CONCLUSION

BEVEILIGINGSBELEID ECOSYSTEEM

Auteur
Roel Gloudemans
(roel.gloudemans@conclusion.nl)

Met medewerking van
Chris Gralike, Ricky Hoots, Artien Bel, Dennis Pieterse, Paul Schoorl, P. Mensink, A. van der Lee, M. Baak, G. Heysteeg en E. van Boxtel

Status: Definitief
Versie: 1.1 (04-03-2022 08:58:00)
Ten minste houdbaar tot: 2023-03-03

Versietabel			
Datum	Versie	Door	Aanpassing
21-09-13	0.1	R. Gloudemans	Eerste concept
21-10-06	0.2	R. Gloudemans	Review door P. Schoorl, C. Gralike en A. Bel.
21-11-03	0.3	R. Gloudemans	Review door R. Hoots en D. Pieterse. Geleerde lessen uit de meest recente cyberoefening; toevoeging security incident management, securitydienstverlening en verbetering CSIRT-aansturing.
21-11-16	0.4	R. Gloudemans	Review P. Mensink
22-01-28	1.0	R. Gloudemans	Review A. van der Lee en M. Baak
22-03-03	1.1	R. Gloudemans	Review G. Heysteeg en E. van Boxtel. Toevoeging doel “proactief” inclusief principes en prestatie indicatoren.

Accordering	
Document	Versie
Versie	1.0
Geaccordeerd door:	
	E. Verkoren – Algemeen Directeur van Conclusion
Alle hoofdversies van dit document worden geaccordeerd door de algemeen directeur. Kleine verbeteringen en/of aanpassingen vallen onder de verantwoordelijkheid van de Chief Security Officer	
*Dit document is geclassificeerd als **publieke** informatie en kan (in pdf-vorm) beschikbaar worden gesteld aan iedereen voor wie dit beleidsstuk relevant is.*	

Inhoud

1. Managementsamenvatting

Dit is het beveiligingsbeleid voor het Conclusion ecosysteem. Dit beleid moet bijdragen aan het op acceptabele waardes houden van de bedrijfsrisico's rondom informatieverwerking.

Conclusion is een ecosysteem met onafhankelijke bedrijven. Dat houdt in dat de bedrijven eigen keuzes maken daar waar het gaat om de bescherming van informatie en het onder controle houden van risico's. Dit document heeft tot doel de bedrijven te bewegen richting een uniforme aanpak. Zo kan van informatiebeveiliging bijgedragen worden aan het presenteren van een consistent beeld van Conclusion richting de Conclusion klant. De uniforme aanpak vereenvoudigt de onderlinge communicatie en geeft alle bedrijven een beter beeld over hoe we ervoor staan. Dit verbetert de weerbaarheid van het ecosysteem en maakt het eenvoudiger om te sturen op groepsniveau.

Bovenal moet het beveiligingsbeleid een weerspiegeling zijn van wie we zijn. Het Conclusion manifesto is, als weergave van deze identiteit, gekozen als basis voor het beleid.

Hoofdstuk 2: "Inleiding" is een weergave van de Conclusion organisatie en schetst uit welke elementen het beleid bestaat.

Hoofdstuk 3: "De doelen van informatiebeveiliging" koppelt de informatiebeveiligingsdoelen aan het Manifesto. **Op basis van deze doelen worden een aantal verplichte principes (pag. 12) geformuleerd**. Het beveiligingsbeleid van de bedrijven moet borgen dat deze doelen ook behaald worden, onder andere door tegemoet te komen aan de principes. Aan doelen is ook een aantal risico indicatoren gekoppeld zodat de prestaties inzichtelijk gemaakt kunnen worden.

Hoofdstuk 4: "Aansturing" gaat in op de verantwoordelijkheden op groepsniveau en voor een heel klein deel op bedrijfsniveau. Op groepsniveau wordt verwacht dat ieder bedrijf een centrale rol heeft voor informatiebeveiliging; de Information Security Officer (ISO).

Hoofdstuk 5: "Proces voor informatiebeveiliging" is een weergave van het proces op groepsniveau en formuleert de **regels rondom rapportage**. Zowel op groepsniveau als van de bedrijven naar elkaar en de groep.

De appendix bevat de definities van een aantal termen. De belangrijksten hiervan zijn **de definitie van de risicoschaal** (pag. 28) en het **concept "Vertrouwen"** (pag. 26).

2. Inleiding

2.1 Vindplaats

Dit beleidsdocument en onderliggende documenten waarnaar in dit document verwezen wordt zijn te vinden op de “Security” pagina van Start Your Day. (https://conclusionfutureit.sharepoint.com/sites/StartYourDay/SitePages/Privacy-&-Security.aspx)

2.2 Achtergrond en doel

Dit document beschrijft de doelen en opzet van informatiebeveiliging binnen het Conclusion Ecosysteem. Het doel van het informatiebeveiligingsbeleid is het ondersteunen van de missie, visie en strategie van Conclusion als geheel (hierna aangeduid als “Conclusion”) en die van de individuele bedrijven. Dit wordt gedaan door het stellen van meetbare doelen die maat zijn voor de digitale weerbaarheid en gebruikt worden voor het tot acceptabele waarden beperken van de informatierisico blootstelling van Conclusion.

Hierbij wordt “acceptabel” bepaald door de risicobereidheid van de organisatie als geheel.

Dit document gaat over de doelen voor Conclusion en de manier waarop de bedrijven samenwerken om die doelen te bereiken. Hoe de bedrijven deze doelen realiseren is de verantwoordelijkheid van de bedrijven zelf.

Onderliggend zijn nog een aantal andere documenten beschikbaar, waaronder een dreigingsanalyse. Welke documenten dat precies zijn en wat het doel is wordt benoemd in paragraaf 5.6.

2.3 Totstandkoming

Het beveiligingsbeleid gaat uit van het Manifesto van Conclusion. Er is gekozen voor een risico gerichte aanpak, binnen de kaders van wet- en regelgeving, waaronder de privacywetgeving in het bijzonder.

Bij het opstellen van dit en onderliggende beleidsdocumenten is gekeken naar een minimale set van normen en standaarden, waaronder het privacy beleid van Conclusion, de AVG, ISO27001, NEN7510 en de relevante wet- en regelgeving. Mogelijk is op individuele bedrijven extra regelgeving van toepassing. Een overzicht van relevante wet- en regelgeving is te vinden in het document “Relevante Wet en Regelgeving”.

De inhoud van dit document is opgesteld met hulp van de Security Officers van de bedrijven en afgestemd met de directie van Conclusion.

2.4 Scope

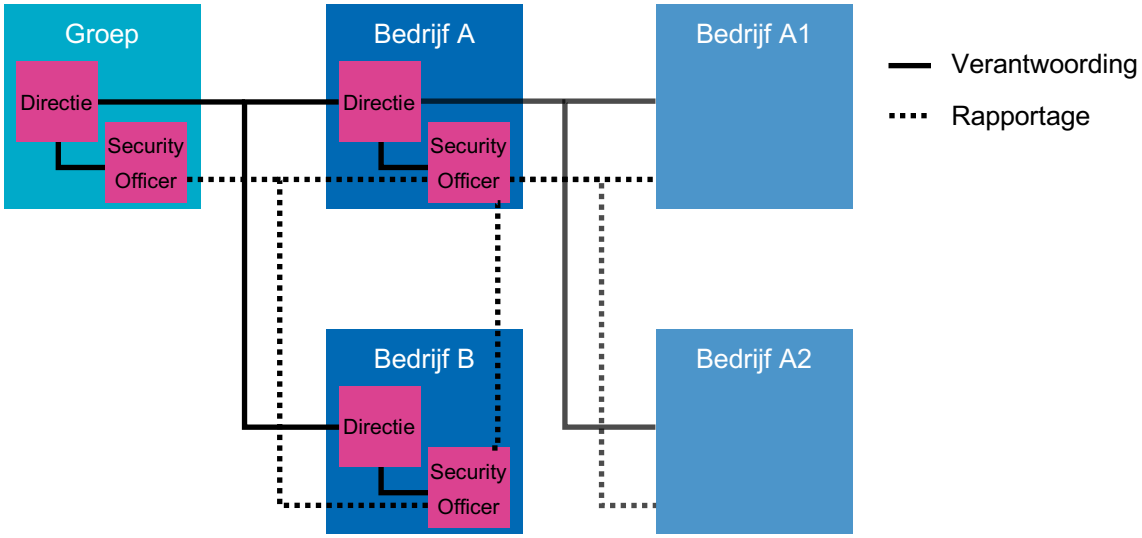
Dit document beschrijft de randvoorwaarden waar de bedrijven moeten voldoen en de rolverdeling met betrekking tot privacy en security op groepsniveau. Hoe de bedrijven hier invulling aan geven is aan de bedrijven zelf.

2.5 Publiek

Medewerkers die acteren op groepsniveau en de directeuren en (chief) security officers van de bedrijven.

2.6 Organisatiestructuur

Conclusion is een ecosysteem van bedrijven. Dat houdt in dat Conclusion bestaat uit een aantal bedrijven die zelfstandig opereren en die vaak de samenwerking zoeken. Deze bedrijven kunnen op zich ook weer bestaan uit meerdere bedrijven. Hierbij lopen de verantwoordingslijnen op directieniveau.

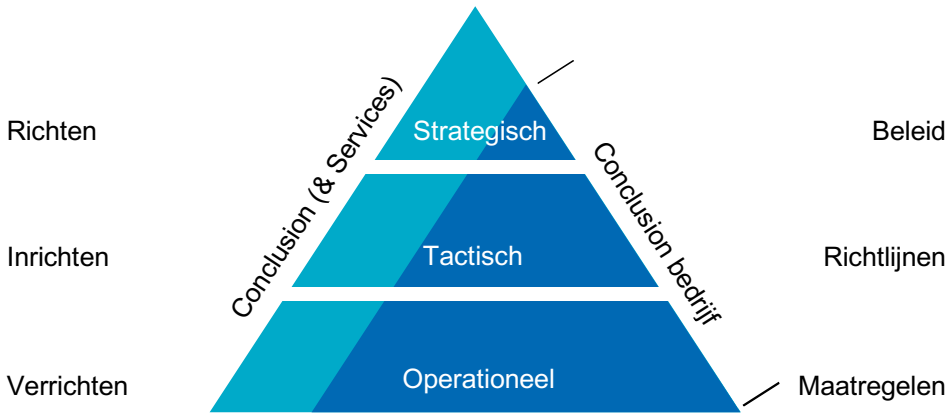


Figuur 1, De Conclusion organisatie

De personen die belast zijn met de rol van security officer leggen in de eerste plaats verantwoording af aan hun eigen directie. Daarnaast vindt er op regelmatige basis contact plaats tussen de security officers van de bedrijven en de security officer van de groep (de Chief Security Officer; de CSO), zodat er een centraal overzicht over de risico's ontstaat.

2.7 Opbouw van informatiebeveiliging

Conclusion geeft op drie niveaus invulling aan informatiebeveiliging. Het raamwerk voor informatiebeveiliging is als volgt opgebouwd:



Figuur 2, Raamwerk informatiebeveiliging

Hierbij is er sprake van een dubbele piramide. Aan de ene kant een (lichtblauwe) Conclusion brede piramide die vanaf de strategie uitmondt in maatregelen die van toepassing zijn op de centrale dienstverlening van Conclusion Services aan de Conclusion bedrijven.

Aan de andere kant voor ieder bedrijf een (donkerblauwe) piramide die aangeeft dat ieder bedrijf verantwoordelijk is voor haar eigen informatiebeveiliging[1] die wel in het geheel van Conclusion moet passen. *Het respecteren van de afspraken in en aansluiten bij de geschetste opbouw in dit document is daar een belangrijke basis voor.* Door een goede onderlinge afstemming kan de Conclusion klanten een consistent geheel geboden worden op het vlak van beveiliging. Daarnaast hebben de bedrijven voor hun beveiliging ook een onderlinge afhankelijkheid in de vorm van gedeelde dienstverlening, zoals de Conclusion website.

2.7.1 Strategisch – Beleid

Op strategisch niveau bestaat het beleid uit een aantal onderwerpen:

1. Beveiligingsbeleid van het ecosysteem (dit document); dit document is gericht op de regie op informatiebeveiliging. Het omvat de doelen, basisprincipes, taken en verantwoordelijkheden evenals het procesmodel, dat op groepsniveau voor beveiliging wordt gehanteerd. Dit document slaat ook de brug naar de risicobereidheid van Conclusion.
2. Jaarplan Informatiebeveiliging voor de groep; ieder jaar wordt een nieuw plan geformuleerd op basis van de constateringen en gebeurtenissen uit het afgelopen jaar. De bedrijven nemen waar nodig elementen uit het jaarplan over in hun eigen plannen.
3. Dreigingsanalyse; deze analyse beschrijft welke externe factoren kunnen verhinderen dat Conclusion de informatiebeveiligingsdoelstellingen niet bereikt. Het betreft hier de dreigingen die op alle bedrijven van Conclusion van toepassing zijn. Ieder bedrijf moet deze analyse aanvullen met een analyse voor de eigen context (binnen de eigen piramide).
4. Stakeholder analyse; dit document beschrijft de context waarin Conclusion opereert en de verschillende belanghebbenden bij de informatiebeveiliging van Conclusion

2.7.2 Tactisch – Richtlijnen

Voor het tactische niveau worden de richtlijnen gedefinieerd voor een aantal aandachtsgebieden. Een voorbeeld hiervan is de richtlijn dataclassificatie. Deze richtlijn bevat het classificatie raamwerk. Zo zijn er ook richtlijnen voor infrastructuur en processen. De richtlijnen zijn zo technologie neutraal mogelijk geformuleerd.

Bij het definiëren van de richtlijnen wordt uitgegaan van de doelstellingen en opzet zoals deze in dit document zijn vastgesteld. De richtlijnen dienen, indien van toepassing, door de verantwoordelijken te worden vertaald naar operationele maatregelen[2].

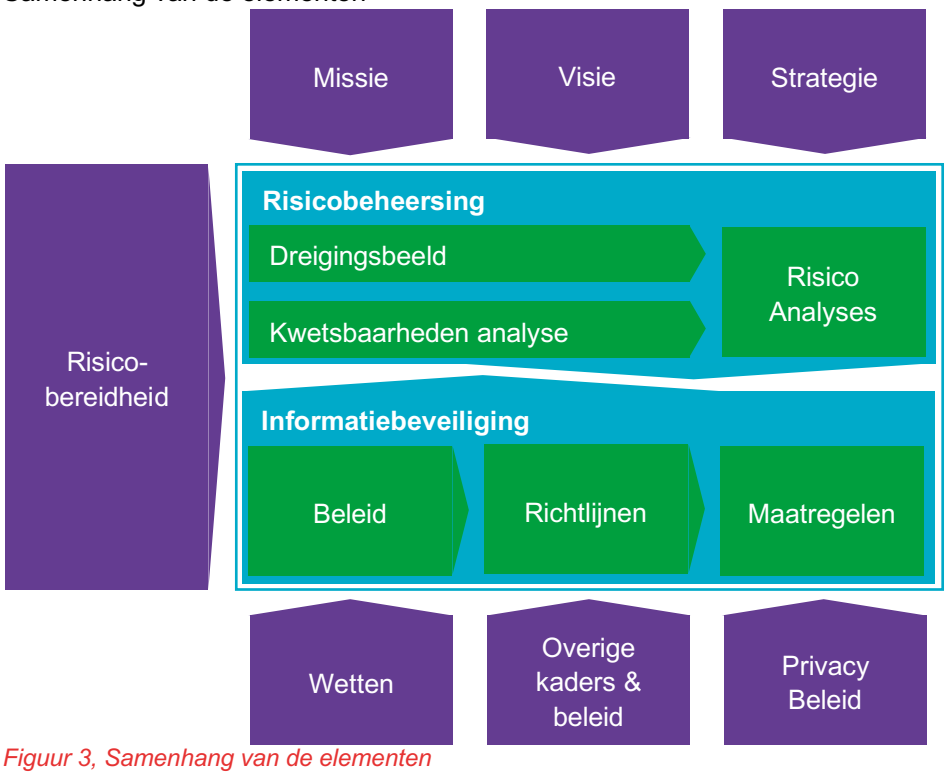
2.7.3 Operationeel – Maatregelen

Hoe de richtlijnen vertalen naar operationele maatregelen ligt soms voor de hand, maar soms ook niet. Het is de taak van de verantwoordelijken voor de assets[3] om deze te vertalen naar operationele maatregelen, dan wel aan te geven dat een richtlijn bewust niet wordt geïmplementeerd.

---

[1] Hierbij kan het bedrijf een eigen opzet gebruiken of de Conclusion brede aanpak kopiëren.
[2] De richtlijnen die opgesteld zijn voor Conclusion Services kunnen als template dienen voor de bedrijven die dat willen.
[3] In deze context kan een asset zowel een proces, system, applicatie als een dataset zijn. De verantwoordelijke voor de asset wordt normaliter beschouwd als de eigenaar van de asset.

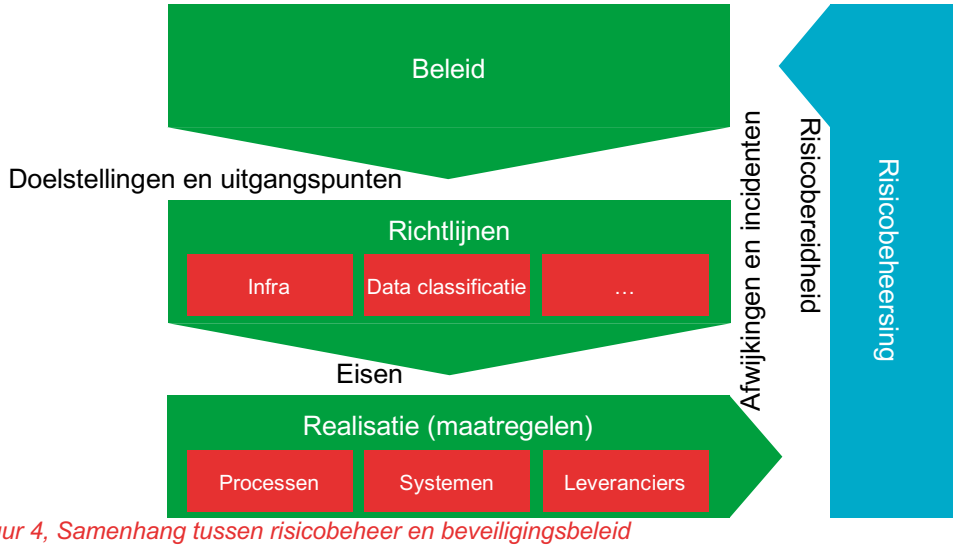
2.7.4 Samenhang van de elementen



Figuur 3, Samenhang van de elementen

De basis voor zowel de (informatie) risicobeheersing en informatiebeveiliging is de risicobereidheid van Conclusion. Deze wordt vertaald naar beleid en middelen voor risicobeheersing en informatiebeveiliging met behulp van de missie, visie en strategie, waarbij wetten, privacy en ander beleid worden gebruikt als kaderstellend. Risicobeheersing en Informatiebeveiliging hebben een wisselwerking met elkaar. Beveiliging op basis van de risico's en risico's op basis van de beveiliging.

Hierbij ontstaan beleidsstukken, richtlijnen en maatregelen, die wanneer deze gevolgd worden, automatisch garanderen dat de acties binnen de strategie en wetgeving vallen.



Figuur 4, Samenhang tussen risicobeheer en beveiligingsbeleid

Risicobeheer vindt altijd plaats op basis van twee elementen:

1. Het dreigingsbeeld dat bestaat uit factoren die Conclusion niet zelf onder controle heeft;
2. De kwetsbaarhedenanalyse, waarbij de kwetsbaarheden eigenschappen zijn van de processen, systemen en leveranciers van Conclusion. De basis van de kwetsbaarhedenanalyse wordt gevormd door de richtlijnen waaraan niet voldaan is, aangevuld met overige kwetsbaarheden. Deze overige kwetsbaarheden kunnen bijvoorbeeld geïdentificeerd worden aan de hand van incidenten en meldingen.

Door in een risicoanalyse het dreigingsbeeld met de kwetsbaarhedenanalyse te combineren ontstaan risicoscenario's die een impact hebben op de doelstellingen van de bedrijfsprocessen van Conclusion.

Op regelmatige basis wordt daarna bekeken of op basis van de risico scenario's en/of veranderde kaders informatiebeveiliging moet worden bijgesteld om zo beter de missie, visie en strategie van Conclusion te ondersteunen.

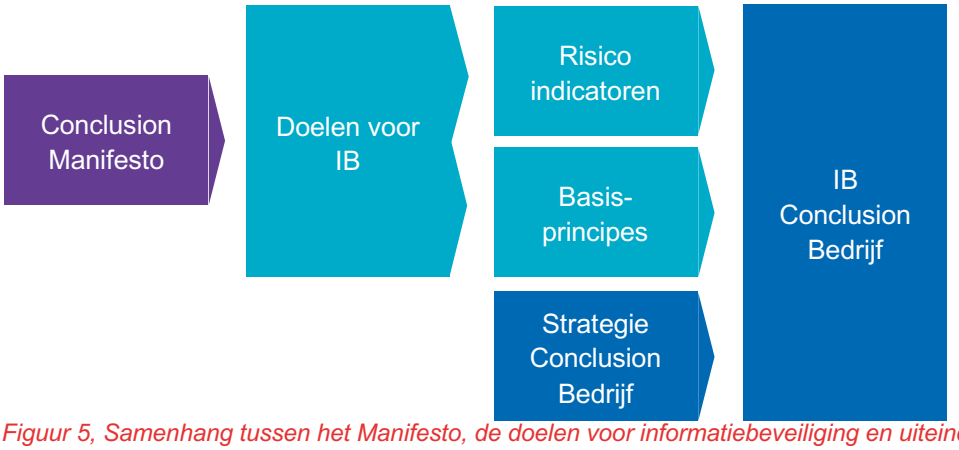
3. De doelen van informatiebeveiliging

3.1 Opzet

De doelen voor informatiebeveiliging (IB) zijn gedefinieerd aan de hand van het Manifesto van Conclusion. Dit Manifesto omvat negen kernbegrippen die een beschrijving zijn van het hart zijn van Conclusion. Op basis van dit Manifesto zijn een achttal doelen voor informatiebeveiliging gedefinieerd in drie kerngebieden. “Wie we zijn”, “Wat we voor onze klant doen” en “Wat we voor elkaar doen”.

Van de bedrijven wordt verwacht dat ze een bijdrage leveren aan het bereiken van deze doelen.

Voor ieder van deze acht doelen zijn vervolgens risico indicatoren en de basisprincipes van het Conclusion ecosysteem gedefinieerd.



Figuur 5, Samenhang tussen het Manifesto, de doelen voor informatiebeveiliging en uiteindelijk de informatiebeveiliging van de Conclusion bedrijven.

De risico indicatoren geven aan de ene kant aan in hoeverre Conclusion als ecosysteem de doelen waarmaakt en aan de andere kant kunnen de risico indicatoren gebruikt worden om uitdrukking te geven aan de risicobereidheid, door voor iedere indicator een minimum en maximum te definiëren en een doelwaarde.

Het Conclusion Manifesto kan gevonden worden op “Start Your Day” (https://conclusionfutureit.sharepoint.com/:b:/r/sites/StartYourDay/Gedeelde%20documenten/CONCLUSION%20%E2%80%93%20manifesto%20online.pdf?csf=1&web=1&e=DdaMg6)

3.2 De doelen voor Informatiebeveiliging

#	Doel	Toelichting	*Manifesto*
Wie we zijn			
DI1	Bedrijven nemen hun **EIGEN RISICO'S**	Ieder bedrijf neem en heeft controle over zijn eigen risico's. Hierbij wordt wel de risicobereidheid van Conclusion als geheel in acht genomen. Geen enkel bedrijf vormt een onacceptabel risico voor de groep.	*Authenticiteit, Samenwerken, Hoe we met elkaar omgaan*
DI2	we **VERTROUWEN** elkaar	Conclusion bedrijven moeten elkaar kunnen vertrouwen. Dat vertrouwen wordt gerechtvaardigd doordat we van elkaar weten welke risico's we nemen en hoe we deze onder controle houden. Dit vertrouwen kan nooit opgelegd worden.	*Ecosysteem, Samenwerken, Hoe we met elkaar omgaan*
DI3	tonen van onze **LEF** faciliteren	Maatregelen voor het borgen van de privacy en het beperken van de risico's dragen bij aan het creëren van omstandigheden waarin we onze lef kunnen tonen, zonder dat dit onacceptabele gevolgen heeft.	*Authenticiteit, Autoriteit blijven, Vakmanschap*
Wat we voor onze klant doen			
DK1	**BESCHERMD** zijn	Klanten, medewerkers en andere betrokkenen zijn beschermd wanneer zij zakendoen of interactie hebben met Conclusion. We zijn transparant in hoe we deze bescherming bieden.	*Hoe we met klanten omgaan, Wat we voor klanten doen, Hoe we met elkaar omgaan*
DK2	een **VOORBEELD** voor onze klanten	De manier waarop we het risicobeheersing, privacy en informatiebeveiligingsraamwerk vormgeven en gebruiken is een voorbeeld voor (potentiële) klanten. Onze maatregelen passen bij wat we doen en hoeveel risico we daarbij willen nemen.	*Autoriteit blijven, Wat we voor klanten doen, Vakmanschap*
DK3	we zijn **PROACTIEF**	We wachten de problemen niet af, we zoeken actief naar kansen en zijn altijd voorbereid op wat komen gaat.	*Wat we voor klanten doen, Autoriteit blijven*
Wat we voor elkaar doen			
DE1	onze organisatie is **WEERBAAR**	Conclusion is een weerbare organisatie. Dat houdt in dat onze inrichting "tegen een stootje" kan en dat als het mis gaat we onszelf kunnen herpakken met minimale impact op de betrokkenen en stakeholders.	*Autoriteit blijven, Hoe we met klanten omgaan, Vakmanschap*
DE2	we doen dingen **VOOR ELKAAR**	We helpen elkaar bij het onder controle brengen van onze risico's. Hierbij maken we de goede ideeën en dienstverlening voor privacy en informatieveiligheid van het ene bedrijf beschikbaar voor het andere.	*Hoe we met elkaar omgaan, Vakmanschap, Bedrijfsvoering*
DE3	we **ONTZORGEN** het ecosysteem	Dienstverlening en standaarden rondom de beheersing van risico's, privacy en informatieveiligheid worden centraal opgepakt om de individuele bedrijven te ontzorgen en om te voorkomen dat er kwetsbare naden ontstaat in de verdediging van Conclusion.	*Vakmanschap, Bedrijfsvoering*

3.3 Basisprincipes voor informatiebeveiliging

#	Principe
	Eigen risico's
ER1	Ieder bedrijf doet minimaal jaarlijks een risicoanalyse, met als minimale scope de verwerking van informatie en privacy. Hierbij worden dreigingen en kwetsbaarheden expliciet geadresseerd en wordt gebruik gemaakt van onder andere de centrale dreigingsmatrix en centrale richtlijnen.
ER2	Ieder bedrijf stelt de risicoanalyses beschikbaar aan alle directies van de Conclusion bedrijven. *Dit verbetert het overzicht over de risico's en plaatst de risicobereidheid van de individuele bedrijven in perspectief.*
ER3	Ieder bedrijf heeft een expliciet control framework/stelsel van maatregelen en neemt de afwijkingen hierop mee als kwetsbaarheid in de risicoanalyses. *Dit stelsel van maatregelen kan een eigen stelsel zijn, maar het bedrijf kan ook het centraal beschikbare Conclusion stelsel gebruiken dat ook gebruikt wordt voor de centrale dienstverlening, of een aanpassing daarvan.*
ER4	Ieder bedrijf rapporteert minimaal eens per kwartaal over privacy & security. *Als een bedrijf al beschikt over een interne rapportage, dan kan die voor dit doel hergebruikt worden. Bij weinig bijzonderheden kan de rapportage ook mondeling plaatsvinden.*
	Vertrouwen
Ve1	Risico rapportages, dreigingen en kwetsbaarheden worden onderling uitgewisseld tussen de bedrijven van de Conclusion groep.
Ve2	Ieder bedrijf doet minimaal eens per drie jaar een interne audit op alle bedrijfsprocessen en eens per anderhalf jaar voor bedrijven met zorgklanten. *Deze frequentie is afgestemd op de ISO27001 en NEN7510 eisen. De best practise is om een regulier auditschema op te stellen, waarbij iedere paar maanden een deel/proces van de organisatie wordt geaudit.*
Ve3	Audit rapporten worden gedeeld tussen de directies van de bedrijven van de Conclusion groep.
	Lef
Le1	Hoge (privacy) risico's worden altijd gemitigeerd om zo ruimte te houden om nieuwe risico's te nemen.
	***Beschermd** (nooit, alle principes dragen bij aan "beschermd")*
Be1	We voldoen aan wet en regelgeving tenzij… (pas toe of leg uit)
Be2	Alle bedrijven hebben hun bedrijfsvoering dusdanig op orde dat ISO27001 of NEN7510 certificering zonder veel inspanning behaald moet kunnen worden.
	Voorbeeld
Vo1	Ieder bedrijf heeft zijn processen inzichtelijk vastgelegd, inclusief, procesdoelen, kaders en RASCI. *Er zal documentatie beschikbaar gesteld worden om te helpen dit op een efficiënte manier te doen en ervoor te zorgen dat het resultaat bijdraagt aan het overzicht dat de medewerkers hebben over de organisatie en het inzicht in de risico's binnen het proces.*
Vo2	Ieder bedrijf heeft een expliciet verbeterproces

#	Principe
	Ieder bedrijf is bereid haar informatiebeveiligingsbeleid te delen met de andere Conclusion bedrijven, klanten en leveranciers.
Vo3	*Zo geven we onze klanten het vertrouwen en kunnen we makkelijk communiceren met elkaar, klanten en leveranciers over de maatregelen die we met elkaar moeten nemen. Noot: het advies is wel om de manier waarop maatregelen geïmplementeerd zijn te beschouwen als vertrouwelijk.*
Proactief	
Pr1	We gaan het gesprek aan met onze klanten over welke dreigingen zij zien *Bedreigingen voor onze klanten zijn ook bedreigingen voor onze eigen bedrijfsvoering. Daarom gaan we op regelmatige basis het gesprek aan om zo dreigingsinformatie uit te wisselen. We herijken onze eigen risico's op basis van de opgedane kennis.*
Pr2	We houden continue het overzicht over onze kwetsbaarheden en lossen deze waar mogelijk zo snel mogelijk op *Kwetsbaarheden worden minimaal eens per jaar beoordeeld in de risicoanalyses, er wordt continue gemonitord op het ontstaan van nieuwe kwetsbaarheden, op technisch en organisatorisch niveau. Waar mogelijk nemen we nieuw ontstane kwetsbaarheden zo snel mogelijk mee. We moedigen medewerkers aan kwetsbaarheden zie zij zien te melden binnen hun eigen organisatie.*
***Weerbaar** (noot, alle principes dragen bij aan "weerbaar")*	
We1	Alleen expliciet en context afhankelijk vertrouwen. *De keuze om een entiteit te vertrouwen is altijd een expliciete keuze. Deze keuze is onderbouwd met argumenten van commerciële en/of bedrijfskundige aard. We proberen het impliciet overerven van vertrouwen (b.v. niet standaard de leverancier van een leverancier vertrouwen) zo veel mogelijk te voorkomen. Vertrouwen is voorts altijd binair. Wanneer we een entiteit vertrouwen, is er naast de reden van het vertrouwen geen sprake van additionele maatregelen. We mogen er dan vanuit gaan dat alles reeds binnen deze entiteit geregeld is.*
We2	Privacy & Security is een verantwoordelijkheid van iedereen, zowel op groepsniveau als binnen de bedrijven.
We3	Ieder bedrijf heeft iemand die verantwoordelijk is voor het opstellen van en monitoren op de naleving van een privacy en securitybeleid. Deze rol heeft een directe rapportagelijn naar de directie van het bedrijf. De persoon in deze rol noemen we typisch Information Security Officer (ISO) of Privacy Officer (PO)
We4	Ieder bedrijf stelt een privacy & security jaarplan op.
We5	Alle privacy & security incidenten met grote impact of incidenten die meldingsplichtig zijn bij de autoriteit persoonsgegevens worden gemeld bij de CSO.
We6	Incidenten die de dienstverlening aan klanten in gevaar brengen of die gerelateerd zijn aan onderkende strategische risico's worden gemeld bij de CSO. *Hiervoor bestaat een overkoepelend security incident management proces binnen Conclusion. Dit proces sluit aan op de lokale processen van de bedrijven.*
We7	Alle medewerkers van een bedrijf zijn aantoonbaar vaardig voor de context waarin zij werken op het vlak van privacy & security.
Voor elkaar	
VE1	Ieder bedrijf werkt mee aan het Conclusion security officers gilde (CSOG). *Hier vallen o.a. de volgende werkgroepen onder:* 1. *Het voorzien in hulp voor interne audits* 2. *Het Centrale Cyber Security Incident and Response Team (CSIRT)*

#	Principe
Ontzorgen	
On1	Bij iedere centrale dienst die niet wordt afgenomen dienen de redenen geformuleerd te worden. *Ter ondersteuning van het verbeterproces voor de centrale dienstverlening.*
On2	Bij een Cybercalamiteit[4] dient ieder bedrijf de hulp in te roepen van het Conclusion CSIRT team *De focus van het CSIRT-team is om zo snel mogelijk de operatie te hervatten met respect voor forensisch bewijs dat gebruikt kan worden in de analyse van het incident en de eventuele vervolging van de overtreder.*

[4] Zie paragraaf 6.1.4 voor de definitie van en cybercalamiteit.

3.4 Risico indicatoren

#	Risico Indicator
Eigen Risico's	
PI1	Percentage (%) bedrijven met een recente (privacy) risico rapportage
PI2	% bedrijven met gedefinieerde Privacy & Security risico indicatoren
PI3	% bedrijven met een gedefinieerde risicobereidheid
Vertrouwen	
PI4	% bedrijven dat de risico rapportage deelt
PI5	% bedrijven met een recent intern of extern audit rapport
PI6	% bedrijven dat de audit rapporten deelt
Lef	
PI7	Aantal (#) gemiste deals of deals die we hebben laten lopen vanwege ons, risico, privacy, security of compliance landschap
PI8	# niet gemitigeerde hoge risico's en belangrijke audit findings (totaal in de groep)
Beschermd	
PI5	*% bedrijven met een recent intern of extern audit rapport*
PI8	*# niet gemitigeerde hoge risico's en belangrijke audit findings (totaal in de groep)*
PI9	% bedrijven met minimaal 1 certificering op het gebied van privacy of security
PI10	# datalekken in het afgelopen jaar
Voorbeeld	
PI10	*# datalekken in het afgelopen jaar*
PI11	% van de bedrijven dat gebruikt maakt van de beleidstemplates
PI12	# presentaties voor klanten over de opzet van het Conclusion raamwerk in het afgelopen jaar
Proactief	
PI12	# gesprekken over het dreigingslandschap met klanten
PI13	% bedrijven met eigen infrastructuur dat technische kwetsbaarhedenmonitoring heeft ingericht voor het hele productielandschap
PI14	% bedrijven met een expliciet verbeterproces; waar alle medewerkers verbeteringen kunnen aanmelden.
Weerbaar	
PI15	% bedrijven met een uitgeschreven en gedeeld proceslandschap
PI16	% bedrijven dat de risicoanalyse op bedrijfsprocesniveau doet
PI17	% medewerkers dat met succes heeft deelgenomen aan de awareness trainingen
PI18	# security incidenten waarbij de dienstverlening in gevaar kwam
Voor Elkaar	
PI15	*% bedrijven met een uitgeschreven en gedeeld proceslandschap*
PI19	% templates dat actueel is en aangepast aan wat de bedrijven willen

PI20	# interne audits die de bedrijven op elkaar hebben uitgevoerd
Ontzorgen	
PI19	*% templates dat actueel is en aangepast aan wat de bedrijven willen*
PI21	gemiddeld % bedrijven dat een security dienst gebruikt
PI22	# goed gedefinieerde securityservices

4. Aansturing

Eindverantwoordelijk voor de informatiebeveiliging van het ecosysteem is de algemeen directeur van Conclusion. De directies van de bedrijven, waaronder ook Conclusion Services zijn eindverantwoordelijk voor het beleid van hun eigen bedrijven. Tactische en operationele verantwoordelijkheden zijn gedelegeerd binnen de bedrijven. Aan het einde van dit hoofdstuk in paragraaf **Error! Reference source not found.** worden de rollen en verantwoordelijkheden samengevat in een matrix.

4.1 Besturing van Informatiebeveiliging

Er bestaat een aantal taken bij de besturing van informatiebeveiliging. Ten eerste de bepaling en formulering van het informatiebeveiligingsbeleid voor het ecosysteem en afgeleide richtlijnen voor besturing van de gemeenschappelijke dienstverlening. Dit is de eindverantwoordelijkheid van de algemeen directeur, waarbij de Chief Security Officer (CSO) verantwoordelijk is voor het opstellen van het beleid en de richtlijnen. Hierbij is de CSO verplicht dit zoveel mogelijk in afstemming met de bedrijven te doen.

De directeuren van de bedrijven zorgen voor de implementatie van beleid van het ecosysteem en de definitie en invulling van het beleid van de bedrijven onder hun hoede. Hierbij geholpen door de CSO en de eigen security officer(s) die zowel een adviserende als een controlerende rol invullen.

Eventuele strategische risico's dienen gemeld te worden bij de directie van Conclusion.

De functionaris gegevensbescherming draagt bij aan de besturing van informatiebeveiliging door het aanleveren van een privacy beleid dat richting geeft aan het informatiebeveiligingsbeleid.

4.2 Uitvoering van informatiebeveiliging

Iedere medewerker heeft een taak bij de uitvoering van informatiebeveiliging, met de directeuren en diegenen aan wie zij de taken rondom beveiliging delegeren.

De CSO heeft tot taak dat de directeuren van de bedrijven, de medewerkers en alle andere relevante stakeholders op de hoogte zijn van het beleid van het ecosysteem, de richtlijnen die gebruikt zijn voor het implementeren van de gedeelde dienstverlening en in hoeverre de gedeelde dienstverlening daaraan voldoet.

De directeuren moeten, met de hulp van hun security officers, ervoor zorgen dat de risico's binnen hun bedrijven de risicobereidheid niet overschrijden, het beleid van en uitvoering binnen het bedrijf compatible is met het groepsbeleid. Om dit aan te tonen wordt er op regelmatige basis gerapporteerd.

Voor wat betreft privacyvraagstukken zal de functionaris gegevensbescherming adviserend optreden.

4.3 Bescherming van Privacy & Security Officers

Privacy & Security officers moeten zonder gevaar voor de eigen positie in het bedrijf kunnen rapporteren wat zij waarnemen volgens de in dit document benoemde lijnen voor rapportage.

4.4 RASCI-matrix

(R) verantwoordelijk voor de invulling;
(A) eindverantwoordelijk en dus acceptant;
(S) mogelijk ondersteunend/meewerkend;
(C) wordt geraadpleegd (verplicht);
(I) wordt altijd geïnformeerd over de uitkomst

	Algemeen directeur	Directie Conclusion	CSO/Privacy Officer	Functionaris Gegevensb.	Directeur Bedrijf	ISO/PO bedrijf
Besturing centraal						
Informatiebeveiligingsbeleid Ecosysteem	A	I	R	C/S	I	C/I
Formulering richtlijnen	A	C/I	R	C/I	I	C/S
Implementatie van beleid	A	R	C/I	C/I	I	I
Rapportage aan directie	I	I	A/R	C/S	I	I
Risicobeheersingsproces	A	R[5]/I	C/I	C/I	I	I
Privacybeleid Conclusion breed	A	I	C/S	R	I	I
Inzet Computer Security Incident Reponse Team	A	I	R	I	I	C[6]
Aanwijzen coördinator CSIRT (per incident)	A/R	I	C/I	I	I	C/I[6]
Besturing binnen de bedrijven						
Informatiebeveiligingsbeleid	I	I	I	I	A	R
Formulering richtlijnen			S/I	S/I	A	R
Implementatie van beleid			S/I	S/I	A/R	C/I
Rapportage aan eigen directie			I	I	A	R/I[6]
Risicobeheersingsproces			I	I	A/R	C/I
Risico's centraal & binnen de bedrijven						
Acceptatie strategische informatie risico's	A	R	C/I		R[7]	C/I
Acceptatie tactische informatie risico's		I	I		A/R	C/I
Acceptatie operationele informatie risico's					A/R	C/I
Uitvoering centraal						
Security Architectuur Conclusion Services			A/R	C/I		C/I
Ontzorgende securitydiensten (zie ook 4.4.3)	S/I	S/I	A/R	C	C/I	C/I
Verwerkingsregister			I	A/R		
Verwerkingsovereenkomsten		A/R	C/I			I
Uitvoering lokaal						
Verwerkingsregister			I	I		A/R
Verwerkingsovereenkomsten			I	I	A/R	C/I
Melden van verstorende incidenten aan de CSO (zie ook 4.4.4)			C/I		A	R

[5] CFO
[6] Information Security Officers informeren elkaar over hun rapportages
[7] Van het betrokken bedrijf

Overig

4.4.1 Computer Security Incident Response Team (CSIRT)

Het Computer Security Incident Response Team (CSIRT) is een crisisorganisatie die bij de initiële inzet in ieder geval bestaat uit de CSO (coördinator), de bij het incident betrokken ISO's en afhankelijk van de situatie of het incident aangevuld met enkele experts.

Afhankelijk van de situatie kan de algemeen directeur na inzet van het CSIRT bepalen dat er van voorzitter gewisseld moet worden en/of de samenstelling veranderd moet worden, omdat dat meer recht doet aan de omstandigheden. Bij "uitruk" is de samenstelling als beschreven om snel te kunnen acteren.

De taak van het CSIRT is om na een cybercalamiteit dreigende ernstige impact op de primaire processen te ondervangen en/of de primaire processen zo snel mogelijk te herstellen. Het CSIRT kan tijdens de werkzaamheden tijdelijk de rol van "asset owner" overnemen binnen ieder willekeurig Conclusion bedrijf, om snel en slagvaardig te kunnen handelen.

Dit houdt in, dat zo lang de noodsituatie nog van kracht is het CSIRT bepaalt wat er gebeurt met de getroffen systemen, processen en diensten.

Na herstelwerkzaamheden als gevolg van een incident dat de primaire processen ernstig verstoord heeft:

- legt de coördinator van het CSIRT (normaal gesproken de CSO) verantwoording af over de genomen acties aan de betrokken directeuren.
- laat de CSO het CSIRT een root-cause analyse uitvoeren.

4.4.2 Interne Auditor

De rol van de interne auditor is om te controleren dat de staat en operatie van informatiebeveiliging op orde is en dat processen en maatregelen functioneren volgens beschrijving.

De auditor rapporteert periodiek en direct aan de directeur en ISO van het betreffende Conclusion bedrijf. Met betrekking tot deze rapportage geniet de auditor een beschermde positie. Zij/hij moet vrijelijk kunnen rapporteren, zonder dat hierbij de positie van de auditor in het bedrijf in gevaar komt.

De interne auditrol is typisch een bijrol van een medewerker. Hierbij geldt als randvoorwaarde dat een interne auditor nooit een audit mag uitvoeren binnen de eigen directie/stafafdeling.

Hierbij wordt aangemoedigd dat de Conclusion bedrijven elkaars interne audits uitvoeren om zo van elkaar te leren.

4.4.3 Ontzorgende securitydiensten

Het inrichten van een goed beveiligingslandschap is maatwerk. De bouwstenen waarmee het maatwerk is opgebouwd zijn vaak standaard. Daarom worden vanuit Conclusion Services een aantal standaard diensten aangeboden, die of aan alle bedrijven geleverd worden, of op aanvraag leverbaar zijn.

Voorbeelden hiervan zijn de maandelijkse Internet scan, de wachtwoordmanager en het de security monitoring op veelgebruikte leveranciers. Deze diensten worden beheerd

door de CSO. De CSO is verantwoordelijk om de behoeftes van de bedrijven continue in kaart te houden en ervoor te zorgen dat de centrale securitydienstverlening enerzijds aansluit op de behoeftes van de bedrijven en anderzijds tegemoetkomen aan de risicobereidheid van de groep.

4.4.4 Incident management

Incidenten die mogelijk een gevaar opleveren voor de continuïteit van de dienstverlening en/of de primaire processen moeten altijd zo snel mogelijk bij de CSO gemeld worden via security@conclusion.nl. De CSO kan dan bepalen of het incident ook gevaar oplevert voor de andere bedrijven binnen het ecosysteem, of dat inzet van het CSIRT noodzakelijk is.

Het incident kan pas afgesloten worden als de bronoorzaak inzichtelijk is en als eventuele noodzakelijke verbeteringen zijn ingepland.

Incidenten bij klanten; de afhandeling daarvan is onderdeel van de normale dienstverlening/bedrijfsprocessen. *Wanneer het incident mogelijk kan uitbreiden naar Conclusion, of wanneer het mogelijk tot reputatieschade voor Conclusion kan leiden, moet de CSO op de hoogte gebracht worden (security@conclusion.nl)*

Incidenten bij leveranciers; zie de afhandeling van incidenten bij klanten.

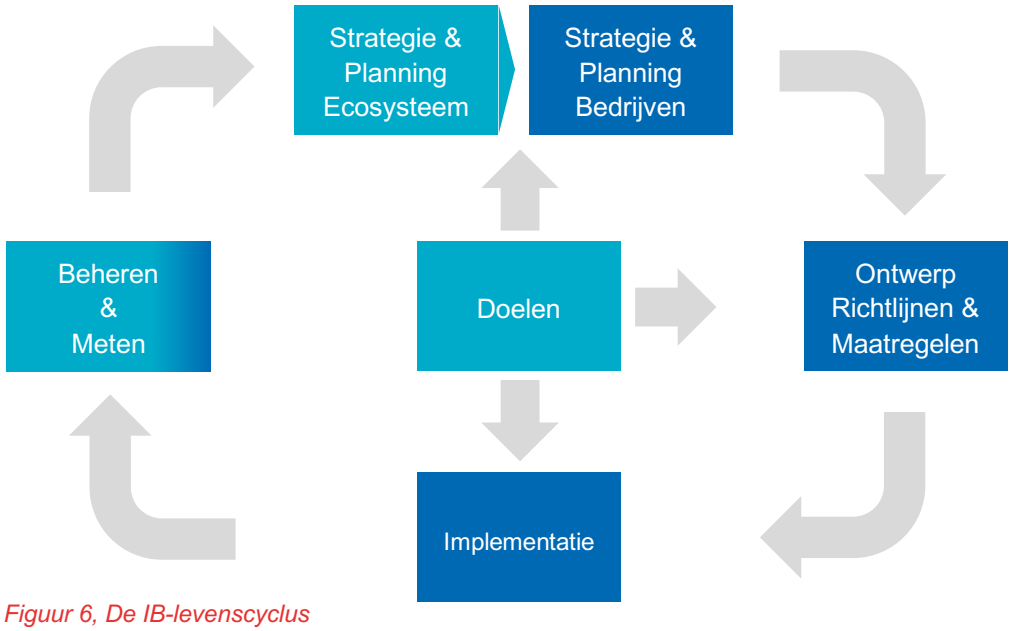
5. Proces voor informatiebeveiliging

5.1 De levenscyclus

Conclusion ziet informatiebeveiliging als een continu proces en nadrukkelijk niet als eenmalige activiteit.

Startpunt van het proces is het Manifesto en de daaraan gekoppelde informatiebeveiligingsdoelen, risico indicatoren en basisprincipes. Dit is de basis voor het cybersecurity hoofdstuk in de jaarlijkse risicoschatting en analyse. Het resultaat van deze analyse wordt meegenomen in:

- het bepalen/herijken van de juiste doelen en basisprincipes;
- het jaarlijkse beveiligingsplan met de te ondernemen beveiligingsactiviteiten;
- het bepalen/herijken van de richtlijnen voor de gemeenschappelijke dienstverlening.



Figuur 6, De IB-levenscyclus

5.2 Risicoanalyses

Jaarlijks wordt er op ecosysteem niveau een risico-inventarisatie en analyse gemaakt. Voor wat betreft het informatie/cyber deel wordt deze gevoed door de risicoanalyses van de individuele bedrijven. In deze risicoanalyses dient zowel de context van de bedrijven (security) meegenomen te worden als die van de betrokkene (privacy). Doordat de bedrijven relevante dreigingen en kwetsbaarheden onderling delen wordt ook de impact die de bedrijven op elkaar hebben zichtbaar.

De risicoanalyses dienen plaats te vinden op de bedrijfsprocessen, zodat een risico altijd gekoppeld is aan een bedrijfsdoel. Niet voldoen aan richtlijnen, maatregelen en (wettelijke) kaders dient expliciet meegenomen te worden als kwetsbaarheid.

De CSO kan (dwingend) adviseren een risicoanalyse op een eerder dan het reguliere tijdstip uit te voeren, als zij/hij denkt dat het risico de bereidheid overstijgt.

5.3 Rapportage

Minimaal eens per 4 maanden[8] zal de CSO een rapportage opstellen voor de directie van Conclusion. Deze rapportage wordt samengesteld aan de hand van de rapportages van de individuele bedrijven, status van de uitvoering van het jaarplan, plus eventuele observaties van de CSO.

In de rapportage worden de volgende onderwerpen toegelicht:

1. noemenswaardige incidenten binnen Conclusion en ander zaken;
2. staat van de uitvoering van het centrale beveiligingsplan;
3. waarden van de risico indicatoren;
4. belangrijkste risico's.

Deze rapportage is ter inzage beschikbaar voor de directeuren van de Conclusion bedrijven en de Information Security Officers.

5.4 Revisie intervallen

De CSO hanteert de volgende levenscyclus voor de volgende beleidsdocumenten:

- De set beleidsdocumenten wordt minimaal eens per 3 jaar herijkt;
- rapportage aan de directie over de uitvoer van het beveiligingsplan vindt eens per kwartaal plaats;
- rapportage aan de directie over de risico indicatoren vindt eens per kwartaal plaats;
- de tactische richtlijnen worden minimaal eens per jaar herijkt (t.b.v. de centrale dienstverlening);
- risicoanalyses op de processen t.b.v. de centrale dienstverlening dienen minimaal jaarlijks plaats te vinden en/of na grote veranderingen in het proces.

Hierbij worden alle documenten opgeleverd door de CSO, behalve de risicoanalyses die de verantwoordelijkheid zijn van de proceseigenaren.

5.5 Controle op de uitvoering van maatregelen

Heel Conclusion is verantwoordelijk voor de interne controle op de uitvoering van het beleid, de richtlijnen en de maatregelen. Deze controles zijn zoveel mogelijk onderdeel van de reguliere processen. Op onderdelen kan in overleg met dan wel op initiatief van de CSO bij alle bedrijven van Conclusion een zogenaamde verbijzonderde interne controle of externe controle worden uitgevoerd. De CSO ziet toe op de uitvoering hiervan.

De Conclusion bedrijven zijn zelf verantwoordelijk voor de controle van de werking van de maatregelen die door henzelf zijn ingesteld. De resultaten van controles dienen ook beschikbaar te worden gesteld aan de CSO van Conclusion.

5.6 Goedkeuring van documenten voor beleid en richtlijnen

Onder dit beleid hangt een set van richtlijnen. De richtlijnen zijn specifiek voor bepaalde doelen en kunnen regelmatig aangepast worden op basis van voortschrijdend inzicht. De richtlijnen zijn van toepassing op de centrale dienstverlening, dienen gebruikt te worden voor de identificatie van kwetsbaarheden in risicoanalyses en zijn zo opgesteld dat de Conclusion bedrijven, wanneer zij dit wensen, deze documentatie als template kunnen gebruiken voor hun interne beveiliging.

[8] De rapportagemaanden zijn typisch: februari, juni en oktober. In bijzondere omstandigheden zal er vaker gerapporteerd worden.

Voor de vaststelling van het beleid voor het ecosysteem krijgen alle security officers en bedrijfsdirecteuren de kans om het document te reviewen, waarna de vaststelling gebeurt door de algemeen directeur van Conclusion.

De richtlijnen documenten worden goedgekeurd door de CSO, met als voorwaarde dat de documenten door ten minste vier andere security officers van de Conclusion bedrijven gereviewed zijn en dat het commentaar naar tevredenheid is verwerkt. Voortschrijdend inzicht wordt zo snel mogelijk in de richtlijnen documenten verwerkt.

Kleine veranderingen aan de documenten vallen onder de verantwoordelijkheid van de CSO van Conclusion.

Alle beleid en richtlijnen documentatie worden geclassificeerd als publieke informatie en mogen in pdf-vorm gedistribueerd worden aan belanghebbenden.

6. Appendices

6.1 Definities

6.1.1 Beschikbaarheid (continuïteit, responstijd).
De mate waarin informatiesystemen en de informatie binnen de organisatie in bedrijf zijn op het moment dat een gebruiker informatie nodig heeft.

6.1.2 Integriteit (juistheid, volledigheid, tijdigheid, geoorloofdheid).
De mate waarin de informatie binnen de informatiesystemen volledig en juist is. Hierbij geldt ook dat onder volledigheid dient te worden verstaan dat niet méér dan de benodigde informatie in het systeem is opgenomen.

6.1.3 Vertrouwelijkheid (exclusiviteit).
De mate waarin de toegang tot en de kennisname van de informatie beperkt is tot een gedefinieerde groep van gebruikers, die allen schriftelijk hebben verklaard op een juiste en zorgvuldige wijze om te zullen gaan met de informatiesystemen en de daarin opgenomen informatie.

6.1.4 Cybercalamiteit
Gebeurtenis waarbij een externe actor erin slaagt een deel van de Conclusion infrastructuur onder controle te krijgen. Dit is bijvoorbeeld het geval van Malware, zoals een cryptolocker.

6.1.5 Cybersecurity
Dat deel van informatiebeveiliging dat gaat over de bescherming van informatie die via digitale weg ontsloten is. Cybersecurity is daarmee een deelgebied van informatiebeveiliging.

6.1.6 Security incident
Ieder incident dat de continuïteit van de dienstverlening of de organisatie in gevaar brengt. Daaronder vallen niet alleen incidenten met betrekking tot de betrouwbaarheid en de juistheid (integriteit) van informatie maar ook de beschikbaarheid.

6.1.7 Weerbaarheid
Het uiteindelijke doel van dit beleid, de informatierisico's die gekoppeld zijn aan de processen van Conclusion binnen acceptabele grenzen te houden, is sterk afhankelijk van de herkenning van risico's.

Feit is dat nooit alle risico's onderkend worden. Daarom is het belangrijk in de maatregelen de focus te leggen op digitale weerbaarheid. Digitale weerbaarheid is het vermogen van de organisatie om te reageren op onvoorziene gebeurtenissen.

Weerbaarheid			
	Mens	Proces	Techniek
Preventie			
Beperken Impact			
Weet wat er gebeurt			
Vermogen om snel te reageren			

Om dat te bereiken zijn maatregelen nodig op het vlak van mens, proces en techniek en dienen deze maatregelen niet alleen gefocust te zijn om preventie, maar ook op het beperken van de impact wanneer het mis gaat, verspreiden van informatie, zodat duidelijk is wat de verwachtingen zijn en zodat uitzonderingen gedetecteerd kunnen worden en om snel te kunnen reageren op gebeurtenissen.

6.2 Uitwerking van het concept vertrouwen

In basisprincipe We1 wordt gesteld “Alleen expliciet en context afhankelijk vertrouwen”. Deze paragraaf zet een aantal kenmerken van vertrouwen in de informatiebeveiligingscontext uiteen.
Deze kenmerken zijn bepalend bij de discussie over en de toepassing van het concept vertrouwen in de onderliggende richtlijnen en het modelleren van vertrouwen in architectuur.

6.2.1 Vertrouwen is binair

Vertrouwen is een binair concept. Iets is wel of iets is niet vertrouwd. Standaard wordt er niets vertrouwd. Alleen na evaluatie, bijvoorbeeld van geïmplementeerde maatregelen, kan besloten worden om iets te vertrouwen. Dit vertrouwen dient periodiek opnieuw geëvalueerd te worden.

Het treffen van maatregelen betekent niet automatisch dat iets vertrouwd kan worden. Een grenscontrole maakt nog niet dat iedereen binnen de grenzen van het land vertrouwd wordt. De status is in dat geval “niet vertrouwd, maar wel gecontroleerd”.

Als informatie vanuit een vertrouwde naar een niet vertrouwde context wordt getransporteerd, of tussen niet vertrouwde contexten, moet er altijd sprake zijn van een controle/maatregel op het moment van overgang.

6.2.2 Vertrouwen is context-afhankelijk

Het concept vertrouwen kan onder andere toegepast worden in de volgende contexten:

Personen
Binnen Conclusion worden personen vertrouwd voor de rol in de bedrijfsprocessen waarvoor zij zijn ingezet. Een persoon kan in deze een medewerker of externe zijn. De betreffende medewerker of externe wordt niet vertrouwd met data uit bedrijfsprocessen waarin zij/hij geen rol heeft. Dit principe geeft op het gebied van medewerkers dus aanleiding tot een “least privilege” beleid.

Organisaties
Externe organisaties zijn nooit vertrouwd, tenzij er een overeenkomst is plus daarbij horende maatregelen die het vertrouwen mogelijk maken. In die overeenkomst moet duidelijk worden dat de belangen van de partijen voldoende overlappen en er moeten maatregelen ingericht zijn om te kunnen controleren of het vertrouwen gerechtvaardigd is (b.v. audits).

Een verwerkersovereenkomst is een voorbeeld van zo’n overeenkomst, waarbij een organisatie vertrouwd wordt voor een bepaalde dataset. Dat betekent dan ook dat de basis van dit vertrouwen gecontroleerd moet worden.

Infrastructuur
Infrastructuur kan vertrouwd worden, wanneer:

- Er maatregelen geïmplementeerd zijn om dat vertrouwen af te dwingen;

- er in die infrastructuur alleen door Conclusion beheerde componenten te vinden zijn, waardoor Conclusion voor 100% in controle is over deze infrastructuur.

Wanneer er niet wordt voldaan aan deze twee regels, kan er toch voor gekozen worden om een infrastructuur te vertrouwen, bijvoorbeeld wanneer deze beheerd wordt door een vertrouwde partij en er afspraken zijn gemaakt over het beheer van deze infrastructuur

Databronnen
Data in een vertrouwde databron wordt voor waar aangenomen. De inhoud van vertrouwde databronnen wordt gereguleerd middels vastgelegde en meetbare processen.

Zijn deze voorwaarden afwezig dan:
- Kan het zijn dat de data uit deze bron via een andere weg geverifieerd moet worden, voordat deze in de bedrijfsprocessen van de Conclusion gebruikt kan worden;
- mag data uit een vertrouwde databron mogelijk niet naar deze databron geëxporteerd worden. Dit is afhankelijk van de vertrouwelijkheid en integriteitseisen van de informatie in de vertrouwde databron.

Overerfbaarheid
Vertrouwen is van nature overerfbaar. Bijvoorbeeld: als Conclusion ervoor kiest een leverancier te vertrouwen, dan worden ook de leveranciers van de leverancier in deze context vertrouwd.

Conclusion gaat expliciet en context-afhankelijk om met vertrouwen. Conclusion staat alleen een directe connectie tussen twee entiteiten toe wanneer zij dezelfde vertrouwensstatus hebben. Zo wordt de overerving zo veel mogelijk vermeden.

Conclusion past compartimentering toe op het gebied van infrastructuur, applicatie, data en fysieke landschap om hier invulling aan te geven.

Voorbeeld: Een medewerker mag een niet vertrouwde Bring Your Own laptop niet verbinden met een vertrouwd netwerk. De laptop zou anders de vertrouwde status overerven. Daarom is er een apart netwerk compartiment dat niet vertrouwd wordt maar waar wel additionele maatregelen worden genomen om het werken tegen acceptabele risico's mogelijk te maken.

6.2.3 Gevolgen van het concept "Vertrouwen"

Het juist toepassen van het concept vertrouwen leidt tot lichtere, meer werkbare en dus goedkopere maatregelen in ruil voor afgenomen controle.

Het concept vertrouwen heeft de volgende gevolgen:
- In alle architecturen en informatiestromen dient aangegeven te worden in welke vertrouwenscontext de be- of verwerking wordt gedaan;
- in alle inkooptrajecten dient de gewenste en uiteindelijke vertrouwensstatus van de leverancier aangegeven te worden.

Onderling vertrouwen betekent dat na het vaststellen dat een entiteit vertrouwd is (identificatie) geen additionele maatregelen nodig zijn buiten de maatregelen die toch al gelden in die context.

Voorbeeld; een medewerker identificeert zichzelf bij de voordeur. Daar wordt vastgesteld dat de medewerker een vertrouwde entiteit is. De medewerker mag zich daarna vrij bewegen in het pand binnen de context van de algemeen toegankelijke ruimtes. Voor een bezoeker worden wel additionele maatregelen getroffen in deze context (bijvoorbeeld dat de bezoeker begeleid moet worden).

Samenvatting van de genoemde gevolgen van dit principe:

- Least privilege;
- compartimentering;
- zonder overeenkomst en maatregelen met een andere partij geen vertrouwen;
- randvoorwaarden aan de uitwisseling van data;
- vertrouwen moet expliciet gemaakt worden.

6.3 Risico classificatie

Dit beleid schrijft een risico gebaseerde aanpak voor. Het nemen van risico's stelt Conclusion beter in staat om op relatief korte termijn tegen acceptabele kosten diensten te realiseren.

Om te borgen dat de risicobereidheid niet ongecontroleerd wordt overschreden dienen risico's geclassificeerd te worden, zodat duidelijk is wie mag beslissen over het nemen van een risico.

Binnen Conclusion wordt gesproken van:

- Strategische risico's als de impact van deze risico's:
    - de lange termijn planning, identiteit van Conclusion en strategische doelen in gevaar brengen;
    - de continuïteit van Conclusion als geheel in gevaar brengen;
    - kritische diensten voor langere tijd niet beschikbaar zijn.
- Tactische of projectrisico's als:
    - de impact van de risico's van nadelige invloed is op de (kritische) dienstverlening van Conclusion, waarbij er op de korte termijn geen alternatieven zijn.
    - wanneer het de uitvoer van een project of een enkele klant betreft Impact blijft beperkt binnen een Conclusion bedrijf.
- Operationele risico's, wanneer de impact op de dienstverlening beperkt is.

De beslissing tot het nemen van strategisch risico's is altijd een zaak van de directie van Conclusion. Directeuren van Conclusion bedrijven zijn vrij om tactische en operationele risico's te nemen. Binnen de context van het Conclusion bedrijf kan een andere risicoclassificatieschaal gebruikt worden. Een Conclusion breed tactisch risico is bijvoorbeeld in de context van een enkel Conclusion bedrijf mogelijk strategisch.

6.4 Implementatie en inrichting van security binnen de Conclusion bedrijven

Conclusion bestaat uit een grote verzameling van bedrijven met verschillende groottes en risicoblootstellingen. Sommige bedrijven, met een hoge risicoblootstelling, hebben de bedrijfsprocessen goed in kaart, een uitgebreid stelsel van maatregelen in gebruik en één of meer security officers.

Andere bedrijven vertrouwen voor een heel groot deel van de informatievoorziening en bedrijfsprocessen op de Conclusion Services organisatie en hebben maar één of twee eigen bedrijfsprocessen, zoals bijvoorbeeld sales en recruitment.

Het grootste deel van de bedrijven valt ergens tussen deze twee uitersten.

Om deze bedrijven te helpen de informatierisico's onder controle te houden zijn er twee diensten:

1. **Security as a Service (SecaaS)**: Deze dienst is beschikbaar voor de bedrijven die maar één of twee eigen processen hebben en voor het overige deel gebruik maken van de diensten van Conclusion Services. Deze bedrijven kunnen aanhaken op de beveiliging van Conclusion Services. Het enige dat zij zelf moeten doen is het in kaart brengen van de eigen processen, daar een risicoanalyse op doen en de resulterende maatregelen implementeren, voor zover deze geen onderdeel zijn van de dienstverlening van Conclusion Services.

   Voor de invulling wordt gebruik gemaakt van het raamwerk van maatregelen en methodes van Conclusion Services. Deze hoeven dus niet door de afnemende bedrijven zelf opgesteld te worden.

   Let wel: *de uiteindelijke eindverantwoordelijkheid (accountability) voor de informatieveiligheid van het bedrijf wordt niet overgedragen aan Conclusion Services. De leiding van deze bedrijven moet dus wel blijven sturen op de resultaten die door Conclusion Services opgeleverd moeten worden.*

2. **Security Officer as a Service (SOaaS)**: Deze dienst is beschikbaar voor de bedrijven die geen noodzaak hebben voor een full-time security officer. Onder deze dienst krijgt het afnemende bedrijf de beschikking over een security officer voor een afgesproken aantal uren per week. Hierbij wordt de inzet verdeeld over diverse personen, zodat er altijd iemand met de juiste kennis en ervaring beschikbaar is.

   Onder "Security Officer as a Service" wordt er gewerkt met een standard methode die geschikt is voor ISO27001 en NEN7510 certificering.

   De verantwoordelijkheid voor het doen van risicoanalyses blijft bij de proceseigenaren binnen het bedrijf. Ook het implementeren van maatregelen blijft een verantwoordelijkheid van het bedrijf zelf. Hierbij mag wel verwacht worden dat de security officer de verantwoordelijken voorziet van de juiste informatie en coaching.

Zie de aangepaste RASCI-tabel op de volgende pagina voor de verdeling van verantwoordelijkheden bij afname van SecaaS of SOaaS.

	Directeur Bedrijf	Proces-eigenaar	ISO Services (SecaaS)	SOaaS
Informatiebeveiligingsbeleid	A	I	R	R
Formulering richtlijnen	A	I	R	R
Implementatie van beleid (SOaaS)	A	R		C/I
Implementatie van beleid (SecaaS)	A		R	
eigen (niet met services gedeelde) processen	A	R	C/I	
Rapportage aan eigen directie	A	C/I	R	R
Risicobeheersingsproces	A/R	I	R	R
Maken van risicoanalyses (SOaaS)	A	R		C/S
Maken van risicoanalyses (SecaaS)	A		R	
in eigen processen	A	R	C/S	
Risico's centraal & binnen de bedrijven				
Acceptatie strategische informatie risico's	R	C/I	C/I	C/I
Acceptatie tactische informatie risico's	A/R	C/I	C/I	C/I
Acceptatie operationele informatie risico's (SOaaS)	A	R		C/I
Acceptatie operationele informatie risico's (SecaaS)	A		R	
in eigen processen	A	R	C/I	
Uitvoering lokaal				
Verwerkingsregister			A/R	A/R
Verwerkingsovereenkomsten (SOaaS)	A	R		C/I
Verwerkingsovereenkomsten (SecaaS)	A		R	
in eigen processen/eigen contracten	A	R	C/I	
Melden van verstorende incidenten aan de CSO (zie ook 4.4.4)	A		R	R

CONCLUSION

CONTACT
Roel Gloudemans
Chief Security Officer
roel.gloudemans@conclusion.nl
+31-6-13372217