiseren.

Bij het doen van een risicoanalyse of BIA is het voor een organisatie essentieel om te weten wat haar TBB's zijn (op de verschillende abstractieniveaus).

De in deze publicatie in kaart gebrachte TBB's van jouw organisatie kunnen dienen als input voor een risicoanalyse of BIA.

NIS2 en risicoanalyse

De NIS2 stelt verplicht dat entiteiten passende en evenredige technische, operationele en organisatorische maatregelen moeten 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.[1]

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

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

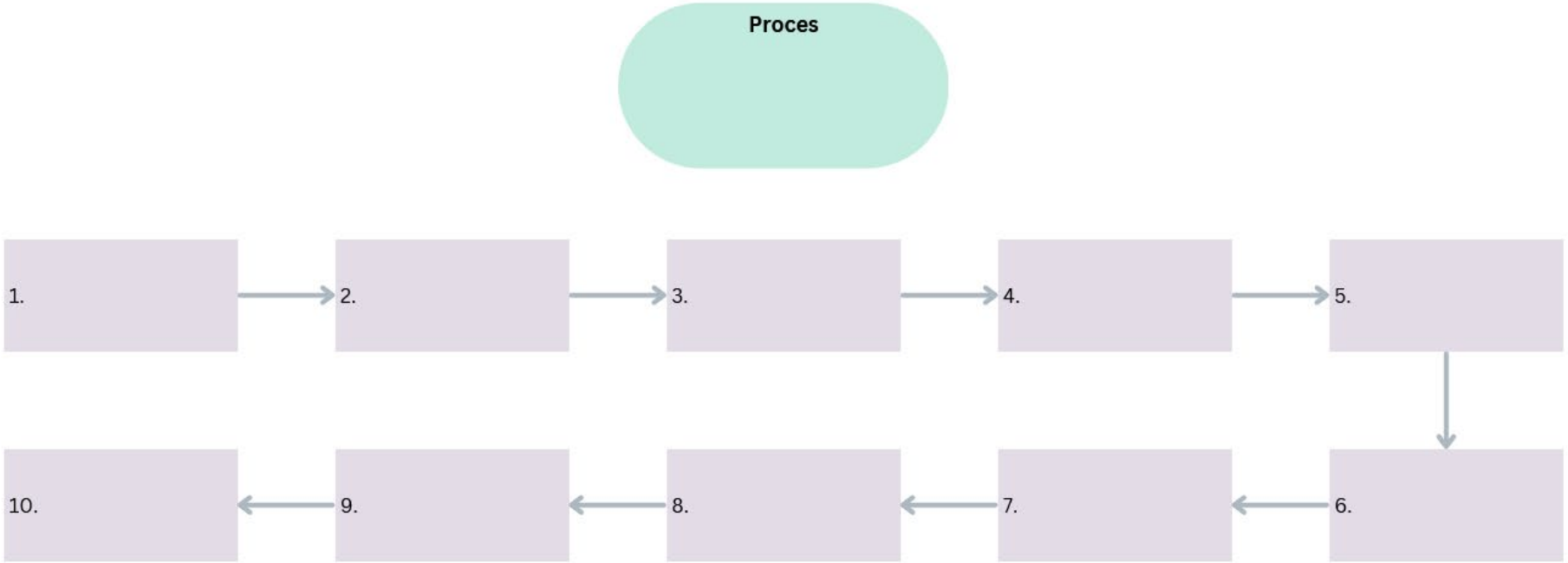
Om meer zicht te krijgen op de huidige digitale weerbaarheid van jouw organisatie, zie:

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

Door een risicoanalyse uit te voeren kun je de passende beheersmaatregelen kiezen om de risico's voor jouw organisatie tot een acceptabel niveau terug te brengen.

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

Bijlage 1: Flowchart



Bijlage 2: BIV-Scores

	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Niveau 4: zeer hoog			
Niveau 3: hoog			
Niveau 2: midden			
Niveau 1: laag			
Niveau 0: geen			

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

[Oktober] [2024]