Risicomanagement

Toepassing van de NIST 800-30 op een primair proces

Scriptie ter afronding van de post-graduate opleiding IT-audit aan de Vrije Universiteit te Amsterdam

Jan Otto Dijkstra
Rico Dijkstra

Leeuwarden, september 2008
Vrije Universiteit Amsterdam
FEWEB, afdeling IT-audit

Voorwoord

Ter afsluiting van de Postgraduate IT Audit opleiding aan de Vrije Universiteit van Amsterdam hebben wij deze scriptie geschreven. In de scriptie moet een probleem of vraagstuk uit de dagelijkse praktijk op academisch verantwoorde wijze uitgewerkt worden. Wij hebben een scriptie geschreven met als onderwerp de toepassing van de NIST 800-30 als risicoanalyse methode. Hieraan gekoppelde aandachtspunten zijn geënt op de toepasbaarheid van deze methode op een proces met een stelsel van gebruikers controls, applicatieve controls en general IT controls.

Gezien de actualiteit van het onderwerp Risicomanagement en de toenemende vraag om een goede risicoanalysemethode in te zetten, vinden wij dit een interessant onderwerp om onze scriptie over te schrijven.

Vanuit de Vrije Universiteit Amsterdam is de heer Cees Coumou aangewezen als onze afstudeerbegeleider. Wij willen hem bedanken voor de goede inhoudelijke ideeën, zijn uitleg en het doorlezen van onze stukken. Zijn enthousiasme en vakkundig inzicht hebben ons geholpen in het opleveren van dit uiteindelijke resultaat.

Wij willen onze bedrijfsbegeleider Marco Benda bedanken voor de opstartfase van de scriptie en het meelezen en adviseren tijdens onze uitvoerende fase.

Ten slotte willen we de docenten bedanken voor de leerzame colleges van de afgelopen drie jaar. Dit alles heeft ons geholpen bij het schrijven van deze scriptie, maar ook bij het verbreden van onze vakkennis op het gebied van EDP auditing.

Jan Otto Dijkstra
Rico Dijkstra

Leeuwarden, september 2008

Leeswijzer

Deze scriptie bevat een aantal hoofdstukken. Wij hebben geprobeerd de hoofdstukken elkaar zo logisch mogelijk te laten opvolgen.

In hoofdstuk 1 staat de Samenvatting beschreven en in hoofdstuk 2 de Inleiding. Hoofdstuk 3 behandelt de hoofdvraag en onderzoeksvragen en de methode van onderzoek. In hoofdstuk 4 behandelen we de theorie van risicomanagement, de toepassing van risicomanagement en – analyse bij de organisatie OrgaQ en de risicoanalyse methode NIST 800-30. In hoofdstuk 5 worden de risicoanalyse methoden bij OrgaQ en de NIST 800-30 geanalyseerd en de bevindingen besproken en in hoofdstuk 6 worden de aanbevelingen beschreven. In Hoofdstuk 7 wordt de conclusie behandeld en de hoofdvraag beantwoord.

Inhoudsopgave

Hoofdstuk
1

Samenvatting

De NIST 800-30 omvat een risicoanalyse die een structuur verschaft voor de ontwikkeling van een effectief risico management programma dat zowel de definities als de praktische ondersteuning biedt voor het beoordelen en mitigeren van risico's geïdentificeerd binnen IT-systemen. Het ultieme doel is om organisaties te helpen bij het beter besturen van hun IT-gerelateerde missie risico's. Organisaties kunnen daarbij kiezen om de uitgebreide processen en stappen in de NIST 800-30 uit te breiden of juist te verkleinen en deze dusdanig aan te passen dat ze passen in hun omgeving voor het beheersen van IT-gerelateerde missie risico's.

In dit scriptieonderzoek hebben we willen vaststellen of de risicoanalyse aanpak volgens NIST 800-30 toepasbaar is op een proces met een stelsel van gebruikers controls, applicatieve controls en general IT controls. Hierbij is het primaire proces bij OrgaQ als toegepast proces genomen. Geanalyseerd is hoe de huidige risicoanalyse methode bij OrgaQ zich verhoudt tot de methode NIST 800-30 en in hoeverre er voldaan is aan de doelstellingen die de proceseigenaar aan het primaire proces stelt inzake risicoanalyse. Daarbij is gekeken naar overeenkomsten en verschillen, wat voor effect de verschillen hadden op de uitkomst en wat de oorzaak hiervan was.

Daarbij is gebleken dat de stappen die uitgevoerd worden door beide methoden goed te vergelijken zijn. De NIST kent wel meer structuur met een duidelijke in- en output. De analyse maakt inzichtelijk dat de stappen goed uitwisselbaar zijn. Het doel van de stappen is in beide methoden vergelijkbaar, de manier om tot het doel te komen verschilt. Daarmee is aangegeven dat de structuur van de NIST 800-30 ook toepasbaar is op de relevante aandachtsgebieden van het primaire proces OrgaQ.

Met het combineren van de naar voren gekomen sterke punten van beide methoden zouden de doelstellingen die de proceseigenaar stelt aan het primaire proces inzake risicoanalyse met grotere zekerheid gerealiseerd kunnen worden. Het combineren van beide methoden zou dan leiden tot een methode met een duidelijke structuur, geënt op de relevante aandachtsgebieden voor het primaire proces OrgaQ, met de juiste diepgang en met een goede basis voor het ontwikkelen van risicobewustzijn bij de betrokken medewerkers.

Hoofdstuk
2

Inleiding

Een belangrijk element van modern risicomanagement is een integrale benadering van risico's. Dat wil zeggen dat alle typen risico's van een organisatie (of business unit, proces etc.) tegelijkertijd in ogenschouw worden genomen. Dit in tegenstelling tot meer traditionele vormen van risicomanagement die veelal zijn gericht op specifieke risicogebieden (bijv. verzekeringsrisico's, ARBO). Er zijn vele bronnen van risico, zowel binnen de organisatie als extern, die elkaar bovendien beïnvloeden. Het is daarom verstandig om op integrale wijze de interne en externe omgeving te blijven monitoren op mogelijke gebeurtenissen die van invloed kunnen zijn op het behalen van de doelstellingen van de organisatie[1].

Daarbij staat de IT-auditor voor een nieuwe rol. Volgens Paans (2008) heeft IT-audit de aansluiting met de klant verloren. Het overgrote deel van de opgeleverde rapportages levert niet de verwachte meerwaarde op voor de klant. Er is te weinig begrip voor de cultuur bij management en omgeving, er is onvoldoende inzicht in de werkelijke eisen die moeten worden gelegd op de technische en organisatorische infrastructuur, er zijn geen adequate methoden en technieken voor zorgvuldige oordeelsvorming en er wordt niet geredeneerd vanuit de echte risico's voor de ondersteunde bedrijfsprocessen.[2]

De bestuurder realiseert de doelstelling en missie van de organisatie met een afweging van de risico's. Daarbij staat risicomanagement centraal (vanuit marktpositie, bedrijfsprocessen et cetera.). Hij maakt zich zorgen over risico's, maar veel breder dan alleen die van IT. Er is dus behoefte aan een goed onderbouwde risico-inschatting die veelsoortige risico's betreft. Daarbij is inzicht nodig in de omgeving van de bestuurder: markt, processen, zakenrelaties, stakeholders, concurrenten, toezichthouders, compliance, kwetsbaarheden et cetera. Dit resulteert in het begrip voor wat hun echte zorgen zijn, en welke echte risico's zij lopen.

De eerste stap voor de nieuwe IT-auditor is dan ook de business van de klant in kaart te brengen met het gehele krachtenspel. Daarbij hoort een risicoanalyse, vanuit de rol van de bestuurder en vanuit de risico's die de bestuurder loopt. Er zijn goede methoden, zoals de NIST 800-30, echter heeft de methode vaak gebrek aan goede input op het punt van bedreigingen. Nu wordt vaak gesproken over een aardbeving, een overstroming, een brand, uitval server et cetera. Maar waar vooral bedreigingen van in kaart moeten worden gebracht zijn: marktpositie, omzet, winst, tevredenheid klanten en stakeholders et cetera.

De NIST 800-30 is een risicoanalyse methode ontwikkeld om bedreigingen op IT gebied te analyseren. In deze scriptie beantwoorden we de vraag of de NIST 800-30 toepasbaar is op een willekeurig proces. Het gekozen proces is een primair proces met een stelsel van gebruikers controls, applicatieve controls en general IT controls, waarbij de proceseigenaar een aantal doelstellingen heeft geformuleerd betreffende risicoanalyse. Indien de NIST 800-30 kan voldoen aan deze doelstellingen, zal met deze toepasbaarheid het inzicht worden verschaft dat de NIST 800-30 ontwikkelt kan worden tot een methode voor risicoanalyse gericht op business en IT.

1 Risicomanagement, de praktijk in Nederland. Herziene uitgave, 2006
2 Presentatie Ronald Paans, IT-auditor, repressief of juist preventief optreden? Vurore Seminar april 2008

Hoofdstuk
3

Vraagstelling

3.1 Hoofdvraag en onderzoeksvragen

Vanuit het onderwerp Risicomanagement en de NIST 800-30 hebben we de volgende onderzoeksvraag samengesteld:

“Is de aanpak van risico management volgens NIST 800-30 toepasbaar op een proces met een stelsel van gebruikers controls, applicatieve controls en general IT controls?”

Om antwoord te geven op deze onderzoeksvraag worden de volgende deelvragen beantwoord:

- Wat is risicomanagement volgens NIST 800-30?
- Hoe wordt in de huidige situatie risicomanagement uitgevoerd?
- Wat zijn de verschillen tussen de huidige aanpak en die van NIST 800-30, waar worden deze door veroorzaakt en welk effect hebben deze op de uitkomsten van het proces?
- In hoeverre biedt de NIST 800-30 toegevoegde waarde in de vorm van een gestructureerde aanpak en inhoudelijk relevante aandachtsgebieden voor risicomanagement?
- Hoe kan de NIST 800-30 als aanpak voor risicomanagement worden ingepast in het primaire proces van OrgaQ?

Hoofddoelstelling van het afstudeeronderzoek is het onderbouwen van de stelling dat risico management volgens NIST 800-30 toepasbaar is op een proces met een stelsel van gebruikers controls, applicatieve controls en general IT controls.

Als casus zal het primaire proces bij OrgaQ fungeren. Daarbij is het uitgangspunt dat deze casus in de scriptie niet herleidbaar is naar de werkgever.

3.2 Methode van onderzoek

Door middel van een uitgebreide literatuurstudie, interviews met de beschrijfcoach bij OrgaQ (de heer Marco Benda), de riskmanager bij OrgaQ, senior analisten en de proceseigenaar van het door ons bestudeerde proces (de heer Wopke Jorritsma), discussies met de scriptiebegeleider (de heer Cees Coumou) en het bestuderen van de toegepaste Risicomanagementmethode bij OrgaQ, en natuurlijk onze eigen kennis en inzichten, hebben we deze scriptie samengesteld.

Bij het toepassen van de onderzoeksmethode voor het verzamelen van informatie hebben we ons in eerste instantie laten leiden door de vraag: wat willen we eigenlijk te weten komen? Dat heeft geleid tot een expliciete vraagstelling met subvragen. De tweede vraag die we ons stelden was of we genoeg basisinformatie hadden. Onze indruk was dat dit wel deels aanwezig was, maar de informatie uit de praktijk onvoldoende was. Op basis van deze vraag

en de vraag of we al genoeg basisinformatie hadden hebben we besloten om deels kwalitatief onderzoek toe te passen in dit onderzoek. Dit in de vorm van het vrije interview waarbij het doel was om vooraf een bepaald kader te definiëren, waarbinnen het gesprek diende te blijven, maar afhankelijk van de wending die het gesprek nam, konden andere vragen gesteld worden.

In figuur 1 staat schematisch weergegeven hoe het onderzoek is gedaan. In de toelichting wordt één en ander verduidelijkt, bovendien staat hier een verwijzing naar het hoofdstuk/de paragraaf in de scriptie waarin dit is uitgeschreven.

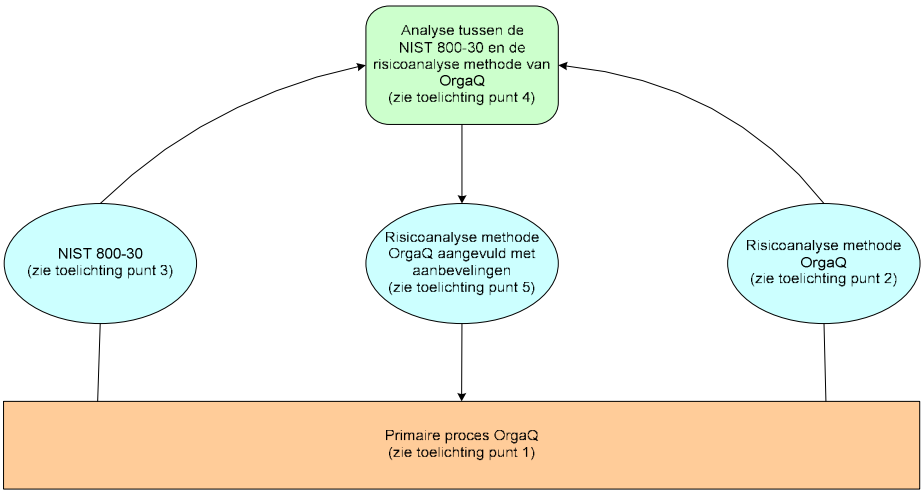

Fig. 1 Onderzoeksmethode

Toelichting figuur 1:

1. Het primaire proces moet minimaal een stelsel van gebruikers controls, application controls en general IT controls. Zie paragraaf 4.2.

2. De risicoanalyse methode die door het primaire proces bij OrgaQ wordt gebruikt, dient te worden beschreven. Zie paragraaf 4.2.

3. De NIST 800-30 dient in kaart te worden gebracht en daarbij aangeven of er in de NIST 800-30 aandacht wordt besteed aan gebruikers controls, application controls en general IT controls. Zie paragraaf 4.3.

4. Als de stappen 1 t/m 3 zijn doorlopen kan er een analyse worden gedaan betreffende de verschillen en/of overeenkomsten tussen de risicoanalyse methode bij OrgaQ en de NIST 800-30. De bevindingen betreffende de analyse dienen te worden beschreven. Zie hoofdstuk 5.

5. N.a.v. de bevindingen zijn aanbevelingen geven. OrgaQ kan de huidige methode aanpassen n.a.v. de aanbevelingen. Zie hoofdstuk 6.

Hoofdstuk
4

Risicomanagement

Corporate Governance (behoorlijk bestuur en toezicht) is inmiddels een niet meer weg te denken begrip. Een onderdeel van corporate governance is een goede interne beheersing. Het middel om te komen tot een adequaat systeem van interne beheersing is risicomanagement. Organisatie Q (verder OrgaQ) opereert in een dynamische omgeving waar sprake is van toenemende concurrentie en kritische consumenten. Ontwikkelingen op het vlak van ICT en internet spelen hierbij een belangrijke rol. Daarnaast is er de toename en complexiteit van huidige en toekomstige wetgeving die ook de nodige consequenties heeft voor inrichting van processen. Al deze ontwikkelingen en wettelijke eisen hebben gemeen dat ze gevolgen hebben voor de inrichting van de interne beheersing (processen) en de wijze waarop de organisatie omgaat met risico's. Risicomanagement draait om het beheersen van risico's die het bereiken van de organisatiedoelstellingen in gevaar kunnen brengen.

OrgaQ betreft een zorgverzekeraar. Binnen deze organisatie is er sprake van een tweetal primaire processen. Het ene proces betreft een proces waarbij het contactbeheer met de klant centraal staat. Het primaire proces welke gebruikt is voor dit onderzoek is een proces welke gericht is op de behandeling en administratieve afhandeling van claims. De claims worden voor ongeveer 85% elektronisch aangeboden en afgehandeld en ongeveer 15% wordt via papieren nota's aangeboden en handmatig in het schadesysteem gebracht. De elektronisch aangeboden declaraties worden geheel door het systeem gecontroleerd, achteraf wordt er door analyses nagegaan of er ook misbruik plaatsvindt. De papieren nota's worden door zowel een medewerker als het systeem gecontroleerd. De proceseigenaar heeft de beschikking over een team procesondersteuning, dit team is o.a. verantwoordelijk voor de kwaliteit en beheersing van het proces. Activiteiten zijn het onderhoud van de procedures, bewaking en toetsen van de kwaliteit, opstellen en doen van risicoanalyses, nagaan of de systeemcontroles volledig en juist zijn. Een stelsel aan gebruikers controls, applicatieve controls en general IT controls zorgen ervoor dat kwaliteit gewaarborgd wordt.

4.1 Wat is risicomanagement?

Onder risicomanagement [3]wordt verstaan:

'het bewust, integraal en dynamisch onderkennen van alle gevaren en het streven naar een permanent en evenwichtig pakket van maatregelen om die gevaren
te beperken tot een voor het management aanvaardbaar (kosten)niveau.'

Door middel van risicomanagement is het voor de organisatie mogelijk om beslissingen te nemen die gericht zijn op het voorkomen of minimaliseren van de nadelige effecten die het optreden van risico's met zich mee kunnen brengen. Op deze manier wordt risicomanagement toegepast als stuurinstrument.

Met risicomanagement wordt een aantal zaken beoogd:

[3] Handboek EDP-auditing, B.4.1.4. Interne controleplan (Bewerkt door Prof. H.B. Moonen RA)

- Continue risico's expliciet maken en beheersen;
- Risicoalertheid creëren;
- Pro-actief met risico's omgaan in plaats van reactief;
- Bewust met risico's omgaan en bijbehorende beheersmaatregelen afwegen.

Het doel van Risicomanagement is de organisatie te ondersteunen in het bereiken van haar bedrijfsdoelstellingen.[4] Dit impliceert het vormen van een integraal beleid. Hierdoor wordt de kans dat risico's gemist worden kleiner en doordat er integraal inzicht verkregen wordt in risico's en beheersmaatregelen ontstaat synergie en efficiency.

Door middel van het implementeren van risicomanagement kan door de organisatie het volgende worden bereikt:[5]

- Een betere beheersing van risico's;
- Betere waarborging van het bereiken van de gestelde organisatie doelstellingen;
- Het kunnen stellen van prioriteiten op basis van de risico's; door een risico analyse ontstaat inzicht in de belangrijkste, meest risicovolle onderwerpen;
- Het ondersteunen van een beslissing; het uitvoeren van een risicoanalyse kan helpen om te komen tot een keuze;
- Aansluiting op het procesdenken in de organisatie;
- Bewust, transparant en gestructureerd omgaan met risico's.

Er is wel een aantal voorwaarden verbonden aan het succesvol implementeren van risicomanagement:

- Risicomanagement wordt pas effectief als managers verantwoordelijk zijn voor risico's op alle niveaus in de organisatie, als onderdeel van integraal management;
- Risicomanagement moet aansluiten bij de bestaande werkwijze;
- Risicomanagement is de verantwoordelijkheid van iedereen. Iedereen is verantwoordelijk voor het signaleren van risico's en treffen van maatregelen voor de risico's die binnen dienst verantwoordelijkheid vallen;
- Ontwikkeling en bepaling van een risicotolerantie (risk appetite). De bereidheid om ook risico's te accepteren. De tone at the top is hierbij essentieel.

Natuurlijk zijn er ook valkuilen, we lichten er één belangrijke uit. De kans bestaat dat er teveel risicomijdend gedrag ontstaat, waardoor de ondernemingsgeest wordt verkleind en de snelheid van reageren door de organisatie wordt vertraagd. Ook kan risicomijdend gedrag leiden tot het doorschieten in het treffen van beheersingsmaatregelen. Van belang is om een juiste balans te vinden tussen risicomijdend gedrag in relatie tot de vier strategieën: het mitigeren, het overdragen, het vermijden of simpelweg het accepteren van het risico. De ruggengraat van het risicomanagement is de risicoanalyse. Risicoanalyse is[6]:

'Risicoanalyse is het op systematische wijze onderkennen, inventariseren en evalueren van maatregelen tegen mogelijk optredende ongewenste gebeurtenissen, zodat hieruit gemotiveerde conclusies kunnen worden getrokken.'

Risicoanalyse helpt onzekerheid om te zetten in inzicht. Daarmee kan een beslissing worden genomen. De formule is eenvoudig en bekend: Risico = Kans x Gevolg x Gevoeligheid. Het gaat er nu om de formule op een of andere manier zo toe te passen dat er bruikbare resultaten uit komen. Liefst verifieerbaar en controleerbaar.[7]

[4] KPMG. Educatiemateriaal juni 2008
[5] KPMG. Educatiemateriaal juni 2008
[6] Inleiding EDP-auditing, Jan van Praat, Hans Suerink, 2001
[7] Cees Coumou. Het proces van risicomanagement als uitgangspunt. 2003

Overigens welke methode ook gebruikt wordt, het blijft altijd eerder een kwestie van schatten en waarderen van risico's dan een kwestie van meten. Welke methode het meest geschikt is, hangt af o.a. van het doel van de analyse, de karakteristieken van het betrokken beleidsveld, het beschikbare tijdpad en de beschikbare expertise[8].

4.1.1 Risicomanagement bij OrgaQ

Het beheersen van risico's bij OrgaQ is primair de verantwoordelijkheid van de proceseigenaren en hoofden. Om dit voldoende te waarborgen en de verantwoordelijkheden helder te maken is inrichting van de interne beheersing volgens het principe van de drie beheersingslinies best practice. Dit principe wordt door OrgaQ gehanteerd. Hierbij sluiten de control- activiteiten goed op elkaar aan en worden doublures voorkomen. In figuur 2 is de beheersingsstructuur qua verantwoordelijkheden verder uitgewerkt.

Drie beheersingslinies

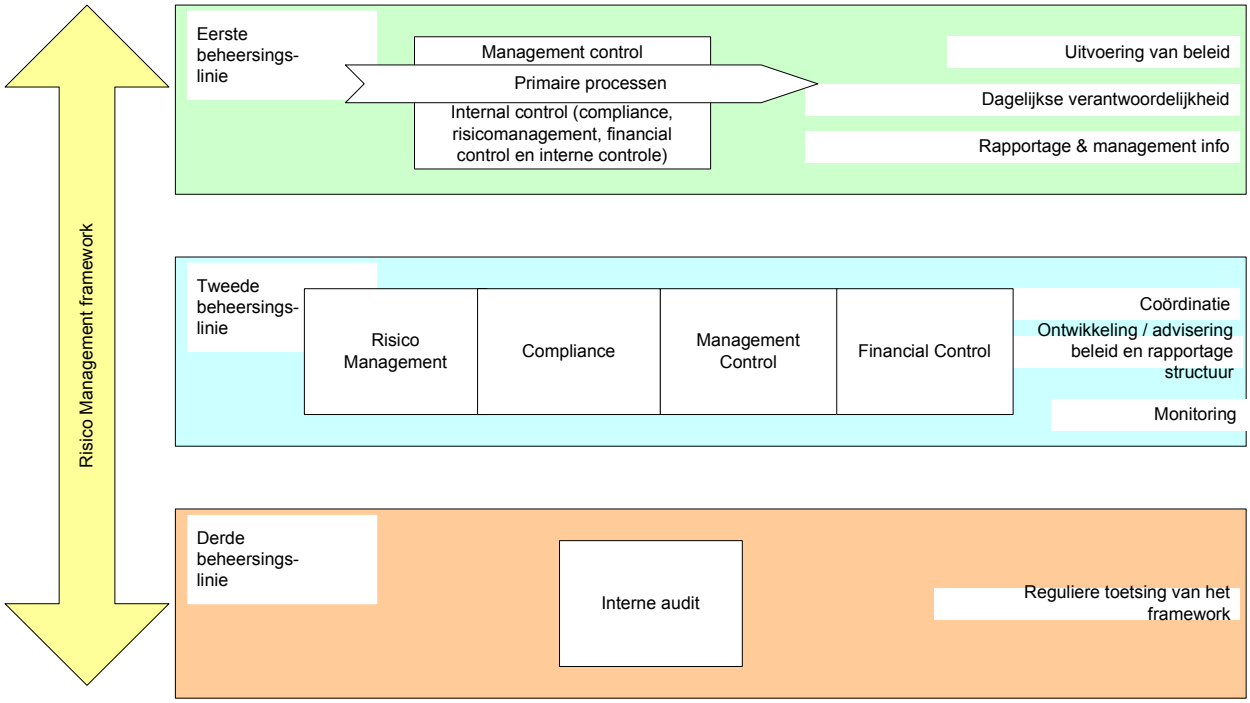

Fig. 2 Drie beheersingslinies bij OrgaQ

Eerste beheersingslinie
Om de naleving van wet- en regelgeving, ondernemingsdoelstellingen, kwaliteit processen en betrouwbare verslaggeving te waarborgen worden beheersmaatregelen getroffen. Deze AO/IC maatregelen maken onderdeel uit van het (administratieve) proces. Voorbeelden hiervan zijn functiescheiding en visuele- en systeemcontroles. De uitvoering is de verantwoordelijkheid van de proceseigenaar.

De proceseigenaar heeft tevens de verantwoordelijkheid om toe te zien op de werking van de beheersmaatregelen. Internal control is het proces bedoeld om hier redelijke zekerheid over te verschaffen. Hierbij kan gedacht worden aan de interne (formele) controle zoals die

8 Zicht op risico's, Handboek Risicoanalysemethodieken" (geschreven door Berenschot i.s.m. de TU Delft, in opdracht van het ministerie van Economische Zaken, februari 2006).

belegd is bij de TPO's (de primaire processen hebben de beschikking over een ondersteuningsteam die Team Proces Ondersteuning worden genoemd), maar ook risicomanagement en financial control. Management control is het geheel van maatregelen dat redelijke zekerheid moet bieden dat de door het management gestelde doelen worden bereikt. Over het bereiken van de gestelde doelen wordt gerapporteerd.

Tweede beheersingslinie
Deze functies zijn verantwoordelijk voor coördinatie, ontwikkeling van en advisering omtrent het te voeren beleid. Hier is het overzicht van geldende wetgeving c.q. normen, welke processen (proceseigenaren) dit raakt en wat de getroffen beheersmaatregelen zijn. Daarnaast wordt op basis van het Enterprise Risk Management model (ERM-COSO II) gefaciliteerd bij het gestructureerd in kaart brengen en beheersen van de (belangrijkste) risico's. Een belangrijk aspect vanuit het ERM is de monitoring. Hierbij wordt in principe gebruik gemaakt van de internal control activiteiten en rapportage van de eerste linie.

Derde beheersingslinie
Interne audit is verantwoordelijk voor toetsing van de werking van het ERM-COSO II framework. Feitelijk systeemgericht, waarbij de focus ligt op de toepassing van de elementen van het framework en de kwaliteit van de interne beheersstructuur, de basis voor monitoring van de werking van beheersmaatregelen. De resultaten van de audits zijn derhalve een belangrijke bron van informatie voor management control, financial control en de compliance & risk officer uit de 2^{e} beheersingslinie.

4.2 Risicomanagement bij het primaire proces

4.2.1 Achtergrond

OrgaQ is conform het typologiemodel van Starreveld een financiële dienstverlener. Het primaire proces welke is gebruikt voor dit onderzoek is één van de twee primaire processen binnen deze organisatie. Dit proces bezit/maakt gebruik voor de beheersing een stelsel van:

- *general IT-controls*, hierbij kan onder andere gedacht worden aan de ITIL processen (zoals bijvoorbeeld Changemanagement), logische toegangsbeveiliging en fysieke toegangsbeveiliging.

- *application controls*, zoals onder andere geautomatiseerde controles en logging van transacties/wijzigingen.

- *gebruikers controls*, zoals onder andere functiescheidingen en beschrijving AO/IC.

Dit primaire proces heeft een eigen ondersteuningsteam (TPO) dat via risicomanagement en eventuele maatregelen betreffende restrisico's de proceseigenaar een in control statement geeft.

De activiteiten die binnen dit primaire proces plaatsvinden zijn financiële activiteiten, waarbij een uitgebreide wet- en regelgeving op van toepassing is. Het stelsel van beheersmaatregelen is er met name gericht op compliant zijn en kostenbeheersing. De omzet van dit proces zal in 2008 de één miljard benaderen. Jaarlijks wordt door het ondersteuningsteam een aanzienlijke besparing behaald. Deze besparing zit voor het grootste deel in de applicationcontrols en voor een kleiner deel in aanvullende controles achteraf.

De risicoanalyseactiviteiten binnen het genoemde proces, maken onderdeel uit van operational riskmanagement. Er wordt geen gebruik gemaakt van een beschreven methode. De methode die gebruikt wordt is een methode vanuit logisch denken. Vastlegging van het risicomanagement

wordt gedaan in Excel. De risicoanalyses worden eens per jaar uitgevoerd en vormen o.a. de basis van controleplannen. Bij wijzigingen in de procedures en de wet- en regelgeving gedurende het jaar worden er risicoanalyse uitgevoerd.

In figuur 3 is het verband aangegeven tussen het geselecteerde primaire proces en de elementen van het risicomanagement framework.

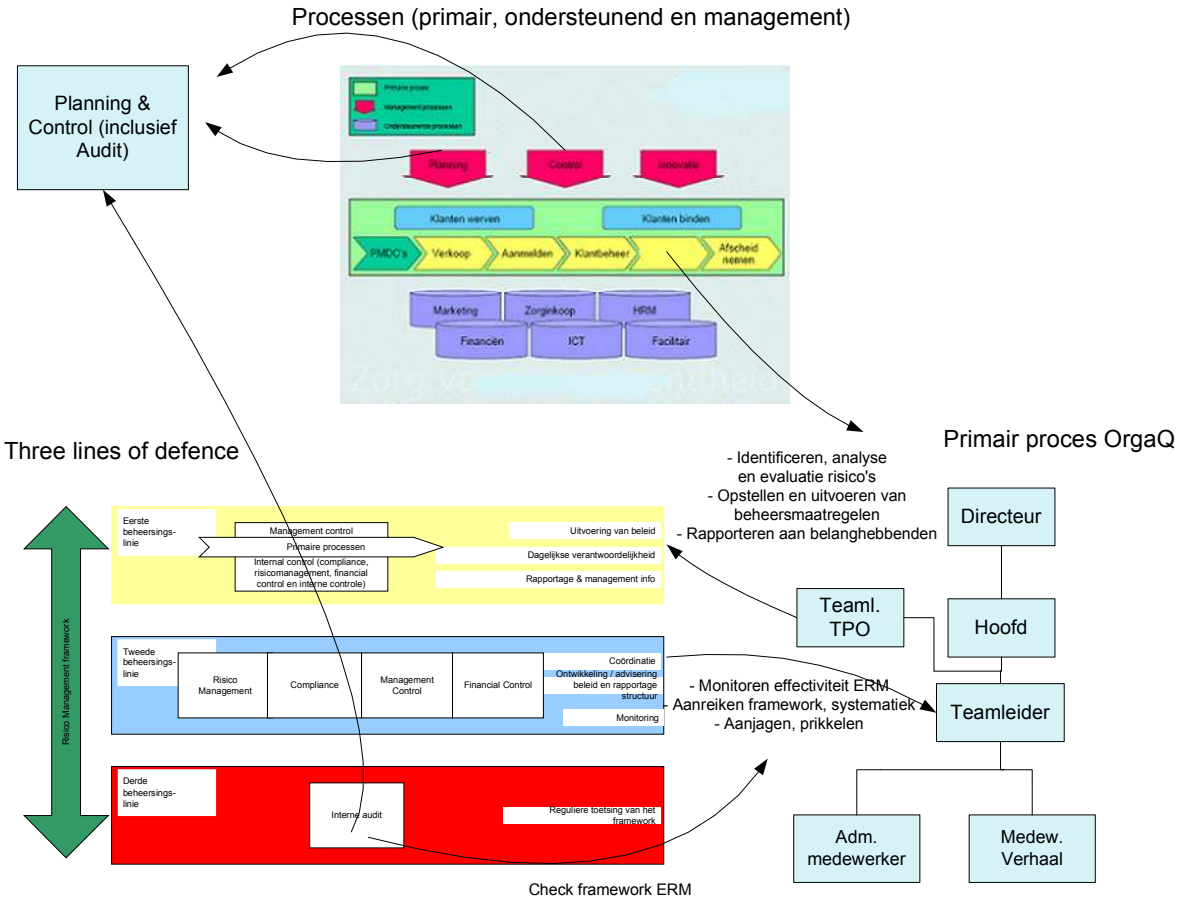

Fig. 3 Verband geselecteerde primaire proces en het risicomanagementframework

4.2.2 Doel van risicomanagement bij het primaire proces

De proceseigenaar heeft betreffende het risicomanagement een duidelijke visie. Hij wil namelijk een integrale aanpak voor de beheersing van het proces. Een directe koppeling tussen risicomanagement met alle binnen OrgaQ aanwezige beheersmaatregelen. Hij wil dat de beheersing van zijn proces continue is.

Er moet volgens de proceseigenaar meer aandacht komen voor de focus en de samenhang met het risicomanagement van andere primaire processen en ondersteunende processen. Hij wil graag inzicht in wat nu precies wat raakt, en wat daar de risico's bij zijn. Daarnaast wil hij graag (meer) zekerheid hebben volledig te zijn in de reikwijdte van risicoaanpak en het benoemen van de risico's.

Risicomanagement en de bijbehorende maatregelen dienen actueel te zijn. De voorkeur geniet dat er meer proactief risicomanagement wordt toegepast. Ook wil hij meer bewustzijn creëren bij de werknemers op het gebied van risicomanagement. Dat wil zeggen dat het natuurlijker wordt

dat de werknemers binnen het primaire proces bij de uitoefening van hun werk ook denken in risico's en de gevolgen daarvan.

Dit alles in het kader van het belang van de proceseigenaar om zijn gestelde doelen te halen, waarbij hij niet gehinderd wordt door negatieve gebeurtenissen. De proceseigenaar wil graag de mate van onzekerheid verminderen door meer inzicht te krijgen in de onzekerheden binnen zijn proces. Op basis van dit inzicht kan hij prioriteren en keuzes maken.

Dit leidt tot het volgende doel van risicomanagement bij het primaire proces:

"Het doel van het uitvoeren van risicomanagement is om bij te dragen aan de beheersing van het primaire proces om aan de procesdoelstellingen te voldoen door (1) proactief risicomanagement toe te passen op het primaire proces dat (2) op een eenduidige wijze wordt toegepast binnen het primaire proces, waarbij (3) volledigheid van de relevante risico's wordt nagestreefd en (4) dat aansluit op de integrale aanpak van beheersmaatregelen bij OrgaQ. Daarbij wordt risicobewustzijn beschouwd als randvoorwaardelijk (5)".

4.2.3 Beschrijving van het risicoanalyse proces

Hieronder is in figuur 4 grafisch weergegeven hoe binnen het risicomanagement bij het primaire proces de risicoanalyse bij OrgaQ wordt uitgevoerd.

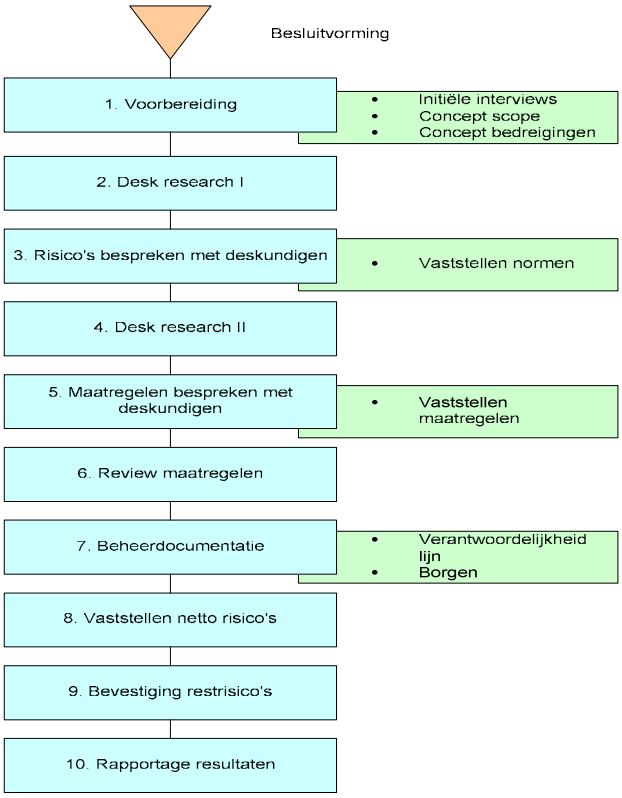

Fig. 4 risicoanalyse bij het primaire proces OrgaQ

Algemeen

De proceseigenaar bepaalt de ruwe scope (zie voorbereiding) en geeft opdracht tot het doen van risicoanalyses. De risicoanalyse wordt gecoördineerd en uitgevoerd door een (senior) Analist bij TPO, hij/zij zal de bij de verschillende stappen gebruik maken van de volgende personen:

leidinggevenden, procesdeskundigen en materiedeskundigen. Het resultaat uit de risicoanalyse (risicomatrices) worden vervolgens vastgesteld door de proceseigenaar. De proceseigenaar bepaalt of risico's al dan niet geaccepteerd worden.

1. Voorbereiding

De risicoanalyse bij het primaire proces wordt ingedeeld in meerdere afgebakende onderdelen. Tijdens de voorbereiding wordt de definitieve scope vastgesteld. Er wordt nagegaan welke wet- en regelgeving van toepassing is. En er wordt nagegaan wat de omvang van het totale risico binnen het afgebakende onderdeel is.

2. Deskresearch I

In deze fase worden de theoretische risico's aan de hand van de wet- en regelgeving (dit bevat wetten alsmede overeenkomsten) benoemd. D.m.v. benchmarking/ toepassing van statistische analyse wordt gezien waar eventuele theoretische risico's liggen. Er wordt in deze fase beoordeeld hoe hoog de theoretische risico's maximaal kunnen zijn.

3. Risico's bespreken met deskundigen

De theoretisch risico's worden besproken met procesdeskundigen en materiedeskundigen. Daarnaast worden er vragen aan deze personen gesteld welke risico's meer voor kunnen komen, hier kan gedacht worden aan risico's gericht op misbruik.

4. Deskresearch II

Nagegaan wordt welke maatregelen dienen te worden genomen/ al zijn genomen om de risico's te mitigeren.

5. Maatregelen bespreken met deskundigen

De maatregelen worden besproken met de bij punt 3 genoemde procesdeskundigen en materiedeskundigen. De maatregelen zullen worden beoordeeld naar haalbaarheid en impact. Met impact wordt bedoeld welke effecten de maatregelen hebben op de strategische belangen van de organisatie en wat de directe/indirecte effecten zijn voor de klant.

6. Review maatregelen

Door middel van analyse zal worden nagegaan of de maatregelen effect zullen hebben om het risico af te dekken.

7. Beheerdocumentatie

De AO/IC en werkinstructies zullen worden aangepast. Indien er een systeemwijziging dient te worden gedaan dan dient het functioneel ontwerp te worden aangepast. In deze fase wordt nagegaan waar aanpassingen moeten worden gedaan.

8. Vaststellen netto risico's

In deze fase wordt beoordeeld wat de kans is dat de theoretisch risico's voorkomen. Wat de realistische schade van de risico's is als er geen (extra) maatregelen worden genomen. In hoeverre huidige maatregelen deze risico's al mitigeren.

9. Bevestiging restrisico's

Uiteindelijk zal worden nagegaan wat het restrisico is als er bijvoorbeeld wel/niet maatregelen zijn genomen.

10. Rapportage resultaten

Periodiek worden resultaten gerapporteerd betreffende de werking van de maatregelen en de monitoring van de restrisico's. Indien restrisico's alsnog hoger uitvallen dan eerder gedacht kan er op deze manier alsnog maatregelen worden getroffen om de restrisico's alsnog te mitigeren. In Excel worden de resultaten van het risicomanagement vastgelegd

4.3 NIST 800-30

The National Institute of Standards and Technology (NIST) is een federale instantie binnen het Amerikaanse departement van Handel en opgericht in 1901. De missie van NIST is het promoten van de innovatieve en industriële concurrentie van de Verenigde Staten (VS) door het verbeteren van onder andere standaards en technologie op manieren die de economische veiligheid bevorderen en de kwaliteit van leven vergroten.

De Information Technology Labaratory (ITL) van de NIST bevordert het economische en publieke welvaren van Amerika door het verschaffen van technische kennis op het gebied van standaarden. ITL ontwikkelt onder andere testen, test methodes, proof-of-concept[9] implementaties en technische analyse om de ontwikkeling en het gebruik van informatie technologie te bevorderen.

Iedere organisatie heeft een missie. In dit digitale tijdperk gebruiken organisaties geautomatiseerde informatiesystemen om hun informatie te verwerken ter ondersteuning van hun missie. Risicomanagement speelt hierbij een voorname rol in het beschermen van de informatiebronnen van de organisatie, en daarmee haar missie, vanuit een IT gerelateerd risico. Een effectief risicomanagement proces is een belangrijk onderdeel van een succesvol IT beveiligingsprogramma. Het voornaamste doel van het risicomanagement proces van een organisatie zou moeten zijn het beschermen van de organisatie en haar vermogen om haar missie uit te oefenen, niet alleen haar IT bezittingen. Daarom zou het risicomanegementproces niet alleen moeten worden beschouwd als een technische functie uitgevoerd door IT experts die het IT-systeem uitvoeren en besturen, maar als een belangrijke management functie van de organisatie.

4.3.1 Doel NIST 800-30

Risicomanagement is het proces van het identificeren van risico, het beoordelen van risico en het nemen van stappen om de risico's te mitigeren tot een acceptabel niveau. De NIST 800-30 verschaft een structuur voor de ontwikkeling van een effectief risico management programma dat zowel de definities als de praktische ondersteuning biedt voor het beoordelen en mitigeren van risico's geïdentificeerd binnen IT-systemen[10]. Het ultieme doel is om organisaties te helpen bij het beter besturen van hun IT-gerelateerde missie risico's. Organisaties kunnen daarbij kiezen om de uitgebreide processen en stappen in de NIST 800-30 uit te breiden of juist te verkleinen en deze

[9] Proof of concept is a short and/or incomplete realization (or synopsis) of a certain method or idea(s) to demonstrate its feasibility, or a demonstration in principle, whose purpose is to verify that some concept or theory is probably capable of exploitation in a useful manner.

[10] NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems. Gary Stoneburner, Alice Goguen1, and Alexis Feringa1, 2002

dusdanig aan te passen dat ze passen in hun omgeving voor het beheersen van IT-gerelateerde missie risico's.

Dit leidt tot het volgende doel van risicomanagement: van de NIST 800-30

"Het doel van het uitvoeren van risicomanagement is om een organisatie in staat te stellen om te kunnen voldoen aan haar missie door het (1) beter beveiligen van IT systemen die bedrijfsinformatie opslaan, verwerken of verzenden en (2) door het management te assisteren in het autoriseren van (de toegang tot) IT systemen op basis van de ondersteunende documentatie die het resultaat is van het uitvoeren van risicomanagement.

De belangrijkste redenen om een risicomanagementproces voor IT-systemen te implementeren zijn het verminderen van negatieve impact voor de organisatie en de behoefte aan een betrouwbare basis voor besluitvorming. Hiervoor dient risicomanagement geheel geïntegreerd te worden in het Systems Development Life Cycle (SDLC). Een SDLC van een IT-systeem heeft vijf fasen: initiatie (initiation), ontwikkeling (development) of aanschaf (acquisition), implementatie (implementation), operatie (operation) of onderhoud (maintenance) en verwijdering (disposal). De risicomanagement methode is dezelfde onafhankelijk van de SDLC fase waarvoor de beoordeling wordt uitgevoerd. Risico management is een iteratief proces dat kan worden uitgevoerd gedurende elke belangrijke fase van de SDLC. In tabel 1 worden de onderscheidingskenmerken beschreven van iedere SDLC fase en laat zien hoe risico management kan worden uitgevoerd ter ondersteuning van iedere fase.

Tabel 1 Integratie van Risicomanagement in het SDLC

SDLC Phases	Phase Characteristics	Support from Risk Management Activities
Phase 1—Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented	• Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2—Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed	• The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design tradeoffs during system development
Phase 3—Implementation	The system security features should be configured, enabled, tested, and verified	• The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation
Phase 4—Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures	• Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)
Phase 5—Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving,	• Risk management activities are performed for system components that will be disposed of or replaced to

	discarding, or destroying information and sanitizing the hardware and software	ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner

4.3.2 Stappen van de NIST 800-30

Het eerste proces in de risicomanagementmethode is risicoanalyse. Organisaties gebruiken risicoanalyse om de hoogte van een mogelijke dreiging en het risico verbonden aan een IT-systeem vast te stellen binnen haar SDLC. De output van dit proces ondersteunt het identificeren van passende maatregelen voor het verkleinen of weghalen van risico gedurende het mitigatie proces. De risicoanalyse methode omvat negen primaire stappen:

- Stap 1 – Typeren van het systeem
- Stap 2 – Identificatie van de dreiging
- Stap 3 – Identificatie van de kwetsbaarheid
- Stap 4 – Control analyse
- Stap 5 – Kans bepaling
- Stap 6 – Impact analyse
- Stap 7 – Risico bepaling
- Stap 8 – Control aanbevelingen
- Stap 9 – Resultaten rapportage

Deze negen stappen worden in paragraaf 3.3.1 tot en met 3.3.9 uitgewerkt. In figuur 5 staat een schematisch overzicht van deze stappen waarbij de input en de output per stap is aangegeven.

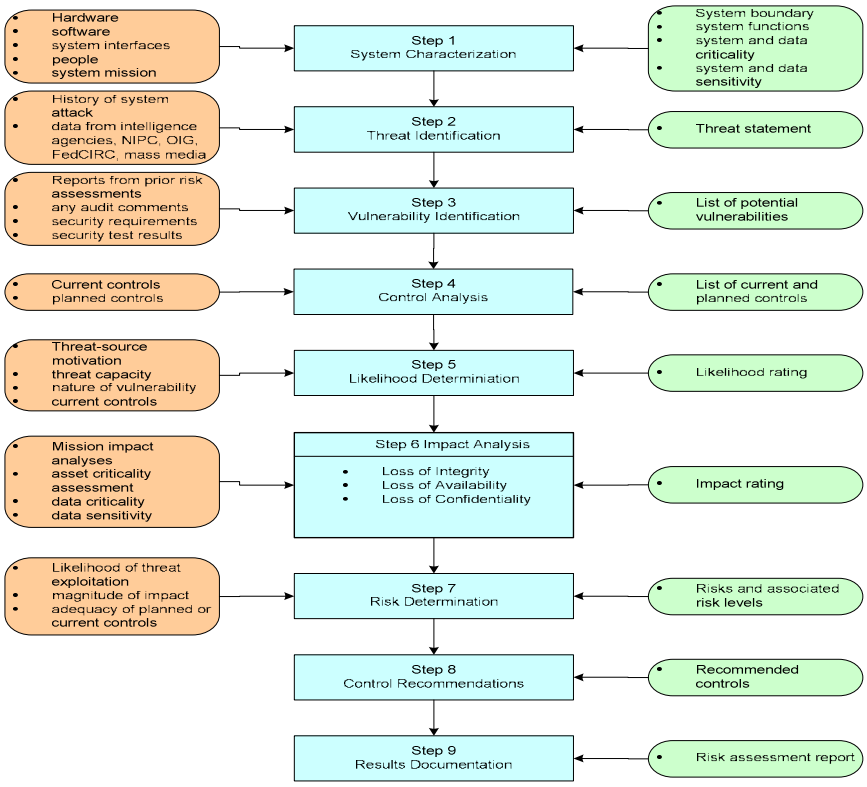

Fig. 5 Stappen NIST 800-30

4.3.2.1 Stap 1 – Typeren van het systeem

Voor het beoordelen van risico's voor een IT-systeem is de eerste stap het definiëren van de scope van dit voornemen. In deze stap zullen de grenzen van het IT-systeem worden geïdentificeerd alsmede met de hulpmiddelen en de informatie die het systeem vormen. De methode beschreven in de NIST 800-30 kan worden toegepast op beoordelingen van alleenstaande of meerdere samenhangende systemen.

Tabel 2 beschrijft de systeemgerelateerde informatie die gebruikt wordt om een IT-systeem en haar operationele omgeving te karakteriseren.

Tabel 2 Systeemgerelateerde en additionele informatie

Systeemgerelateerde informatie
• Hardware
• Software
• System interfaces (e.g., internal and external connectivity)
• Data and information
• Persons who support and use the IT system
• System mission (e.g., the processes performed by the IT system)
• System and data criticality (e.g., the system's value or importance to an organization)
• System and data sensitivity.
Additionele informatie
• The functional requirements of the IT system
• Users of the system (e.g., system users who provide technical support to the IT system; application users who use the IT system to perform business functions)

• System security policies governing the IT system (organizational policies, federal requirements, laws, industry practices) • System security architecture
• System security architecture
• Information storage protection that safeguards system and data availability, integrity, and confidentiality
• Flow of information pertaining to the IT system (e.g., system interfaces, system input and output flowchart)
• Technical controls used for the IT system (e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)
• Management controls used for the IT system (e.g., rules of behavior, security planning)
• Operational controls used for the IT system (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
• Physical security environment of the IT system (e.g., facility security, data center policies)
• Environmental security implemented for the IT system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

Van een systeem dat in de initiatie of ontwerpfase zit, kan systeem informatie worden afgeleid van het ontwikkel - of vereistendocument. Voor een IT-systeem in ontwikkeling is het noodzakelijk om key beveiligings regels en attributen te definiëren voor het toekomstige IT systeem. Voor een operationeel IT-systeem wordt data verzameld over het IT-systeem in haar productieomgeving, inclusief gegevens over systeemconfiguratie, connectiviteit en (niet) gedocumenteerde procedures. De systeembeschrijving kan dan worden gebaseerd op de beveiliging verschaft door de onderliggende infrastructuur of op de toekomstige beveiligingsplannen van het IT-systeem.

4.3.2.2 Stap 2 – Identificatie van de dreiging

Het doel van deze stap is het identificeren van mogelijke bedreigingen en om een rapport met bedreigingen op te stellen met mogelijke bronnen met bedreigingen die van toepassing zijn op het te evalueren IT-systeem. Deze bronnen kunnen natuurlijk, menselijk of uit de omgeving zijn. In tabel 3 zijn deze bedreigingen opgenomen.

Tabel 3: bedreigingen voor IT-systemen

Threat	Source Motivation Threat Actions	Threat
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay,

	Unauthorized data alteration	impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

4.3.2.3 Stap 3 – Identificatie van de kwetsbaarheid

De analyse van de dreiging tot een IT-systeem moet een analyse van de kwetsbaarheden verbonden aan de systeemomgeving bevatten. Het doel van deze stap is het ontwikkelen van lijst met systeem kwetsbaarheden waarvan misbruik gemaakt zou kunnen worden door potentiële bedreigingen.

Aanbevolen methoden voor het identificeren van systeem kwetsbaarheden zijn het gebruik van bronnen gegevens over deze kwetsbaarheden, de kwaliteit het testen van het systeem op veiligheid en de ontwikkeling van een beveiligings vereisten checklist.

Belangrijk in deze fase is dat de typen kwetsbaarheid die voorkomen en de methode nodig om vast te stellen of de kwetsbaarheden aanwezig zijn, gewoonlijk zullen uiteenlopen afhankelijk van de aard van het IT-systeem en de fase waarin het is in de SDLC:

- Indien het IT-systeem nog niet is ontworpen, dan zal de focus van het zoeken naar kwetsbaarheden liggen bij het beveiligingsbeleid van de organisatie, de geplande beveiligings procedures, de definities voor de systeemvereisten en de beveiligings product analyses van de ontwikkelaar of de acquisiteur.
- Bij de implementatie van het IT-systeem dient de identificatie van kwetsbaarheden te worden uitgebreid naar meer specifieke informatie zoals de geplande veiligheidkenmerken beschreven in het beveiligings ontwerp document en de resultaten van de systeemcertificatietest en evaluatie.
- Wanneer het IT-systeem operationeel is dient het proces van identificeren van kwetsbaarheden ook een analyse van de beveiligingskenmerken en – controls van het IT-systeem te omvatten. Naast de procedures die gebruikt worden om het systeem te beschermen.

4.3.2.4 Stap 4 – Control analyse

Het doel van deze stap is het analyseren van de controls die zijn geïmplementeerd, of die gepland staan voor implementatie door de organisatie om de bedreiging ten opzichte van het systeem te verminderen of weg te nemen. Met het overzicht dat er bestaat van de potentiële kwetsbaarheden en de inschatting van de kans dat deze ook daadwerkelijk voor kunnen komen, moet de implementatie van huidige en geplande controls (*waaronder user controls, application controls en general IT controls)* worden overwogen. Bijvoorbeeld een kwetsbaarheid van het systeem zal niet waarschijnlijk worden misbruikt indien er effectieve beveiligings controls zijn die deze kans wegnemen of aanzienlijk reduceren.

De output van deze stap is een lijst met de huidige en geplande controls (*waaronder user controls, application controls en general IT controls)* toegepast op het IT-systeem om de kans op misbruik van een kwetsbaarheid te mitigeren en de impact van een dergelijke gebeurtenis te reduceren.

4.3.2.5 Stap 5 – Kans bepaling

Om te komen tot een totaalbeeld dat de kans indiceert dat een mogelijke kwetsbaarheid zou kunnen worden misbruikt binnen het stelsel van de verbonden bedreigingomgeving, kunnen de volgende heersende factoren overwogen worden:

Tabel 4: ***Likelihood Definitions***

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

4.3.2.6 Stap 6 – Impact analyse

De volgende belangrijke stap in het meten van het risiconiveau is het vaststellen van de schadelijke impact als resultaat van een succesvol uitgevoerde actie ten opzichte van de

kwetsbaarheid. Voordat er begonnen wordt met de impact analyse is het noodzakelijk om de volgende informatie te verkrijgen:

- Systeem missie (het proces uitgevoerd door het IT systeem)
- Systeem en data kriticiteit (de waarde en importantie van het systeem voor de organisatie)
- Systeem en data gevoeligheid

Deze informatie kan worden verkregen van bestaande organisatorische documentatie, zoals het missie impact analyse rapport. Een missie impact analyse (ook bekend als Business Impact Analyse (BIA)) prioriteert de impact niveaus van de bijbehorende informatie bezittingen van de organisatie en is gebaseerd op de beoordeling van de gevoeligheid en kriticiteit van deze bezittingen die de missie van de organisatie ondersteunen. Indien dit niet aanwezig is binnen de organisatie kan de systeem - en datagevoeligheid worden vastgesteld gebaseerd op het niveau van bescherming nodig om de beschikbaarheid, integriteit en betrouwbaarheid van het systeem en de data te handhaven. Belangrijk hierbij is dat de systeem- en informatie-eigenaren verantwoordelijk zijn voor het vaststellen van het impact niveau voor hun eigen systeem en informatie.

Hiermee kan de impact van een ongewilde beveiligings gebeurtenis worden beschreven in termen van het verlies of het verminderen van de volgende drie doelen van beveiliging: integriteit, beschikbaarheid en vertrouwelijkheid. Output van deze stap is de orde van impact (hoog, medium of laag).

4.3.2.7 Stap 7 – Risico bepaling

Het doel van deze stap is het beoordelen van het risico niveau met betrekking tot het IT-systeem. Het vaststellen van het risico voor een bepaalde dreiging/kwetsbaarheid kan worden weergegeven als een functie van

- De kans op een gegeven bedreiging dat wordt uitgevoerd betreffende een gegeven kwetsbaarheid
- De grootte van de impact wanneer een gegeven bedreiging succesvol zou worden betreffende een gegeven kwetsbaarheid
- De adequaatheid van geplande of bestaande beveiligings controls om het risico te reduceren of uit te schakelen.

Om het risico te meten moet een risico schaal en risiconiveau matrix worden ontwikkeld. Een voorbeeld is weergegeven in tabel 5

Kans op bedreiging	Impact		
	Laag (10)	Gemiddeld (50)	Hoog (100)
Hoog (1.0)	Laag 10 X 1.0 = 10	Gemiddeld 50 X 1.0 = 50	Hoog 100 X 1.0 = 100
Gemiddeld (0.5)	Laag	Gemiddeld	Gemiddeld

	10 X 0.5 = 5	50 X 0.5 = 25	100 X 0.5 = 50
Laag (0.1)	Laag 10 X 0.1 = 1	Laag 50 X 0.1 = 5	Laag 100 X 0.1 = 10

Risico schaal: Hoog (>50 tot 100); Gemiddeld (>10 tot 50); Laag (1 tot 10)

Tabel 5 Risico niveau Matrix

Hierbij hoort een risico schaal en de noodzakelijk acties die voortkomen uit het risico. Deze acties dienen door het management, de missie-eigenaren, te worden uitgevoerd voor elk risico niveau.

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

Tabel 6 Risk Scale and Necessary Actions

Output van stap 7 is het risico niveau (Hoog, Gemiddel, Laag)

4.3.2.8 Stap 8 – Control aanbevelingen

Tijdens deze stap van het proces worden controls verschaf om de geïdentificeerde risico's te mitigeren of te elimineren. Het doel van de aanbevolen controls is het reduceren van het risiconiveau waaraan het IT-systeem blootgesteld staat tot een acceptabel niveau. Hierbij spelen de volgende factoren een rol:

- Effectiviteit van de aanbevolen keuzemogelijkheden (systeem comptabiliteit)
- Wetgeving en voorschriften
- Organisatiebeleid
- Operationele impact
- Veiligheid en betrouwbaarheid

De control aanbevelingen zijn het resultaat van het risico beoordelingsproces en verschaffen input voor het risico mitigatie proces, waarbij de aanbevolen procedurele en technische beveiligings controls worden geëvalueerd, geprioriteerd en geïmplementeerd.

4.3.2.9 Stap 9 – Resultaten rapportage

Wanneer de risicobeoordeling is gecompleteerd moeten de resultaten worden gedocumenteerd in een officieel rapport of document. Een risicobeoordeling rapport is een management rapport voor het management ter ondersteuning van haar besluitvorming. Een risicobeoordeling dient gepresenteerd te worden in een systematische en analytische wijze van beoordelen van risico's opdat het senior management de risico's begrijpt en deze op een adequate wijze behandelt. De output van stap 9 is een risico beoordelingsrapport dat de bedreigingen en kwetsbaarheden beschrijft, het risico meet en aanbevelingen verschaft voor de implementatie van controls.

Hoofdstuk
5

Analyse en bevindingen

In de vorige paragrafen is beschreven hoe de methoden voor risicoanalyse worden uitgevoerd. In dit hoofdstuk worden de methoden naast elkaar gelegd om de verschillen te bepalen en worden de criteria voor toepasbaarheid vastgesteld waaraan de risicoanalyse zou moeten voldoen om aan de doelstellingen van de proceseigenaar te kunnen voldoen.

5.1 Relatie tussen de methodieken

In deze paragraaf wordt aangegeven hoe de methodes zich tot elkaar verhouden. Wat zijn de verschillen tussen de huidige aanpak OrgaQ en die van NIST 800-30. Daarbij wordt specifiek gekeken naar de verschillende stappen binnen de methodes. Welke stappen worden gedaan, wat gebeurt er binnen een stap en hoe verhoudt zich dat met de stappen van de andere methode. Dat heeft geleid tot de volgende figuur 6.

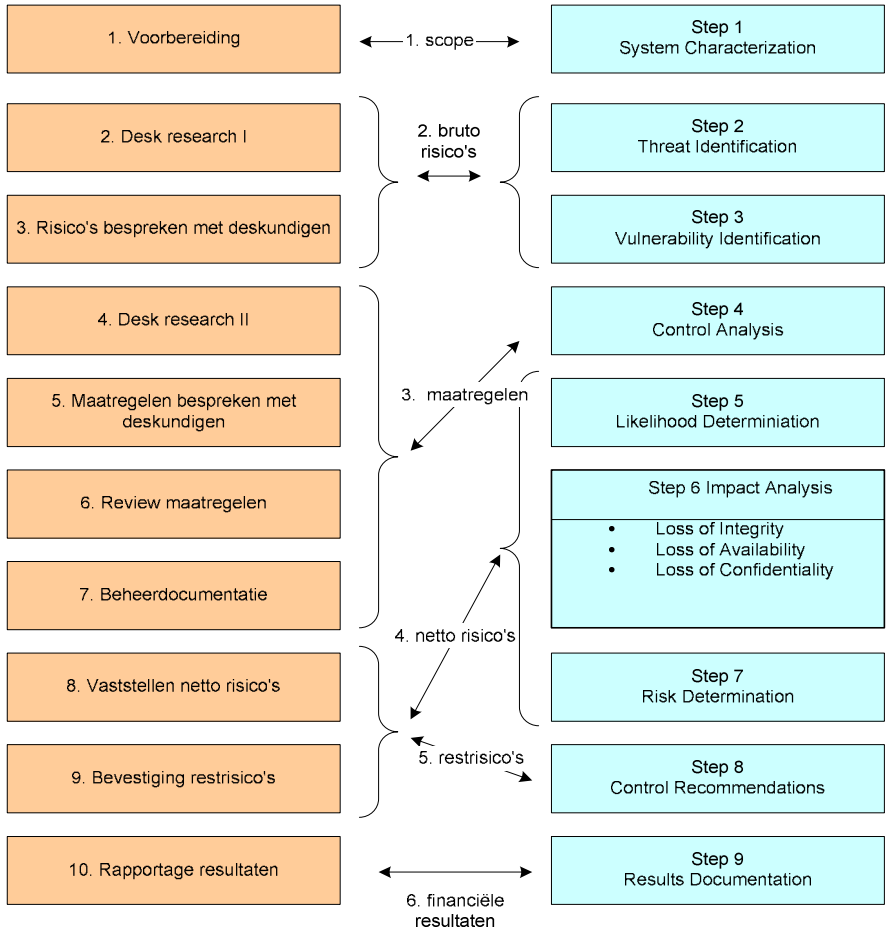

Fig.6. Processtappen OrgaQ vergeleken met NIST 800-30

Toelichting:

1. Scope
Uitkomst van zowel stap 1 bij OrgaQ als bij de NIST is het object voor onderzoek, dus de scope. Dit kan zoals bij NIST een systeem zijn maar ook zoals bij OrgaQ meestal voorkomt een proces of een onderdeel daarvan.

2. Bruto risico's
Bij de stappen 2 en 3 van beide methodes worden de bruto risico's vastgesteld. Dit zijn de bedreigingen en kwetsbaarheden waarbij nog niet gekeken wordt naar eventuele maatregelen die reeds genomen zijn.
3. Maatregelen
Nagegaan zal worden welke maatregelen reeds zijn geïmplementeerd of nog zullen worden geïmplementeerd ten aanzien van de bruto risico's.

4. Netto risico's
De netto risico's worden vastgesteld in stap 8 en 9 van OrgaQ en de stappen 5, 6 en 7 van de NIST. De netto risico's betreffende de dreigingen/kwetsbaarheden verrijkt met de kans, de impact en een beoordeling van het risico.

5. Restrisico's
Bij stap 8 van de NIST worden mitigerende en eliminerende maatregelen (controls) vastgesteld. Hieruit voortvloeiende kun ook de restrisico's bepalen. Bij stap 9 van OrgaQ worden de restrisico's vastgesteld. Deze restrisico's worden gerapporteerd aan de proceseigenaar, de proceseigenaar beslist of deze restrisico's acceptabel zijn of dat er moet worden onderzocht of er onderzoek moeten gedaan naar de haalbaarheid van eventuele aanvullende maatregelen.

6. Financiële resultaten
Zoals bij 5 genoemd worden bij OrgaQ de resultaten gerapporteerd. Bij het primaire proces van OrgaQ resulteert dit meestal in een financieel risico, daarom staat er een financiële rapportage genoemd. Stap 9 van de NIST kan ook een financiële component bevatten.

In de volgende paragraaf worden de criteria verzameld waaraan de methode NIST 800-30 zou moeten voldoen opdat de methode toepasbaar is op het primaire proces OrgaQ.

5.2 Criteria voor toepasbaarheid NIST 800-30

Nu de vergelijking in processtappen en de inhoud hiervan is benoemd is de volgende stap te kijken in hoeverre de doelstellingen worden gehaald van de risicoanalysemethode binnen het proces OrgaQ. De doelstellingen vormen namelijk een belangrijk uitgangspunt voor de vraagstelling van deze scriptie: "Is de aanpak van risico management volgens NIST 800-30 toepasbaar op een proces met een stelsel van gebruikers controls, applicatieve controls en general IT controls? Indien de doelstellingen van de methode OrgaQ niet met de methode NIST 800-30 gehaald kunnen worden, is de methode ook niet toepasbaar op het proces OrgaQ.

De doelstellingen van risicoanalyse OrgaQ vastgesteld door de proceseigenaar (zie paragraaf 4.2.2) zijn als volgt:

"Het doel van het uitvoeren van risicomanagement is om bij te dragen aan de beheersing van het primaire proces om aan de procesdoelstellingen te voldoen door (1) proactief risicomanagement toe te passen op het primaire proces dat (2) op een eenduidige wijze wordt toegepast binnen het

primaire proces, waarbij (3) volledigheid van de relevante risico's wordt nagestreefd en (4) dat aansluit op de integrale aanpak van beheersmaatregelen bij OrgaQ. Daarbij wordt risicobewustzijn beschouwd als randvoorwaardelijk (5)."

De risicoanalyse methode die door het primaire proces van OrgaQ wordt gehanteerd sluit zoals verwacht mag worden grotendeels aan bij de doelstellingen, maar verbeterpunten zijn goed te benoemen.[11]

(1) Het proactieve moet nog verbeterd worden. Risicoanalyses werden van oudsher met name gemaakt ter ondersteuning van de controles achteraf. Nu wordt er verwacht dat proactief de risico's in kaart zijn gebracht en dat er maatregelen zijn genomen om de risico's te mitigeren of te elimineren.

(2) De doelstelling eenduidigheid wordt grotendeels behaald, maar kan nog wel verbeterd worden. De methode is goed bekend binnen het proces, maar de vaste structuur staat onvoldoende beschreven, kent onvoldoende formele beslissingsmomenten en wordt niet altijd eenduidig uitgevoerd.

(3) Voor wat betreft de volledigheid van de relevante risico's is gebleken dat de relevante aandachtsgebieden wel zoveel mogelijk worden behandeld. De methode maakt gebruik van de deskundigheid van het personeel om zowel in persoonlijke sessies als in workshops de risico's in volledigheid zoveel mogelijk te inventariseren. Daarbij wordt ook gebruik gemaakt van checklist van relevante aandachtsgebieden, en wordt er op gelet dat de juiste mensen (kennis en kunde) aanwezig zijn bij de sessies. De volledigheid wordt echter niet altijd gehaald in termen van diepgang en breedte van aandachtsgebieden. De IT aspecten krijgen onvoldoende aandacht en ook is het aandachtsgebied omgeving (onder andere markt)[12] onderbelicht.

(4) De methode biedt nog onvoldoende waarborgen op het aspect volledigheid (zie (3)) maar is in potentie goed te hanteren als risicoanalysemethode. De aansluiting in een stelsel van integrale beheersmaatregelen zou op basis daarvan goed realiseerbaar moeten zijn. Deze invalshoek gaat verder op het vlak van risicomanagement en valt buiten de scope van deze scriptie.

(5) De methode heeft geen benoemd aspect dat bijdraagt aan het risicobewustzijn van de betrokken medewerkers van het primaire proces OrgaQ[13].

Vanuit het perspectief van de proceseigenaar en vanuit het perspectief van meerwaarde ten opzichte van de huidige methode OrgaQ zijn criteria voor toepasbaarheid opgesteld. Deze criteria zijn beredeneerd vanuit de doelstellingen van de risicoanalyse op het primaire proces OrgaQ door de proceseigenaar, en de analyse naar de realisatie hiervan (zie hierboven).

1. De methode dient voldoende structuur te bieden, waardoor de werknemers van het primaire proces OrgaQ door de risicoanalyse worden geleid.

2. De methode dient een dusdanige structuur te hebben dat voldoende formele afstemmingsmomenten kunnen worden uitgevoerd.

3. De methode dient een structuur te bieden waarmee de volledigheid (scope) van de risicoanalyse ten opzichte van de oude methode beter geborgd is.

[11] Bron: interview medewerker primair proces OrgaQ
[12] Bron: interview medewerker primair proces OrgaQ
[13] Bron: interview medewerker primair proces OrgaQ

4. De methode dient aan te sluiten op het proactief omgaan met risico's en bij te dragen aan het risicobewustzijn van de werknemers betrokken bij het primaire proces.

5.3 Bevindingen uit de analyse

In deze paragraaf wordt vastgelegd in hoeverre de NIST 800-30 aansluit op de criteria die gesteld zijn aan de toepasbaarheid ten opzichte van het primaire proces. Daarbij wordt ook gekeken in hoeverre de doelstellingen van de NIST 800- 30 aansluiten bij deze criteria.

In onderstaande tabel 7 is weergegeven per criterium hoe de toepasbaarheid van de NIST 800-30 zich daartoe verhoud.

Nr	Criterium	Toepasbaarheid
1	de methode dient voldoende structuur te bieden, waardoor werknemers van het primaire proces OrgaQ meer gestructureerd door de risicoanalyse worden geleid	De NIST 800-30 heeft een duidelijke, vastgelegde stappenplan. De negen stappen geven eenduidig weer welke activiteiten moeten worden uitgevoerd, wat daarvan de input is en tot welke output deze leiden
2	de methode dient een dusdanige structuur te hebben waardoor voldoende formele afstemmingsmomenten kunnen worden uitgevoerd	De methode kent duidelijke input en output. Hierdoor is het goed mogelijk om formele afstemmingsmomenten te organiseren waar op basis van deze output beslissingen kunnen worden genomen
3	de methode dient een kader te bieden waarmee de volledigheid (scope) van de risicoanalyse ten opzichte van de methode OrgaQ beter geborgd is	De risicoanalyse NIST 800-30 is opgesteld met als doel het beter beveiligen van IT systemen die bedrijfsinformatie opslaan, verwerken of verzenden. De methode biedt daarmee een kader die aanvullend is op de huidige risicoanalyse methode van OrgaQ.
4	de methode dient bij te dragen aan het pro-actief omgaan met risico's en aan het risicobewustzijn van de werknemers betrokken bij het primaire proces	Een duidelijke structuur nodigt uit tot het zorgvuldig uitvoeren van een risicoanalyse. Deze handreiking is een hulpmiddel om pro-actief invulling te geven aan het omgaan met risico's en die bijdraagt aan de uitvoering, waarmee het risicobewustzijn ook kan worden ontwikkeld

Tabel 7 toepasbaarheid van de NIST 800-30 op criteria primair proces

Nu is vastgelegd in hoeverre de NIST 800-30 aansluit op de gestelde criteria, is het nu van belang om vast te stellen in hoeverre de doelstellingen van de NIST 800- 30 aansluiten bij deze criteria.

Het doel van risicomanagement: van de NIST 800-30 luidt als volgt:

"Het doel van het uitvoeren van risicomanagement is om een organisatie in staat te stellen om te kunnen voldoen aan haar missie door het (1) beter beveiligen van IT systemen die bedrijfsinformatie opslaan, verwerken of verzenden en (2) door het management te assisteren in het autoriseren van (de toegang tot) IT systemen op basis van de ondersteunende documentatie die het resultaat is van het uitvoeren van risicomanagement.

De risicoanalyse zal dan ook in het licht van deze doelen moeten kunnen worden uitgevoerd. Als we kijken naar de doelen (1) en (2) dan kan vastgesteld worden dat deze goed aansluiten op de criteria van tabel 7. De methode biedt een structuur (1) (2) (3) met als doel het beter beveiligen van IT systemen die bedrijfsinformatie opslaan, verwerken of verzenden. Waarmee indirect in beginsel aan (4) en (5) kan worden voldaan, omdat een eenduidige vastgelegde structuur met input en output betrokkenen een kader geeft om pro-actief invulling te geven aan het omgaan met risico's en bijdraagt in het zorgvuldig uitvoeren van een risicoanalyse, waarmee het risicobewustzijn kan worden ontwikkeld.

5.4 Overeenkomsten en verschillen NIST 800-30 en methodiek Primaire proces

In het voorgaande hoofdstuk is geanalyseerd welke criteria gelden voor de risicoanalyse voor het proces OrgaQ en in hoeverre deze gehaald worden. Deze criteria zijn vastgesteld aan de hand van de doelstellingen die de proceseigenaar met de risicoanalyse wil bereiken. Daarnaast is geanalyseerd welke doelstellingen de NIST 800-30 nastreeft en in hoeverre deze aansluiten op de doelstellingen/criteria van OrgaQ. In deze paragraaf worden de verschillen geanalyseerd en aangegeven waardoor deze veroorzaakt worden en welke effecten deze hebben op de uitkomsten van het proces. Hierbij worden het accent gelegd op de aandachtsgebieden die benoemd kunnen worden aan de hand van de doelstellingen die de proceseigenaar heeft opgesteld (zie paragraaf 5.2). Deze zijn in tabel 8 weergegeven. Horizontaal zijn de risicoanalyse methoden weergegeven, verticaal de criteria.

	Analyse OrgaQ	Effect op uitkomst	Oorzaak	Analyse NIST 800-30	Effect op uitkomst	Oorzaak
Struc-tuur	De methode is goed bekend binnen het proces, maar de vaste structuur staat onvoldoende beschreven, kent onvoldoende formele beslissingsmomenten en wordt niet altijd eenduidig uitgevoerd.	Betrokkenen hebben onvoldoende inzichtelijk welke stappen moeten worden gedaan en met welke in- en output. Dit gaat ten koste van de kwaliteit van de risicoanalyse	Het ontbreken van een eenduidige methode met een duidelijke structuur voorzien van voldoende formele beslissingsmomenten	De NIST 800-30 heeft een duidelijke, vastgelegde stappenstructuur. Deze geven eenduidig weer welke activiteiten moeten worden uitgevoerd, en wat daarvan de input en output is, incl. formele beslissingsmomenten	Duidelijke en kwalitatief goede risicoanalyse op het vlak van beveiliging van IT-systemen	Een eenduidige en volledige risicoanalyse met een duidelijke structuur
Scope	De relevante aandachtsgebieden worden zoveel mogelijk behandeld. Dit wordt gewaarborgd door zoveel mogelijk gebruik te maken van de deskundigheid van het personeel (pers. sessies, workshops). Ook wordt gebruik gemaakt van checklist van relevante	Doordat er relevante aandachtsgebieden zijn die niet belicht worden, is het resultaat van de risicoanalyse van minder kwaliteit doordat er geen inzicht is van de invloed van deze aandachtsgebieden	In de structuur ontbreekt een systematiek die de volledigheid van de risicoanalyse waarborgt, waardoor het resultaat van de risicoanalyse inzake de volledigheid onvoldoende geborgd is.	De risicoanalyse NIST 800-30 is opgesteld met als doel het beter beveiligen van IT systemen die bedrijfsinformatie opslaan, verwerken of verzenden	Een risicoanalyse met een scope gericht op het beveiligen van IT systemen	De risicoanalyse heeft een scope die niet verder reikt dan het beveiligen van IT-systemen

	Analyse OrgaQ	Effect op uitkomst	Oorzaak	Analyse NIST 800-30	Effect op uitkomst	Oorzaak
	aandachtsgebieden. Daarbij wordt de omgeving (onder andere markt) onderbelicht					
Diepgang	Enkele aandachtsgebieden verdienen meer diepgang. Meest in het oog springend hierbij zijn de IT aspecten ter beveiliging van de proces ondersteunende systemen	Onvoldoende inzicht in de risico's inzake de procesonder-steunende systemen	Te weinig bewustzijn en kennis van risicoanalyse op het gebied van beveiliging van IT-systemen	De diepgang van de risicoanalyse inzake het beter beveiligen van IT systemen die bedrijfsinformatie opslaan, verwerken of verzenden is adequaat uitgewerkt	Een risicoanalyse met voldoende diepgang voor het inzichtelijk krijgen van enkel de risico's mbt de beveiliging van IT-systemen	De risicoanalyse is opgezet met als doel het inzichtelijk krijgen van risico's voor het beveiligen van IT-systemen met voldoende diepgang
Risico-bewust-zijn en pro-activi-teit	De huidige methode kent verbeterpunten (scope, diepgang, structuur) voor het zorgvuldig uitvoeren van een risicoanalyse. Dit is van invloed op het risicobewustzijn van de betrokken medewerkers	Beïnvloeding van het risicobewustzijn in negatieve zin omdat het risicobewustzijn minder dagelijkse routine kan worden.	Het ontbreken van voldoende scope, diepgang en structuur in de huidige methode	De methode biedt een duidelijke structuur aan voor het zorgvuldig uitvoeren van een risicoanalyse. Dit heeft een positieve invloed op het risicobewustzijn van de betrokkenen.	Positieve beïnvloeding van het risicobewustzijn omdat het risicobewustzijn meer dagelijkse routine kan worden. Echter alleen op het vlak van de beveiliging van IT-systemen	Het aanwezig zijn van voldoende diepgang en structuur in de methode echter alleen op het vlak van beveiliging van IT-systemen

Tabel 8 verschillen methode OrgaQ en NIST 800-30 op criteria primair proces

Tabel 8 geeft weer hoe de beide risicoanalysemethoden zich verhouden tot de criteria die de proceseigenaar stelt aan het proces ten opzicht van risicoanalyse. De tabel geeft aan dat bij beide methoden aanvullingen gewenst zijn om aan deze criteria te kunnen voldoen. Ook kan worden gesteld dat de methoden elkaar aanvullen op deze criteria. De NIST 800-30 biedt structuur, diepgang, kaders voor pro-activiteit en indirect risicobewustzijn, de methode OrgaQ biedt meer scope. De proceseigenaar zou met dit inzicht dus gebaat zijn bij een methode waarin het beste van beide methoden is verenigd. Aangezien de NIST 800-30 hierin leidend is gebleken (tabel 8) wordt in de volgende paragraaf de methode OrgaQ stapsgewijs afgegaan en wordt aangegeven hoe de NIST 800-30 hierin kan worden toegepast. Dit moet resulteren in een nieuwe methode OrgaQ die aan de criteria van de proceseigenaar zou moeten kunnen voldoen.

In het volgende hoofdstuk 6 worden aanbevelingen gedaan om de huidige methode OrgaQ aan te vullen met inzichten opgedaan uit de vergelijking met de NIST 800-30 opdat deze vernieuwde methode aansluit op de criteria zoals gesteld.

Hoofdstuk
6

Aanbevelingen

6.1 Aanbevelingen risicoanalyse methodiek OrgaQ

In figuur 6 is geconstateerd dat de processtappen in beide methoden terugkomen. Het verschil tussen beide methoden ligt vooral in de uitwerking van deze stappen. Daarnaast zijn er nog aspecten van de methoden die indirect bijdragen aan de criteria van de proceseigenaar. Een voorbeeld hiervan is het risicobewustzijn.

In de volgende paragrafen zullen de aanbevelingen worden behandeld. Vervolgens zal per stap de vergelijking met de NIST 800-30 worden gemaakt en indien nodig aangevuld (zie voor de criteria van de proceseigenaar paragraaf 4.2.2).

In overleg met de procesverantwoordelijken is besloten om de methode OrgaQ als leidend te nemen voor de aanbevelingen, en niet de NIST 800-30. Zoals in tabel 8 is aangegeven zijn de verschillen en overeenkomsten in relatie tot de doelstellingen bekend. Aangezien de methode OrgaQ bekend is binnen het proces, geeft de proceseigenaar de voorkeur aan een veranderingstraject met aanvullingen uit de NIST 800-30, dan het introduceren van de methode NIST 800-30 met aanvullingen. Dit traject wordt minder belastend verondersteld.

De eerste aanbeveling betreft het beschrijven van het proces. Hiervoor is een aantal goede redenen van toepassing:

- als kennis voornamelijk in de hoofden van de mensen zit, dan heeft het bedrijf een probleem als een ervaren medewerker vertrekt
- om de kwaliteit van een proces te kunnen beoordelen, moet duidelijk zijn welke kwaliteitsregels in welk(e) proces(stap) gerealiseerd worden
- taken, verantwoordelijkheden en bevoegdheden: het moet duidelijk zijn wie wat doet in het proces en wie verantwoordelijk is
- om het bedrijfsresultaat werkelijk te verbeteren moeten de processen beheerst worden
- om een proces te kunnen verbeteren moet je eerst de processen in kaart gebracht hebben
- de diverse processen moeten op elkaar aansluiten, zowel intern als in samenwerking met externe partners
- Informatiearchitectuur: de meeste processen worden ondersteund door informatiesystemen; het moet duidelijk zijn bij welke processtappen een informatiesysteem gebruikt wordt

Het beschrijven van de processen is randvoorwaardelijk om te kunnen voldoen aan de doelstellingen van de proceseigenaar. Zonder het inzicht dat hiermee verkregen wordt zijn onder andere monitoring, verbeterslagen en verantwoording onvoldoende beheerst uitvoerbaar.

In onderstaande figuur 7 is aangegeven welke aanbevelingen gedaan worden, en hoe die zich binnen het proces tot elkaar verhouden. Daarna worden de verbeterpunten ten aanzien van de

methode behandeld. In de figuur zijn deze verbeterpunten gekenmerkt van A tm F. In de uitwerking van deze verbeterpunten, wordt in de aanbevelingen verwezen naar deze letters.

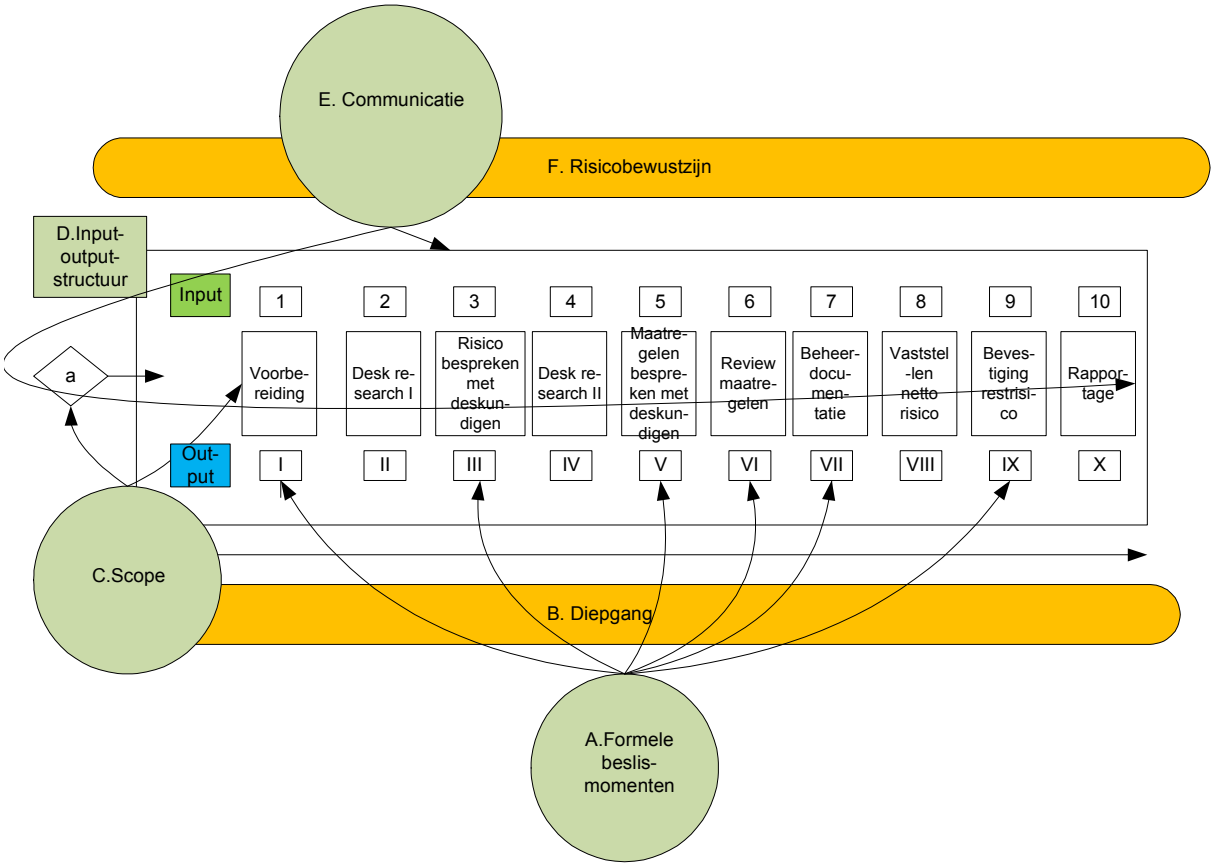

Fig. 7 Verbeterpunten risicoanalysemethode OrgaQ

Verbeteringen aan de methode

1) Geef in de methode duidelijk aan welke input nodig is en welke output elke stap moet opleveren (D). Een dergelijke opzet zorgt voor een duidelijke structuur en kan indirect bijdragen aan het risicobewustzijn van de betrokken doordat een duidelijke structuur helpt bij de reproduceerbaarheid bij betrokkenen en daardoor in de toepassing bij de werkzaamheden van medewerkers binnen het proces. Een voorbeeld van deze structuur voor het proces OrgaQ is te zien in tabel 9.

2) Neem in de methode OrgaQ formele beslismomenten (A) op. Geef daarbij aan welke input daarvoor noodzakelijk is, en wie (welke rol) daarover gaat beslissen. Geef daarbij duidelijk aan hoe de relatie ligt ten opzichte van de eindverantwoordelijke, de proceseigenaar.

Toepassing van de methode

3) Bepaal aan het begin van de risicoanalyse de scope (C). Dit wordt al gedaan, in eerste instantie richtinggevend door de proceseigenaar, en later met input van de senior analist, echter het is goed om eens te kijken in hoeverre deze scope kan worden uitgebreid met elementen die ook van belang zijn. Hierbij valt te denken aan bijvoorbeeld omzet, concurrenten en prijsontwikkelingen. Een hulpmiddel hierbij is het toepassen van een lijst met risicocategorieën bij het bepalen van de scope. Doel van deze stap is bewust te worden van de diverse factoren die invloed kunnen hebben op de doelstellingen.

4) Bepaal per processtap de diepgang van de stappen (B). De NIST 800-30 geeft een kader voor wat betreft de bedreigingen in relatie tot IT. Deze methode presenteert een structuur met stappen die toe te passen zijn binnen de methode OrgaQ (zie figuur 5). Deze diepgang is op meerdere aandachtsgebieden en stappen mogelijk. Bepaal waar deze behoefte bestaat en onderzoek de mogelijkheden tot de gewenste verdieping.

5) Het uitvoeren van een risico-identificatie en –analyse is niet iets dat slechts eenmalig uitgevoerd wordt, maar dient met een zekere periodiciteit herhaalt te worden. Op dit moment gebeurt dit bij OrgaQ eenmaal per jaar. Het verdient aanbeveling om te onderzoeken in hoeverre deze frequentie voldoende is om aan de doelstellingen van de proceseigenaar te voldoen. Wanneer in de scope aspecten als concurrentie en marktpositie mee wordt genomen, zou het in het kader van het proactief omgaan met risico's niet ondenkbaar zijn de risicoanalyse frequenter toe te passen.

Randvoorwaardelijk voor methode

6) Creëer voldoende risicobewustzijn bij de betrokken van het proces. De kritieke succesfactor is namelijk het ontbreken van voldoende risicobewustzijn bij het lijnmanagement. Wanneer deze houding en het bijbehorende gedrag ontbreken, wordt elke handeling met betrekking tot risicoanalyse als aanvullend en belastend gezien, terwijl het juist een onderdeel van de dagelijkse werkzaamheden dient te zijn. [14]

De volgende activiteiten kunnen helpen bij het versterken van het risicobewustzijn:

- Zorg voor natuurlijke betrokkenheid en voorbeeldgedrag van het management
- Maak lijnmanagement expliciet eigenaar van risico's
- Betrek het procesverantwoordelijken bij het vormgeven van de methode risicoanalyse in de organisatie
- Praat en discussieer over risico's en het managen ervan in groepsverband, bijvoorbeeld bij managementbijeenkomsten, werkoverleg, interne conferenties
- Verzorg opleiding en training
- Maak Risicoanalyse onderdeel van de dagelijkse werkzaamheden, bijvoorbeeld door standaard onderwerp te laten zijn op de agenda van vergaderingen, doelstellingen op het gebied van ERM in zijn algemeen en risicoanalyse in het bijzonder op te nemen in persoonlijke jaarplannen en door medewerkers te beoordelen op hun bijdrage aan ERM en risicoanalyse.

7) Binnen het proces worden al een aantal maatregelen genomen die de kwaliteit van de uitkomsten van het proces bevorderen. Zo wordt onder andere binnen het TPO team in teams gewerkt, waardoor er altijd minimaal twee mensen inbreng hebben gehad in de werkzaamheden voor de risicoanalyse, en worden voor de sessies voor het vaststellen van de risico's en de maatregelen nadrukkelijk gekeken naar de inbreng van deskundigen. De communicatie tijdens het traject kan echter verbeterd worden. Immers de communicatie over de risico's is bepalend voor het succes van de risicoanalyse[15]. Een goede communicatie helpt bij het versterken van het risicobewustzijn. Een belangrijk onderdeel van deze communicatie wordt bepaald door de perceptie van de risico's: de wijze waarop de deelnemers aan de risicoanalyse de risico's beleven en op waarde schatten. Van belang is ook het inwinnen van informatie door de risicoanalist tijdens een risicoanalyse en het uitdragen van informatie. Hoe kan omgegaan worden met de perceptie van risico's tijdens een risicoanalyse? Hiervoor is een vijftal succesfactoren benoemd:

[14] Risicomanagement, de praktijk in Nederland.PriceWaterhouseCoopers, Herziene uitgave, 2006
[15] Communicatie over risico's, ir. J.M. Fukken, e.a, 1999

a) het is van belang om mensen te wijzen op het bestaan van heuristiek (mensen maken bij het praten over en het schatten van risico's gebruik van vuistregels). Doel hiervan is om enige zelfreflectie op te roepen waardoor mensen worden gedwongen om kritisch hun eigen interpretaties te overwegen.
b) het kan erg praktisch zijn om een vraag op meerdere manieren te stellen. De deelnemers zullen de neiging hebben om de antwoorden onderling te vergelijken en eventueel hun antwoorden bij te stellen.
c) het is goed om de deelnemers aan een risicoanalyse te laten oefenen met het schatten van risico's en ze te leren welke fouten ze kunnen maken door het gebruik van heuristische regels.
d) het presenteren van de resultaten van een analyse is niet genoeg. Een risico is namelijk pas een risico als het ook zo wordt gevoeld: er is een wereld van verschil tussen rationele en emotionele herkenning van risico's. Daarom worden sommige beheersmaatregelen als zeer afstandelijk ervaren: het risico wordt niet gevoeld. Het is van belang om hierin tijd te investeren en verantwoordelijkheden te delegeren zodat de deelnemers voelen waar het om gaat.
e) het kweken van de attitude "omgaan met risico's" zou een belangrijk aandachtspunt kunnen zijn bij de opleiding en training. Selectie van risicobewuste medewerkers door middel van bijvoorbeeld certificering kan ook een stap in de goede richting zijn.

Tijdens het *inwinnen* van informatie doet zich een aantal valkuilen voor waarvoor de risicoanalist beducht moet zijn. Een aantal hiervan heeft te maken met "lastige" deelnemers aan een risicoanalyse. Belangrijk hierbij is dat de analist het doel van de risicoanalyse uitdraagt en daadwerkelijk laat zien dat de risicoanalyse vertrouwelijk wordt behandeld. Bovendien moet dit vertrouwen niet worden beschaamd. Daarnaast kunnen "techneuten" onwillig zijn om te praten over "softe" onderwerpen als organisatie en communicatie. Om deze personen mee te krijgen moet het doel van de risicoanalyse tot hen doordringen. Hiervoor is de analist de aangewezen persoon.

Informatie *uitdragen* door de risicoanalist kan verschillende doelen hebben. Dit kan gericht zijn op:
- voorlichting en educatie: bijvoorbeeld over het doel en de aanpak van de risicoanalyse

- gedragswijziging van een groep of individu: bijvoorbeeld bewustwording van risico's of het bespreekbaar maken van risico's

- gezamenlijke besluitvorming en conflictoplossing: bijvoorbeeld prioritering van risico's of keuze van beheersmaatregelen.

Het is van belang dat de methode op toepassing van deze communicatietoepassingen wordt geanalyseerd. Deze toepassingen dragen bij tot een hoge kwaliteit van de output van het proces.

Toepassing op de stappen binnen de methode

Per stap kunnen aan de hand van deze verbeterpunten suggesties worden gedaan ter verbetering. Het is aan te bevelen om te kijken in hoeverre deze voorstellen het beste aansluiten op het proces. Daarvoor dient het proces geanalyseerd te worden en keuzes gemaakt te worden ter implementatie. Een matrix kan hierbij helpen. Een voorbeeld hiervan is tabel 9.

Input	Wie	Stap	Output	Beslis-mom-enten	Scope	Diepgang
Elementen die de scope gaan bepalen	Proceseigenaar en senior analist	1. Voorbereiding	Scopebepaling	X	toepassen van een lijst met risicocategorieën bij het bepalen van de scope.	
(Historische) feiten mbt scope	(senior) analist	2. Desk research I	Lijst met historische feiten mbt scope			Bepalen van diepgang op meerdere aandachtsgebieden. Bepalen per stap waar deze behoefte bestaat en onderzoek de mogelijkheden tot de gewenste verdieping.
Verzamelen van expertise en brainstormen over brutorisico's	(senior) analist samen met procesdeskundigen en materiedeskundigen	3. Risico bespreken met deskundige	Lijst met bruto risico's	X		idem
Verzamelen van al geïmplementeerde maatregelen	(senior) analist	4. Desk research II	Lijst met al geïmplementeerde maatregelen			idem
Expertise verzamelen en bepalen maatregelen voor de brutorisico's	(senior) analist samen met proces- en materiedeskundigen	5. Maatregelen bespreken met deskundigen	Lijst met maatregelen voor brutorisico's	X		idem
Te analyseren maatregelen op effectiviteit en /of consequenties	(senior) analist samen met proces- en materiedeskundigen	6. Review maatregelen	Lijst met aandachtspunten van maatregelen	X		idem
Bepalen consequenties voor de beheerdocumentatie (bijvoorbeeld AO/werkinstructies)	(senior) analist en procesondersteuner	7. Beheerdocumentatie	Overzicht met te nemen acties	X		idem
Bruto risico's + vastgestelde maatregelen	(senior) analist	8. Vaststellen netto risico	Lijst met netto risico's			idem
Expertise verzamelen en beoordelen restrisico	(senior) analist	9. Bevestiging restrisico	Lijst met restrisico's	X		idem
Verzamelen gegevens over werking maatregelen	(senior) analist	10. Rapportage	Rapport			idem

Tabel 9 Voorbeeld matrix van verbeterpunten risicoanalyse OrgaQ

Nu de verschillen tussen de huidige aanpak en die van NIST 800-30 zijn geanalyseerd en vastgesteld, en de verbeterpunten voor de methode OrgaQ zijn aangeven, kunnen nu de laatste deelvragen worden beantwoord. Deze deelvragen zullen in hoofdstuk 7 worden beantwoord.

Hoofdstuk
7

Conclusie

In voorgaande hoofdstukken is een aantal subvragen van de vraagstelling al beantwoord. De eerste subvraag “Wat is risicomanagement volgens NIST 800-30?” is in hoofdstuk 4 aan de orde geweest. De huidige uitvoering van risicomanagement en risicoanalyse bij OrgaQ is in hoofdstuk 5 behandeld en de effecten en oorzaken van de verschillen tussen de risicoanalysemethoden OrgaQ en de NIST 800-30 zijn in hoofdstuk 6 aan de orde geweest. Ook zijn in hoofdstuk 6 de verbeterstappen voor de methode OrgaQ behandeld, opdat aan de doelstellingen van de proceseigenaar wordt voldaan.

In dit hoofdstuk worden de laatste subvragen uitgewerkt, waarmee uiteindelijk ook antwoord gegeven kan worden op de vraagstelling:

“Is de aanpak van risico management volgens NIST 800-30 toepasbaar op een proces met een stelsel van gebruikers controls, applicatieve controls en general IT controls?”

De vierde subvraag luidde: “In hoeverre biedt de NIST 800-30 toegevoegde waarde in de vorm van een gestructureerde aanpak en inhoudelijk relevante aandachtsgebieden voor risicomanagement?”

De NIST 800-30 biedt toegevoegde waarde in de vorm van een gestructureerde aanpak. De methode heeft een duidelijke structuur bestaande uit een negental stappen waarin input en output helder zijn weergegeven en formele beslissingsmomenten goed inpasbaar zijn (zie hoofdstuk 6). De huidige methode biedt duidelijk minder structuur, waardoor de NIST 800-30 hier zeker van toegevoegde waarde is. De toegevoegde waarde inzake de inhoudelijke aandachtsgebieden zijn ook goed te benoemen. De huidige methode biedt een brede scope, echter heeft ook verbeterpunten. Qua scope worden niet alle aspecten meegenomen (onder andere markt, stakeholders) en ook qua diepgang zou de methode kunnen worden aangescherpt. De NIST 800-30 biedt op het gebied van het beveiligen van IT-systemen deze diepgang.

De laatste subvraag luidde: “Hoe kan de NIST 800-30 als aanpak voor risicomanagement worden ingepast in het primaire proces OrgaQ?” In voorgaande hoofdstukken zijn de verschillen en overeenkomsten tussen beide risicoanalysemethoden beschreven. Daarbij hebben we kunnen vaststellen dat de methode OrgaQ meer structuur nodig heeft, uitgebreid kan worden met relevante aandachtsgebieden en bij een aantal aandachtsgebieden meer diepgang moet toepassen. De NIST 800-30 heeft structuur en diepgang inzake de beveiliging van procesondersteunende IT-systemen, maar mist de toepassing op uitgebreide relevante aandachtsgebieden voor het primaire proces OrgaQ. De meerwaarde van de NIST 800-30 ten opzichte van de huidige methode is daarmee goed te benoemen. Met het aanvullen van de sterke punten van de NIST 800-30 aan de methode OrgaQ zullen de doelstellingen van de proceseigenaar zoals benoemd in hoofdstuk 4 gerealiseerd kunnen worden. Deze aanvulling zou dan leiden tot een nieuwe methode met een duidelijke structuur, geënt op de relevante aandachtsgebieden voor het primaire proces OrgaQ, met de juiste diepgang en met een goede basis voor het ontwikkelen van risicobewustzijn bij de betrokken medewerkers.

In hoofdstuk 5 zijn de stappen van de risicoanalyse OrgaQ en de NIST 800-30 naast elkaar gelegd. Daarbij is gebleken dat de stappen die uitgevoerd worden qua stappen goed te vergelijken zijn. De NIST 800-30 kent meer structuur met een duidelijke in- en output. Deze analyse maakt inzichtelijk dat de stappen goed uitwisselbaar zijn. Het doel van de stappen is in beide methoden vergelijkbaar. Daarmee is ook aangegeven dat de structuur toepasbaar is op de relevante aandachtsgebieden van het primaire proces OrgaQ.

Op de vraagstelling of de aanpak van risico management volgens NIST 800-30 toepasbaar is op een proces met een stelsel van gebruikers controls, applicatieve controls en general IT controls kunnen we dan ook bevestigend antwoorden. Daar waar de methoden verschillen, zijn met de uitvoering van het stappenplan elementen uit de NIST 800-30 toegevoegd aan de methode OrgaQ. Een volgende logische stap zou vervolgens zijn voor het stafteam ter ondersteuning van het primaire proces OrgaQ om de verbeterstappen in hoofdstuk 6 te bestuderen en uit te voeren. De ontwikkeling van deze nieuwe methode is het product van de toepasbaarheid van de methode NIST 800-30 op het proces. Dit zou moeten resulteren in een methode voor risicoanalyse waarmee met de uitwerking hiervan het stafteam met grotere zekerheid een in control statement zou kunnen geven aan de proceseigenaar.