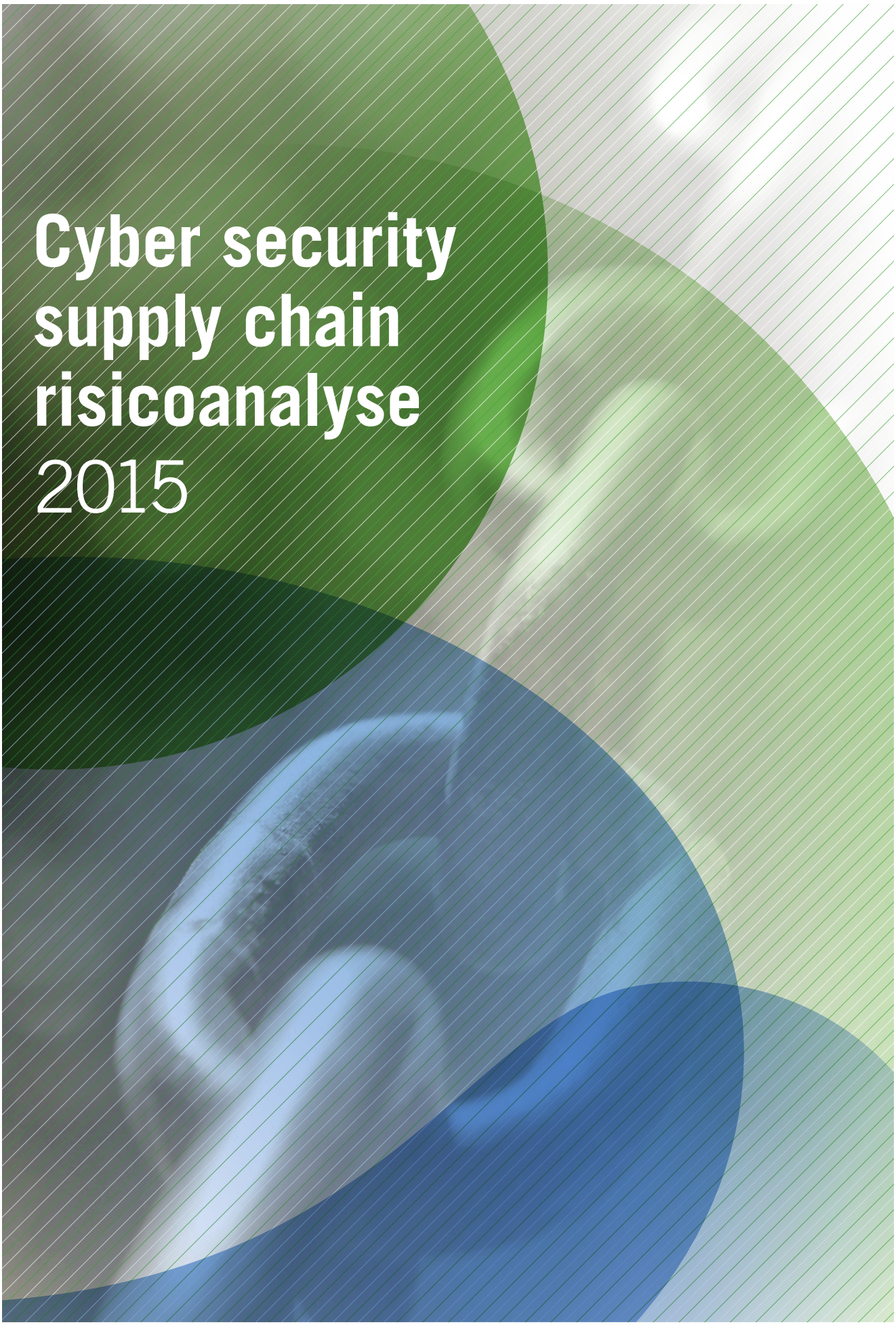
# Cyber security supply chain risicoanalyse 2015



# Cyber security supply chain risicoanalyse 2015

# Inhoudsopgave


| | | |
|---|---|---|
| **Management samenvatting** | | **4** |
| **1** | **Voorwoord** | **5** |
| **2** | **Introductie** | **7** |
| 2.1 | Achtergrond | 7 |
| 2.2 | Doel van het document | 7 |
| 2.3 | Opbouw document | 8 |
| **3** | **Overzicht cyber security supply chain risicoanalyse methodiek** | **9** |
| 3.1 | Algemeen | 9 |
| 3.2 | Uitvoering van de risicoanalyse methodiek | 10 |
| 3.3 | Voorbeeld supply chain | 11 |
| **4** | **Stap 1: bepalen scope** | **12** |
| 4.1 | Inleiding | 12 |
| 4.2 | Voorbereidingen | 12 |
| 4.3 | Uit te voeren activiteiten | 12 |
| 4.4 | Te bereiken resultaten | 14 |
| **5** | **Stap 2: beschrijven supply chain** | **15** |
| 5.1 | Inleiding | 15 |
| 5.2 | Voorbereidingen | 15 |
| 5.3 | Uit te voeren activiteiten | 15 |
| 5.4 | Te bereiken resultaten | 19 |
| **6** | **Stap 3: bepalen impact verstoring supply chain** | **20** |
| 6.1 | Inleiding | 20 |
| 6.2 | Voorbereidingen | 20 |
| 6.3 | Uit te voeren activiteiten | 20 |
| 6.4 | Te bereiken resultaten | 21 |
| **7** | **Stap 4: vaststellen omvang cyberbedreigingen en risico's** | **22** |
| 7.1 | Inleiding | 22 |
| 7.2 | Voorbereidingen | 22 |
| 7.3 | Uit te voeren activiteiten | 22 |
| 7.4 | Te bereiken resultaten | 24 |
| **8** | **Stap 5: bepalen maatregelen en opstellen actieplannen** | **25** |
| 8.1 | Inleiding | 25 |
| 8.2 | Voorbereiding | 25 |
| 8.3 | Uit te voeren activiteiten | 25 |
| 8.4 | Te bereiken resultaten | 26 |
| **9** | **Bijlagen** | **27** |
| 9.1 | Bijlage 1: Definities | 27 |
| 9.2 | Bijlage 2: Schema analyseproces | 28 |
| 9.3 | Bijlage 3: Template initiatie document | 29 |
| 9.4 | Bijlage 4: Checklist scope bepaling | 30 |
| 9.5 | Bijlage 5: Voorbeeld BIV classificatie | 31 |
| 9.6 | Bijlage 6: Matrix vastlegging resultaten risiconalayse | 32 |
| 9.4 | Bijlage 7: Template vastlegging gevolgen calamiteiten | 33 |
| 9.8 | Bijlage 8: Template actieplan | 34 |
| 9.9 | Bijlage 9: Matrix voorbeeld supply chain | 35 |

# Management samenvatting

Cyber security is bij uitstek een domein waarbij samenwerking, tussen zowel publieke en private organisaties, als tussen private organisaties onderling, noodzakelijk is om de toegenomen cyber dreigingen het hoofd te bieden.

Shell en TenneT hebben gemeend dat het belangrijk is dat, mede gelet op de grote onderlinge afhankelijkheid en verwevenheid, organisaties in een supply chain gezamenlijk het beste in staat zijn de juiste maatregelen te definiëren en initiatieven te ontplooien om cyber security risico's te verlagen.

Het inzichtelijk maken van de cyber security risico's binnen een supply chain vraagt van alle betrokken organisaties een bepaalde inzet. Belangrijk is dat naast de beschikbaarheid van voldoende middelen er tussen de organisaties voldoende vertrouwen bestaat om gevoelige informatie met elkaar te delen.

In de ontwikkelde methodiek, beschreven in dit document, is een gelaagdheid aangebracht om inzichtelijk te maken welke risico's, die voortkomen uit de informatieverwerkende systemen, een bedreiging vormen voor de bedrijfsprocessen. Risico's in de bedrijfsprocessen kunnen uiteindelijk de continuïteit van de gehele supply chain verstoren.

Om supply chain risico's te verlagen zijn maatregelen nodig bij de (individuele) organisaties die deel uitmaken van de supply chain. Deze maatregelen kunnen zowel binnen de bedrijfsprocessen als binnen de systemen worden gerealiseerd.

# 1 Voorwoord

Voor u ligt de risicoanalyse methodiek ontwikkeld in het kader van het onderzoek naar de risico's van cyber security dreigingen binnen de energievoorziening supply chain `van gas tot elektriciteit´.

Dit onderzoek is geïnitieerd door Shell en TenneT, naar aanleiding van een discussie in de Cyber Security Raad. Daarnaast is het onderzoek in lijn met een aanbeveling uit de Nederlandse Nationale Cyber Security Strategie 2. Het onderzoek is in 2014 uitgevoerd door Shell, Gasunie, Nuon, TenneT en Alliander, met ondersteuning door het Nationaal Cyber Security Centrum. Al deze vijf organisaties hebben een rol in de energievoorziening supply chain in Nederland.

*Het doel van het onderzoek is tweeledig:*

- In gezamenlijkheid de cyber security risico's buiten de grenzen van de eigen onderneming in kaart brengen om daarmee de risico's van cyber gerelateerde dreigingen voor de gehele supply chain te inventariseren.
- Een gevolgde cyber security risicoanalyse methodiek, gebaseerd op de ervaringen opgedaan gedurende het onderzoek, te documenteren zodat deze in andere sectoren toegepast kan worden.

De deelnemers willen middels de resultaten van dit onderzoek een bijdrage leveren aan de veiligheid van Nederland.

| Wam Voster | Paul Bloemen | Martin Beumer | Henrie Mathijssen | Aad Dekker |
|---|---|---|---|---|
| *Shell* | *Gasunie* | *Nuon* | *TenneT* | *Alliander* |

# 2 Introductie

Dit document beschrijft een flexibel inzetbare risicoanalyse methodiek voor het onderzoeken en inzichtelijk maken van de cyber security gerelateerde risico's binnen een (vitale) supply chain. De methodiek zoals in dit document beschreven is ontstaan vanuit een *Proof of Concept* dat is uitgevoerd door Shell, TenneT en enkele andere organisaties uit de energiesector om de gehele supply chain van gaswinning tot aan het stopcontact in beeld te brengen. De centrale vraag die aan de *Proof of Concept* ten grondslag ligt is: waar zitten de grootste cyber risico's voor deze *supply chain?*

## 2.1 Achtergrond

In de tweede Nationale Cyber Security Strategie[1] is speciale aandacht voor vitale infrastructuur van Nederland. Shell en TenneT hebben de handen ineengeslagen om tezamen met andere organisaties uit de Nederlandse energiesector te werken aan een "*Proof of Concept* (PoC)" om zodanig de bescherming van vitale diensten onder de loep te nemen. Dit geschiedt niet slechts binnen één organisatie maar door de gehele supply chain. Deze PoC richt zich op één van de supply chains die verantwoordelijk is voor de elektriciteitsvoorziening in Nederland en omvat de volgende processtappen:

- gastransport en gasdistributie
- elektriciteitsproductie
- elektriciteitstransport
- elektriciteitsdistributie

Waar het in kaart brengen van vitale processen en objecten en het uitvoeren van crisisoefeningen kan leunen op eerdere ervaringen in zowel Nederland als in de rest van de wereld is het minder duidelijk hoe te komen tot een realistische cyber security risico-inschatting voor kritieke processen in supply chains. Hoe te komen tot bedrijfsoverstijgende effectieve verbeterprogramma's voor cyber security weerbaarheid? Wat is een effectieve rol van de overheid hierin?

Grotere organisaties binnen vitale sectoren hebben reeds ervaring met risico management en verbeterprogramma's binnen hun eigen onderneming, die tevens handvatten bieden op het gebied van weerbaarheidsverhoging met betrekking tot cyber security risico's. Uit deze ervaringen is gebleken dat het stellen van heldere prioriteiten en het focussen op de gebieden waar de risico's het grootst zijn (een *"risk based approach"*) en het implementeren van effectieve "assurance" fundamenteel zijn voor een succesvol beleid.

Brede, niet risico gedreven, maatregelen blijken niet altijd een goede besteding van de beperkte middelen en resources; certificering en regelgeving leiden namelijk niet altijd tot vermindering van het risico en zouden op die manier een gevoel van schijnveiligheid kunnen opwekken. Voor supply chains die onderdeel zijn van vitale nationale processen komen er bovendien nieuwe aspecten aan de orde, bijvoorbeeld de rol van de overheid en de noodzaak om rollen en verantwoordelijkheden tussen verschillende organisaties te regelen. Het is daarom belangrijk dat door organisaties in de supply chain zelf best practices worden ontwikkeld en toegepast om deze supply chains afdoende te beschermen tegen de toegenomen cyber security dreigingen.

## 2.2 Doel van het document

De betrokken organisaties, Shell, Gasunie, Nuon, TenneT en Alliander zijn al werkend op zoek gegaan naar een effectieve methodiek om kritieke IT-systemen en de daaraan gerelateerde cyber risico's binnen een supply chain inzichtelijk te maken. De vijf organisaties willen de gevolgde methodiek delen met andere organisaties binnen de energie sector. Bovendien kunnen ook andere (vitale) sectoren en andere 'supply chains' deze methodiek toepassen om de risico's in hun supply chains inzichtelijk te maken. Hiermee wordt een gemeenschappelijk en eenduidig beeld van de cyber security risico's voor supply chains in (vitale) sectoren gecreëerd. Dit document beschrijft de ontwikkelde methodiek en geeft handvatten hoe een cyber security risicoanalyse effectief en doelmatig uit te voeren.

[1] Nationale Cyber Security Strategie 2 - *link*

## 2.3 Opbouw document

In hoofdstuk drie is een overzicht gegeven van de gehele methodiek en is een fictieve supply chain beschreven die dient ter illustratie van bepaalde stappen in de methodiek. In de hoofdstukken vier tot en met acht zijn vervolgens de vijf stappen van de methodiek uitgewerkt, waarbij handreikingen zijn gegeven voor de uitvoering van elke stap.

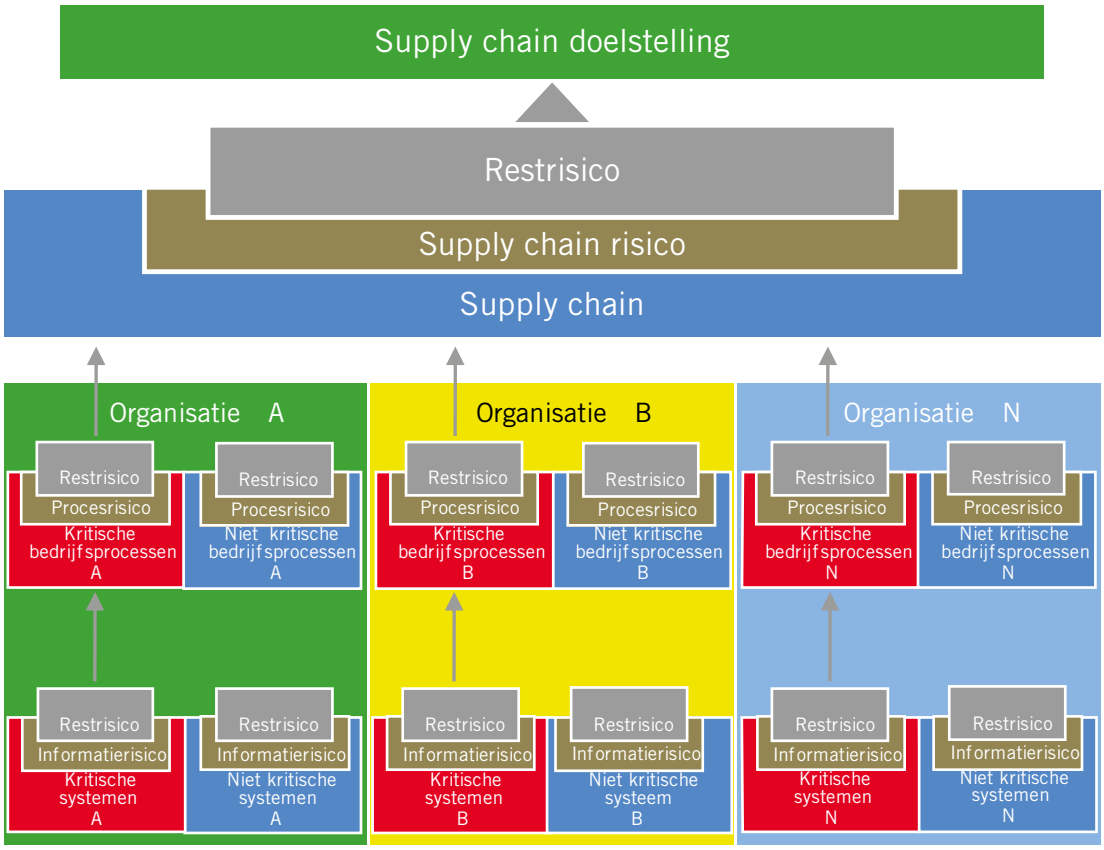
# 3 Overzicht cyber security supply chain risicoanalyse methodiek

Voor het identificeren van cyber security risico's binnen een supply chain is een methodiek ontwikkeld die bestaat uit een vijftal stappen. In dit hoofdstuk is eerst een algemene toelichting gegeven op de manier waarop risico's in informatieverwerkende systemen kunnen leiden tot risico's in de supply chain. Vervolgens is een korte beschrijving gegeven van elke stap in de risiconanalyse methodiek. Als laatste wordt een korte beschrijving gegeven van een fictieve supply chain die wordt gebruikt om bepaalde stappen te illustreren.

## 3.1 Algemeen

Om de werkelijke cyber security supply chain risico's te identificeren is het noodzakelijk om risico's vanuit zowel de informatieverwerkende systemen (hierna: systemen) als vanuit de bedrijfsprocessen te identificeren. In de onderstaande afbeelding zijn geheel onderaan voor elk van de organisaties, die onderdeel uitmaken van de te analyseren supply chain, de informatieverwerkende systemen weergegeven. Hierbij is een onderscheid gemaakt in 'kritieke' en 'niet kritieke' systemen bij elk van de organisaties die onderdeel zijn van de supply chain. Onder kritieke systemen wordt verstaan systemen die noodzakelijk zijn voor de uitvoering van de bedrijfsprocessen die noodzakelijk zijn voor het leveren van het eindproduct uit de supply chain. Eenzelfde onderverdeling in 'kritisch' en 'niet kritisch' is gemaakt voor de bedrijfsprocessen.

In het model is een gelaagdheid aangebracht. Het idee hierachter is dat risico's die voortkomen uit de systemen een bedreiging vormen voor de bedrijfsprocessen. De risico's vanuit de systemen kunnen worden geadresseerd door risicomitigerende maatregelen te treffen op de systemen zelf of door de




*Figuur 1: Visualisatie risicomodel*

risico's te mitigeren door maatregelen te treffen in de bedrijfsprocessen. De restrisico's vanuit de verschillende bedrijfsprocessen die betrokken zijn in de supply chain leiden uiteindelijk tot bedreigingen voor het supply chain proces. Wanneer deze supply chain risico's niet in voldoende mate worden geadresseerd kan dit uiteindelijk resulteren in het niet kunnen leveren van het eindproduct en daarmee kan mogelijk de supply chain doelstelling niet worden bereikt. Afhankelijk van de gekozen supply chain doelstelling (bijv. electriciteitsvoorziening in Nederland) hoeft het niet kunnen leveren van een eindproduct vanuit de supply chain niet direct te leiden tot het niet kunnen bereiken van de supply chain doelstelling. Dit is wel het geval als de supply chain doelsteling 'het leveren van elektriciteit vanuit gas' is.

Om supply chain risico's te verlagen zijn maatregelen nodig bij de individuele organisaties die deel uitmaken van de supply chain. Deze maatregelen kunnen zowel binnen de bedrijfsprocessen worden getroffen als binnen de systemen. Door de risico's binnen elke organisatie te adresseren worden uiteindelijk ook de supply chain risico's verlaagd.

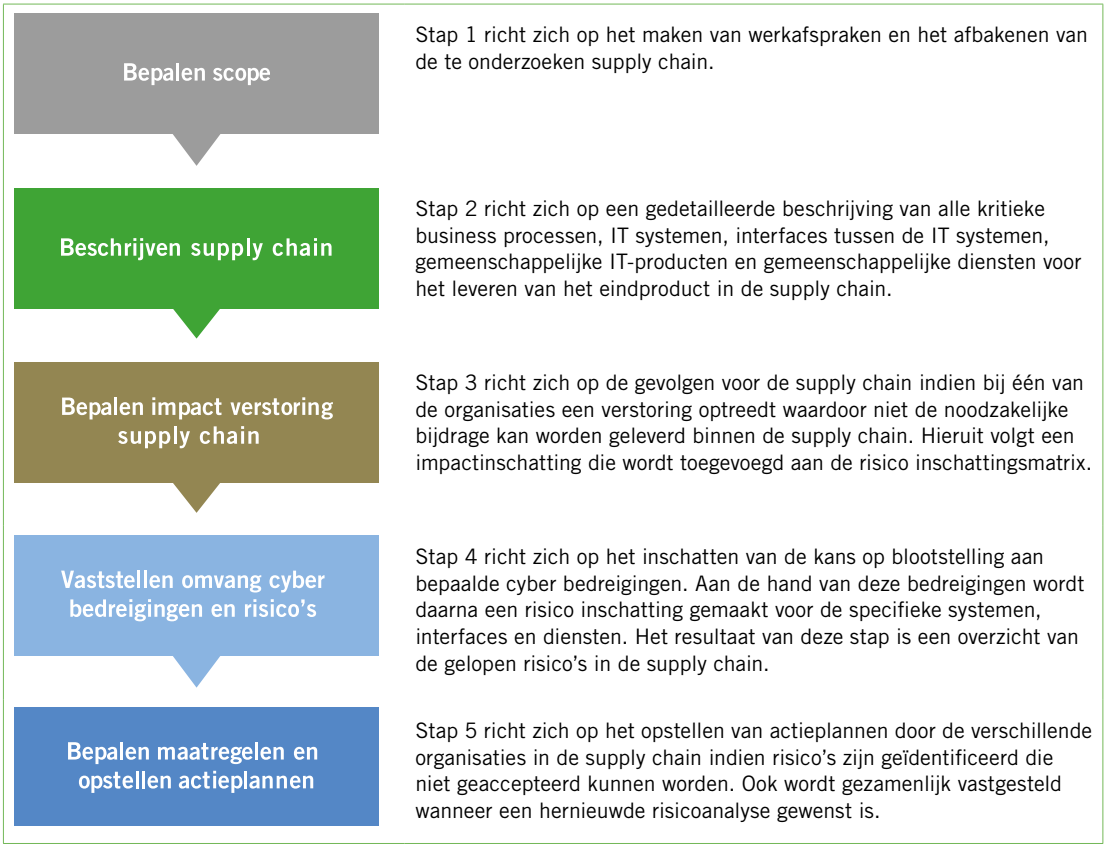
## 3.2 Uitvoering van de risicoanalyse methodiek

De methodiek richt zich op cyber security risico's in een supply chain waarbij de systemen (inclusief interfaces en gemeenschappelijke IT producten en diensten) en bedrijfsprocessen worden onderzocht die deel uitmaken van de supply chain en bestaat uit vijf stappen:

1. Bepalen scope
2. Beschrijven supply chain
3. Bepalen impact verstoring supply chain
4. Vaststellen omvang cyber bedreigingen en risico's
5. Bepalen maatregelen en opstellen actieplannen

In figuur 2 zijn deze vijf stappen schematisch weergegeven waarbij per stap de benodigde input is weergegeven, de uit te voeren activiteiten en het uiteindelijk te bereiken resultaat. De verschillende stappen hoeven niet allemaal chronologisch doorlopen te worden. Stap 3 en 4 kunnen, indien gewenst, parallel worden uitgevoerd.

*Figuur 2: Stappen methodiek*




## 3.3 Voorbeeld supply chain

Om bepaalde stappen toe te lichten wordt gebruik gemaakt van een fictieve productieketen "Van boom tot papier". Het betreft hier een eenvoudige supply chain waarin vier verschillende organisaties betrokken zijn voor het produceren van papier.

In de onderstaande tabel is per organisatie in de supply chain weergegeven welke kritieke processen ze uitvoeren voor de supply chain.

*Supply chain: Van boom tot papier*

| Organisatie | Kritieke processen voor supply chain | Supply chain proces |
|---|---|---|
| **A (Bosbouwer)** | - Kappen bomen | Aanleveren grondstoffen |
| **B (Papierfabriek)** | - Maken houtpulp<br>- Persen papier | Productie papier |
| **C (Vervoersbedrijf)** | - Planning routes | Transport papier |
| **D (Groothandel)** | - Voorraadbeheer | Distributie papier |

In bijlage 9 is de gebruikte matrix voor het vastleggen van de resultaten uit de analyse ingevuld voor de voorbeeld supply chain.

# 4 Stap 1: bepalen scope

| Input | Proces | Resultaat |
|---|---|---|
| Supply chains | Bepalen scope | Afgebakend onderzoeksgebied |

## 4.1 Inleiding

De eerste stap richt zich op het afbakenen van de te onderzoeken supply chain en bestaat uit een tweetal activiteiten. De eerste activiteit in deze stap is het maken van werkafspraken tussen de verschillende deelnemende organisaties. Hierna kan gestart worden met de tweede activiteit, het afbakenen van het onderzoeksgebied. Voor elke activiteit is beschreven welke acties uit te voeren en zijn handvatten gegeven voor het maken van de benodigde keuzes.

| | |
|---|---|
| Input | Supply Chains |
| Processtap | Bepalen Scope |
| Resultaat | • Overzicht van de te onderzoeken supply chain, inclusief de te betrekken organisaties<br>• Overzicht van de te betrekken systemen<br>• Overeenstemming van de geldende randvoorwaarden<br>• Afgestemde werkafspraken tussen de deelnemende organisaties<br>• Initiatiedocument voor het uitvoeren van de analyse |

## 4.2 Voorbereidingen

Alvorens te starten met de eerste activiteit zijn enkele voorbereidingen noodzakelijk:

- Verkrijg inzicht in de supply chain waarin de organisatie zich bevindt. Door een stakeholders analyse uit te voeren ontstaat inzicht in de organisaties die deelnemen in de supply chain.
- Stel vast waarom de behoefte is ontstaan om de cyber security risico's in de keten in kaart te brengen.

Het is tevens belangrijk om vast te stellen of de volgende randvoorwaarden zijn ingevuld:

- Concurrentie moet geen rol spelen; hiertoe kunnen de juridische afdelingen van alle organisaties worden geraadpleegd.
- Informatie moet kunnen worden gedeeld binnen het team. Daarom zijn afspraken nodig over de wijze waarop er met vertrouwelijke gegevens om wordt gegaan.
- Het inzichtelijk maken van de cyber security risico's binnen een supply chain vraagt van alle organisaties een bepaalde inzet aan kosten en capaciteit. Belangrijk is dat de initiator(s) voldoende middelen ter beschikking heeft vanuit de eigen organisatie om de analyse uit te kunnen voeren.
- Bereidheid om open alle 'what if' scenario's te bezien, ook die waarvan de kans als zeer klein kan worden gezien. Vertegenwoordigers van de deelnemende organisaties moeten op bepaalde momenten tijdens het proces de mate waarin zij zelf in control zijn ter discussie durven te stellen.

## 4.3 Uit te voeren activiteiten

### 4.3.1 Activiteit 1: maken werkafspraken

Deze activiteit start met een initiator of meerdere initiatoren die een voorstel doen om de risico's in kaart te brengen van een bepaalde supply chain. Voor het goed laten verlopen van de analyse is het belangrijk dat vertrouwen tussen de deelnemende organisaties ontstaat. Tijdens de gehele analyse wordt vertrouwelijke informatie over bijvoorbeeld kwetsbaarheden besproken. Het is daarom belangrijk om reeds in het begin aandacht te besteden aan dataclassificatie en protocollen om vertrouwelijke data op de juiste wijze met de andere organisaties uit te kunnen wisselen. Het vastleggen van deze afspraken draagt bij aan een voorspoedige samenwerking tussen de diverse organisaties gedurende de analyse.

Daarnaast worden afspraken gemaakt ten aanzien van de randvoorwaarden waaraan invulling te geven. Houdt hierbij rekening met eventuele voorwaarden die bepaalde deelnemende organisaties stellen en de eisen met betrekking tot de inhoud en vorm van het eindresultaat.

Alle gemaakte afspraken worden genotuleerd en ter goedkeuring verzonden aan alle deelnemende organisaties.

### 4.3.2 Activiteit 2: afbakenen onderzoeksgebied

Nadat duidelijke werkafspraken zijn gemaakt kan gestart worden met het bepalen van de scope. De eerste vragen die hierbij gesteld worden om het onderzoeksgebied van de analyse af te bakenen zijn:

- Welke supply chain wordt onderzocht? In deze activiteit van de scopebepaling wordt gekeken welke supply chain te onderzoeken. Binnen één sector kunnen meerdere supply chains naast elkaar bestaan. Eén organisatie kan in meerdere supply chains een (kritieke) rol spelen. Doorgaans komen de initiatiefnemer(s) reeds uit deze sector en de betrokken organisaties zullen voldoende inzicht hebben om de supply chain te selecteren waarvan verstoring de grootste impact heeft.
- Welke organisaties zijn onderdeel van deze supply chain? Aan de hand van de supply chain kan bepaald worden welke organisaties hierin een kritieke rol spelen. Het is denkbaar dat meerdere organisaties eenzelfde rol hebben binnen het supply chain proces. Het is in dat geval mogelijk om één, enkele of alle organisaties te betrekken bij de analyse.

Vervolgens betrekt de initiator de relevante organisaties bij de voorbereiding van de analyse. Tevens wordt er een initiatiedocument opgesteld wat kan dienen bij het verkrijgen van de vereiste commitment van het bestuur van de organisaties. Het initiatiedocument dient tevens als startpunt voor de volgende stap. In bijlage 3 is een template voor het initiatiedocument opgenomen.
Na het betrekken van de relevante organisaties wordt de exacte scope vastgesteld. Tijdens een kick off bijeenkomst van de risicoanalyse wordt tezamen vastgesteld met welke diepgang het kritieke product of dienst[2] wordt onderzocht. Wordt alleen het Business-to-Business gedeelte van de supply chain onderzocht of bevat de scope ook het Business-to-Consumer gedeelte van de supply chain?
Een ander scope-aspect wat hier ter sprake komt is wanneer sprake is van kritische systemen voor de supply chain. De uitkomsten van deze bijeenkomst worden vastgelegd en leiden tot een afgebakend onderzoeksgebied.

TIPS:

- Bij het bepalen van de te betrekken organisaties dient balans gevonden te worden om tussen enerzijds de vertegenwoordiging vanuit alle organisaties in dezelfde laag van de supply chain te hebben en anderzijds de grootte van het team beheersbaar te houden. Wanneer per laag één organisatie wordt gekozen blijft het aantal deelnemers beperkter waardoor de analyse sneller en efficiënter uitgevoerd kan worden. Wanneer meer organisaties per laag worden geselecteerd vergt dit extra inspanning bij het beschrijven van de supply chain. Tevens introduceert dit mogelijk extra complicaties op het gebied van concurrentie tussen organisaties in dezelfde laag van de supply chain.
- De afgevaardigden beschikken in ieder geval over zicht en invloed op het securityproces bij hun organisatie. Dit stelt de afgevaardigden in staat om een inschatting te maken van de kwetsbaarheden in de kritische systemen van de supply chain.
- De afgevaardigden hebben een bepaalde mate van technisch inzicht.
- Gebruik de checklist in bijlage 4 om te controleren of in de scopebepaling volledig is.

**Welke objecten dienen minimaal in scope gebracht te worden?**
De systemen die noodzakelijk zijn voor het leveren van het eindproduct dienen minimaal in scope te zijn. Dit zijn meestal de systemen die een hoge BIV-classificatie hebben gekregen. De overige systemen, zoals financiële systemen, kunnen buiten scope blijven of in een separaat traject worden beoordeeld.

[2] Deze methodiek is zowel toepasbaar op producten als op diensten. Wanneer gesproken wordt van een ‘product’ dan kan dit ook vervangen worden door ‘dienst’

## 4.4 Te bereiken resultaten

Na het uitvoeren van de activiteiten in de 1e stap zijn de volgende resultaten bereikt:

- ❑ Afgestemde werkafspraken tussen de deelnemende organisaties.
- ❑ Overeenstemming over de geldende randvoorwaarden.
- ❑ Overzicht van de te onderzoeken supply chain, inclusief de te betrekken organisaties.
- ❑ Overzicht van de te betrekken systemen.
- ❑ Initiatiedocument voor het uitvoeren van de analyse.

# 5 Stap 2: beschrijven supply chain

| Input | Proces | Resultaat |
|---|---|---|
| **Processen, informatiesystemen, Interfaces en classificaties** | **Beschrijven supply chain** | **Gedetailleerde topologie supply chain** |

## 5.1 Inleiding

In deze stap van de analyse wordt een gedetailleerde topologie (overzicht) gecreëerd van het gehele IT landschap in de supply chain en wordt de te hanteren BIV classificatie vastgesteld. Voor het opstellen van de topologie geldt als uitgangspunt de vastgestelde scope in de eerste stap.

| | |
|---|---|
| Input | Processen, informatiesystemen, interfaces en classificaties |
| Processtap | Beschrijven supply chain |
| Resultaat | • Gedetailleerde topologie supply chain<br>• Vastgestelde BIV classificatie voor de supply chain |

## 5.2 Voorbereidingen

Alvorens te starten met de beschrijving van de supply chain topologie zijn de volgende voorbereidingen noodzakelijk:

- Per organisatie is de gehanteerde BIV-classificatie beschikbaar
- Per organisatie is in kaart gebracht welke business processen kritiek zijn voor de supply chain
- Per organisatie welke systemen deze kritieke business processen faciliteren/ondersteunen

## 5.3 Uit te voeren activiteiten

Voor de beschrijving van de supply chain wordt vastgelegd welke (kritieke) processen en systemen betrokken zijn. Daarnaast worden de interfaces tussen de systemen van de supply chain organisaties geïdentificeerd en wordt vastgesteld welke gezamenlijke IT producten en diensten gebruikt worden in de supply chain.

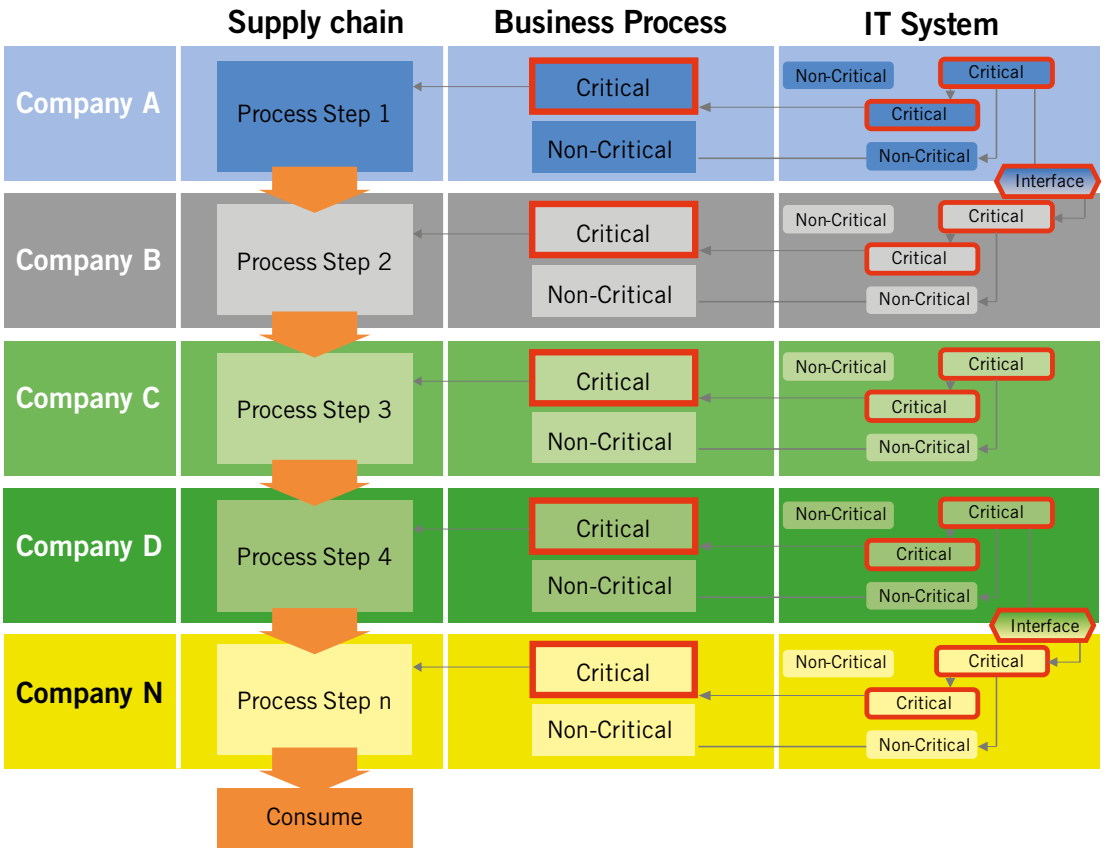
In de figuur 3 is een visualisatie gegeven van een supply chain.

Voor het beschrijven van de supply chain wordt per organisatie vastgesteld welke bedrijfsprocessen kritisch zijn voor de supply chain. Met kritisch wordt bedoelt die processen die noodzakelijk zijn voor de daadwerkelijke levering van het eindproduct. Wanneer de kritieke processen zijn geïdentificeerd worden vervolgens de systemen die deze business processen ondersteunen in het overzicht opgenomen.

Bij de inventarisatie van de systemen worden vier verschillende categorieën toegepast:

| Categorie | Systeem |
|---|---|
| 1 | Bedrijfsspecifieke systemen |
| 2 | Interfaces |
| 3 | Gemeenschappelijke ICT producten |
| 4 | Gemeenschappelijke diensten |

Elk van de betrokken organisaties draagt zorg voor categorie 1, de bedrijfsspecifieke systemen in het overzicht. Hier kan eventueel gebruik worden gemaakt van zogenaamde challenge sessions, waarbij andere organisaties in de supply chain doorvragen of bepaalde systemen daadwerkelijk kritisch zijn of anderzijds of echt alle kritieke systemen in het overzicht zijn opgenomen.
Interfaces tussen systemen vallen in twee categorieën: de interfaces tussen één of meerdere interne




*Figuur 3: Visualisatie supply chain*

systemen en interfaces tussen verschillende organisaties binnen de supply chain. Kritieke interfaces BINNEN één organisatie worden onder de bedrijfsspecifieke systemen (categorie 1) in het overzicht opgenomen terwijl interfaces TUSSEN verschillende organisaties in de supply chain onder interfaces (categorie 2) worden geregistreerd.

Om gemeenschappelijke afhankelijkheden inzichtelijk te krijgen wordt gekeken naar bedrijfsoverstijgende IT producten en diensten, categorie 3 en 4 in bovenstaand overzicht. Denk hierbij voor de gemeenschappelijke IT producten aan branche specifieke en/of industriële automatiseringsproducten. De categorie diensten omvat bijvoorbeeld gemeenschappelijke datacenters of (IT) dienstverleners.

Door het inventariseren van de verschillende systemen (categorie 1 t/m 4) wordt het inzichtelijk welke kwetsbaarheden het supply chain proces heeft.

Om een bepaalde waarde te geven aan de mate van belang van specifieke systemen in het supply chain proces wordt gebruik gemaakt van een BIV-classificatie. Dit is een veelgebruikte methode, waarbij op een eenvoudige manier, via een geharmoniseerde BIV-classificatie, een eenduidig beeld gevormd kan worden van het belang van de systemen.

Het vaststellen van een geharmoniseerde BIV classificatie en het beschrijven van de supply chain is hieronder per activiteit beschreven.

### 5.3.1 Activiteit 1: vaststellen geharmoniseerde BIV classificatie

Organisaties werken doorgaans niet met dezelfde methodiek voor het classificeren van systemen en

informatie. In deze methodiek wordt gebruik gemaakt van een BIV[3] classificatie. Deze classificatie geeft het belang aan van het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie. Hoe hoger een systeem is geclassificeerd des te groter de impact voor de organisatie is wanneer een of meerdere van deze drie aspecten wordt gecompromitteerd. Niet ieder organisatie hanteert eenzelfde BIV classificatie. Om een BIV classificatie voor de supply chain op te stellen is het noodzakelijk dat de BIV classificaties van de deelnemende organisaties worden geharmoniseerd.

Voor het verkrijgen van een geharmoniseerde BIV classificatie kan bijvoorbeeld gekozen worden voor een 5-punts schaal, waarbij per organisatie wordt gekeken hoe de organisatie specifieke BIV classificatie hier het beste in past.

De gekozen BIV classificatie maakt gebruik van de onderstaande schaal:

1: Very Low
2: Low
3: Medium
4: High
5: Very High

Voor elke categorie is het gewenst om een beschrijving te geven van de categorie. Een voorbeeld is in bijlage 5 opgenomen.

**Welke schaal te hanteren?**
Bij het opstellen van deze methodiek is gekozen voor het hanteren van 5-punts schalen voor classificaties en het inschatten van risico's, kansen en impacts. Het hanteren van een 5-punts schaal is niet noodzakelijk om deze methodiek te gebruiken. Het voordeel van een 5-punts schaal ten opzichte van een 3-punts is de mogelijkheid om in de analyse meer nuances te onderkennen.

TIP:

- Voor het bepalen van de BIV classificatie van een systeem wordt altijd de hoogste waarde genomen van de individuele B, I en V waarde van het systeem. Voorbeeld: Wanneer de beschikbaarheid voor een systeem 1 is bij een uitvalsduur van één week en 4 voor de uitvalsduur van één dag dan wordt de waarde 4 gehanteerd als classificatie van de beschikbaarheid. De uiteindelijk hoogste waarde van de B, I en V van het systeem wordt gebruikt voor de impact score van het systeem. Dus bij een BIV classificatie van B(4), I(2), V(3) wordt 4 gebruikt als impact score.

### 5.3.2 Activiteit 2: beschrijven bedrijfsspecifieke processen en systemen

De tweede activiteit in het inzichtelijk krijgen van cyber security risico's binnen de supply chain is om per organisatie vast te stellen welke kritieke processen en systemen noodzakelijk zijn voor het leveren van het product. Elke afzonderlijke organisatie beschrijft, voor zichzelf, welke processen betrokken zijn bij de supply chain. Voor alle kritieke processen wordt hierbij tevens geïnventariseerd welke systemen hierbij betrokken zijn. Hierbij worden alleen de kritieke systemen betrokken. Een systeem is kritiek indien het noodzakelijk is voor het functioneren van de supply chain. Elke organisatie heeft hiermee inzicht verkregen in de kritieke systemen die nodig zijn voor het functioneren van de supply chain. Nadat elke organisatie deze analyse heeft uitgevoerd wordt een bijeenkomst georganiseerd waarbij elke organisatie de resultaten presenteert. Het doel van deze bijeenkomst is om in gezamenlijkheid een overzicht te krijgen van elkaars kritieke processen en systemen en over het totaal aan kritieke processen in de supply chain. Hiermee wordt een beeld gecreëerd van de opbouw van de gehele supply chain en de bedrijfsspecifieke systemen die hierbij betrokken zijn.

De uiteindelijke resultaten worden vastgelegd in een matrix waarin per organisatie de kritieke systemen staan die betrokken zijn in het supply chain proces. Per systeem is tevens de bijbehorende geharmoniseerde BIV classificatie weergegeven.
Een voorbeeld van de matrix is in bijlage 6 opgenomen.

[3] Beschikbaarheid, Integriteit en Vertrouwelijkheid

### 5.3.3 Activiteit 3: beschrijven interfaces

In de derde activiteit worden de koppelvlakken (interfaces) die aanwezig zijn tussen de verschillende organisaties in de supply chain geïnventariseerd. Het gaat hierbij niet om interfaces tussen systemen binnen een organisatie maar om de interfaces die systemen in twee of meer verschillende organisaties met elkaar koppelen.

Voor de inventarisatie is het aan te raden om steeds twee organisaties die elkaar opvolgen in de supply chain tezamen de inventarisatie van de interfaces tussen de twee organisaties uit te laten voeren. In scope zijn hierbij systemen die met elkaar verbonden zijn middels het internet of via een dedicated verbinding (private network).

In de inventarisatie wordt vastgelegd of de interface voor eenzijdige[4] of tweezijdige[5] uitwisseling wordt gebruikt. Daarnaast worden aan de hand van de gemeenschappelijke BIV-classificatie, de interfaces geclassificeerd. Hiermee wordt het inzichtelijk als er discrepanties ontstaan in het niveau van aanduiding van de systemen. Wanneer organisatie A de interface van zeer hoge classificatie voorziet, terwijl Organisatie B daar een veel lagere classificatie aangeeft, dan ontstaat er een discrepantie in de perceptie van het risico.

Deze resultaten worden vastgelegd in de matrix zoals opgenomen in bijlage 6.

### 5.3.4 Activiteit 4: beschrijven gemeenschappelijke IT producten

Voor de vierde activiteit wordt, na de inventarisatie van de kritieke processen, systemen en interfaces binnen de gehele supply chain, vastgesteld welke gemeenschappelijke IT producten worden gebruikt. Het gebruik van identieke, supply chain specifieke hard- en software kan een extra risico in de supply chain introduceren. Daarom wordt in deze stap geïnventariseerd welke onderliggende hard- en software wordt gebruikt voor de kritieke systemen. Deze gemeenschappelijke IT producten worden ook betrokken voor het bepalen van de cyber security bedreigingen en risico's in stap 4.

TIPS:

- Besteed extra aandacht aan deze activiteit indien in de supply chain veel gebruik wordt gemaakt van SCADA[6] systemen. Indien bijna alle organisaties in de supply chain gebruik maken van hetzelfde SCADA systeem voor hun supply chain specifieke systemen kan een kwetsbaarheid in het SCADA systeem verstrekkende gevolgen hebben voor de gehele supply chain.
- Afhankelijk van de eerder afgesproken scope kan er voor gekozen worden om Software zoals bijvoorbeeld het Operating System Microsoft Windows of het protocol TCP/IP buiten beschouwing te laten. Dit omwille van het beheersbaar houden van de scope en de focus te houden op de specifieke risico's binnen de supply chain.

### 5.3.5 Activiteit 5: beschrijven gemeenschappelijke diensten

Als laatste worden de gemeenschappelijke IT- *diensten of dienstverleners* geïnventariseerd die gebruikt worden voor het leveren en ondersteunen van de in stap 2 t/m 4 geïdentificeerde systemen en processen. De deelnemers geven daarom inzicht in de individuele diensten die gebruikt worden in hun gedeelte van de gehele supply chain. Bij dit soort diensten valt te denken aan zaken als Internet Service Providers (ISPs), externe datacenters en telecom providers.

Wanneer alle organisaties in de supply chain een overzicht hebben gegeven van de diensten en dienstverleners die de kritieke processen voor de supply chain faciliteren kan worden beoordeeld of bepaalde diensten door meer dan één organisatie worden gebruikt. Het gebruik van één dienst of één dienstverlener door meerdere organisaties in de supply chain kan leiden tot een Single Point of Failure in de supply chain. Een outage van zo'n derde partij zou wellicht door één van de organisaties opgevangen kunnen worden maar wanneer meerdere organisaties in de supply chain hiermee te

[4] Hierbij zendt een systeem uit categorie 1 van organisatie A informatie/data naar organisatie B
[5] Hierbij zendt een systeem uit categorie 1 van organisatie A informatie/data naar organisatie B en omgekeerd
[6] Supervisory Control and Data Aqcuisition

maken krijgen zou dit tot aanvullende risico's kunnen leiden. Deze gemeenschappelijke diensten worden daarom betrokken bij het inschatten van de cyber security bedreigingen en risico's in stap 4

## 5.4 Te bereiken resultaten

Na het uitvoeren van de activiteiten in de 2e stap zijn de volgende resultaten bereikt:

- ❑ Een vastgestelde BIV classificatie die ingezet kan worden voor het classificeren van de in de supply chain gebruikte systemen.
- ❑ Een gedetailleerde topologie van de supply chain met daarin:
  - De kritieke bedrijfsspecifieke processen en systemen.
  - De interfaces van de systemen tussen de verschillende organisaties.
  - De gemeenschappelijke IT producten.
  - De gemeenschappelijke IT diensten of dienstverleners.
- ❑ De systemen in de supply chain hebben een BIV classificatie toegewezen gekregen.

# 6 Stap 3: bepalen impact verstoring supply chain

| Input | Proces | Resultaat |
|---|---|---|
| Gedetailleerde topologie supply chain | Bepalen impact verstoring supply chain | Procesrisico's |

## 6.1 Inleiding

In deze stap wordt op basis van verschillende scenario's onderzocht wat de impact op de supply chain zou zijn wanneer één organisatie niet meer in staat blijkt te zijn om zijn bijdrage aan de supply chain te leveren.

| | |
|---|---|
| Input | Gedetailleerde topologie supply chain |
| Processtap | Bepalen impact verstoring supply chain |
| Resultaat | Het uitvoeren van deze stap leidt tot de volgende resultaten:<br>• Een overzicht van mogelijke calamiteiten scenario's in de supply chain<br>• Een overzicht van de impact op de supply chain voor alle geïdentificeerde calamiteiten scenario's |

## 6.2 Voorbereidingen

Alvorens te starten met de impact bepaling zijn de volgende voorbereidingen noodzakelijk:

- Beoordeel in hoeverre voldoende kennis aanwezig is binnen het analyse team om de impact van een verstoring bij een van de supply chain organisaties goed in te kunnen schatten. Betrek zonodig aanvullende (business)expertise vanuit de deelnemende organisaties voor deze stap.
- Stel een template op waarmee per verstoringsscenario kan worden vastgelegd wat de impact is bij de verschillende supply chain organisaties. In bijlage 7 is een voorbeeld opgenomen.

## 6.3 Uit te voeren activiteiten

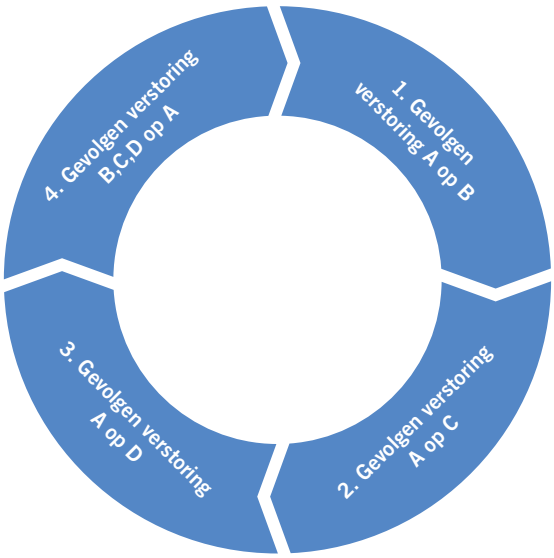
Voor het uitvoeren van de impact analyse wordt in een workshop een scenario analyse uitgevoerd op de mogelijke verstoringen die kunnen optreden in de supply chain. Hiervoor wordt bij elke organisatie in de supply chain steeds bepaald wat de impact is op de gehele supply chain indien de organisatie niet of gedeeltelijk de benodigde bijdrage kan leveren aan de supply chain. Hierbij wordt steeds vastgelegd wat de impact is voor elke organisatie in de supply chain.

Het resultaat van de workshop is een overzicht van mogelijke calamiteiten scenario's en een kwalitatieve beschrijving van de impact op de supply chain.

### 6.3.1 Activiteit 1: Bepalen impact per scenario

Voor het bepalen van de impact wordt telkens per organisatie de volgende vraag gesteld: "Wat is de impact op de gehele supply chain indien mijn organisatie, ten gevolge van een calamiteit, niet in staat is om de benodigde bijdrage te leveren voor de supply chain?".

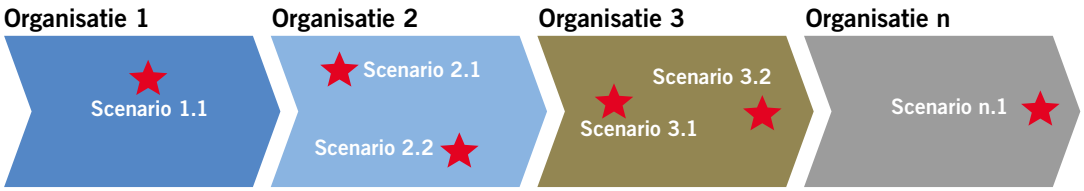
Om deze impact voor de supply chain te bepalen wordt begonnen bij de eerste organisatie aan het begin van de supply chain. Vervolgens wordt beoordeeld wat de impact is voor de opvolgende organisatie of organisaties in de supply chain. In onderstaande cirkeldiagram is het te doorlopen proces weergegeven.




In dit voorbeeld wordt begonnen bij organisatie A, waarbij vervolgens wordt beoordeeld wat de impact voor organisatie B is wanneer organisatie A niet haar benodigde bijdrage aan de supply chain kan leveren. Dit wordt daarna ook bij de opvolgende organisaties C en D gedaan. Tevens wordt beoordeeld of de calamiteit die begon bij organisatie A versterkt kan worden door eventuele gevolg calamiteiten verderop in de supply chain. Dit kan bijvoorbeeld het geval zijn wanneer organisatie A zijn productie moet stoppen omdat organisatie B geen grondstoffen meer kan verwerken.

Uiteindelijk wordt voor elk scenario een kwalitatieve beschrijving gemaakt van de impact voor elk van de organisaties.

Als deze beoordeling is afgerond voor organisatie A wordt verder gegaan met organisatie B. Hierbij wordt wederom de gehele supply chain doorlopen om uiteindelijk weer bij organisatie B uit te komen. Wanneer dit voor elke organisatie binnen de supply chain is uitgevoerd ontstaan meerdere calamiteiten scenario's. Deze scenario's kunnen het beste in een overzicht worden weergegeven en voorzien van een korte beschrijvende scenario naam zoals hieronder in de tabel weergegeven.




*Figuur: Grafische weergave scenario's*

| Scenario nr. | Scenario naam | Beschrijving impact |
|---|---|---|
| 1.1 | Bosbrand | Wanneer geen nieuwe grondstoffen aangeleverd kunnen worden bij organisatie A binnen 48 uur valt de productie stil bij organisatie B. |
| 2.1 | ... | ... |
| 2.2 | | |
| Etc. | | |

## 6.4 Te bereiken resultaten

Na het uitvoeren van de activiteiten in de 3e stap zijn de volgende resultaten bereikt:

- ❑ Een overzicht van mogelijke calamiteiten scenario's in de supply chain.
- ❑ Een overzicht van de impact op de supply chain voor alle geïdentificeerde calamiteiten scenario's.

# 7 Stap 4: vaststellen omvang cyberbedreigingen en risico's

| Input | Proces | Resultaat |
|---|---|---|
| **Cyber bedreigingen, beveiligingsmaatregelen en topologie supply chain** | **Vaststellen omvang cyber bedreigingen en risico's** | **Overzicht relevante bedreigingen en supply chain risico's** |

## 7.1 Inleiding

In deze stap wordt vastgesteld in welke mate cyberbedreigingen leiden tot risico's voor de supply chain. Hiervoor wordt gebruik gemaakt van de resultaten die verkregen zijn in de voorgaande stappen.

| | |
|---|---|
| Input | Cyberbedreigingen, beveiligingsmaatregelen, topologie supply chain |
| Processtap | Vaststellen omvang cyber bedreigingen en risico's |
| Resultaat | Het uitvoeren van deze stap leidt tot de volgende resultaten:<br>• Een overzicht van de te onderzoeken cyberbedreigingen<br>• Een inschatting van de kans dat de IT-systemen in de supply chain worden getroffen door de cyberbedreigingen<br>• Een inschatting van de impact van de cyberrisico's op de supply chain |

## 7.2 Voorbereidingen

Alvorens te starten met deze stap zijn de volgende voorbereidingen noodzakelijk:

- Vastgestelde lijst met te onderzoeken cyberbedreigingen

Voor het vaststellen van de te onderzoeken cyberbedreigingen is het aan te raden om te beginnen met een standaard lijst aan bedreigingen[7]. Uit deze standaard lijst kan dan een selectie worden gemaakt van de meest relevante bedreigingen. Bedreigingen die niet cyber specifiek zijn, zoals overstromingen of brand, vallen buiten scope.

Nadat duidelijk is welke cyberbedreigingen onderzocht gaan worden kan de verdere analyse plaatsvinden.

## 7.3 Uit te voeren activiteiten

Om de omvang van de cyberbedreigingen vast te stellen wordt als eerste een inschatting gemaakt van de kans dat de geselecteerde cyberbedreigingen daadwerkelijk leiden tot een verstoring van de BIV van de categorie 1 t/m 4 systemen. Hierbij wordt gekeken naar het 'netto risico' dat wordt gelopen. Dit wil zeggen dat rekening wordt gehouden met de reeds getroffen beveiligingsmaatregelen voor het inschatten van de kans dat een cyberbedreiging manifest wordt op een van de systemen.

Na het vaststellen van het dreigingsniveau wordt een risico-inschatting gemaakt voor de verschillende systemen. Deze inschatting wordt gemaakt door de dreigingsniveau's te confronteren met de geharmoniseerde BIV-waarden van de systemen in de supply chain. Hieruit volgt een overzicht van de risico's per systeem. Voor de hoge risico's wordt aanvullend nog beoordeeld welke impact dit kan hebben voor de supplychain. Hiervoor wordt gebruik gemaakt van de resultaten verkregen uit stap 3.

Elke supply chain organisatie voert deze analyse uit voor zijn eigen kritieke systemen (categorie 1). Supply chain organisaties die een interface delen (categorie 2), voeren voor de desbetreffende interface deze analyse gezamenlijk uit. Gemeenschappelijke IT producten en –diensten (categorie 3, 4) die door de meerderheid van de organisaties worden gebruikt dienen in de analyse betrokken te worden. De individuele analyses van elke supply chain organisatie worden plenair besproken met de overige supply chain organisaties.

[7] Om een overzicht te krijgen van de meest relevante cyberbedreigingen kan bijvoorbeeld gebruik gemaakt worden van het ENISA threat landscape 2014 rapport. (https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014)

Alle resultaten worden uiteindelijk verwerkt tot een overzicht van de gelopen risico's binnen de supplychain. Om een visuele weergave te krijgen van de supplychain risico's kan gekozen worden voor het opstellen van een risk heat map.

Het vaststellen van de omvang van de cyberbedreigingen en de risico's die hieruit volgen voor de supply chain is hieronder nader beschreven.

### 7.3.1 Activiteit 1: Inschatten omvang cyberbedreigingen

Voor elke te onderzoeken cyberbedreiging (zie voorbereiding van deze stap) wordt op een vijf-punts schaal (bijv. zeer laag tot zeer hoog), per IT-systeem, aangegeven hoe hoog de bedreiging wordt ingeschat. Deze inschatting houdt rekening met de reeds getroffen beveiligingsmaatregelen voor het desbetreffende systeem. Wanneer bijvoorbeeld de kans op een DDoS wordt ingeschat, dient hierbij rekening gehouden te worden met de reeds getroffen maatregelen tegen een DDoS aanval. De resterende kans op een succesvolle DDoS-aanval wordt uiteindelijk ingevuld.

| | | **Impact (1-5)** | | **Threat scenarios (1=Low, 5=Very High)** | | | |
|---|---|---|---|---|---|---|---|
| | | Eigen BIV rating | gem.sch. BIV rating | Virus | Hacking | (D)DoS | Threat n |
| **Categorie 1 (binnen één org)** | | | | | | | |
| Organisatie A (Bosbouwer) | 365FarmNet | 4 | 4 | 4 | 2 | 5 | |
| | SAP | 4 | 4 | 3 | 2 | 3 | |
| Organisatie B (Papierfabriek) | Simatic WinCC | 4 | 5 | 4 | 5 | 4 | |
| | SAP - HANA | 3 | 4 | 2 | 3 | 3 | |

*Figuur 4 Cyberbedreigingen supply chain 'Van boom tot papier'*

De inschatting van de cyberbedreigingen wordt voor de categorie 1 IT-systemen door elke supply chain organisatie individueel uitgevoerd. De categorie 2 IT-systemen worden door de supply chain organisaties die betrokken zijn bij de interface gezamenlijk beoordeeld. Categorie 3 en 4 van de IT-systemen worden door elke supply chain organisatie individueel voorbereid en uiteindelijk in een plenaire bijeenkomst gezamenlijk ingeschat.

Elke supply chain organisatie kan zijn resultaten invullen in de matrix zoals weergegeven in bijlage 6.

### 7.3.2 Activiteit 2: Inschatten omvang supplychain risico's

Na het vaststellen van de mate waarin de IT-systemen kwetsbaar zijn voor de cyberbedreigingen wordt een inschatting gemaakt van het gelopen risico. Hiertoe wordt de hoogste cyberdreigingsscore voor elk IT-systeem (kans) geconfronteerd met de BIV-waarde (impact) van het desbetreffende systeem. In onderstaande tabel is een voorbeeld gegeven hoe op basis van kans en impact tot een risicoinschatting te komen. In dit voorbeeld leidt alleen een zéér hoge kans en zéér hoge impact tot een zéér hoog risico. Afhankelijk van de risk appetite van de betrokken organisaties kan dit anders vormgegeven worden.

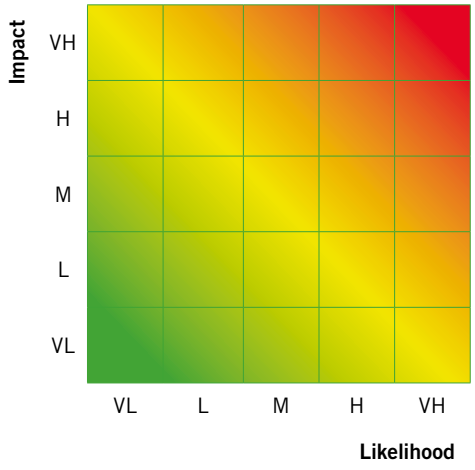
| Kans/ Impact | ZL(1) | L | M | H | ZH (5) |
|---|---|---|---|---|---|
| ZL(1) | 1 | 2 | 3 | 4 | 5 |
| L | 2 | 4 | 6 | 8 | 10 |
| M | 3 | 6 | 9 | 12 | 15 |
| H | 4 | 8 | 12 | 16 | 20 |
| ZH (5) | 5 | 10 | 15 | 20 | 25 |

Voor elk systeem kan hiermee een risicoinschatting worden gemaakt op de geselecteerde cyberbedreigingen zoals die eerder zijn vastgesteld. Alle hoge risico's worden vervolgens plenair besproken om te beoordelen tot welke supplychain risico's ze kunnen leiden. Hiervoor worden de supply chain risico's die in Stap 3 zijn geïdentificeerd zoveel mogelijk gerelateerd aan de IT-systemen. Door deze koppeling is inzichtelijk vanuit welke IT-systemen risico's kunnen ontstaan voor de supply chain.

| | | **Impact (1-5)** | | **Threat scenarios (1=Low, 5=Very High)** | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Eigen BIV rating | gem.sch. BIV rating | Virus | Hacking | (D)DoS | Threat n | Risico | Link tot gevolg |
| **Categorie 1 (binnen één org)** | | | | | | | | | |
| Organisatie A (Bosbouwer) | 365FarmNet | 4 | 4 | 4 | 2 | 5 | | 20 | Scenario 1.1 |
| | SAP | 4 | 4 | 3 | 2 | 3 | | 12 | |

*Figuur 5: Supply chain risico's 'Van boom tot papier'*

Om te zorgen dat de risico's voor de gehele supply chain in één oogopslag inzichtelijk zijn, kan een risk heat map gemaakt worden. Hiertoe wordt in een grafiek de kans van de risico's op de horizontale as uitgezet en de impact ervan op de verticale as. Vervolgens kunnen de geïdentificeerde risico's hierin geplot worden. Men kan ervoor kiezen om *alle* risico's op deze manier weer te geven of een subset, bijvoorbeeld de top-10 of de meest onverwachte risico's.




*Figuur 6: Risk heat map*

## 7.4 Te bereiken resultaten

Na het uitvoeren van de activiteiten in de 4e stap zijn de volgende resultaten bereikt:

- ❑ Een overzicht van de te onderzoeken cyberbedreigingen.
- ❑ Een inschatting gemaakt van de kans dat de systemen in de supply chain worden getroffen door de cyberbedreigingen.
- ❑ Een inschatting gemaakt van de impact van de cyberrisico's op de supply chain.
- ❑ Optioneel: Een visualisatie van de supply chain cyberrisico's.

# 8 Stap 5: bepalen maatregelen en opstellen actieplannen

| Input | Proces | Resultaat |
|---|---|---|
| Supply chain risico's | Bepalen maatregelen en opstellen actieplannen | Overzicht geaccepteerde risico's en actieplannen |

## 8.1 Inleiding

Deze laatste stap richt zich op het bepalen van de te treffen maatregelen en het opstellen van actieplannen. Alleen voor geïdentificeerde risico's die buiten de risicotoleraties liggen van een supply chain organisatie worden maatregelen bepaald en vastgelegd in een actieplan. Ter afsluiting van de risicoanalyse wordt gezamenlijk een nieuwe datum vastgesteld waarop de risicoanalyse wordt geactualiseerd. Tevens worden de belangrijkste uitkomsten uit de analyse gedocumenteerd en gedeeld met de deelnemende organisaties.

| | |
|---|---|
| Input | Supply chain risico's |
| Processtap | Bepalen maatregelen en opstellen actieplannen |
| Resultaat | Het uitvoeren van deze stap leidt tot de volgende resultaten:<br>• Per organisatie een overzicht van de geaccepteerde en niet geaccepteerde risico's<br>• Per organisatie een actieplan (indien van toepassing)<br>• Een datum waarop de supply chain risicoanalyse wordt geactualiseerd<br>• Een vastlegging (bijv. presentatie) van de belangrijkste resultaten uit de supply chain risicoanalyse |

## 8.2 Voorbereiding

Alvorens te starten met deze stap zijn de volgende voorbereidingen noodzakelijk:

- Voor elke organisatie is inzichtelijk welke risico's buiten zijn risicotoleratie vallen.

Elke organisatie dient op basis van de gevonden risico's zelfstandig te bepalen in hoeverre deze risico's geaccepteerd kunnen worden. Dit kan afhankelijk zijn van meerdere factoren en dient door elke organisatie individueel afgewogen te worden. Als leidraad kan gesteld worden dat hoge risico's normaliter buiten de risicotoleratie vallen.

Nadat helder is welke risico's geaccepteerd worden en welke risico's niet kan gestart worden met het bepalen van de maatregelen.

## 8.3 Uit te voeren activiteiten

Elke supply chain organisatie bepaalt, voor de onacceptabele risico's die gelopen worden op de categorie 1 systemen (organisatie specifieke systemen), zelfstandig welke maatregelen het beste getroffen kunnen worden voor het verlagen van het risico. Voor de categorie 2 systemen (interfaces) wordt samengewerkt tussen de betrokken supply chain organisaties bij het desbetreffende systeem. Indien risico's voortkomen uit de categorieën 3 en 4 systemen (gezamenlijke IT producten/diensten) wordt het actieplan plenair opgesteld.

Na het opstellen van de actieplannen wordt een nieuwe datum vastgesteld waarop de risicoanalyse wordt geactualiseerd. Daarnaast wordt door een van de deelnemende organisaties een samenvatting gemaakt van de belangrijkste uitkomsten uit de analyse en gedeeld met alle deelnemers.

De activiteiten in deze laatste stap zijn hieronder nader beschreven.

### 8.3.1 Activiteit 1: Bepalen maatregelen

Voor elk onacceptabel risico's wordt als eerste per IT-systeem beoordeeld welke maatregelen getroffen kunnen worden om het risico te verlagen. Het kunnen hierbij maatregelen zijn die technisch, maar ook organisatorisch, van aard zijn. Voor elke mogelijke maatregel wordt ingeschat welke inspanning

benodigd is om de maatregel in te voeren en wat de verwachte effectiviteit is van de maatregel. Voor elk risico kunnen meerdere maatregelen worden getroffen. Na inventarisatie van de maatregelen wordt vastgesteld welke maatregelen ingevoerd kunnen worden.

Het selecteren van de in te voeren maatregelen kan het beste geschieden door op basis van de verhouding tussen resultaat en inspanning van een bepaalde maatregel, die maatregelen te selecteren die de risico's zo effectief en efficiënt mogelijk terugbrengen tot een acceptabel risico.

Afhankelijk van de categorie IT-systeem waar het risico betrekking op heeft dient samengewerkt te worden met één of meerdere supply chain organisaties bij het bepalen van de maatregelen.

### 8.3.2 Activiteit 2: Opstellen actieplan

Nadat elke organisatie heeft vastgesteld welke maatregelen gewenst zijn voor het verlagen van de onacceptabele risico's stelt elke organisatie een actieplan op. In dit actieplan wordt per maatregel aangegeven wie verantwoordelijk is voor de realisatie, welke acties noodzakelijk zijn en op welke termijn de maatregel is gerealiseerd. Het actieplan biedt hiermee een overzicht van alle noodzakelijke acties voor het verlagen van de risico's binnen de risicotoleratie van de organisatie.

In bijlage 8 is een template opgenomen voor het opstellen van een actieplan.

### 8.3.3 Activiteit 3: afronden risicoanalyse

Ter afronding van de cyber security supply chain risicoanalyse wordt een nieuwe datum vastgesteld voor het actualiseren van de analyse. Hiermee wordt geborgd dat de supply chain organisaties tezamen blijven werken aan het beheersen van de risico's in de supply chain. Eventuele verbeteringen die zijn doorgevoerd, bijvoorbeeld naar aanleiding van de actieplannen, kunnen meegenomen worden tijdens de herbeoordeling. Aangeraden wordt om minimaal twee-jaarlijks een herbeoordeling uit te voeren. Als laatste wordt in een plenaire sessie de belangrijkste resultaten uit de supply chain risicoanalyse vastgelegd. Hierbij is het aan te raden dat één van de supply chain organisaties het voortouw neemt voor de vastlegging.

## 8.4 Te bereiken resultaten

Na het uitvoeren van de activiteiten in de 5e stap zijn de volgende resultaten bereikt:

- ❑ Per organisatie een overzicht van de geaccepteerde en niet geaccepteerde risico's.
- ❑ Indien van toepassing: Per organisatie een actieplan.
- ❑ Een datum waarop de supply chain risicoanalyse wordt geactualiseerd.
- ❑ Een vastlegging (bijv. presentatie) van de belangrijkste resultaten uit de supply chain risicoanalyse.

# 9 Bijlagen

## 9.1 Bijlage 1: Definities

**(Informatie)systeem:**
Een informatiesysteem is een samenhangende gegevensverwerkende functionaliteit voor de besturing of ondersteuning van één of meer bedrijfsprocessen.
Toelichting: Een informatiesysteem bestaat o.a. uit apparatuur, basisprogrammatuur, communicatievoorzieningen, applicaties, databases, technische voorzieningen, procedures en mensen

**Beschikbaarheid:**
De mate waarin informatie op het juiste moment beschikbaar is voor de gebruikers. Beschikbaarheid kent de volgende kenmerken:
- Tijdigheid: kan de informatie worden geleverd op het moment dat deze nodig is.
- Continuïteit: kan de informatie ook in de toekomst worden geleverd.
- Robuustheid: is de informatie bestand tegen verstoringen.

**Integriteit:**
De mate waarin de gegevens een afspiegeling zijn van de werkelijkheid. Integriteit kent de volgende kenmerken:
- Correctheid: klopt de informatie en wordt deze correct weergegeven.
- Volledigheid: is de informatie volledig.
- Geldigheid: Is de informatie geldig.
- Authenticiteit: Is de bron van de ontvangen informatie juist.
- Onweerlegbaarheid: heeft de verzender de informatie inderdaad verzonden.
- Nauwkeurigheid: de mate van detail en afronding van de informatie.
- Controleerbaarheid: in hoeverre kan de informatie worden gecontroleerd.

**Vertrouwelijkheid:**
De mate waarin de toegang tot en het gebruik van de gegevens beperkt is tot de juiste personen. Vertrouwelijkheid kent de volgende kenmerken:
- Exclusiviteit: kan de informatie worden afgeschermd voor onbevoegden.
- Privacy: wordt er op een correcte manier omgegaan met persoonlijke gegevens.

**Supply chain:**
Logistieke keten vanaf de grondstoffenwinning tot aan de levering van gereed product aan de uiteindelijke afnemer.

## 9.2 Bijlage 2: Schema analyseproces

# Cyber security supply chain risicoanalyse

| Input | Proces | Resultaat |
|---|---|---|
| Supply chains | Bepalen scope | Afgebakend onderzoeksgebied |

| Input | Proces | Resultaat |
|---|---|---|
| Processen, informatiesystemen, Interfaces en classificaties | Beschrijven supply chain | Gedetailleerde topologie supply chain |

| Input | Proces | Resultaat |
|---|---|---|
| Gedetailleerde topologie supply chain | Bepalen impact verstoring supply chain | Procesrisico's |

| Input | Proces | Resultaat |
|---|---|---|
| Cyber bedreigingen, beveiligingsmaatregelen en topologie supply chain | Vaststellen omvang cyber bedreigingen en risico's | Overzicht relevante bedreigingen en supply chain risico's |

| Input | Proces | Resultaat |
|---|---|---|
| Supply chain risico's | Bepalen maatregelen en opstellen actieplannen | Overzicht geaccepteerde risico's en actieplannen |

## 9.3 Bijlage 3: Template initiatie document

# Project Initiatie Document

### Introductie

*<beschrijf in algemene termen waarom dit project plaats vindt>*

### Doel van dit document

Doel van dit document is om de belangrijkste elementen van het project te identificeren en te beschrijven. Dit met het doel om de verwachtingen van alle in het project betrokken organisaties en eventuele andere stakeholders te begrijpen, vast te leggen en overeen te komen voordat het project van start gaat.

### Achtergrond

*<Beschrijf de achtergrond waarom dit project plaats vindt in meer detail. Wat is hieraan vooraf gegaan?Vermijd jargon en zorg dat deze achtergrond ook duidelijk is voor organisaties die niet direct bij (de uitvoering van) het project betrokken zijn.>*

### Doelstellingen en gewenste uitkomst

*<Beschrijf wat het te verwachten eindresultaat is. Wat hier beschreven wordt is van belang voor externe stakeholders dus geen jargon of technische details. Deze doelstellingen met alle (externe) stakeholders afstemmen voordat het project begint.>*

### Randvoorwaarden & aannames

*<Aan welke voorwaarden dient voldaan te worden om het project tot een succes te maken? Wanneer moet het klaar zijn? Hoeveel inzet wordt van de deelnemers verwacht? Wanneer bepaalde zaken nog niet 100% duidelijk zijn beschrijf dan welke aannames de basis zijn geweest om dit project toch door te laten gaan.>*

### Scope & deliverables

*<Beschrijf in detail welke zaken er opgeleverd zullen worden aan het einde van het project. Welk niveau van detaillering? Wat voor bestandsformaten? Tevens wordt hier beschreven wat de grenzen van het project zijn: Wat wordt wel onderzocht? Wat niet?>*

### Aanpak

*<Beschrijf HOE het eindresultaat tot stand gaat komen. Bijvoorbeeld maandelijks een hele dag bijeenkomen? Wordt een bestaande methodiek gevolgd? Wordt er werk uitbesteed?>*

### Organisatie

*<beschrijf WIE er aan het project werken en wat hun specifieke rol in het project is.>*

### Projectplan en kosten

*<Beschrijf welke milestones er in het project zijn en wanneer bepaalde deliverables opgeleverd dienen te worden.>*

### Stakeholders

*<Beschrijf wie er (behalve het project team wat al onder "Organisatie" is beschreven) op welke wijze bij het project betrokken worden.>*

### Projectrisico's en afhankelijkheden

*<Beschrijf wat de risico's zijn die het succesvol kunnen leveren van het gewenste eindresultaat (zie "Doelstellingen en gewenste uitkomst" en "Scope en Deliverables") kunnen verhinderen. Geef per risico een actie op die genomen kan worden mocht het risico zich inderdaad manifesteren.>*

## 9.4 Bijlage 4: Checklist scope bepaling

- ❑ De scope van de risicoanalyse is helder gedefinieerd waarbij duidelijk is:
  - Welke supply chain wordt beoordeeld
  - Welke organisaties betrokken dienen te worden in de analyse
  - Welke objecten worden meegenomen in de analyse:
    vi. De IT-systemen en interfaces die direct betrokken zijn bij de levering van het product / dienst
    vii. De kritieke IT-systemen die ter ondersteuning dienen van het product / de dienst en het (productie)proces dat daaraan ten grondslag ligt
    viii. De bedrijfsprocessen die nauw verbonden zijn met het gekozen proces;
    ix. De Gemeenschappelijke IT systemen
    x. De Gemeenschappelijke diensten
  - Of de financiële afhandeling van het te onderzoeken product wordt betrokken in de analyse
- ❑ Naar welke uitkomst(en) wordt gestreefd:
    xi. Inzichtelijk maken van risico's
    xii. Gezamenlijk gecoördineerde vervolgacties ondernemen, bijvoorbeeld verbeterpunten of een actieplan af te spreken
    xiii. Aanpassen/verbeteren van het gevolgde proces
- ❑ Met welke geografische afbakening rekening wordt gehouden?
    xiv. Lokaal,
    xv. Regionaal,
    xvi. Nationaal,
    xvii. Internationaal;
- ❑ Welke standaarden worden gehanteerd binnen de betreffende sectoren; (bijv. ISO 27000)
- ❑ Welke onderzoeken uit het verleden relevante informatie opleveren voor de huidige risicoanalyse
- ❑ Welke geldende specifieke regelgeving voor de te analyseren supply chain van toepassing is
- ❑ Werkafspraken zijn vastgelegd in een initiatiedocument en goedgekeurd door alle betrokken organisaties

## 9.5 Bijlage 5: Voorbeeld BIV classificatie

Voorbeeld BIV classificatie tabel

| | |
|---|---|
| Very low | An information security incident causing loss of confidentiality, integrity, availability or traceability of the information in the information asset could not cause any or neglectable damage to the organisation. |
| Low | An information security incident causing loss of confidentiality, integrity, availability or traceability of the information in the information asset could not cause any significant damage to the organisation. |
| Medium | Information security incidents with the information asset could cause damage to the organisation, but within the limits of normal business risk. The negative impact can be managed within normal operating budget using standard procedures and capacity. |
| High | The negative effect of an information security incident could cause significant damage to the organisation. The potential damage would exceed normal business risk and normal operating budget. Specific incident or crisis management would be needed to manage an incident. |
| Very High | The potential damage of an information security incident with the information in the information asset could seriously threaten business continuity. The damage would have a significant negative impact on financial results on corporate level or the position of (board) executives could be at stake. |

## 9.6 Bijlage 6: Matrix vastlegging resultaten risiconalayse

| | | | Impact (1-5) | | Threat scenarios (1=Low, 5=Very High) | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Eigen BIV rating | gem.sch. BIV rating | Virus | Hacking | (D)DoS | Threat n | Risico | Link tot gevolg |
| **Categorie 1 (binnen één org)** | | | | | | | | | | |
| A | A1 | | | | | | | | | |
| | A2 | | | | | | | | | |
| | A3 | | | | | | | | | |
| | A4 | | | | | | | | | |
| B | B1 | | | | | | | | | |
| | B2 | | | | | | | | | |
| | B3 | | | | | | | | | |
| | B4 | | | | | | | | | |
| C | C1 | | | | | | | | | |
| | C2 | | | | | | | | | |
| | C3 | | | | | | | | | |
| | C4 | | | | | | | | | |
| **Categorie 2 (systeem interface)** | | | | | | | | | | |
| | Van | Naar | | | | | | | | |
| A - B | A1 | B1 | | | | | | | | |
| A - B | A2 | B1 | | | | | | | | |
| A - C | A1 | C1 | | | | | | | | |
| B - C | B3 | C4 | | | | | | | | |
| B - D | B2 | D3 | | | | | | | | |
| n - m | Nn | Mm | | | | | | | | |
| **Categorie 3 (gemeenschappelijke producten voor deze industrie)** | | | | | | | | | | |
| Zie tabblad Components, services | | | | | | | | | | |
| **Categorie 4 (gemeenschappelijke diensten)** | | | | | | | | | | |
| Zie tabblad Components, services | | | | | | | | | | |

## 9.4 Bijlage 7: Template vastlegging gevolgen calamiteiten

# Project Initiatie Document

| | |
|---|---|
| 1 | Beschrijving calamiteit |
| 2 | Beschrijving gevolg calamiteit bij organisatie A voor organisatie B |
| 3 | Beschrijving gevolg calamiteit bij organisatie A voor organisatie C |
| 4 | Beschrijving gevolg calamiteit bij organisatie A voor organisatie D |
| 5 | Beschrijving gevolg calamiteit bij organisatie B,C,D voor organisatie A |

## 9.8 Bijlage 8: Template actieplan

| **Actieplan: Organisatie A** | | | | | |
|---|---|---|---|---|---|
| **Nr** | Risico | Maatregelen | Prioriteit | Verantwoordelijke | Tijdsvlak |
| **Systeem 1** | | | | | |
| 1 | <<Omschrijving risico>> | <<Omschrijving maatregel>> | <<H,M,L>> | <<Naam >> | |
| 2 | | | | | |
| **Systeem 2** | | | | | |
| 4 | | | | | |
| 5 | | | | | |

## 9.9 Bijlage 9: Matrix voorbeeld supply chain

| | | | Impact (1-5) | | Threat scenarios (1=Low, 5=Very High) | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Eigen BIV rating | gem.sch. BIV rating | Virus | Hacking | (D)DoS | Threat n | Risico | Link tot gevolg |
| **Categorie 1 (binnen één org)** | | | | | | | | | | |
| Organisatie A (Bosbouwer) | 365FarmNet | | 4 | 4 | 4 | 2 | 5 | | 20 | Scenario 1.1 |
| | SAP | | 4 | 4 | 3 | 2 | 3 | | 12 | |
| Organisatie B (Papierfabriek) | Simatic WinCC | | 4 | 5 | 4 | 5 | 4 | | 25 | Scenario 2.1 |
| | SAP - HANA | | 3 | 4 | 2 | 3 | 3 | | 12 | |
| Organisatie C (Vervoersbedrijf) | SCExpert | | 4 | 4 | 2 | 2 | 2 | | 8 | |
| | JDA Transportation Manager | | 5 | 5 | 2 | 2 | 2 | | 10 | |
| Organisatie D (Groothandel) | JDA retail planning | | 4 | 4 | 1 | 4 | 1 | | 16 | Scenario 4.2 |
| | Bypos kassasysteem | | 4 | 4 | 1 | 1 | 1 | | 4 | |
| **Categorie 2 (Systeem interface)** | | | | | | | | | | |
| | Van | Naar | | | | | | | | |
| A - B | SAP | SAP - HANA | | 4 | 2 | 2 | 2 | | 8 | |
| A - B | 365Farmnet | SAP - HANA | | 5 | 2 | 2 | 2 | | 10 | |
| B - C | SAP - HANA | SCExpert | | 3 | 2 | 2 | 2 | | 6 | |
| B - D | SAP - HANA | JDA retail planning | | 3 | 2 | 2 | 3 | | 9 | |
| C - D | SCExpert | JDA retail planning | | 4 | 2 | 2 | 4 | | 16 | Scenario 4.1 |
| n - m | Nn | Mm | | | | | | | | |
| **Categorie 3 (gemeenschappelijke producten voor deze industrie)** | | | | | | | | | | |
| Zie tabblad Components, services voor meer detail | CISCO ASA 5500-X | | | 4 | 1 | 1 | 4 | | 16 | Scenario 1.1 |
| **Categorie 4 (gemeenschappelijke diensten)** | | | | | | | | | | |
| Zie tabblad Components, services voor meer detail | Telecomprovider Vodafone | | | 4 | 2 | 2 | 2 | | 8 | |

# Colofon

**Eindredactie**
Wam Voster (Royal Dutch Shell), Jeffrey de Bruijn (Power of 4)

**Onderzoek uitgevoerd door**
Royal Dutch Shell, Nederlandse Gasunie, Nuon, TenneT, Alliander

**Met ondersteuning van**
Nationaal Cyber Security Centrum



Eerste druk, januari 2016