Risico Reductie Overzicht

Handleiding

Auteurs	Hellen Havinga en Olivier Sessink
Datum	7 juli 2014
Versie	1.0

Inhoudsopgave

1.Risico Reductie Overzicht in vogelvlucht.....4

2.Wie kan Wat met een Risico Reductie Overzicht?.....6

3.Risico Reductie Overzicht uitgelegd.....8

4.Voorbeeld.....10

5.Hoe maak je een Risico Reductie Overzicht.....12

6.Hoe review je een Risico Reductie Overzicht.....16

7.Terminologie.....18

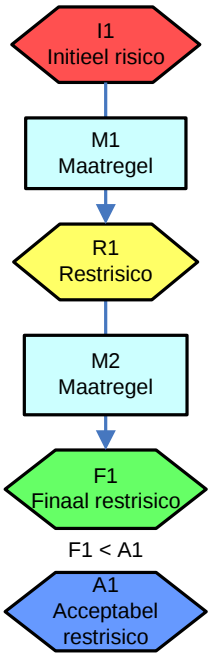
1. Risico Reductie Overzicht in vogelvlucht

Risico management is de balans vinden tussen risico's en te treffen maatregelen. Het "Risico Reductie Overzicht" (RRO) is een visualisatie methode om de samenhang tussen risico's, maatregelen en restrisico's weer te geven.

Het Risico Reductie Overzicht bestaat uit twee delen: een stroomdiagram met alle oorspronkelijke risico's, maatregelen, restrisico's en uiteindelijk de te accepteren restrisico's en een bijlage met een detailbeschrijving van al deze risico's en maatregelen.

De methodiek van het Risico Reductie Overzicht is ontwikkeld ter ondersteuning van het management bij het nemen van besluiten over complexe beveiligingsvraagstukken in de ICT. De methodiek kan iedere onderneming helpen bij de besluitvorming over complexe vraagstukken.

De meeste ICT-ontwerpen gaan wel in op de verschillende beveiligingsmaatregelen die getroffen zijn, maar geven geen inzicht in hun samenhang en de restrisico’s die overblijven. Het is heel lastig om als lezer van een ontwerpdocument uit de documentatie af te leiden wat de restrisico’s zijn die overblijven na implementatie en in te schatten of die restrisico’s acceptabel zijn. Met een Risico Reductie Overzicht kan de ontwerper het doorgronden van zijn ontwerp vergemakkelijken voor collega's en managers die er over moeten beslissen.



Figuur 1: Basis elementen van een RRO

Het Risico Reductie Overzicht is een stroomdiagram. De stroom begint bovenaan met de initiële risico’s, die door de toepassing van maatregelen steeds verder worden gereduceerd, tot er aan het einde van de stroom een finaal restrisico overblijft. Bij de finale restrisico’s wordt omschreven wat de impact is als het risico optreedt en wat de kans is dat het risico werkelijkheid wordt. Het is aan het management om te bepalen of het finale restrisico voldoet aan het Acceptabele Risico, dat wil zeggen, het door de organisatie vastgestelde acceptabele risiconiveau. Zo niet, dan moeten meer maatregelen worden genomen. Het management zal dus beslissen om het acceptabele risico aan te passen, dan wel meer budget vrij te maken voor aanvullende maatregelen.

Een Risico Reductie Overzicht maakt een complex probleem inzichtelijker voor reviewers, auditors, managers en bestuurders, door risico’s en maatregelen in samenhang te presenteren. Door de eenvoud geeft het direct inzicht in de initiële risico’s (op bijvoorbeeld een ICT systeem) waar in het ontwerp rekening mee is gehouden en welke restrisico’s overblijven als opeenvolgende
preventieve en reactieve maatregelen worden getroffen. Maatregelen kunnen gericht zijn op mensen (opleiden), procedures en op technische maatregelen. Samen reduceren zij de risico’s.

Een RRO geeft geen garantie dat een systeem veilig is, het geeft aan welke beveiliging er wél is genomen, en maakt het makkelijker om te zien welke beveiliging er niet in zit en wat de restrisico's zijn.

De methodiek geeft overzicht, helpt de discussie, en stimuleert een bewuste afweging van ofwel keuze tussen diverse maatregelen. Aldus leidt dit tot ook tot een heldere en traceerbare besluitvorming.

Pagina 4 van 18

2. Wie kan Wat met een Risico Reductie Overzicht?

1) Een **ontwerper** die een RRO maakt wordt tijdens het maken gedwongen om nog een keer goed na te denken welke oorspronkelijke risico's er zijn, waarom elke maatregel genomen is en wat het effect van die maatregel is. Door een RRO te maken wordt het voor de maker vaak duidelijk of de set van maatregelen inderdaad alle risico's afdekken (of niet). De RRO geeft daarnaast ook overzicht van de lagen van de beveiliging en de diversiteit van maatregelen die zijn toegepast.

2) Een **ontwerper** kan met behulp van het RRO zijn ontwerp optimaliseren. Dubbele maatregelen, of maatregelen die een risico niet verder reduceren worden makkelijk ontdekt. Ook kan de volgorde van maatregelen invloed hebben op de kosten van het ontwerp. Als een goedkope maatregel als eerste verdedigingslinie al veel risico wegneemt, kan een volgende verdedigingslinie kleiner worden uitgevoerd.

3) Een **reviewer** van een RRO krijgt direct een overzicht welke oorspronkelijke risico's meegenomen zijn bij het ontwerp van het systeem. Als een bepaald risico niet in de lijst van oorspronkelijke risico's staat, is dat een indicatie dat de maker van het systeem dat risico niet onderkend heeft en dus dat het systeem wellicht niet veilig is.

4) Een **reviewer** kan bij elke beveiligingsmaatregel kijken of hij het eens is met het restrisico. Als het restrisico in werkelijkheid veel hoger is dan wordt de effectiviteit van de maatregel wellicht schromelijk overschat. Ook dit kan een indicatie zijn dat het systeem niet veilig is. Als de restrisico's na een maatregel niet kloppen dan zullen de uiteindelijke te accepteren risico's ook niet kloppen.

5) De **objecteigenaar** krijgt met een RRO een overzicht van de risico's, de maatregelen en allerbelangrijkst de te accepteren maatregelen. Als de te accepteren maatregelen uiteindelijk niet acceptabel blijken te zijn bij de verantwoordelijken dan moet er een beter ontwerp komen. Door de RRO uit te zetten bij een aantal reviewers kan de **objecteigenaar** ook snel een inschatting krijgen van de kwaliteit van de RRO en van de kwaliteit van het ontwerp.

6) Risico's veranderen door de tijd. Nieuwe kwetsbaarheden verschijnen, en ook de kans dat een bepaalde kwetsbaarheid wordt uitgebuit, verandert in de tijd. Door de nieuwe risico's in de RRO te zetten kan een **ontwerper** het effect zien op de te accepteren risico's. De **objecteigenaar** zal de nieuwe te accepteren risico's moeten accepteren, of anders moeten er extra maatregelen genomen worden.

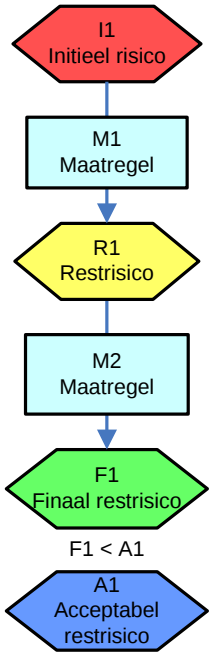
7) Een bestaande RRO kan voor een **ontwerper** als inspiratie dienen voor het ontwerp van een nieuw of vergelijkbaar systeem, en kan voor een **reviewer** worden gebruikt om de beveiliging van verschillende systemen te vergelijken.

Pagina 6 van 18

3. Risico Reductie Overzicht uitgelegd

Een RRO bestaat uit twee delen: een stroomdiagram en een bijlage. Het stroomdiagram geeft inzicht in de samenhang tussen alle risico's, maatregelen en finale (rest)risico's. Aan de plaats en de relaties van een maatregel in het stroomdiagram is te zien of een maatregel een andere maatregel versterkt (*defence in depth*), aanvult (de maatregel reduceert een ander aspect van het risico) of onafhankelijk is van andere maatregelen (de maatregel wordt getroffen tegen een heel ander risico). In de bijlage staan de details beschreven over elk risico en elke maatregel.

Het stroomdiagram (figuur 1) is gebaseerd op 2 basis elementen: risico's en maatregelen. We delen de risico's in vier types:
1) oorspronkelijke risico's;
2) restrisico's;
3) finale restrisico’s; en
4) acceptabele risico’s
Acceptabele risico's zijn in de praktijk vooraf meestal niet bekend en worden daarom vaak weggelaten.



Figuur 1: Basis elementen van een RRO

Alle stroomlijnen in het RRO stroomdiagram volgen hetzelfde stramien: een stroom begint bij een oorspronkelijk risico, één of meer maatregelen worden getroffen om het risico te reduceren, welke leiden tot restrisico's. Uiteindelijk eindigt elke stroom in een finaal (rest)risico. Als vooraf bekend is welk risico acceptabel is, kan in het diagram worden aangegeven of het finale restrisico groter of kleiner is dan het acceptabele restrisico. Het stroomdiagram start met alle oorspronkelijke risico's die voor het ontwerp zijn geïdentificeerd. De stroom is niet noodzakelijk lineair. Soms leveren verschillende maatregelen uiteindelijk hetzelfde restrisico op. Soms leidt een maatregel tot meerdere restrisico's.

Alle risico's en maatregelen in het RRO hebben een uniek kenmerk (het bijbehorende hekje staat voor een uniek getal):

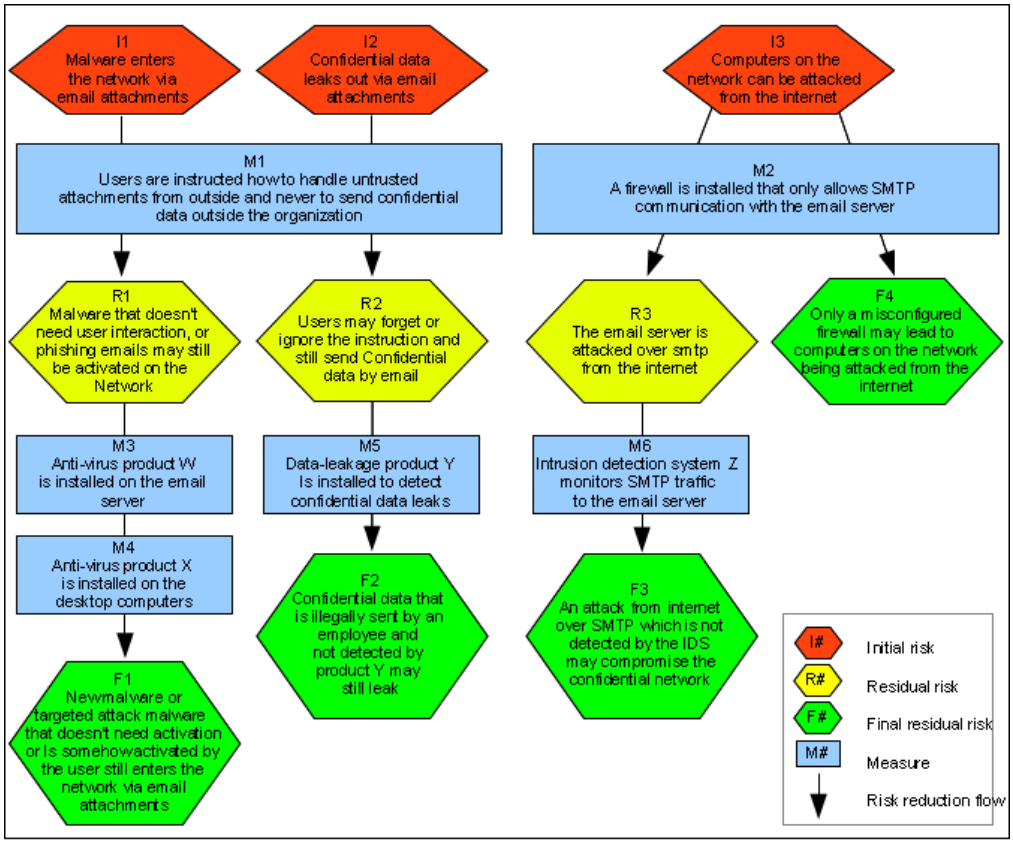
I# kenmerk van een oorspronkelijk risico
R# kenmerk van een restrisico
M# kenmerk van een maatregel
F# kenmerk van een finaal restrisico
A# kenmerk van een acceptabel restrisico

In het stroomdiagram wordt elk uniek kenmerk gevolgd door een korte beschrijving van het risico of de maatregel. In de bijlage die bij het RRO hoort staan alle risico's en maatregelen in meer detail beschreven.

Pagina 8 van 18

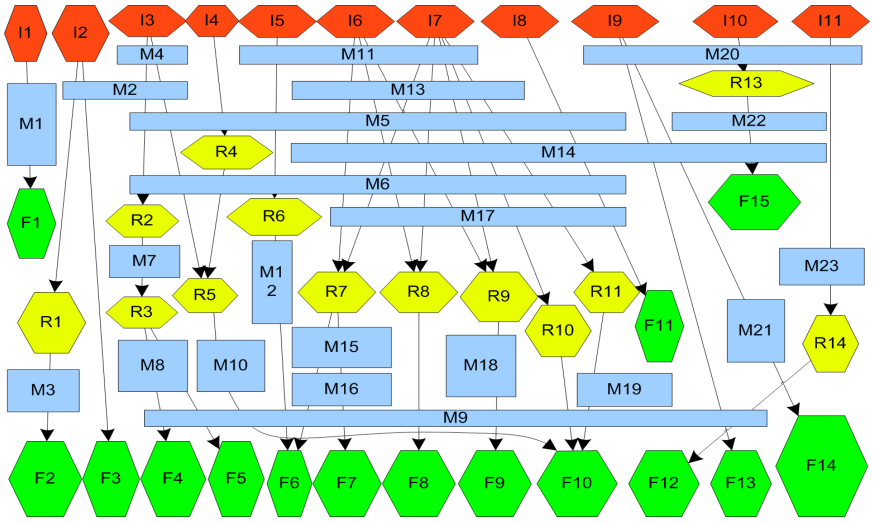
4. Voorbeeld

Ter illustratie van een risico reductie stroom gebruiken we in figuur 2 een zeer gesimplificeerd voorbeeld: Wat gebeurt er als er e-mail verkeer wordt toegestaan tussen een vertrouwelijk netwerk en internet. Dit voorbeeld is slechts ter illustratie verzonnen. Risico reductie overzichten van echte koppelvlakken bestaan soms wel uit 20 oorspronkelijke risico's en meer dan 20 maatregelen (figuur 3).



Figuur 2. Voorbeeld RRO (Engelse versie)

Het voorbeeld in figuur 2 laat een wijziging zien op een vertrouwelijke ICT infrastructuur. Het bijbehorende risico reductie overzicht laat zien welke risico's door de wijziging worden geïntroduceerd, welke maatregelen daartegen worden getroffen en welke restrisico's er overblijven.



Figuur 3: Voorbeeld van een oorspronkelijke RRO, waaruit de teksten zijn verwijderd

Pagina 10 van 18

5. Hoe maak je een Risico Reductie Overzicht

STAP 1
De eerste stap is het plaatsen van alle geïdentificeerde oorspronkelijke dreigingen boven aan het stroomdiagram. Oorspronkelijke risico's zijn alle risico's die men zou lopen als er geen enkele maatregel zou zijn getroffen. De oorspronkelijke risico's kun je afleiden van de dreigingen voor de bedrijfsvoering gecombineerd met de mogelijke kwetsbaarheden van je systemen, processen en medewerkers.

Maak vervolgens een lijst van de verschillende technische en procedurele maatregelen die je voor ogen hebt om je systeem te beveiligen. Plaats de maatregelen onder de oorspronkelijke risico's en leidt de restrisico's af die overblijven na implementatie van een maatregel. Maatregelen die elkaar aanvullen, worden onder elkaar geplaatst, om het restrisico nog verder te reduceren. Je hebt vaak preventieve maatregelen om het risico te voorkomen en reactieve maatregelen om de impact van een risico te verkleinen, als hij ondanks de preventieve maatregelen toch optreedt. De reactieve maatregelen komen na de preventieve maatregelen.

Ga door totdat alle maatregelen een plaats hebben gekregen en alleen acceptabele risico's overblijven onder aan het stroomdiagram. Als twee maatregelen een identieke risico reductie opleveren (defence in depth), dan worden ze direct onder elkaar geplaatst, zonder restrisico er tussen, zie maatregelen 3 en 4 in het e-mail voorbeeld hierboven.

Vergelijkbare maatregelen kunnen het beste bij elkaar in de buurt worden geplaatst, zodat het in de volgende stappen makkelijker is om het diagram te vereenvoudigen. De eerste stap van het maken van een RRO geeft vaak een overzicht dat groot is en lastig te begrijpen. Er zijn een paar technieken om het stroomdiagram te optimaliseren en te vereenvoudigen tot een meer compact en simpeler overzicht. Die staan beschreven in stappen twee en drie.

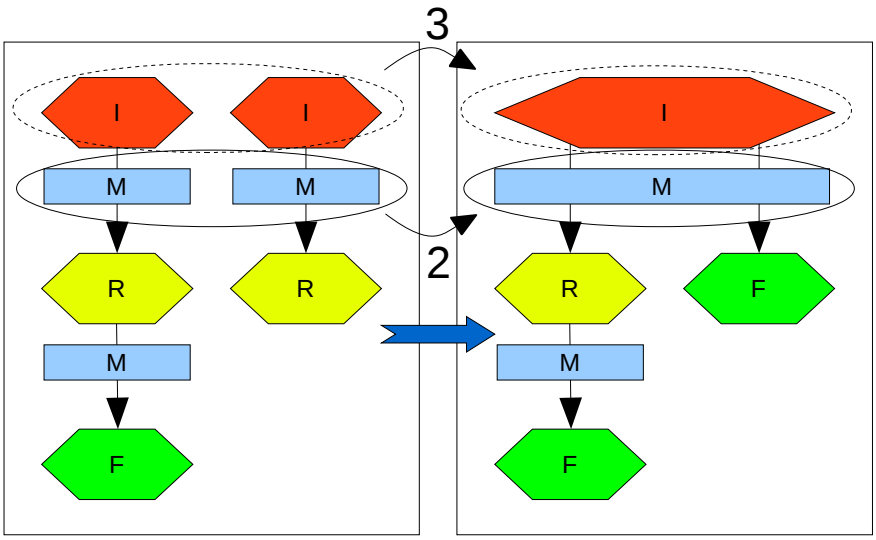
Uniform taalgebruik is belangrijk in het model. Uniforme beschrijvingen maken het mogelijk snel en eenduidig door een model heen te lezen. Als in beschrijvingen onderwerp, lijdend voorwerp en gevolg in verschillende volgorden gebruikt worden, kost het meer concentratie om het model te lezen. Door de beschrijving uniform grammaticaal te structureren wordt het model sneller leesbaar. Een paar richtlijnen:

1. Begin een risicobeschrijving met het kwetsbare element. Bijvoorbeeld: “Attachments worden niet gecontroleerd op virussen”, “Firewalls worden zelden ge-update”.
2. Begin een maatregelbeschrijving met de maatregel. Bijvoorbeeld: “Een virusscanner scant attachments vóór aflevering bij gebruiker”.

STAP 2
De tweede stap is om identieke maatregelen samen te voegen en de bijbehorende stromen daaraan aan te passen (pijl 2 in figuur 4). Deze optimalisatie werkt het best als je ervoor zorgt dat samengevoegde maatregelen al vroeg in het stroomdiagram worden geplaatst (bovenin). Als je de positie van maatregelen in een stroomdiagram wijzigt, dan wijzigen alle restrisico's mee. Als je generieke maatregelen bovenin het stroomdiagram plaatst, dan zijn de restrisico's daarna veel specifieker. Waardoor de details toch nog zichtbaar blijven in het overzicht.

Als twee risico’s of maatregelen samengevoegd worden om een overzicht te versimpelen, pas dan ook de beschrijving van het nieuwe gemeenschappelijke risico of de nieuwe maatregel aan. De nieuwe beschrijving moet dan de twee oorspronkelijke elementen afdekken middels een generieke verwoording.

Pagina 12 van 18



Figuur 4: voor en na stap 2 en 3

STAP 3

In stap drie worden vergelijkbare risico's samengevoegd (pijl 3 in figuur 4). Het is vaak mogelijk om restrisico's net even anders te formuleren, waardoor ze kunnen worden samengevoegd tot een wat algemener restrisico, vroeger in het stroomdiagram. Meestal is het niet mogelijk om restrisico's onder in het stroomdiagram samen te voegen, omdat die vaak erg specifiek zijn. Als deze risico's worden gecombineerd heeft dat tot gevolg dat essentiële details verdwijnen.

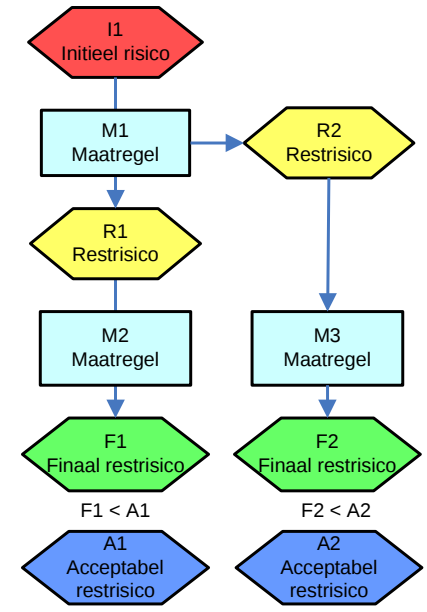
Soms introduceert een maatregel ook een nieuw risico. Neem ook deze risico’s op in het stroomdiagram door een pijl te tekenen vanuit de maatregel naar het nieuwe restrisico (figuur 5).

STAP 4

De laatste stap is het beschrijven van elk risico en elke maatregel in de bijlage. De bijlage bestaat uit drie delen:

1. beschrijving van alle maatregelen. Het bevat voldoende detail voor de lezer om te kunnen beoordelen of een maatregel inderdaad het beoogde risico reducerende effect heeft.
2 beschrijving van alle oorspronkelijke risico's en restrisico's.
3. beschrijving van alle eind restrisico's (die de BA moet accepteren om toestemming te geven voor productie).

Bij elk risico moet worden beschreven wat de kans is dat het risico daadwerkelijk optreedt en de schade die het heeft op de bedrijfsvoering. De beschrijving moet een beveiligingscoördinator of de objecteigenaar voldoende heldere en complete informatie bieden om te beoordelen of een eind restrisico in het RRO ook werkelijk acceptabel is. Soms kan een indicatie van de kosten van de maatregelen of een indicatie van mogelijke schade de besluitvorming stimuleren. De toelichting is als volgt gestructureerd:



Figuur 5: Maatregel (1) introduceert nieuw restrisico (2)

Pagina 14 van 18

Voor een risico:

Risico <kenmerk>	Titel van het risico zoals deze in de flowchart is weergegeven
Impact	Beschrijving wat de impact is als de dreiging werkelijkheid wordt, met voldoende detail dat een systeem eigenaar dit kan meenemen in een afweging
Frequentie	Indicatie wat de kans is dat de dreiging werkelijkheid wordt, met voldoende detail dat een systeem eigenaar dit kan meenemen in een afweging

Voor een maatregel:

Maatregel <kenmerk>	Titel van de maatregel zoals deze in de flowchart is weergegeven
Beschrijving	Beschrijving van de maatregel, en wat het effect van de maatregel is op de impact en/of op de kans van het risico, met voldoende detail dat een technisch architect hieruit kan afleiden wat voor bouwsteen er nodig is en hoe die bouwsteen moet worden geconfigureerd.
Implementatie	(optioneel) Beschrijving hoe de huidige implementatie er uit ziet. Dit geeft extra informatie aan beheerders en ontwerpers hoe e.e.a. geconfigureerd moet worden

6. Hoe review je een Risico Reductie Overzicht

1) Maak vóór dat je de RRO gaat bekijken voor je zelf een lijst van risico's die je van toepassing vindt op het systeem. Open nu het stroomdiagram en kijk naar de top rij van oorspronkelijke risico's. Worden alle risico's genoemd of missen er risico's? Als er risico's missen is de RRO niet compleet. Geef het missende risico door aan de architect of ontwerper, zodat deze het risico kan opnemen en kan beoordelen of extra maatregelen noodzakelijk zijn.

2) Loop alle maatregelen af en bekijk het risico dat er voor staat en het risico dat er na staat. Is de maatregel inderdaad zo effectief als gesteld wordt? Zijn er nog extra restrisico's die moeten worden benoemd? (bijv. het gebruik van de toegangspas voor zowel fysieke toegang als toegang tot de computer verhoogt het risico van een keylogger, omdat je dan de PIN code kunt afvangen).

3) Kijk naar de te accepteren restrisico's. Zijn deze inderdaad acceptabel voor de business? Hoe verhouden ze zich tot de geaccepteerde restrisico's van andere systemen?

Pagina 16 van 18

7. Terminologie

Dreiging: de mogelijkheid dat een kwetsbaarheid wordt benut die de informatie in gevaar kan brengen doordat de integriteit, exclusiviteit of de beschikbaarheid van informatie wordt aangetast.

Risico: de kans dat de dreiging optreedt en het verlies (of impact) als de dreiging realiteit wordt.

Maatregel: de actie die een mogelijk risico vermindert door de impact van de dreiging te reduceren of door de kans dat de dreiging realiteit wordt te reduceren.

Restrisico: overgebleven risico nadat een maatregel genomen is, of nieuw risico dat ontstaat bij de implementatie van de maatregel.

Finaal restrisico: uiteindelijke restrisico als alle maatregelen genomen zijn. Als deze finale risico's geaccepteerd zijn door de Objecteigenaar, dan worden het geaccepteerde restrisico's.

Acceptabel restrisico: overgebleven risico waar geen maatregel meer voor wordt genomen. De eigenaar van het systeem heeft dit risico geaccepteerd.

Pagina 18 van 18