oktober 2010 nummer 6

INFORMATIEBEVEILIGING

Zwichten voor autoriteit

‘Gescoopt’ Risico Management

Rekenen aan Malware

ACTA en netneutraliteit

PvIB
Platform voor InformatieBeveiliging

ib

‘Gescoopt’ Risico Management

Auteur: Rieks Joosten > Rieks Joosten doet onderzoek in het Claims-based lab van TNO in Groningen op het gebied van robuuste, op bedrijfsregels gebaseerde processen. Speciale aandacht hierbij heeft het ontwerpen en het beheren van deze regels op basis van risico analyses, alsmede een op information cards gebaseerde infrastructuur hiervoor. Hij is bereikbaar via rieks.joosten@tno.nl.

Vanuit de geschiedenis weten we dat kleine gebeurtenissen en verwaarloosbaar ingeschatte risico’s, grootschalige uitval van dienstverlening tot gevolg kunnen hebben. Daarom is een actueel overzicht van dreigingen en goed ingeschatte risico’s onontbeerlijk. Binnen grote organisaties zoals overheden, telecom operators, energieleveranciers, en ziekenhuizen, is het beheersen en inzichtelijk maken van risico’s geen sinecure. Niet alleen zijn de aantallen risico’s binnen zulke organisaties onoverzichtelijk groot, maar ook de samenhang ertussen is erg complex. Veel methoden voor de analyse en het managen van risico’s werken weliswaar goed voor kleinere organisaties, maar schalen niet goed naar grote organisaties. Dit artikel beschrijft een werkwijze voor risico management die wel schaalbaar is.

Risico management (RM) binnen grote organisaties is om een aantal redenen zeer complex. Grote organisaties kunnen gemakkelijk tientallen of honderden gebouwen hebben, duizenden systemen, en tienduizenden applicaties, processen en registraties. Alleen al voor systemen bevatten standaardlijsten van mogelijke risico’s en dreigingen er al gauw tien- tot honderdtallen. PriceWaterhouseCoopers [PWC08] stelt dat bijna de helft van de organisaties geen kwetsbaarheden kan aanwijzen die geleid hebben tot security-incidenten.

Een verklaring hiervoor is dat de aantallen risico’s en dreigingen voor mensen eenvoudigweg te groot is om te overzien en lastig te inventariseren en dit actueel te houden. Miller [Miller56] merkte meer dan een halve eeuw geleden al op dat de grens waarbij mensen nog informatie kunnen opnemen en verwerken, heel erg beperkt is. Nu schrijven standaarden en guidelines als ISO [ISO31000] en NIST [NIST02] voor dat als eerste stap in het RM-proces de scope en context van het systeem moeten worden vastgesteld. Dat maakt RM overzichtelijk voor organisaties wiens systemen elk afzonderlijk voldoende overzichtelijk zijn.

De echt grote organisaties hebben echter systemen of diensten die onoverzichtelijk zijn. Daar blijven we dus tegen de fysiologische grenzen van ons mens-zijn aanlopen.

Een tweede reden dat RM complex is heeft te maken met de samenhang tussen risico’s onderling, en tussen risico’s en maatregelen. Een oliecrisis kan bijvoorbeeld leiden tot uitval van het elektriciteitsnet, waardoor noodstroomvoorzieningen extra worden belast. Het gevolg is dat het risico op uitval van vitale systemen (bijvoorbeeld beademingsapparatuur) groter wordt. De maatregel om een operatingsysteem te vervangen door een veiligere variant, met als doel het risico van een virusuitbraak te reduceren, ook tot gevolg hebben dat die kleine applicatie waarmee de ‘speciale service’ wordt geleverd die een paar grootzakelijke klanten hebben afgedwongen, niet langer beschikbaar is. Reason [Reason90] beschrijft dit aan de hand van zijn ‘Swiss Cheese’ model. Alleen organisaties die zulke samenhangen beheersen, kunnen voorzien dat deze maatregel het risico van het verlies van een paar grootzakelijke accounts met zich meebrengt.

Naast deze redenen zijn er tal van praktische redenen die RM kunnen bemoeilijken. Als bijvoorbeeld de verantwoordelijkheden voor diensten, processen of systemen niet eenduidig zijn belegd, dan is daarmee ook niet duidelijk wie verantwoordelijk is voor het inventariseren en behandelen van de bijbehorende risico’s. Dat geldt ook als het kan voorkomen dat bij het niet langer beschikbaar zijn van de verantwoordelijke persoon, (ziekte, verandering van werkkring) de verantwoordelijkheid niet opnieuw wordt belegd of de nieuwe verantwoordelijke hiervan niet actief in kennis wordt gesteld.

Afbakenen

Bij risicomanagement moeten alle voorkomende taken behapbaar blijven. Alleen deze taken kunnen consciëntieus en min of meer foutloos worden uitgevoerd. Een kenmerk van goede RM-methodes, is dat met het groeien van het aantal bedrijfsmiddelen (en daarmee het aantal risico’s), het aantal RM-taken evenredig groeit en daarmee het benodigde aantal uitvoerende personen.

ISO [ISO31000], NIST [NIST02] en andere standaarden en guidelines schrijven in het RM-proces als eerste stap voor dat de scope en context moeten worden vastgesteld. Concreet betekent dit dat het bepaalde afbakeningscriterium (‘scopecriterium’) vaststelt wat binnen de scope valt en wat daarbuiten en daarmee deel uitmaakt van de context. Het belang van afbakenen is echter niet alleen om te kunnen onderscheiden wat al dan niet binnen de scope van RM valt. Een goede afbakening beoogt ook het bijbehorende werk behapbaar te houden. Dat maakt dat elk scopecriterium aan twee bruikbaarheidseisen moet voldoen.

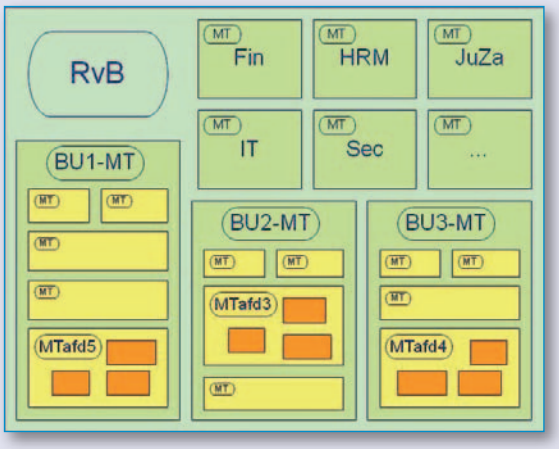

Fig. 1. Scoping met de organieke lijn.

De eerste eis aan scopecriteria, die we de *'behapbaarheidseis'* noemen, moet zijn dat het af te bakenen gebied overzichtelijk is voor mensen. Anderson [Anderson95] stelde al dat mensen op enig tijdstip niet meer dan zeven concepten tegelijk kunnen overzien. Wie dat toch probeert gaat fouten maken. Als RM via de organieke lijn is belegd, heeft deze eis de ogenschijnlijk paradoxale consequentie dat de organisatiebrede RM een scopecriterium moet hebben die zich slechts over een deel van de (hele) organisatie kan uitstrekken. Dit geldt ook voor grote organisatie-eenheden zoals business units. Fig. 1 maakt dit zichtbaar. De buitenste rechthoek stelt een (grote) organisatie voor, met het bijbehorende management team (MT, hier aangegeven als RvB). Binnen de organisatie zitten stafafdelingen (aangegeven met Fin, HRM, JuZa, IT, Sec, enz.) en business units (BU1, BU2 en BU3) die elk een eigen MT hebben. We willen hier benadrukken dat binnen de buitenste rechthoek alleen het lichtstgroene gedeelte de scope vormt waarbinnen zich het organisatiebrede RM zich afspeelt. Alles wat zich binnen de stafafdelingen en BU's afspeelt hoort bij het RM-proces van de betreffende afdeling/BU. De groengekleurde stafafdelingen en BU's bestaan immers om de RvB van zekere taken te ontlasten, en horen dan ook de daarbij behorende risico's zelf te managen. Later gaan we in op hoe dit dan samenhangt met de bedrijfsbrede RM. We merken op dat, aangezien de structuur binnen de BU's dezelfde is als hiervoor beschreven (namelijk dat binnen elke BU (staf)afdelingen zitten met elk hun eigen MT) het RM daarbinnen ook volgens dezelfde principes en samenhangen geregeld kan worden.
De tweede eis, die we de *'eenduidigheidseis'* noemen, is dat scopecriteria zodanig eenduidig moeten zijn dat alle (verschillende) stakeholders het er over eens zijn wat binnen en wat buiten de scope valt. Hierdoor kunnen vaak lange maar nutteloze discussies worden vermeden, wat de efficiency van het werk ten goede komt. Het voldoen aan deze eis faciliteert ook het eenduidig beleggen van verantwoordelijkheden, bijvoorbeeld door voor elke scope personen aan te wijzen die plichtverantwoordelijk en/of taakverantwoordelijk (accountable en/of responsible[1]) zijn voor alles wat binnen de scope gebeurt.

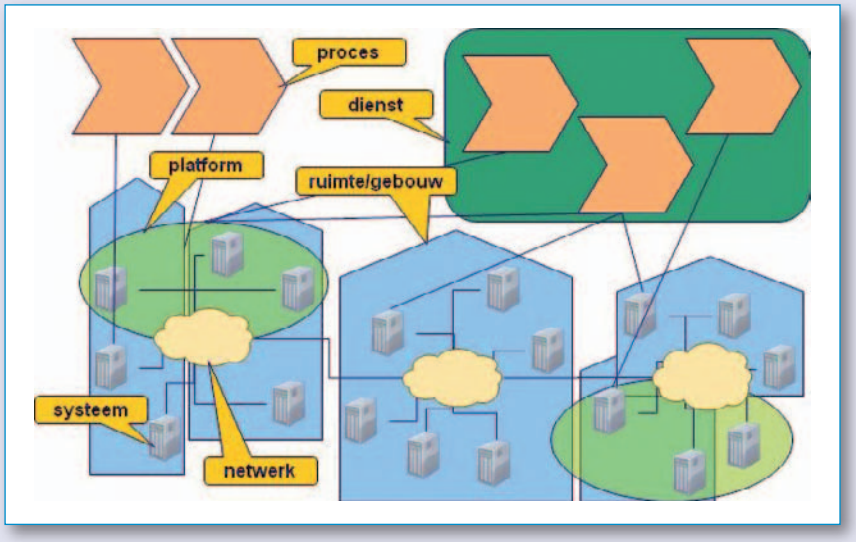

Fig. 2. Samenhang tussen bedrijfsmiddelen.

Het hebben van goede scopecriteria is niet alleen van belang voor 'de lijn', maar ook in de organisatie waar operationeel werk plaatsvindt waarbij werk over afdelingen heen loopt. Als een organisatie bijvoorbeeld specifiek haar HRM-risico's wil managen, moet als eerste een goede afbakening plaatsvinden van wat dit behelst. Een afbakeningscriterium 'HRM' volstaat alleen als alle betrokkenen binnen de organisatie dezelfde antwoorden geven op vragen als: 'Valt het beheer van mobiele telefoons voor werknemers hieronder?' of 'Valt de Peoplesoft-applicatie ook binnen de scope?' Eenduidigheid verkrijgen voor dit type afbakeningen is moeilijker dat voor de organieke lijn.

Fig laat schematisch zien hoe verschillende soorten bedrijfsmiddelen met elkaar samenhangen. De figuur toont bijvoorbeeld dat systemen via netwerken aan andere systemen gekoppeld zijn, zich in ruimtes (gebouwen) bevinden, en onderdeel kunnen zijn van een (service)platform. Ook zien we dat diensten bestaan uit processen die weer van systemen en/of platformen gebruikmaken. De figuur laat zien dat bedrijfsmiddelen getypeerd kunnen worden, bijvoorbeeld als dienst, proces, platform, applicatie, systeem, gebouw, ruimte, enzovoort. Ook andere typeringen zijn mogelijk zoals bijvoorbeeld applicatie, registratie en meer. De figuur toont ook dat individuele bedrijfsmiddelen onderling een samenhang vertonen en het moge duidelijk zijn dat die samenhang onoverzichtelijker wordt naarmate het aantal bedrijfsmiddelen groeit. Eerder is al opgemerkt dat een compleet en courant zicht op deze samenhang noodzakelijk is om risico's goed in kaart te kunnen brengen.

Met behulp van een bedrijfsmiddelen-inventarisatie kunnen scopes als 'HRM' concreet worden gemaakt. Als bijvoorbeeld 'HRM' wordt voorgesteld door het groene vlak in Fig, dan zien we drie processen die afhankelijk zijn van één platform (links) en enkele systemen. Echter, als de scope 'HRM' al deze systemen, platformen en processen zou omvatten, dan is weliswaar aan de eenduidigheidseis voldaan (het is immers duidelijk wat wel en wat niet tot 'HRM' behoort), maar niet aan de behapbaarheidseis. Immers, er zitten niet alleen meer dan zeven onderdelen in 'HRM, maar ze zijn bovendien van verschillende soort, wat het overzicht belemmert.

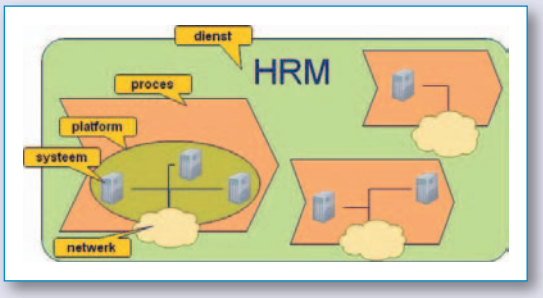

Fig. 3. Scoping met bedrijfsmiddelen.

Fig. 3 laat zien dat we 'behapbaarheid' op vrijwel dezelfde manier kunnen krijgen als we dat (in Fig. 1) met de organieke lijn hebben gedaan. Als we het lichtgroene vlak als de scope 'HRM' zien, en de drie

1 Hiermee past wat we doen binnen het RA(S)CI besturingsmodel.

Voorbeeld

Stel, een organisatie beschikt over een gebouw dat we GN3 noemen. Op de computerzaal staat server S4711, waarop de applicatie DOCA draait. Deze applicatie draait ook op system S1234 die in gebouw AMS1 staat en met server S4711 verbonden is via netwerk NW5. Dat DOCA het documentenarchief is maakt dat voor het opslaan van digitale documenten vrijwel alle bedrijfsprocessen ervan gebruikmaken. Fig. 3 toont deze opzet schematisch, waarbij de gestippelde lijnen de afhankelijkheden aangeven tussen de verschillende scopes.

Als de organisatie gescoopt RM inricht, betekent dit dat de beheerders van beide gebouwen, beide systemen, het netwerk, DOCA, en de processen, allemaal een RM-proces hebben voor dezelfde scope als waarvoor ze beheerder zijn. Zo zal de beheerder van S1234 een risico-analyse (RA) moeten uitvoeren voor dit systeem. Als hij de dreigingen inventariseert, zal daar 'stroomtoevoer naar S1234 valt uit' onder vallen. Dat is een goede dreiging omdat het geheel is geformuleerd in termen die zinvol zijn binnen de eigen scope. Een tekst als 'stroomuitval door bliksemінslag' zal niet worden geaccepteerd als dreiging, omdat (het op orde hebben van) de stroomvoorziening buiten de scope valt. Dit zou weer wel een goede dreiging zijn voor de scopes AMS1 en GN3, omdat de stroomvoorziening voor wat zich in die gebouwen afspeelt binnen deze scopes valt. De beheerder van AMS1 zal in de RA voor zijn scope deze dreiging opnemen en koppelen aan het risico 'stroomtoevoer naar alle (niet van noodstroom voorziene) elektronische apparatuur (binnen AMS1) valt uit'. Als de beheerder van AMS1 dit risico doorgeeft aan de beheerder van S1234, dan kan die dat als dreiging interpreteren en nagaan wat het risico is dat hij daarbij loopt vanuit S1234. Hij moet dit risico dan weer doorgeven aan de beheerder van DOCA die dit weer ziet als een dreiging, enz. Op deze manier propageren alle risico's en dreigingen door de verschillende scopes zodat binnen elke scope een kundige risicoinschatting[2] kan worden gemaakt. Elk RM-proces dat in een scope draait zorgt vervolgens dat de risico's binnen die scope niet uit de hand lopen. Dat kan onder meer door te besluiten maatregelen te nemen die deze risico's reduceren. Dat heeft dan niet alleen effect op de hoogte van het risico, maar ook op de dreigingen van scopes die van de eerste scope afhankelijk zijn. Bilateraal overleg tussen scopebeheerders van onderling afhankelijke scopes is essentieel om de maatregelen af te stemmen zoals bijvoorbeeld in de vorm van een SLA.

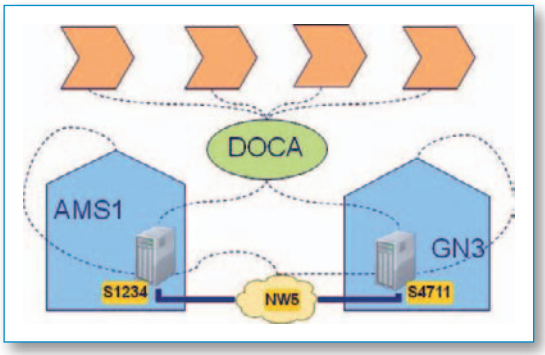

Fig. 4. Voorbeeld van samenhangende scopes.

processen als subscopes daarvan, dan is de taak van 'HRM' om te organiseren en te bewaken dat deze processen in de bedoelde onderlinge samenhang werken. Dat wil zeggen: zorgen dat (1) de processen gezamenlijk de HRM-dienstverlening adequaat vormgeven, (2) de processen daartoe alle benodigde gegevens van/naar andere processen krijgen/sturen en (3) ze onderling resultaten uitwisselen waar nodig. Op soortgelijke wijze kunnen we van elk proces zeggen dat de afbakening wordt weergegeven door de betreffende kleur in het vlak. Dus zonder de platformen, systemen en netwerken die voor de procesondersteuning zorgen, die immers weer eigen scopes zijn en waarbij zodanig de regie wordt gevoerd over de onderliggende scopes dat de resultaten waarvoor het proces verantwoordelijk is, worden geleverd.

Gescoopt Risico Management

Een organisatie die afbakeningscriteria gebruikt die aan beide bruikbaarheidseisen voldoen, ziet zich geconfronteerd met een veelheid aan scopes, waarbij binnen elke scope een RM-taak ligt. Deze waarneming leidt gemakkelijk tot het idee dat overall, RM een welhaast onbegonnen taak zou zijn. Om dit te voorkomen moet consciëntieus met de verschillende RM-taken worden omgegaan.

Criteria

Onder 'gescoopt RM' verstaan we een RM-werkwijze waarbij binnen elke scope:

a) een RM proces[3] draait voor het beheersbaar houden van de risico's binnen deze scope;
b) elke dreiging en elk risico is geformuleerd in termen die horen binnen de eigen scope;
c) elk geïdentificeerd (en gekwalificeerd of gekwantificeerd) risico wordt doorgegeven aan elke scope die van de eigen scope afhankelijk is;
d) elk risico dat naar de eigen scope wordt doorgegeven vanuit scopes waarvan de eigen scope afhankelijk is, wordt behandeld als een dreiging binnen de eigen scope.

Met betrekking tot a) kan een willekeurig RM-proces dienst doen die binnen de kaders van ISO [ISO31000] valt. Denk hier bijvoorbeeld aan ITIL, SEI [SEI93], NIST [NIST02], AS/NZS [AS/NZS4360] en dergelijke. De eigenschap onder b) is een noodzakelijke voorwaarde om aan c) en d) te kunnen voldoen. De eigenschappen c) en d) maken dat risico's als het ware kunnen 'propageren' door verschillende scopes.
Een organisatie (of bedrijfsonderdeel) heeft gescoopt RM ingericht als daarbinnen de volgende criteria[4] worden nageleefd:

a) elk van diens bedrijfsmiddellen is ondergebracht in één scope;
b) voor elk bedrijfsmiddel en elke scope is vastgesteld van welke andere bedrijfsmiddelen c.q. scopes het afhankelijk is voor diens goede functioneren;
c) voor elke scope is één persoon (functionaris) verantwoordelijk voor de RM;
d) binnen elke afbakening is aan de criteria voor gescoopt RM voldaan.

Het werkt eenvoudiger als de afbakening voor bedrijfsmiddelen ook wordt gebruikt

2 Het ligt voor de hand om deze propagatie-eigenschap te gebruiken voor het construeren van Fault Trees IEC [IEC61025]. Daar hebben we echter niet naar gekeken.
3 Dit houdt dus in dat daar dreigingen en risico's worden geïnventariseerd en ingeschat, maatregelen gedefinieerd en geïmplementeerd, etc., zoals dat gebruikelijk is voor een RM proces.
4 Deze criteria zouden deel uit kunnen maken van de organisatie brede risico management policy.

als scope voor RM, zodat de verantwoordelijke voor het bedrijfsmiddel ook voor de scope verantwoordelijk kan worden gemaakt. Deze persoon weet immers al van welke andere bedrijfsmiddelen zijn bedrijfsmiddel afhankelijk is, en welke bedrijfsmiddelen van het zijne afhankelijk zijn. Zo weet hij ook van welke bedrijfsmiddelen hij zijn dreigingen kan verwachten en naar welke bedrijfsmiddelen hij zijn risico's moet exporteren. Daarnaast hoeft hij alleen maar de dreigingen en risico's in kaart te brengen die vanuit zijn eigen bedrijfsmiddel stammen.
Een organisatieonderdeel kan ook als een bedrijfsmiddel worden gezien, dat bijvoorbeeld nodig is om werkkracht (bijvoorbeeld operators) te leveren aan andere bedrijfsmiddelen. Omdat managers van een organisatieonderdeel vaak accountable zijn voor bedrijfsmiddelen, kun je ook zeggen dat de goede werking van dat onderdeel afhankelijk is van die bedrijfsmiddelen. Daarmee kunnen organisatieonderdelen en bedrijfsmiddelen wederzijds van elkaar afhankelijk zijn.

Afspraken tussen scopes

Gescoopt RM helpt bij het maken van afspraken tussen organisaties en/of onderdelen daarvan door de term **'risico'** te definiëren als de inschatting van de waarschijnlijkheid dat een zekere verplichting die op de scope rust, niet waargemaakt gaat worden. **'Verplichtingen'** van een scope zijn dus zaken waarvoor binnen die scope werk moet worden verzet. Verplichtingen zijn er niet alleen ten aanzien van externe partijen (in contracten), maar kunnen ook door wet- of regelgeving zijn opgelegd, of kunnen targets zijn. Het **risico-overzicht** van een scope bestaat dan uit een overzicht van al haar verplichtingen, waarbij voor elk daarvan een inschatting is gegeven van de waarschijnlijkheid dat de verplichting niet kan worden nagekomen: het risico (zie figuur 5).
Fig. **4** geeft een voorbeeld van een risico-overzicht van een scope op een hoog organiek niveau, gezien het strategische karakter van de erin genoemde verplichtingen. Voor scopes lager in de organisatie, zullen de verplichtingen veel specifieker en dus ook veel toetsbaarder zijn.

Met behulp van zo'n risico-overzicht kan een scopeverantwoordelijke besluiten het te accepteren, reduceren, op te heffen of af te wentelen. Afwentelen kan bijvoorbeeld door de boete van het niet nakomen te

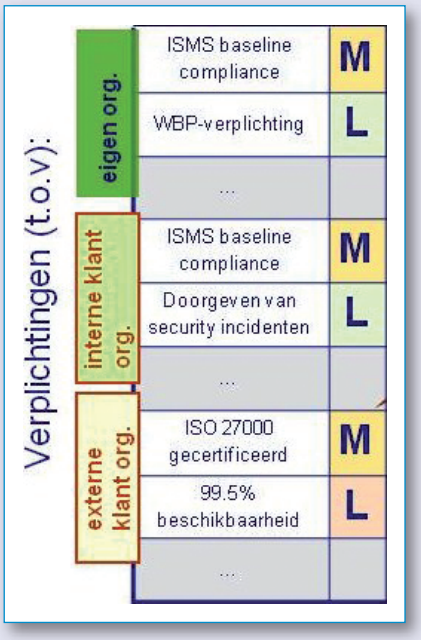

Fig. 5. Risicolijst.

verzekeren, opheffen door na te gaan of de verplichting kan worden verzacht en reduceren betekent doorgaans het specificeren van 'controls'.
Specificaties van controls kunnen we zien als **verwachtingen** die een scope heeft, en wel zo dat als er aan wordt voldaan, risico's worden gereduceerd. Als aan alle verwachtingen is voldaan, dan zijn de resterende risico's acceptabel. Zo worden controls geselecteerd. Daarom is het van belang dat verwachtingen toetsbaar zijn. Dat kan met prestatie-indicatoren (PI's). Als een verwachting van een scope niet wordt waargemaakt, dit een **dreiging** omdat het betekent dat de scope mogelijk niet meer aan (alle) verplichtingen kan voldoen.
Door verwachtingen uit te zetten bij andere scopes (bijvoorbeeld via een SLA of een contract waarin de PI's zijn opgenomen), of binnen de eigen scope (bijvoorbeeld door middel van targets, die eigenlijk al PI's zijn) wordt duidelijk wie vanuit de scope moet worden aangesproken mocht niet aan de verwachting zijn voldaan. Verwachtingen die uitgezet zijn bij een andere scope, worden voor die andere scope verplichtingen op het moment dat deze ze accepteert. Verwachtingen die binnen de eigen scope worden uitgezet worden voor de eigen scope (ook) verplichtingen, en moeten in het risico-overzicht worden opgenomen. Er zijn ook nog verwachtingen die niet kunnen worden uitgezet zoals bijvoorbeeld ten aanzien van het weer of andere niet toe te rekenen verwachtingen die, als ze als dreiging worden geformuleerd, onder de noemer 'acts of God' vallen.

Risicomatrix

Het analyseren van de risico's kan eenvoudig worden gedaan met behulp van een risicomatrix. Eén as van de matrix gaat over de verplichtingen die binnen de scope waargemaakt moeten worden, met (per verplichting) het risico dat niet aan die verplichting wordt voldaan in termen van 'L', 'M' of 'H', precies als de risicolijst uit Fig. **4**. De andere as betreft de verwachtingen (controls) die binnen de scope leven, op grond waarvan de verplichtingen van die scope waargemaakt kunnen worden (en die zijn uitgezet bij een andere of de eigen scope). Voor elke verwachting is de kans ingeschat dat *niet* aan de verwachting (zoals die is uitgezet) zal worden voldaan in termen van L(aag), M(idden) of H(oog). De matrix coëfficiënten bevatten de symbolen '0', '+', '++', '+++' die de mate aangeven

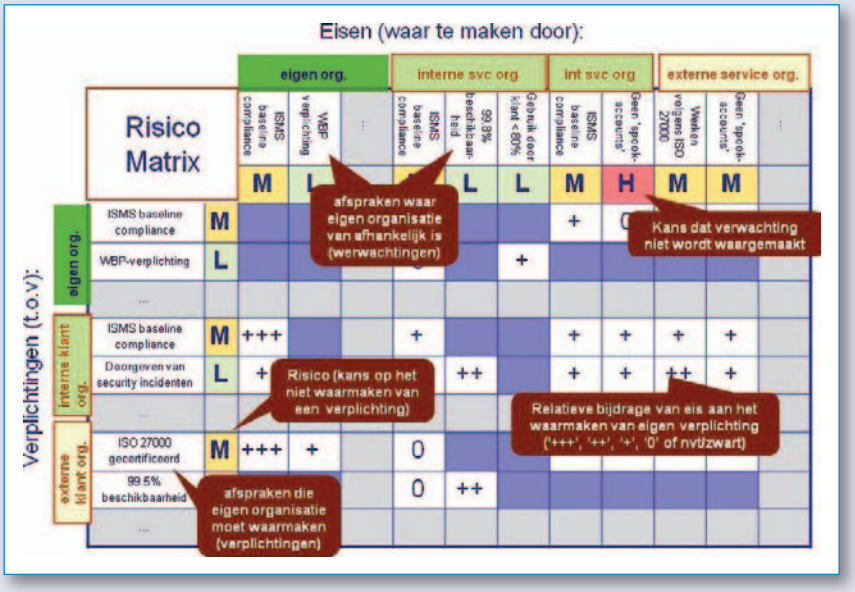

Fig. 6. Risicomatrix van één scope.

waarin de betreffende verwachting en verplichting van elkaar afhankelijk zijn (donkerblauw gekleurde velden geven aan dat er geen afhankelijkheid van toepassing is). Fig. 6 laat een voorbeeldmatrix zien.

Als we deze matrix bekijken, zien we bijvoorbeeld dat de verplichting '99.5% beschikbaarheid' (die door een externe klant wordt geëist) erg (++) afhankelijk is van de verwachting '99,8% beschikbaarheid' (uitgezet aan de interne serviceorganisatie), en niet ('0') afhankelijk is van de verwachting 'ISMS baseline compliance' (uitgezet aan diezelfde serviceorganisatie) en dat de andere afhankelijkheden niet van toepassing zijn. Ook zien we dat alleen de verplichtingen 'Doorgeven security-incidenten' en '99.5% beschikbaarheid' afhankelijk zijn van de verwachting '99,8% beschikbaarheid', en beide in sterke mate (++).
Als we voor één verplichting kijken naar alle verwachtingen waarvan deze afhankelijk is, en we zien bij elke verwachting de kans dat niet aan die verwachting wordt voldaan, dan kunnen we, rekening houdend met de afhankelijkheidscoëfficiënten, een schatting maken voor de kans dat niet aan de verplichting wordt voldaan. Neem bijvoorbeeld de verplichting 'ISMS baseline compliance' (naar de interne klantorganisatie. Deze is van (op één na) alle verwachtingen in dezelfde mate afhankelijk, en (op één na) zijn de kansen dat niet aan de verwachtingen is voldaan, ingeschat als 'M'. Het risico is dan 'M' als we de hiervoor gebruikelijke formule R = K * I (Risico = Kans * Impact) hanteren en aannemen dat de Impact ook 'M' is. Als we dus voor elke verplichting de Impact (= max. hoeveelheid schade die kan ontstaan door niet aan de verplichting te voldoen) inschatten, kunnen met behulp van deze matrix risico's uitrekenen.

Risicomanagement

We beginnen het risicomanagement voor een scope met het opzetten van de risicomatrix. We maken eerst een lijst van verplichtingen en schatten per verplichting de maximale schade (Impact) die voor de scope ontstaat als deze de verplichting niet nakomt, in termen van L, M of H en sorteren deze lijst, waarbij de verplichtingen met de hoogste impact vooraan staan. Dit wordt ook weleens Business Impact Assessment (BIA) genoemd.
Vervolgens gaan we per verplichting (eerst die met impact H, dan die met impact M en die met impact L doen we niet omdat er toch geen bloed uit vloeit) na aan welke verwachtingen moet zijn voldaan om erop te kunnen vertrouwen dat de verplichting kan worden nagekomen. Hiermee vullen we de bovenkant van de matrix en we vullen ook de afhankelijkheidscoëfficiënten in tussen de betreffende verplichting en de ingevulde verwachtingen. Dit is de dreigingeninventarisatie.
In de volgende stap (kansinschatting en risicoberekening) geven we per verwachting met L, M, of H aan of we denken dat *niet* aan de verwachting wordt voldaan. Aan de hand van de afhankelijkheidscoëfficiënten en deze kansinschattingen kunnen we per verplichting bepalen wat de kans is dat de verplichting niet wordt nagekomen (ook weer in L, M of H). Vervolgens bepalen we per verplichting het risico door deze kans te 'vermenigvuldigen' met de bij de verplichting behorende impact. Dat is de bekende formule R = K * I.
Als er 'H'-gescoorde risico's zijn, ligt het voor de hand om een of meer voorstellen te maken die elk betrekking hebben op aanpassingen aan de verplichtingen aan en/of verwachtingen van de scope, zodanig dat als met deze wijzigingen de risicomatrix zou worden gevuld, er geen H-risico's meer in zouden staan. Voor zover het afspraken binnen de eigen scope betreft moeten die worden voorzien van een kostenplaatje en/of andere zaken die het MT nodig heeft om de voorstellen af te kunnen wegen en er over te besluiten. Voor zover het afspraken met andere scopes betreft moeten die met de betreffende eigenaren worden uitonderhandeld - dit is buiten de scope van dit document.

We zien dus dat een scopeverantwoordelijke zijn scope kan besturen met behulp van de risicomatrix, en van elk risico kan bepalen wat ermee te doen. Maar dat hadden we in het begin van dit hoofdstuk al opgeschreven, zodat daarmee de (PDCA)cyclus rond is.

Bedrijfsbreed RM

Omdat RM een gewoon (maar wel bedrijfskritisch) proces is en processen bedrijfsmiddelen zijn, ligt het voor de hand om op het RM-proces zelf ook een RM-proces in te richten. Om dit te kunnen doen zal de RvB zichzelf verplichten dat alle risico's in kaart zijn gebracht, controls zijn gedefinieerd, enz. Als voorbeeld gebruiken we hier de verplichting van de RvB aan zichzelf dat 'hoogstens 3% van alle risico's binnen de organisatie als 'H' mag zijn gekwalificeerd'. Gescoopt RM maakt het mogelijk om deze verplichting 'door te vertalen' naar verwachtingen ten aanzien van de business units of BU's (scopes van het type organisatie-eenheid). De verwachting dat 'hoogstens 3% van alle risico's als 'H' mag zijn gekwalificeerd' hoeft niet voor elke BU met dezelfde tekst te worden doorvertaald: als bijvoorbeeld een (grote) BU 'hoogstens 1%' kan halen, dan zou de bijbehorende verplichting van de RvB ook zijn gehaald als een andere BU 4% scoort. Het doorvertalen van verplichtingen naar verwachtingen levert dus mogelijkheden terwijl je overall toch in control blijft. De keerzijde ervan is dat je wel even moet nadenken over hoe je verwachtingen zodanig doorvertaalt dat als de rapportages terugkomen, jijzelf aan jouw verplichtingen hebt voldaan.

Zijn de verplichtingen (van de RvB) eenmaal doorvertaald naar verwachtingen (van de RvB) voor de BU's, dan moeten de BU's daaraan voldoen. Een verwachting van de RvB ten aanzien van een BU is voor die BU een verplichting. Zo begint het spel opnieuw, maar nu voor de (verschillende) BU(s). Dat levert weer per BU verwachtingen op, die voor de onderliggende bedrijfsonderdelen die weer verplichtingen zijn. Het doorvertalen blijft langs de organieke lijn plaatsvinden, totdat er een bedrijfsonderdeel is dat ook accountable is voor diensten, bedrijfsmiddelen of andersoortige scopes waarop RM plaatsvindt. Dan vindt doorvertaling naar die scopes plaats, en - omgekeerd - wordt vanuit die scopes gerapporteerd en dit weer geaggregeerd tot de rapportage van het bedrijfsonderdeel omhoog de organieke lijn in. Omdat elke scope heeft nagedacht hoe de rapportages die betrekking hebben op haar verwachtingen moeten worden geaggregeerd tot rapportages over de eigen verplichtingen, kan uiteindelijk voor het bedrijf als geheel over alle verplichtingen worden gerapporteerd, en kan bovendien worden onderbouwd met rapportages uit alle hoeken en gaten van de organisatie, waarop de rapportage is gebaseerd.

Discussie

Doordat de voorgestelde werkwijze werkt met meerdere scopes wordt het mogelijk om taken aan scopes te binden en daardoor overzichtelijk en behapbaar te maken. Zowel in onderzoek als in de praktijk zoeken we nog naar een scopetypologie - dat zijn generieke afbakeningen voor systemen, applicaties, gebouwen en dergelijke. Voor elk type scope die we goed kunnen karakteriseren, moet het mogelijk zijn om lijsten van verplichtingen (risico's) en verwachtingen (dreigingen) te maken die voor elke scope van zo'n type relevant zouden kunnen zijn Het hebben van zulke lijsten zou niet alleen RM, maar ook contractmanagement vergemakkelijken. Ook zijn zulke lijsten uitermate nuttig om gebruikt te worden in geautomatiseerde ondersteuning daarvan. In de praktijk lukt dit tot nog toe slechts gedeeltelijk. Een verklaring hiervoor kan zijn dat deze werkwijze toch een heel ander denk- en werkpatroon vereist en de ervaring leert dat zulk soort veranderingen lastig zijn te realiseren binnen organisaties.

We zien dat mensen het lastig vinden hun gedachten, ideeën en zorgen te begrenzen tot één scope. Vanuit de geschiedenis is dit te verklaren doordat niemand goed overzicht had en wie zijn risico's wilde managen dus heel goed moest weten wat al die anderen aan het doen waren. Dat deze scepsis niet zonder meer zal worden afgelegd is dan ook heel begrijpelijk. Geautomatiseerde ondersteuning kan op verschillende manieren nuttig zijn. Zo kan het in de gaten houden dat risico's uit de scopes automatisch worden gepropageerd

als dreigingen binnen afhankelijke scopes. Er kan in de gaten gehouden worden welke geïdentificeerde dreigingen nog niet van een risico-inschatting zijn voorzien, hetgeen bij de scope-eigenaar op een 'to-do' lijst terecht komt. Ook kunnen automatisch managementrapportages worden gegenereerd. Door die als webservices te ontsluiten kan een manager niet alleen op elk moment zien wat de overallstatus van zijn risico's is (groen-geel-rood), maar ook wat de onderbouwing hiervoor is. Tenslotte kunnen managers ook in de gaten houden of de hoeveelheid 'onaf werk' binnen de perken blijft. Mocht de hoeveelheid 'onaf werk' te groot worden, dan kan gericht worden bijgestuurd omdat duidelijk is waar het werk gedaan moet worden. Geautomatiseerde ondersteuning kan ook helpen bij de risico-inventarisatie door voor vaak voorkomende scopes standaard dreigingenlijsten en samenhangen tussen risico's te definiëren zodat deze niet steeds opnieuw bedacht hoeven worden. Dit kan ook helpen bij het onderbouwen van voorstellen voor managementbesluiten.

Conclusies

We hebben een werkwijze voorgesteld voor schaalbaar risicomanagement dat zich kenmerkt door de overzichtelijke en heldere scope-afbakeningen, waarbij de scopes niet groter zijn dan menselijkerwijs is te overzien. Door risicomanagement per scope in te richten blijven de uit te voeren taken overzichtelijk en dus behapbaar. Door de samenhang tussen de scopes expliciet te maken kan risicomanagement over ketens heen, dat wil zeggen bedrijfsbreed (of zelfs over bedrijfsgrenzen heen) zodanig worden gerealiseerd dat niet alleen steeds kan worden nagegaan hoe groot risico's zijn, maar ook wat daar de grondslagen van zijn. Voor het hanteren van deze samenhangen is geautomatiseerde ondersteuning nodig (en mogelijk) waarmee het bovendien mogelijk wordt om (near) real-time aan betrokkenen te signaleren welk werk hij of zij nog moet doen en om soortgelijk overzichten te genereren die management de mogelijkheid bieden erop te sturen dat dit werk ook daadwerkelijk wordt gedaan.

Referenties

[Anderson95] J.R. Anderson: *"Learning and Memory: an integrated approach"*, John Wiley & Sons, 1995, ISBN 0-471-11596-7

[AS/NZS4360] Standards Australia and Standards New Zealand (2004): AS/NZS 4360:2004, *"Risk Management"*, Sydney, NSW.

[IEC61025] Fault Tree Analysis. Edition 2.0. International Electrotechnical Commission. 2006. IEC 61025. ISBN 2-8318-8918-9.

[ISO31000] ISO 31000:2009: *"Risk Management - Principles and Guidelines"*,

[Miller56] George A. Miller: *"The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information"* The Psychological Review, 1956, vol. 63, pp. 81-97

[NIST02] Gary Stoneburner, Alice Goguen, and Alexis Feringa: *"Risk Management Guide for Information Technology Systems"*, National Institute of Standards and Technology, Special Publication 800-30, July 2002

[PWC08] CIO - PriceWaterhouseCoopers (Kim S. Nash): *"The Global State of Information Security 2008"* www.csoonline.com/article/454939/the-global-state-of-information-security-2008

[Reason90] Reason, J. *"Human error"* New York: Cambridge University Press, 1990

[SEI93] Marvin J. Carr e.a.: *"Taxonomy-Based Risk Identification"*, Technical Report CMU/SEI-93-TR-6, ESC-TR-93-183, Software Engineering Institute, Juni 1993