ITIL security management: een kritische beschouwing

Dr. M.E.M. Spruit

Informatiebeveiliging is een beheerproces dat zich richt op het beschermen van de informatievoorziening. Het ligt voor de hand om voor het inrichten van informatiebeveiliging gebruik te maken van het boekje *ITIL Security Management* dat sinds 1999 deel uitmaakt van de ITIL-reeks, de de-factostandaard voor IT-beheer. ITIL wordt echter door sommigen verguisd en door anderen de hemel in geprezen. Hoe zit het met ITIL security management: is dat in de praktijk toepasbaar, of zitten daar misschien ook haken en ogen aan? Een kritische beschouwing van *ITIL Security Management* levert wellicht een antwoord op deze vraag. Potentiële gebruikers kunnen dan op basis daarvan beter beslissen om er al dan niet gebruik van te maken.

Inleiding

Ondernemingen worden voor het realiseren van hun strategische doelstellingen steeds meer afhankelijk van hun informatievoorziening. Een belangrijke rol is veelal weggelegd voor het geautomatiseerde deel van de informatievoorziening (zie figuur 1). De (geautomatiseerde) informatievoorziening hoeft niet in zijn geheel door de onderneming zelf te worden verzorgd; een deel ervan kan bijvoorbeeld uitbesteed zijn aan een externe partij.

Figuur 1. De geautomatiseerde informatievoorziening in haar omgeving.

De geautomatiseerde informatievoorziening omvat informatietechnologie (IT) en de organisatie die verantwoordelijk is voor het beheer ervan, het IT-beheer ([Looi99]).

In figuur 2 is aangegeven welke processen een primair bedrijfsproces ondersteunen ([Over00]). Ten eerste is er het managementproces van waaruit het primaire proces wordt aangestuurd. Daarnaast zijn er ondersteunende processen die zich richten op personeel, materieel, financiën en informatie. Het proces dat zich richt op informatie is het beheer van de informatievoorziening. IT-beheer, dat zich richt op de verzameling IT die de onderneming gebruikt, speelt zich af binnen dit proces.

Een de-factostandaard voor het inrichten van het IT-beheer is ITIL, voluit: Information Technology Infrastructure Library ([Bon99]). ITIL is een verzameling van enige tientallen boekjes (vandaar 'library') die gegroepeerd zijn in zogenaamde sets. Ieder boekje geeft een 'best practice'-beschrijving van één proces van het IT-beheer. De beschrijvingen zijn grotendeels gebaseerd op ervaringen die zijn opgedaan in relatief grote computercentra.

Informatiebeveiliging is één van de processen van het IT-beheer; informatiebeveiliging die betrekking heeft op het niet-geautomatiseerde deel van de informatievoorziening wordt hier buiten beschouwing gelaten. In 1999 is het proces informatiebeveiliging onder de naam *ITIL Security Management* ([Caze99]) opgenomen in de ITIL-reeks. De vraag is hoe het staat met de toepasbaarheid van ITIL security management. Om hierover een uitspraak te kunnen doen kan het nuttig zijn om een referentiekader te hebben voor het bepalen van de volwassenheid van het proces informatiebeveiliging. Vervolgens kan dan aan de hand daarvan worden beoordeeld welke invloed ITIL security management daarop kan uitoefenen. In de volgende paragraaf wordt ingegaan op het neerzetten van een dergelijk referentiekader. In de daaropvolgende paragrafen wordt teruggekomen op ITIL security management.

Volwassenheid

Het proces informatiebeveiliging staat niet op zichzelf, maar is voorwaardenscheppend voor andere bedrijfsprocessen. Informatiebeveiliging komt het best tot haar recht als zij tezamen met andere ondersteunende processen geïntegreerd is in de primaire bedrijfsprocessen die zij ondersteunt. Een dergelijke situatie wordt echter lang niet door elke organisatie bereikt. Tabel 1 toont verschillende niveaus die op weg naar volledige integratie van informatiebeveiliging onderscheiden kunnen worden ([Over00]).

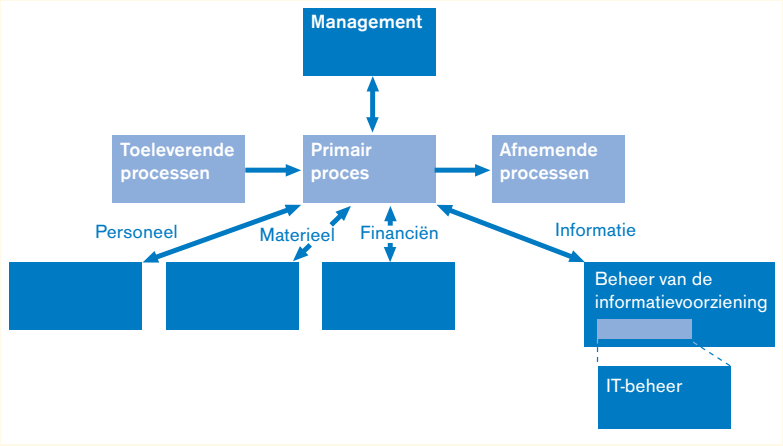
Het proces informatiebeveiliging omvat een scala van activiteiten die meer of minder effectief uitgevoerd kunnen worden. In analogie met het Capability Maturity Model ([Paul93], [Nies00]) zijn verschillende niveaus te onderscheiden voor de effectiviteit van de werkwijze binnen bepaalde processen. Tabel 2 toont de verschillende effectiviteitsniveaus voor de werkwijze binnen het proces informatiebeveiliging.

De mate waarin het proces informatiebeveiliging geïntegreerd is in de andere bedrijfsprocessen en de effectiviteit van de werkwijze binnen het proces informatiebeveiliging zijn tezamen een maat voor de volwassenheid van het proces informatiebeveiliging in de betreffende organisatie.

ITIL security management

Het proces informatiebeveiliging (met betrekking tot de geautomatiseerde informatievoorziening) wordt in de ITIL-reeks beschreven in *ITIL Security Management* ([Caze99]). Deze beschrijving bevat aanwijzingen en richtlijnen voor het inrichten van het proces informatiebeveiliging in een organisatie.

In het boekje *ITIL Security Management* zijn verschillende delen te onderscheiden. Na een korte introductie wordt eerst op beknopte wijze een overzicht van de discipline informatiebeveiliging gegeven. Gevorderden op het gebied van informatiebeveiliging vinden hier een verzameling 'open deuren'. Voor beginners is het wellicht nogal 'kort door de bocht'. Waarschijnlijk zijn beide groepen meer gebaat bij een goed boek over informatiebeveiliging ([Over00]).
Vervolgens wordt uitgebreid ingegaan op de positie van ITIL security management binnen ITIL. Hierbij wordt enige kennis over ITIL verondersteld. Geheel in lijn met de andere ITIL-processen wordt voor security management een manager geïntroduceerd die als 'eigenaar' verantwoordelijk is voor het proces, de security manager. Deze is verantwoordelijk voor de afstemming met de managers van andere processen. Opmerkelijk is dat bij het positioneren van security management enige inzichten uit het daarvoor gegeven overzicht losgelaten worden. Zo wordt informatiebeveiliging geschetst als een afgebakend proces dat verscheidene relaties heeft met een aantal andere ITIL-processen op tactisch en operationeel niveau (zie figuur 3). Hoewel hierbij enige mate van integratie tussen security management en andere ITIL-processen op tactisch en operationeel niveau wordt verondersteld, is er meer sprake van gegevensuitwisseling dan van integratie. De relaties met processen op strategisch niveau worden niet uitgewerkt. Eventuele relaties met andere dan ITIL-processen vallen buiten de scope van ITIL, maar worden toch netjes beschreven in een bijlage. Enkele zaken die cruciaal zijn voor informatiebeveiliging, zoals risicoanalyse en beveiligingsbewustzijn, worden nogal makkelijk naar een bijlage geschoven. Daarentegen wordt wel aandacht besteed aan uitbesteden in relatie tot informatiebeveiliging.
Na het positioneren van security management binnen de ITIL-reeks wordt ingegaan op de te nemen beveiligingsmaatregelen. De voorgestelde maatregelen zijn gebaseerd op de Code voor Informatiebeveiliging ([NNI00]). Het betreffende deel kan beschouwd worden als een korte samenvatting van de Code. In een bijlage worden de daarin gepresenteerde maatregelen gerelateerd aan de daarvoor beschreven ITIL-processen.
Ten slotte wordt nog kort ingegaan op enkele aandachtspunten en ervaringen ten aanzien van het implementeren van informatiebeveiliging in de praktijk. Hoewel deze punten zeker hout snijden maken ze de noodzaak van het inzetten van deskundigen bij het implementeren van informatiebeveiliging niet overbodig.



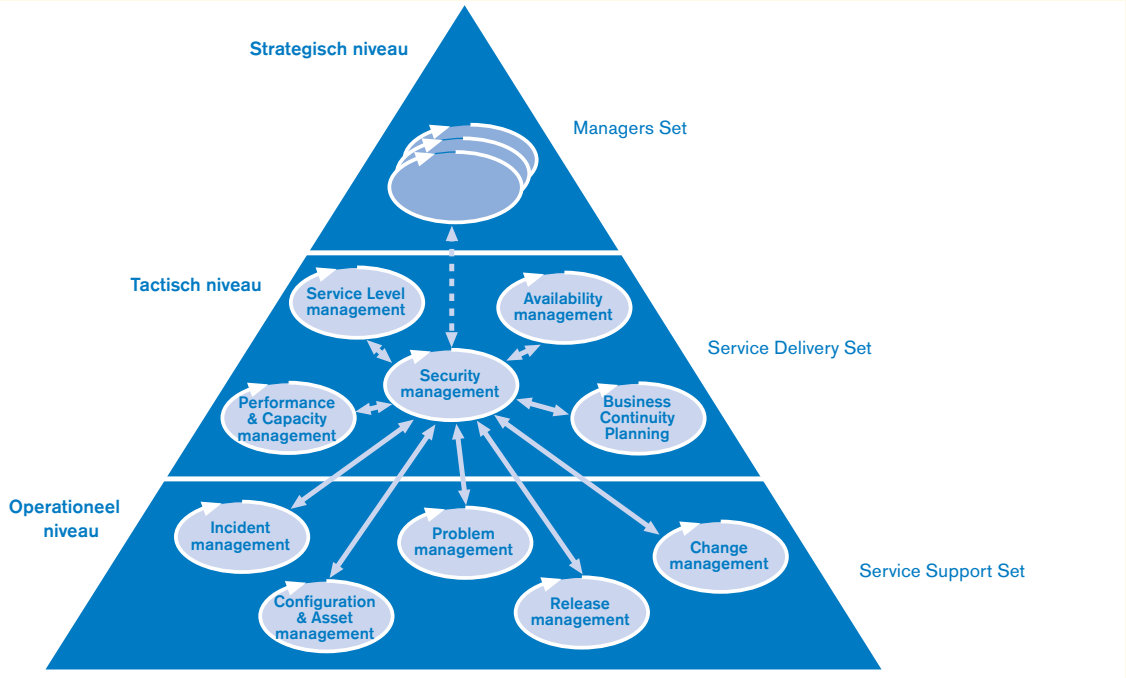
Figuur 2. De positie van het proces IT-beheer ten opzichte van andere processen.

Niveau van integratie	Status van beveiliging
i1 Onbezorgd	* Informatiebeveiliging wordt niet in overweging genomen; er is geen budget voor beveiligingsmaatregelen.
i2 Onbekend	* Informatiebeveiliging wordt nuttig geacht maar heeft geen duidelijke positie in de organisatie; oplossingen worden ad hoc gekozen.
i3 Ontluikend	* Informatiebeveiliging heeft een duidelijke positie in de organisatie; het is een stafaangelegenheid.
i4 Beheerst	* Informatiebeveiliging wordt geacht integraal onderdeel te zijn van ieder proces; het is een lijnmanagementaangelegenheid.
i5 Professioneel	* Informatiebeveiliging wordt geacht integraal onderdeel te zijn van de bedrijfsvoering; het is een directieaangelegenheid en een continu aandachtspunt.

Tabel 1. Verschillende niveaus van integratie.

Niveau van effectiviteit	Werkwijze
w1 Ad hoc	* Er zijn geen eenduidige processen voor informatiebeveiliging te onderkennen.
w2 Herhaald	* Er wordt ten behoeve van informatiebeveiliging procesmatig gewerkt, maar het proces is niet formeel beschreven.
w3 Gedefinieerd	* De processen voor informatiebeveiliging zijn beschreven in formele procedures.
w4 Gecontroleerd	* Binnen het informatiebeveiligingsproces wordt gemeten en bijgestuurd op basis van prestatie-indicatoren.
w5 Geoptimaliseerd	* Het informatiebeveiligingsproces wordt geoptimaliseerd ten behoeve van de ondersteunde primaire processen.

Tabel 2. Verschillende niveaus van effectiviteit van de werkwijze.



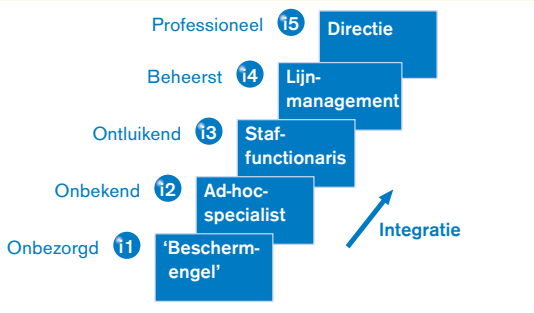
Figuur 3. ITIL security management en de belangrijkste andere ITIL-processen.

Met de introductie van security management als een nieuw proces in de ITIL-reeks is de toch al moeizame afbakening tussen de verschillende ITIL-processen weer wat moeilijker geworden. Zo valt management van beschikbaarheid (availability) onder security management, terwijl het los daarvan gedefinieerde ITIL-proces availability management gehandhaafd blijft. Ook blijft het veelal onder informatiebeveiliging vallende proces contingency planning als apart ITIL-proces gehandhaafd. Aan de andere kant heeft risicoanalyse, dat onlosmakelijk met informatiebeveiliging verbonden is, weliswaar een plaats gevonden in de ITIL-reeks, de wijze waarop dat moet worden uitgevoerd echter niet.

Toepasbaarheid

Op basis van het eerder beschreven referentiekader voor volwassenheid kan beoordeeld worden hoe het staat met de toepasbaarheid van ITIL security management in verschillende organisaties.

In tabel 1 is een vijftal niveaus onderscheiden voor de mate waarin het proces informatiebeveiliging geïntegreerd is in de andere bedrijfsprocessen. Deze niveaus zijn in figuur 4 samengevat.



Figuur 4. De verantwoordelijke voor informatiebeveiliging bij verschillende integratieniveaus.

In de ITIL-reeks wordt ervan uitgegaan dat elk proces duidelijk afgebakend is met betrekking tot zowel inhoud als verantwoordelijkheid. Daarbij hoort ook dat ieder proces een procesmanager krijgt. Voor informatiebeveiliging (security management) is dat de security manager. Alhoewel er tussen het proces informatiebeveiliging en andere ITIL-processen geregeld gecommuniceerd wordt, is er geen sprake van integratie van deze processen. Hiermee staat de in *ITIL Security Management* beschreven integratie op niveau i3 ('ontluikend'). Voor verdergaande integratie van informatiebeveiliging (niveau i4 en i5) biedt de ITIL-beschrijving te weinig handvatten.

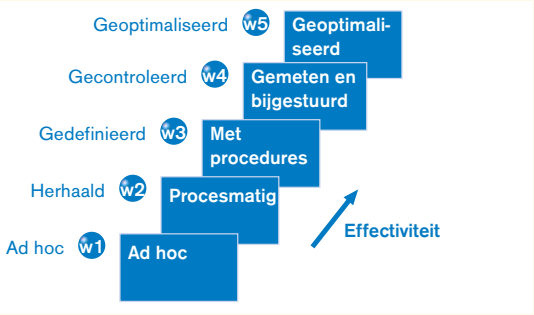
ITIL Security Management is geschreven voor mensen die reeds enige kennis hebben van zowel ITIL als informatiebeveiliging. Het lijkt dan ook niet zinvol om het toe te passen in organisaties waar ITIL niet in gebruik is. Ook is het niet zinvol toepasbaar in organisaties waar informatiebeveiliging geen issue is, ofwel de organisaties die met betrekking tot informatiebeveiliging op integratieniveau i1 ('onbezorgd') zijn blijven steken.

Uit het bovenstaande volgt dat ITIL security management toepasbaar is voor organisaties die al met ITIL werken en die zich met betrekking tot informatiebeveiliging op integratieniveau i2 ('onbekend') bevinden en die de ambitie hebben om op niveau i3 ('ontluikend') te komen.

In tabel 2 is een vijftal niveaus onderscheiden voor de mate van effectiviteit van de werkwijze binnen het proces informatiebeveiliging. Deze niveaus zijn in figuur 5 samengevat.

In de ITIL-reeks wordt ervan uitgegaan dat het IT-beheer procesmatig en gedocumenteerd uitgevoerd wordt. Daarbij hoort dat ieder proces vastgelegd wordt in formele procedures. Bovendien worden afspraken tus-

Figuur 5. De werkwijze ten aanzien van informatiebeveiliging bij verschillende effectiviteitsniveaus.



sen verschillende organisaties vastgelegd in overeenkomsten (service level agreements, ofwel SLA's) die gebaseerd zijn op controleerbare afspraken ten aanzien van de dienstverlening. Er wordt in *ITIL Security Management* nauwelijks aandacht besteed aan het meten en bijsturen van het proces informatiebeveiliging met behulp van prestatie-indicatoren. Dat betekent dat de in *ITIL Security Management* beschreven effectiviteit van de werkwijze op niveau w3 ('gedefinieerd') staat, terwijl nauwelijks handvatten voor een verbetering van de werkwijze tot niveau w4 of w5 gegeven worden.

Ook in relatie tot de effectiviteit van de werkwijze ten aanzien van informatiebeveiliging is het niet zinvol om ITIL, en dus ook niet ITIL security management, toe te passen in organisaties waar informatiebeveiliging geen issue is en die op effectiviteitsniveau w1 ('ad hoc') zijn blijven steken.

Hieruit volgt dat ITIL security management eigenlijk alleen toepasbaar is in organisaties die zich met betrekking tot informatiebeveiliging op integratieniveau w2 ('herhaald') bevinden en die de ambitie hebben om op niveau w3 ('gedefinieerd') te komen.

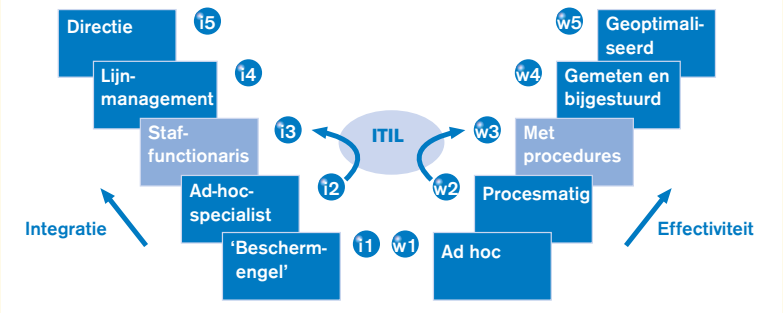
Al met al kan gesteld worden dat ITIL security management toepasbaar is voor organisaties die ook andere processen met behulp van ITIL ingericht hebben en die met betrekking tot informatiebeveiliging vanuit een integratieniveau i2 naar een niveau van i3 willen, en/of vanuit een effectiviteitsniveau w2 naar een niveau van w3 (zie figuur 6). In andere situaties zijn voor het inrichten van informatiebeveiliging alternatieven beschikbaar. Er kan dan bijvoorbeeld gebruik worden gemaakt van de Code van Informatiebeveiliging ([NNI00]) en in aanvulling daarop eventueel het door ICIT ontwikkelde 'Schema voor Certificatie van Informatiebeveiliging op basis van de Code voor Informatiebeveiliging'.

Conclusie

De de-factostandaard ITIL kan voor het inrichten van IT-beheer nuttig zijn. Het in 1999 geïntroduceerde *ITIL Security Management* is een goede aanvulling van de ITIL-reeks. De afbakening van security management is binnen ITIL helaas niet eenduidig en sluit daardoor niet goed aan op de gangbare beschrijving van informatiebeveiliging. Afgezien van dit bezwaar kan ITIL security management in bepaalde situaties nuttig zijn. Met name in organisaties die enerzijds al ervaring hebben opgedaan met het toepassen van ITIL voor andere processen, en die anderzijds informatiebeveiliging vanuit integratieniveau i2 naar i3 willen tillen, en/of de effectiviteit van de werkwijze van niveau w2 naar w3.

Indien ITIL security management toegepast wordt, dient er nog wel aandacht te worden besteed aan ontbrekende zaken zoals risicoanalyse en beveiligingsbewustzijn. Voor een hoge mate van volwassenheid van informatiebeveiliging dient bovendien extra aandacht besteed te worden aan de organisatorische inbedding van het proces informatiebeveiliging en het gecontroleerd bijsturen en optimaliseren ervan. In ieder geval is er voor implementatie van informatiebeveiliging met behulp van ITIL security management een belangrijke rol weggelegd voor terzake deskundigen.

Dr. M.E.M. Spruit is verbonden aan de faculteit Informatietechnologie en Systemen van de Technische Universiteit Delft. Hij is daar universitair hoofddocent voor de disciplines informatiebeveiliging en beheer van informatiesystemen. In deze functie is hij verantwoordelijk voor het geven van onderwijs en het doen van onderzoek. Onderzoeksresultaten zijn verschenen in een reeks publicaties in nationale en internationale tijdschriften. Daarnaast is hij verbonden aan verscheidene gremia die zich richten op informatiebeveiliging en het beheer van informatiesystemen.



Figuur 6. De volwassenheidsniveaus die met ITIL security management kunnen worden bereikt.

Literatuur

[Bon99]
J. van Bon e.a., *IT Service Management, een introductie*, ITSMF, Zeewolde 1999.

[Caze99]
J. Cazemier, P. Overbeek en L. Peters, *ITIL Security Management*, CCTA, London 1999.

[Looi99]
M. Looijen, *Beheer van informatiesystemen*, Kluwer Bedrijfswetenschappen, Deventer 1999.

[Nies00]
F. Niessink, *Perspectives on improving software maintenance*, Proefschrift, Vrije Universiteit, Amsterdam 2000.

[NNI00]
Code voor Informatiebeveiliging, Nederlands Normalisatie Instituut, Delft 2000.

[Over00]
P.L. Overbeek, E. Roos Lindgreen en M.E.M. Spruit, *Informatiebeveiliging onder controle*, Financial Times, Prentice Hall, Amsterdam 2000.

[Paul93]
M.C. Paulk, B. Curtis, M. Chrissis en C.V. Weber, *Capability Maturity Model, Version 1.1*, IEEE Software, Vol. 10, No. 4, 1993, pp. 18-27.