FORTEZZA
MANAGED SECURITY

RISICO ONDERZOEK

RISICO-ONDERZOEK VAN FORTEZZA

Wij helpen u met het afdekken van uw risico's door aangepaste risico-onderzoeken. Dit baseren we op diepgaande kennis van organisaties, bedrijfsprocessen en technologie

WWW.FORTEZZA-MSSP.NL

INHOUD

BANGMAKERIJ HELPT NIET

EEN RISICO-ONDERZOEK EN ADVIES WEL

RISICO-ONDERZOEK IS NIET HET AFWERKEN VAN EEN VRAGENLIJST

COMBINATIE VAN BEDRIJFSKENNIS EN TECHNOLOGISCHE KENNIS

KETENSAMENWERKING EN ZWAKSTE SCHAKEL

RISICOGEBASEERDE BEVEILIGING

HET IDEE ACHTER ONS GELAAGDE AANPAK

DE WERKING VAN EEN RISICOGEBASEERDE BEVEILIGING

KEUZEMODEL RISICO-ONDERZOEK

BANGMAKERIJ HELPT **NIET**

De berichtenstroom over cyberaanvallen neemt toe en vaak zou het voortbestaan van organisaties in gedrang komen. Is dit re□el of slechts ongenuanceerde bangmakerij?

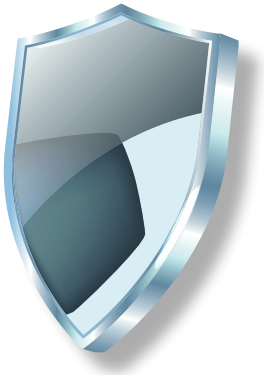
Natuurlijk vinden er geslaagde digitale inbraken plaats maar bij Fortezza vinden we dat het helaas te vaak om bangmakerij gaat. Dit werkt averechts omdat u op de lange duur ongevoelig raakt voor dit soort waarschuwingen.

RISICO-ONDERZOEK EN ADVIES WEL

Een risico-onderzoek rond de informatiebeveiliging helpt bij het afdekken van de risico's.

Een organisatie bepaalt zelf, uitgaande van haar financiële draagkracht, in hoeverre zij het advies wil overnemen en welke risico's zij gaat afdekken. Daarmee bepaalt zij dus hoeveel tijd en geld er geïnvesteerd wordt in de beheersmaatregelen.

Echter, een risico-onderzoek vraagt om diepgaande kennis en ervaring om tot een goed oordeel te komen. Externe adviseurs zien hier mogelijkheden om, veelal aan de hand van een standaard vragenlijst, de risico's voor een organisatie in beeld te brengen. Verder bieden ze daarbovenop adviezen met beheersmaatregelen om deze vervolgens ook te kunnen invoeren.



Risico-onderzoek is niet het afwerken van een vragenlijst

Alhoewel het onderzoeken van risico's prima helpt in de oordeelsvorming bij het onderzoeken en beheersen van risico's, is het zeker geen vragenlijst die men af kan lopen. Diepgaande kennis van een organisatie, zoals primaire bedrijfsprocessen in relatie tot technologie, is noodzakelijk. En dit is nauwelijks te verwerken in een vragenlijst.

Combinatie van bedrijfskennis en technologische kennis

Consultants kennen de wet- en regelgeving en toetsen dit aan de hand van standaarden met beveiligingsrichtlijnen en zijn goed op de hoogte van de bedrijfsprocessen. Maar, al te vaak, ontbreekt het hen aan technologische kennis en ervaring. Dit is noodzakelijk omdat technologie een dominante rol speelt in de ondersteuning van de bedrijfsprocessen.

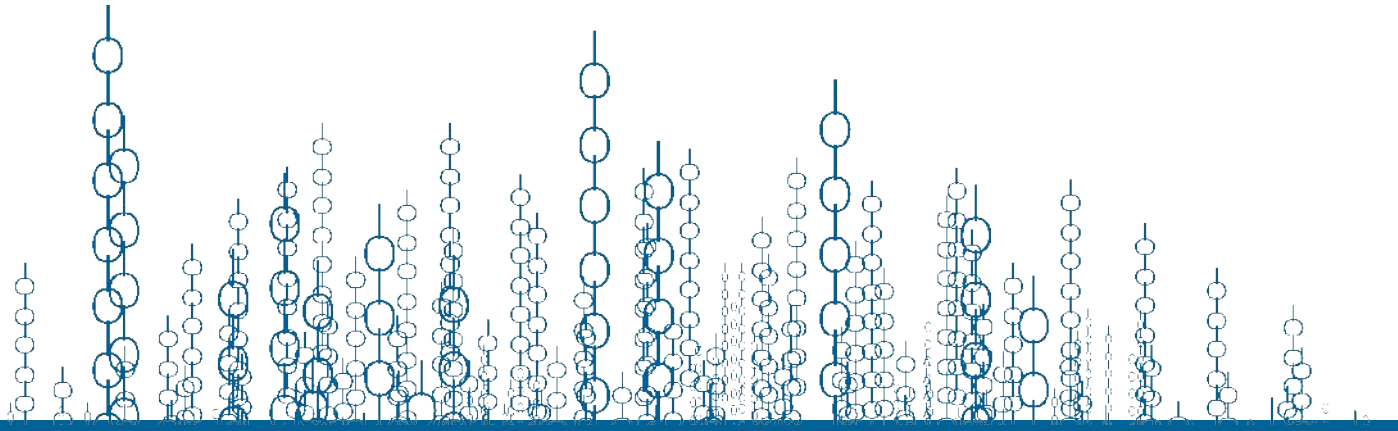
Aan de andere kant zijn technische informatiebeveiligingsspecialisten, door hun enthousiasme en specialisatie, technisch gedreven en verliezen vaak het belang uit het oog. Het gevolg is dat de geboden oplossingen niet goed passen bij het afdekken van de risico's en daardoor onnodig belemmerend werken en te veel geld kosten.

Een ideale, maar helaas zeer schaarse, combinatie van technische kennis en bedrijfskennis is noodzakelijk. Pas dan dekt u tijdens het risico-onderzoek het hele spectrum af van wet- en regelgeving, business processen, technologie, informatiebeveiliging en omgekeerd.

Ketensamenwerking en zwakste schakel

Het gevaar van een allesomvattende benadering van organisatie, mensen, processen en technologie is dat u, vanwege tijd en geld, neigt naar een beperkt of oppervlakkig onderzoek. Dat doet afbreuk aan de resultaten van het onderzoek. U bent daarmee nooit verzekerd van een volledig overzicht van de risico's, dreigingen en zwakste schakels.

Informatiebeveiliging is echter zo sterk als de zwakste schakel in een ecosysteem en dat weten cybercriminelen! Een integrale toetsing is daarom noodzakelijk. Niet alleen binnen een organisatie maar ook binnen de ketens van samenwerkende organisaties en leveranciers. Vooral een integrale toetsing van de ketens wordt steeds belangrijk. Dit enerzijds vanwege de toenemende tendens tot samenwerking om complexe vraagstukken in de zorg en financiële sector op te lossen en anderzijds vanwege het feit dat er (grote) verschillen zijn tussen de organisaties qua beleid, aanpak, risico-management en draagvlak rond de beveiliging in een keten. En dat introduceert juist op de koppelvlakken risico's en kwetsbaarheden.



Risicogebaseerde beveiliging

Organisaties beschikken over een gelimiteerde budget, tijd en middelen omtrent informatiebeveiliging. Dit vraagt om een **doelgerichte inzet** van budget, tijd en middelen. De inzet moet overeenkomen met de risico's en de gevolgen in relatie tot het belang van het bedrijfsmiddel en/of bedrijfsproces. Dit tezamen bepaalt de ernst en is richtinggevend voor de inzet van beveiligingsmaatregelen (risicogebaseerde beveiliging).

Het risico-onderzoek van Fortezza MSSP is een uniek geaggregeerd onderzoek dat op een natuurlijke manier kijkt naar informatiebeveiliging (IB).

Dit onderzoek maakt IB begrijpelijk door inzicht te geven in de impact van bepaalde risico's op de bedrijfsprocessen en sluit aan bij de perceptie van de belanghebbenden van de belangrijke bedrijfsmiddelen en -processen.

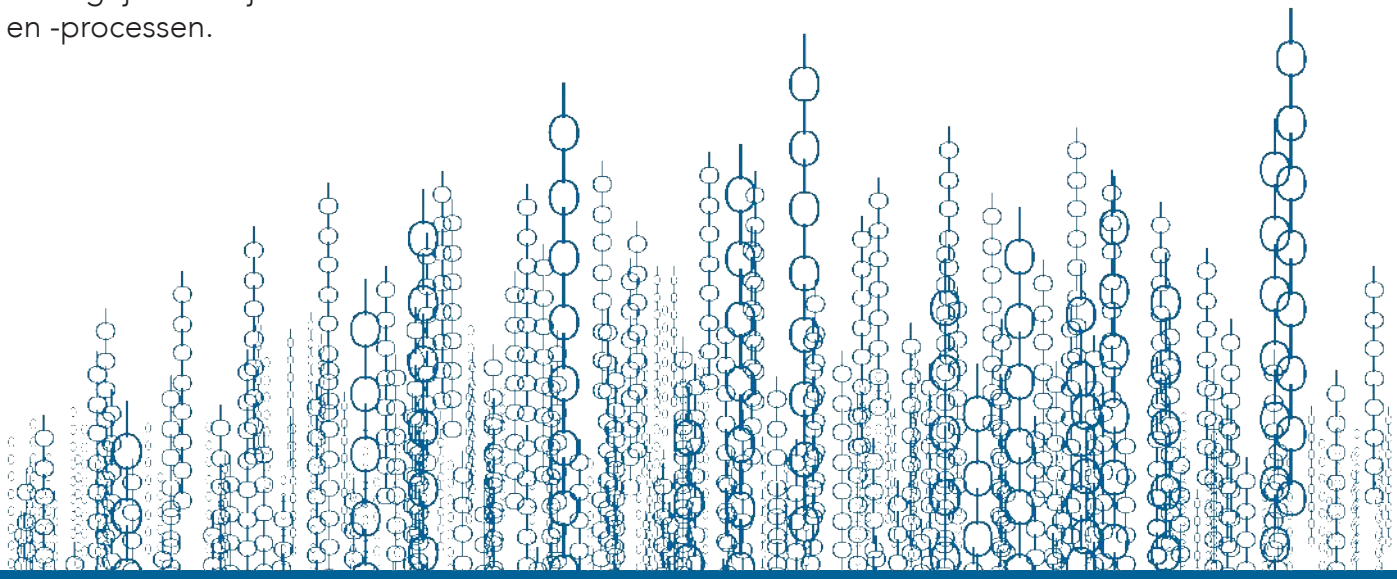
Met een risicogebaseerde beveiliging voorkomt u dat uw organisatie(s) onnodig op kosten jaagt. Bovendien levert dit inzicht en rechtvaardiging om effectieve besluiten te nemen over de informatiebeveiliging en draagt deze bij aan het stellen van de juiste vragen over de informatiebeveiliging.

Indien u bijvoorbeeld webservices aanbiedt via een Cloud provider aan klanten, dan kunt u uw geld waarschijnlijk beter besteden aan twee-factorauthenticatie ter bescherming daarvan, en het upgraden van de bedrijfsfirewalls naar de allerlaatste firewalltechnologie uit te stellen naar volgend jaar. Dit leidt weer tot een beter begrip, bewustwording en betrokkenheid in de organisatie, waardoor men de beveiligingsmaatregelen veel beter naleeft. En tot slot is een risicogebaseerde beveiliging eenvoudig van opzet terwijl de kwaliteit hoog is.

Het idee achter onze gelaagde aanpak

Fortezza MSSP baseert haar risico-onderzoek op een raamwerk met een indeling in zeven categorieën van beveiligingsmaatregelen. Deze maatregelen vormen tezamen een meervoudige en gedifferentieerde gelaagdheid in de verdediging tegen inbreuk op vertrouwelijkheid, integriteit en beschikbaarheid.

Dit betekent, dat wanneer maatregelen in de ene laag niet of onvoldoende werken, informatie en informatiesystemen nog steeds kunnen worden beschermd door maatregelen in de andere laag. Zo blijft u in control over informatiesystemen en data.



	VERTROUWELIJKHEID	INTEGRITEIT	BESCHIKBAARHEID
Laag 1	**Identificatie & Authenticatie:** Identificeren van entiteiten (personen, middelen en informatie) en het verifiëren van de identiteit (authenticatie) om ongeautoriseerde toegang te voorkomen		
Laag 2	**Autorisatie:** Beperken van toegang tot middelen en informatie tot wat een entiteit daadwerkelijk nodig heeft, om onrechtmatige toegang, onrechtmatig gebruik en diefstal te voorkomen		
Laag 3	**Vertrouwelijkheid & Privacy:** Bieden van beschermende maatregelen om middelen en informatie af te schermen van ongeautoriseerde en ongeautoriseerde toegang en om diefstal te voorkomen	**Integriteit & Authenticiteit:** Bescherming van inbreuk op ongewijzigde of ongeschonden toestand van middelen en informatie om onrechtmatige wijzigingen daarvan (sabotage), onopzettelijke fouten en ontkenning van activiteiten te voorkomen	**Beschikbaarheid:** Garanderen van beschikbaarheid van personen, middelen en informatie en van de verwachte prestaties daarvan om de gevolgen van onopzettelijke fouten, falen, omgevingsdreigingen, diefstal, verlies of onbruikbaar maken te beperken
Laag 4	**Content scanning:** Proactief zoeken naar kwaadaardige componenten en kwetsbaarheden om inbreuk op integriteit, beschikbaarheid en vertrouwelijkheid te detecteren en te beperken		
Laag 5	**Logging, auditing & monitoring:** Vastleggen van gegevens over uitgevoerde activiteiten en gebeurtenissen en het controleren daarvan, teneinde (on) geautoriseerde activiteiten te kunnen ontdekken en het genereren van een alarm als er zich een vooraf gedefinieerde gebeurtenis voordoet, om inbreuk op integriteit, beschikbaarheid en vertrouwelijkheid te kunnen detecteren en de gevolgen daarvan te beperken		

DE WERKING VAN RISICOGEBASEERDE BEVEILIGING

UITVOERING stap 1

De beheersmaatregelen uit het raamwerk geven aan wat u zou moeten doen om tot een goede baseline security te kunnen komen en zijn een randvoorwaarde voor het realiseren van een integrale en risicogebaseerde beveiliging.

De basis van het raamwerk bevat een consistente set van meer dan honderd fysieke, personele, organisatorische en technische algemene maatregelen en zijn verdeeld in de bovengenoemde zeven categorieën. Ze bestrijken het volledige informatiebeveiligingsspeelveld en hebben betrekking op alle aspecten van een organisatie.

Toepassing van een evenwichtige verdeling van diverse maatregelen uit alle categorieën is een goede eerste stap om zwakke plekken in de beveiliging te voorkomen.

ONDERWERP – stap 2

In deze stap licht u het gehele ecosysteem door van de organisatie inclusief de technologie. Dit gaat van medewerkers, data, netwerkapparatuur, servers, werkstations, mobiele apparatuur, printers, Internet of Things tot aan industriële IT. Bij het doorlichten van al deze aspecten beoordeelt u of de algemene maatregelen van toepassing zijn.

KWALITEIT stap 3

Als laatste evalueert u de toepassing van de beveiligingsmaatregelen op de infrastructuur-componenten in het ecosysteem van de organisatie. Dit geeft een indicatie van het zekerheidsniveau van de maatregelen. Een hoog dreigingsniveau en een hoge impact vereisen een hoger zekerheidsniveau en dit geldt zeker voor de bedrijfs- en IT-middelen waar primaire bedrijfsprocessen van afhankelijk zijn.

Invoering van de algemene maatregelen in het ecosysteem op alle infrastructuurcomponenten met een zekerheidsniveau dat past bij de data en gegevensverwerkende businessprocessen, is het ideale scenario. De investering en gewenste informatiebeveiliging zijn dan exact in balans met elkaar. Het is geen toeval dat Fortezza MSSP Risk Assessment zich precies hierop richt.

TYPE RISICO-ONDERZOEK	BESCHRIJVING
Risico-onderzoek basis	Dit is de basis variant. Hiermee legt Fortezza MSSP in □□n dag vast welke algemene maatregelen uit het risico-raamwerk zijn toegepast in de organisatie
Risico-onderzoek-standaard	Dit is de uitgebreidere variant. In maximaal drie dagen stellen wij vast of en waar de algemene maatregelen uit het risico-raamwerk in het gehele ecosysteem zijn toegepast. Aan omgevingen die bij het ecosysteem behoren kunt u denken aan eigen datacenter
Risico-onderzoek-uitgebreid	Dit is een uitgebreide variant van een risico-onderzoek. In maximaal 5 dagen leggen wij vast of en waar de algemene maatregelen uit het risico-raamwerk in het gehele ecosysteem zijn toegepast. En tevens onderzoeken wij op welke wijze en met welke middelen (proces, techniek) de maatregelen zijn toegepastomgevingsdreigingen, diefstal, verlies of onbruikbaar maken te beperken
Risico-onderzoek-Compleet	Dit type onderzoek is de meest uitgebreide variant en is een □Risico-onderzoek-uitgebreid□ aangevuld met een audit. De audit stelt het daadwerkelijke zekerheidsniveau vast zoals dat is gecommuniceerd
Risico-onderzoek-specifiek (keten)	Risico-onderzoek-specifiek richt zich op de risicoanalyse van één of meerdere specifieke onderwerpen. Een voorbeeld hiervan is de scope van het risico-onderzoek te beperken tot datgene dat alleen direct de primaire business processen kan be•nvloeden, maar het risico-onderzoek kan zich ook richten op een specifieke koppeling met een derde partij of beoordeling van de informatiebeveiliging van een ketenpartner

Disclaimer: *Het risk risico-onderzoek □Basis□ biedt u echter te weinig zekerheid om vast te stellen of de maatregelen overal en in voldoende mate gerealiseerd zijn. Daarvoor is een uitgebreider risk assessment noodzakelijk.*

RISICO-ONDERZOEK BASIS

ONDERWERP	BESCHRIJVING
Duur	1 dag
Locatie	Op locatie of op afstand
Stakeholders	Een interview van ??n uur met een vertegenwoordiger uit de organisatie Een interview van 2 uren met een vertegenwoordiger van het IT-Management
Onderwerpen	Globaal inzicht te krijgen van de primaire business processen van de organisatie alsmede inzicht te krijgen in de kansen, bedreigingen, zwaktes en sterktes Bepalen wat (globaal) aan algemene maatregelen zijn getroffen aan de hand van een vragenlijst
Resultaten	Rapport benoemen van risico's, kansen, sterktes of zwaktes. Focus ligt op de consequenties van ontbreken van maatregelen op de primaire businessprocessen. Rapport bevat tevens een advies. Evaluatiegesprek Bespreken van de resultaten met directie / management en vervolgafspraken (optioneel)
Overwegingen bij dit type onderzoek	Met het risico-onderzoek-basis krijgt u een algemeen beeld van de mate van toepassing van diverse maatregelen uit het raamwerk. Het bied u aanknopingspunten waar u bij informatiebeveiliging allemaal aandacht aan kan besteden en is daardoor ook te gebruiken als middel om kennisoverdracht te doen van informatiebeveiligingsaspecten naar de organisatie. Deze vorm van risico-onderzoek is daarom erg zinvol als startpunt

Disclaimer: *Het risk risico-onderzoek Basis bied u echter te weinig zekerheid om vast te stellen of de maatregelen overal en in voldoende mate gerealiseerd zijn. Daarvoor is een uitgebreider risk assessment noodzakelijk.*

RISICO-ONDERZOEK STANDAARD

ONDERWERP	BESCHRIJVING
Duur	3 dagen
Locatie	Op locatie of op afstand
Stakeholders	Een interview van één uur met een vertegenwoordiger uit de organisatie Een interview van 2 uren met een vertegenwoordiger van het IT-Management en Een interview met de vertegenwoordigers van de ecosystemen (v.b. ketenpartners)
Onderwerpen	Inzicht in de aanwezigheid van de overkoepelende maatregelen uit het raamwerk die worden toegepast op de diverse ecosysteem-omgevingen aan de hand van een vragenlijst Inzicht in de aanwezigheid van maatregelen van de ecosysteem omgevingen
Resultaten	Rapport – benoemen van risico's, kansen, sterktes of zwaktes. Focus ligt op de consequenties van ontbreken van maatregelen op de primaire businessprocessen. Evaluatiegesprek – Bespreken van de resultaten met directie / management en ketenpartners (optioneel en na goedkeuring van directie / management) en vervolgafspraken (optioneel)
Overwegingen bij dit type onderzoek	Dit type onderzoek biedt u mogelijkheden om uw informatiebeveiliging op orde te brengen op basis van de gevonden risico's waar uw organisatie geen zicht op had. Niet alleen de volwassenheid van uw organisatie qua beveiliging maar die van de ketenpartners kan tegelijkertijd worden verhoogd. En indien de ketenpartner op basis van het onderzoek geen maatregelen kan of wil nemen, dan biedt dit uw organisatie de mogelijkheid om dan extra maatregelen te treffen

RISICO-ONDERZOEK UITGEBREID

ONDERWERP	BESCHRIJVING
Duur	5 dagen
Locatie	Op locatie of op afstand
Stakeholders	- Een interview van □□n uur met een vertegenwoordiger uit de organisatie - Meerdere interviews van 2 □ 3 uren met vertegenwoordiger van de IT-Afdeling
Onderwerpen	- De details van de invoering van de beveiligingsmaatregelen worden meer in detail besproken - Per invoering van een maatregel het bepalen van de scope en zekerheidsniveau maar ook de tekortkoming van een maatregel en de ernst als de impact van deze tekortkoming op het bedrijfsproces
Resultaten	- Rapport □ benoemen van risico□s, kansen, sterktes of zwaktes. Focus ligt op de consequenties van ontbreken van maatregelen op de primaire businessprocessen. - Evaluatiegesprek □ Bespreken van de resultaten met directie / management
Overwegingen bij dit type onderzoek	- Dit type onderzoek biedt meer zekerheid over de uitkomsten van het onderzoek doordat wij in detail doorvragen over de daadwerkelijke inrichting van processen, invoering en configuratie van technische beveiligingsmaatregelen - De resultaten zijn bij uitstek geschikt om een roadmap voor informatiebeveiliging samen te stellen en de prioriteiten te bepalen op basis van ernst, impact en inspanningen

RISICO-ONDERZOEK COMPLEET

ONDERWERP	BESCHRIJVING
Duur	Maatwerk - Afhankelijk van de complexiteit, omvang van de organisatie, in combinatie met de gewenste reikwijdte van het onderzoek.
Locatie	Op locatie of op afstand
Stakeholders	Een interview van n uur met een vertegenwoordiger uit de organisatie Meerdere interviews van 2 3 uren met vertegenwoordiger van het IT-Afdeling Diverse audits om (steekproefsgewijs) vast te stellen of de gecommuniceerde maatregelen ook daadwerkelijk overeenkomen met de praktijksituatie.
Onderwerpen	Afhankelijk van de vraagstelling
Resultaten	De resultaten en rapportage zijn vergelijkbaar met die van Risk Assessment Uitgebreid en tevens krijg u een grotere mate van zekerheid dat men de maatregelen daadwerkelijk op een passende manier toepast in de gehele organisatie en / of bij uw ketenpartners. Bij ontbreken van de gepaste maatregelen heb u de mogelijkheid om hen aan te spreken met heldere argumenten.
Overwegingen bij dit type onderzoek	Het risico-onderzoek geeft de mogelijkheid om daadwerkelijk op basis van de steekproeven te laten zien aan klanten dat de informatiebeveiliging op orde is. Het is vooral geschikt voor organisaties met een relatief hoge volwassenheid ten aanzien van informatiebeveiligingextra maatregelen te treffenom de volwassenheid ten aanzien van informatiebeveiliging in uw organisatie te verhogen.

RISICO-ONDERZOEK SPECIFIEK

ONDERWERP	BESCHRIJVING
Duur	Maatwerk - Duur is afhankelijk van het gekozen thema
Locatie	Op locatie of op afstand
Stakeholders	Een interview van □□n uur met een vertegenwoordiger uit de organisatie en / of vertegenwoordiger van een IT-afdeling
Onderwerpen	Sterk gericht onderzoek waarbij geheel naar wensen van uw organisatie bepaalde aspecten qua risico en dreiging worden onderzocht. □ Voorbeelden: Reikwijdte van het risico-onderzoek te beperken tot datgene dat alleen direct de primaire business processen kan be•nvloeden, □ maar onderzoek kan zich ook richten op een specifieke koppeling met een derde partij of □ De beoordeling van de informatiebeveiliging een ketenpartner. De te onderzoeken aspecten zullen, net zoals bij de andere uitvoeringen, onderhevig zijn aan de algemene maatregelen van het raamwerk
Resultaten	1. Rapport 2. Evaluatiegesprek
Overwegingen bij dit type onderzoek	Dit type onderzoek is sterk geschikt voor organisaties die gaan samenwerken of die te maken krijgen met een fusie of koppeling willen leggen met leveranciers of zich goed bewust zijn van de risico□ maar dit nog niet precies kunnen vaststellen.