Scriptie Voorschrift informatiebeveiliging rijksdienst- bijzondere informatie en de rol van de IT-auditor

Aan Postgraduate IT-Audit Opleiding
Vrije Universiteit Amsterdam

Van Letty Huijbers en Jo Kremers

Datum 15 juni 2007

Kenmerk 713

Bijlagen 3

Inhoud

1 Voorwoord

Voor u ligt onze scriptie waarin verslag is gedaan van ons onderzoek naar het Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie en de rol van de IT-auditor.
Dit onderzoek is uitgevoerd als afsluiting van de Postgraduate IT Audit Opleiding aan de Faculteit der Economische Wetenschappen en Bedrijfskunde (FEWEB) bij de Vrije Universiteit Amsterdam.

Onze interesse in het onderwerp ontstond door:
1) diverse persberichten over 'geheime informatie op straat'. De daaromtrent gestelde kamervragen én de naar aanleiding daarvan door de minister van Binnenlandse Zaken en Koninkrijksrelaties toegezegde evaluatie. Een evaluatie over de stand van zaken van de beveiliging van bijzondere informatie, uit te voeren in het voorjaar 2007.
2) het noemen van de EDP-auditor in het Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie als onafhankelijk deskundige die kan beoordelen in hoeverre de beveiliging van bijzondere informatie in overeenstemming is met het voorschrift[1];
3) de signalen die naar voren kwamen tijdens een onderzoek naar de rubricering van bijzondere informatie binnen het ministerie van Financiën en ons eigen vooronderzoek voor deze scriptie. Signalen die duidden op tekortkomingen in het Vir-bi en een gebrek aan naleving van het Vir-bi. Deze signalen waren aanleiding onze scriptie eerst te richten op het Vir-bi en onze ideeën hoe het draagvlak voor het Vir-bi te verbeteren. Daarna gaan wij in op de rol van de IT-auditor. Hoe kan deze bijdragen aan die verbetering van dat draagvlak en inhoud geven aan de in het Vir-bi genoemde rol van onafhankelijk deskundige?

Voor ons onderzoek hebben wij bij het onderwerp betrokken deskundigen, functionarissen en collega's kunnen interviewen. Hun waardevolle ervaringen, meningen en ideeën over het beveiligen van bijzondere informatie hebben wij met deze scriptie samengebracht.
Wij zijn hen allen bijzonder erkentelijk voor hun medewerking aan ons onderzoek.
Ook danken wij de collega's die ons hebben begeleid tijdens het onderzoek en het schrijven van onze scriptie.

Wij hebben deze scriptie op persoonlijke titel geschreven, maar willen hem graag neerleggen bij onze collega's van de departementen, de Algemene Rekenkamer en de externe partijen die betrokken zijn bij het Vir-bi.

Wij hopen uw interesse voor onze scriptie te hebben gewekt en wensen u veel leesplezier.

Juni 2007

Letty Huijbers
Jo Kremers

[1] Het Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie hierna in deze scriptie aangeduid als Vir-bi

2 Samenvatting op hoofdlijnen

De conclusie van ons onderzoek is dat het Vir-bi geen helder voorschrift is en in de huidige vorm verwarring en onduidelijkheid met zich brengt. Het bevat veel rubriceringen, maar schiet tekort in de uitleg hoe die rubriceringen toe te passen. Wanneer vertrouwelijke informatie ook 'Departementaal Vertrouwelijke informatie' is, is eveneens niet helder voor betrokkenen. Een staatsgeheim is vaker te duiden, maar dan leidt de kwalificatie van de mate van de schade niet tot een indeling die breed wordt gedragen. De maatregelen die worden beschreven als passend bij de rubrieken bijzondere informatie worden doorgaans niet als passende maatregelen gezien. De ervaren rule based benadering kan belemmerend werken op de procesgang en werkt kostenverhogend bij de inrichting van de beveiliging. Dit alles resulteert in een gebrekkig draagvlak voor het Vir-bi en dat staat succesvolle implementatie en toepassing van het voorschrift in de weg.

De vraag is dan hoe bijzondere informatie goed beveiligd kan worden. Hiervoor zijn altijd specifieke en samenhangende beveiligingsmaatregelen nodig. Zowel fysieke en personele maatregelen als de technische en organisatorische maatregelen ter beveiliging van de IT-infrastructuur, inclusief de applicaties. De basis hiervoor is een algemeen geaccepteerde internationale standaard, zoals de Code voor Informatiebeveiliging. Deze Code is ook referentiekader voor het Vir 2007. We stellen voor om in aanvulling op de generieke Code voor Informatiebeveiliging aanvullende, speciale voorschriften te definiëren voor staatsgeheime informatie. En hoewel de departementen zelf verantwoordelijk zijn voor de beveiliging, stellen we daarbij een zogenaamde doelgroepsgewijze aanpak voor. De intentie is immers dat bijzondere informatie slechts onder ogen komt van en wordt gewisseld tussen een zo beperkt mogelijke (doel)groep mensen in een 'ketenproces'. Deze groep kan in beeld worden gebracht. Dit betekent dat afstemming nodig is tussen departementen over de classificatie -wat vindt het management dat bijzondere informatie is-, de voorschriften en de bijpassende maatregelen.

Wij adviseren bij het onderzoek tot verbetering van de beveiliging van de bijzondere informatie ook vertegenwoordigers van externe partijen te betrekken; partijen die ervaring hebben met de implementatie van de Code voor Informatiebeveiliging en met de certificering op basis van die Code.

De IT-auditor kan vanuit zijn advies- respectievelijk assurancerol een waardevolle bijdrage leveren aan (de totstandkoming van) die informatiebeveiliging.

3 Inleiding Vir-bi

Het Vir-bi verscheen in 2004 en verving de Aanwijzingen voor de beveiliging van staatsgeheimen en vitale onderdelen bij de Rijksdienst van 1989.
Het Vir-bi vormt een aanvulling op het Besluit Voorschrift informatiebeveiliging rijksdienst (Vir) dat in 1995 is ingevoerd en in 2007 is vernieuwd. Het Vir bevat algemene regels voor de beveiliging van informatie binnen de rijksdienst. Het Vir-bi bevat regels voor bijzondere informatie.
Het Vir-bi definieert bijzondere informatie als informatie waarvan de kennisname door niet-gerechtigden schade of nadeel op kan leveren voor de Staat, zijn bondgenoten of één of meer ministeries. Om deze reden worden, zo vervolgt het Vir-bi, bij deze informatie hogere eisen gesteld aan de waarborging van de exclusiviteit. Exclusiviteit is volgens het Vir-bi de mate waarin de toegang tot de informatie is beperkt tot een gedefinieerde groep van gerechtigden. Bijzondere informatie die staatsgeheim is, wordt in het Vir-bi gerubriceerd als Staatsgeheim Zeer Geheim, Staatsgeheim Geheim of Staatsgeheim Confidentieel. Bepalend daarbij is de ernst van de schade die kan worden toegebracht aan het belang van de Staat of zijn bondgenoten, indien niet-gerechtigden kennisnemen van de informatie.
Bijzondere informatie die geen staatsgeheim is wordt gerubriceerd als Departementaal Vertrouwelijk. Voor deze rubricering is het criterium dat kennisnemen door niet-gerechtigden nadeel kan toebrengen aan het belang van één of meer ministeries.
Het Vir-bi definieert het begrip rubriceren als volgt: “het vaststellen en aangeven dat een gegeven bijzondere informatie is (staatsgeheim of departementaal vertrouwelijk) en het bepalen van de mogelijke schade die wordt geleden indien onbevoegden er kennis van nemen en daarmee tevens de mate van beveiliging die aan deze informatie moet worden gegeven.”

Informatie wordt in het Vir-bi ruim opgevat: alle kennis die in welke vorm dan ook gecommuniceerd kan worden. Ook ‘materiaal’ waarin deze kennis is opgeslagen, zoals een document of communicatieapparatuur wordt aangemerkt als informatie.
Als aanvulling op het Vir stelt het Vir-bi daarom ook extra eisen aan het elektronische gebruik van bijzondere informatie. Ook wordt met het Vir-bi aangesloten op de regels die gelden voor het omgaan met staatsgeheimen en vertrouwelijke informatie van de Europese Unie en de NAVO.
In het voorschrift is vastgelegd dat iedere minister zelf verantwoordelijk is voor de beveiliging van bijzondere informatie op zijn eigen terrein.
Het Vir-bi schrijft in art. 13 lid 2 letter c dat het de verantwoordelijkheid van de secretaris-generaal binnen een ministerie is, dat het informatiebeveiligingsbeleid voor wat betreft bijzondere informatie iedere twee jaar wordt geëvalueerd door een onafhankelijke deskundige.
Dit zal in 2007 voor het eerst plaatsvinden.
Het voorschrift licht toe “*de onafhankelijke deskundige beoordeelt in hoeverre de beveiliging van bijzondere informatie in overeenstemming is met de eisen van dit voorschrift. De functie van onafhankelijk deskundige kan bijvoorbeeld worden vervuld door een EDP-auditor*”.
Het oordeel van een onafhankelijke deskundige wint nog aan belang gezien de inhoud van artikel 16 Vir-bi en de daarbij gegeven toelichting. Betreffende artikel definieert de verantwoordelijkheid van de Minister van Binnenlandse Zaken voor bijzondere informatie binnen de rijksoverheid: “*De minister van Binnenlandse Zaken en Koninkrijksrelaties rapporteert*

eens in de twee jaar aan de ministerraad over de beveiliging van bijzondere informatie binnen de rijksdienst" wat toegelicht wordt met de woorden "*Voor deze rapportage kan onder meer gebruik worden gemaakt van de gegevens afkomstig uit de evaluatie als bedoeld in artikel 13, tweede lid onder c."*
De minister van BZK heeft op 16 mei 2007 aan de Kamer gerapporteerd over de informatiebeveiliging van bijzondere informatie. Deze rapportage werd niet onderbouwd door interne evaluaties. De intentie is wel uitgesproken dat die evaluaties zullen plaatsvinden.

4 Ons onderzoek

4.1 Aanpak

Zoals in het voorwoord aangegeven, richtte ons onderzoek zich eerst op het Vir-bi en daarna op de rol van de IT-auditor. De rol van de IT-auditor bekijken wij daarbij vanuit twee perspectieven:
- hoe kan de IT-auditor vanuit de adviesrol (het draagvlak voor) de beveiliging van bijzondere informatie verbeteren?
en
- welke stakeholders hebben behoefte aan zekerheid over implementatie en toepassing van die beveiliging? Kan de IT-auditor die assurance verstrekken en onder welke randvoorwaarden?

Voor ons onderzoek hebben wij 20 mensen geïnterviewd die binnen hun functie of op basis van een opdracht betrokken zijn bij het fenomeen bijzondere informatie. Hetzij de verwerking of de beveiliging van bijzondere informatie hetzij de audit daarop.
Het betreft medewerkers van de Algemene Inlichtingen en Veiligheidsdienst (AIVD), het Ministerie van Financiën, het Ministerie van Defensie, de Douane, de Fiscale Inlichtingen- en Opsporingsdienst - Economische Controledienst (FIOD-ECD), de Belastingdienst, de Algemene Rekenkamer en zowel interne als externe IT-auditoren.
De betrokkenheid van de geïnterviewden tot het onderwerp varieerde van:
- het hebben van een A-, B- of C-gecertificeerde functie[2], (een functionaris die na screening door de AIVD of MIVD[3], belast is met het verwerken van bijzondere informatie); (3 personen geïnterviewd)
- het zijn van Beveiligingsambtenaar (BVA) op het departement; (1)
- het zijn van Informatiebeveiligingsfunctionaris binnen een dienstonderdeel; (2)
- het zijn van lijnmanager verantwoordelijk voor de verwerking van bijzondere informatie en de control daarvan; (2)
- het hebben van taken voor de ontwikkeling en evaluatie van het Vir-bi namens de AIVD; (2)
- het zorgdragen voor het Informatiebeveiligingsbeleid binnen het departement, naast of namens de BVA; (2)
- het vervullen van de departementale (IAD) en externe auditfunctie (AR) gericht op de verwerking van bijzondere informatie; (5)
tot
- het vervullen van de adviesrol als interne (IAD en EDP Audit Pool) IT auditor of ingehuurde externe IT auditor. (3 personen)

We hebben ons onderzoek beperkt tot twee departementen.
Wij kozen voor Defensie omdat dit departement enkele keren het nieuws

[2] zie voor toelichting type functies bijlage 2
[3] zie voor de verklaring van afkortingen bijlage 2

haalde naar aanleiding van incidenten met bijzondere informatie. De keuze voor Financiën is, omdat wij beiden werkzaam zijn bij de Auditdienst van Financiën. Om geen misverstand te laten ontstaan benadrukken we dat we het onderzoek niet vanuit onze auditfunctie hebben verricht. Het onderzoek vond plaats binnen onze IT-auditopleiding (zie voorwoord) en we hebben deze scriptie daarom geheel op persoonlijke titel geschreven.

De informatie verkregen tijdens onze interviews, aangevuld met de resultaten van deskresearch en literatuurstudie hebben wij opgenomen in de antwoorden op onze onderzoeksvragen. Deze onderzoeksvragen hebben we als volgt opgesplitst en gestructureerd:

I Beveiliging bijzondere informatie en de adviesrol van de IT-auditor
1. *Is er voldoende draagvlak voor het Vir-bi?*
2. *Hoe kan het draagvlak voor beveiliging van bijzondere informatie worden versterkt?*
3. *Hoe kan de IT-auditor vanuit zijn adviesrol bijdragen aan de versterking van dat draagvlak?*

II Beveiliging bijzondere informatie en de assurancerol van de IT-auditor
1. *Wie zijn de stakeholders bij een goede beveiliging van bijzondere informatie?*
2. *Hoe kunnen deze stakeholders zekerheid krijgen over een goede beveiliging van bijzondere informatie?*
3. *Waarom een IT-auditor inzetten voor het verkrijgen van die zekerheid?*

4.2 Opzet van de scriptie

In hoofdstuk 5 beantwoorden we de vragen die betrekking hebben op “Vir-bi en de adviesrol van de IT-auditor”.
In de paragrafen 5.1 tot en met 5.10 geven wij een analyse en opsomming van de tekortkomingen in het Vir-bi en de bedreigingen voor het draagvlak voor het Vir-bi. Ook geven we voor elke tekortkoming c.q. bedreiging een advies tot verbetering en indien van toepassing de bijdrage die de IT-auditor daarbij kan leveren. Aan het einde van het hoofdstuk vatten we onder 5.11 onze resultaten op hoofdlijnen samen en geven daarmee antwoord op de drie onderzoeksvragen.

In hoofdstuk 6 beantwoorden we de vragen die betrekking hebben op “Vir-bi en de assurancerol van de IT-auditor”. In paragraaf 6.1 beschrijven we “Stakeholders en zekerheid bij een goede beveiliging van bijzondere informatie”. In paragraaf 6.2 beantwoorden we de vraag “Waarom een IT-auditor inzetten?”.
In hoofdstuk 7 beschrijven we de randvoorwaarden bij de werkzaamheden van de IT-auditor binnen de advies- en de assurancerol. Daarop volgend formuleren we in hoofdstuk 8 de algemene conclusie en adresseren we onze algemene adviezen op hoofdlijnen aan:
- op de eerste plaats de wetgever, in het bijzonder het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (hierna kortweg BZK) als coördinerend ministerie waaronder ook de AIVD en de directie Personeel, Organisatie en Informatie Rijk (POIR)[4] ressorteren,
- de departementen, in het bijzonder de BVA’s die de bij hen aanwezige bijzondere informatie moeten beveiligen en tot slot

[4]Het ministerie van BZK draagt de coördinerende taak die de AIVD nu heeft ten aanzien van het Vir-bi over aan de directie POIR, volgens het jaarverslag 2006 van de AIVD. Het POIR is momenteel reeds verantwoordelijk voor het Vir.

- aan onze collega's, de IT-auditoren.

De scriptie kent 3 bijlagen:
Bijlage 1 Lijst met gebruikte afkortingen
Bijlage 2 Lijst met definities van gebruikte begrippen en bronvermelding
Bijlage 3 Deskresearch en literatuurstudie

5 Vir-bi en de adviesrol van de IT-auditor

De belangrijkste uitkomsten van onze interviews, deskresearch en literatuurstudie beschrijven wij hierna in de paragrafen 5.1 tot en met 5.10. Daarbij geven we ook ons advies hoe te komen tot verbetering en, indien van toepassing, de bijdrage die de IT-auditor daarbij kan leveren. Aan het einde van het hoofdstuk vatten we onder 5.11 onze resultaten op hoofdlijnen samen en geven daarmee antwoord op de drie onderzoeksvragen. De paragrafen 5.1 tot en met 5.6 gaan over het Vir-bi als voorschrift. De voornaamste opmerkingen worden benoemd met aanbevelingen om het voorschrift aan te passen.
In de paragrafen 5.7 en 5.8 bespreken we de punten die een rol spelen bij het creëren van draagvlak voor een voorschrift bijzondere informatiebeveiliging. Een draagvlak waarop de implementatie van het Vir-bi gestalte kan krijgen.
De paragrafen 5.9 en 5.10 bespreken randvoorwaarden die worden gesteld om de vertrouwelijkheid van de bijzondere informatie te borgen.

5.1 Richtlijnen om te rubriceren

De indeling van bijzondere informatie in vier rubrieken[5] wordt in het Vir-bi bepaald door de mate van nadeel of schade die kan worden geleden indien een niet-gerechtigde kennis neemt van de informatie. Als leidraad voor het rubriceren van informatie verwijst het Vir-bi naar bijlage 2 van het voorschrift, het schema "voorbeelden van rubriceringen".
De uitkomsten van de rubricering zijn bepalend voor het niveau van de beveiliging en daarmee voor de te nemen beveiligingsmaatregelen.
Uit de interviews blijkt dat het verantwoordelijke management grote moeite heeft deze rubricering op basis van de toelichting en de voorbeelden in bijlage 2 van het Vir-bi toe te passen.
Volgens die bijlage leidt zeer ernstige schade tot de rubricering Stg. Zeer Geheim; ernstige schade tot de rubricering Stg. Geheim en schade tot Stg. Confidentieel. Bijzondere informatie die niet staatsgeheim is, kan op basis van het begrip nadeel (aan het belang van een of meer ministeries) departementaal vertrouwelijk zijn.
Meermalen kwam tijdens de interviews naar voren dat het verschil tussen zeer ernstige en ernstige schade niet is te maken. Er zijn geen richtlijnen voor en de gegeven voorbeelden verduidelijken een keuze niet. Voor het bepalen van het onderscheid tussen de rubricering Stg. Zeer Geheim en de rubricering Stg. Geheim is het verschil tussen zeer ernstige schade en ernstige schade te vaag. Dezelfde opmerking geldt voor de andere rubriceringen, Stg. Confidentieel en Dept. Vertrouwelijk. Want wanneer is sprake van schade en wat is nadeel?

[5] Deze vier rubrieken zijn drie rubrieken Staatsgeheim: Stg. Zeer Geheim, Stg. Geheim, Stg. Confidentieel en de rubriek Departementaal Vertrouwelijk.

Advies

Een beslissingstabel of een questionnaire lijkt ons een beter instrument voor het rubriceren dan de huidige lijst met voorbeelden in bijlage 2 van het voorschrift.
Wij noemen in dit kader enkele voorbeelden van vragen die onderdeel kunnen uitmaken van een dergelijke beslissingstabel of questionnaire.
Heeft kennisname door niet-gerechtigden gevolgen, zo ja welke, voor:

1. het optreden en functioneren van de minister of staatssecretaris?
2. voor de samenwerking met en of het functioneren van de bondgenoten?
3. voor het functioneren van de rijksdienst en of onderdelen daarvan?
4. voor het functioneren en de resultaten van individuele processen?
5. voor het slagen van operaties en missies?
6. voor het functioneren en de veiligheid van groepen of individuele overheidsdienaren?
7. de compliance met van toepassing zijnde nationale of internationale wet- en regelgeving?

Deze vragen zouden moeten worden afgestemd op het doel waarvoor de informatie dient en moeten worden beantwoord door de diverse doelgroepen die zijn te onderscheiden. Als doelgroepen zien wij bijvoorbeeld “Opsporing en vervolging zware criminaliteit”, “Krijgsmacht” en “Internationaal”.
Deze doelgroepen definiëren de extra en specifieke maatregelen. Namelijk bovenop de al conform Vir getroffen maatregelen. Extra, ter afdekking van de verhoogde risico’s die kleven aan de bijzondere informatie die door de doelgroep wordt gebruikt. In een dergelijke benadering moet ook rekening worden gehouden met de voor deze doelgroep geldende specifieke wet- en regelgeving.
De doelgroep “Internationaal” selecteert in haar aanpak specifieke maatregelen die compliant zijn met de internationale wet- en regelgeving van bijvoorbeeld de EU. De doelgroep “Krijgsmacht” onder leiding van de National Security Authority (SNA) toetst haar keuze aan de NAVO regelgeving.
Bij deze doelgroepsgewijze aanpak hoort dan ook interdepartementale samenwerking.

5.2 Rubricering Departementaal Vertrouwelijk

Volgens het Vir-bi gaat het bij departementaal vertrouwelijke informatie om overige (bijzondere) informatie. Informatie die niet staatsgeheim is en waarvan kennisname door niet-gerechtigden nadelige gevolgen kan hebben voor de belangen van een of meer ministeries.
Samen met een aantal geïnterviewden plaatsen wij vraagtekens bij de wenselijkheid of noodzaak van de rubricering “Departementaal Vertrouwelijk”. De Wbp kent vier risicoklassen. De risicoklasse II geldt voor persoonsgegevens met een verhoogd risico en risicoklasse III voor gegevens met een hoog risico. Naar de mening van geïnterviewden zijn concrete beveiligingseisen uitgeschreven voor vertrouwelijke informatie zoals privacygevoelige gegevens (personeel, klanten, verdachten, patiënten, Vips etc) die geclassificeerd worden in II of III van de Wbp. De voorbeeldtabel van het Vir-bi classificeert informatie die tot ongerechtvaardigde verrijking of voordeel voor natuurlijke personen of bedrijven kan leiden als departementaal vertrouwelijk. Betekent dat, dat bijvoorbeeld informatie van en over bedrijven in bijvoorbeeld de productiesystemen van de Belastingdienst, als zodanig gerubriceerd en conform het Vir-bi beveiligd moeten worden? En dat daartoe in te zetten beveiligingsproducten gecertificeerd dienen te worden door de afdeling NBV (Nederlands Bureau Verbindingsbeveiliging) van de AIVD? Deze

verplichte certificering geldt namelijk volgens het Vir-bi al voor producten die ingezet worden ter beveiliging van de informatie met de rubricering Departementaal Vertrouwelijk.
Of kan volstaan worden met de in het Voorschrift Informatiebeveiliging Rijksdienst (Vir) opgenomen algemene regels voor de beveiliging van vertrouwelijk informatie zoals privacygevoelige gegevens (personeel, klanten, verdachten, patiënten, Vips etc)? Het lijkt erop dat departementale beleidsnotities niet meer apart en hoger geclassificeerd hoeven worden. En dat toepassing van het Vir-bi voor 'departementaal vertrouwelijk' alleen al door de grootte van de groep gerechtigden tot een onwerkbare situatie leidt.

Advies
Wij adviseren om de rubriek 'Departementaal vertrouwelijke informatie' niet meer in het Vir-bi op te nemen.
Een beveiligingsniveau gelijk aan dat van vertrouwelijke persoonsgegevens (Wet op de privacybescherming klasse II of III) volstaat. Hierdoor is het Vir van toepassing en niet de aanvullende maatregelen van een voorschrift voor de beveiliging van bijzondere informatie.

5.3 Rule based benadering en actualiteit Vir-bi

Alle geïnterviewden zijn van mening dat het Vir-bi in zijn huidige vorm een te sterke rule based benadering kent. Hoewel het Vir-bi de indruk wekt alleen maar "exclusiviteits"-*eisen* te willen geven, bevat het voorschrift in de bijlagen een groot aantal tot in detail voorgeschreven *maatregelen*. Deze maatregelen worden door veel geïnterviewden ervaren als dwingend voorgeschreven maatregelen, die niet per definitie leiden tot een goede beveiliging van de bijzondere informatie. Voorbeelden die steevast worden genoemd zijn:
- De door de BVA goed te keuren sealbags;
- De voorgeschreven maximale lengte en breedte van de snippers overblijvend na versnippering van gerubriceerde documenten door een versnippermachine;
- Het plaatstaal voor de per rubricering te gebruiken kluis; de dikte van het staal neemt toe bij een hoger beveiligingsniveau;
- Een opsomming van de bergmiddelen die per rubricering dienen te worden geïnstalleerd.

Juist hierdoor wordt het voorschrift ervaren als een sterke beperking van het eigen initiatief en de eigen verantwoordelijkheid van vooral de lijnmanager. De sterke rule based benadering kan volgens geïnterviewden belemmerend werken op de procesgang en werkt kostenverhogend bij de inrichting. In het bijzonder lijnmanagers ervaren dit als een hindernis om marktconform te werken en te beveiligen.

Een dergelijke dwingende, gedetailleerde benadering en beschrijving heeft ook als risico dat de voorgeschreven maatregelen niet meer passen in de actualiteit. Als voorbeeld hiervoor geven we de in de bijlage vermelde diskette als middel voor opslag en uitwisseling van informatie.

Wat betreft die actualiteit geldt dat de rijksoverheid nadrukkelijk in beweging is. Uitbesteding naar shared services en centralisatie van processen zijn voorbeelden van dergelijke reeds lang ingezette ontwikkelingen. Deze ontwikkelingen hebben ook consequenties voor de opslag, verwerking en uitwisseling van bijzondere informatie.
Recenter zijn de ontwikkelingen die in gang zijn gezet waarbij wordt overgegaan van een model van monopolistische dienstverlening naar een

model van samenwerkende ketenpartners. Partners die gebruik maken van een stelsel van gemeenschappelijke basisregistraties binnen de rijksdienst. Ook dit heeft gevolgen voor de inrichting van de informatiebeveiliging en het leidt tot een herverdeling van verantwoordelijkheidsgebieden.
In het Vir-bi zijn dergelijke ontwikkelingen en de gevolgen daarvan niet specifiek geadresseerd.

Advies
De keuze van maatregelen zou, in lijn van een verantwoord risicomanagement, meer marktconform en niet dwingend voorgeschreven kunnen zijn. Daarmee kan ook beter ingespeeld worden op de ontwikkelingen binnen de rijksdienst. Een overleg hierover tussen de werkgroep Vir-bi en de BVA's van de diverse departementen kan een startpunt zijn. Daarna moet er vervolgens ruimte zijn voor de doelgroepbenadering waarbij het verantwoordelijke lijnmanagement het eigen initiatief neemt. Initiatief om op de doelgroep specifiek toegesneden maatregelen te treffen, waarbij rekening kan worden gehouden met lopende en aanstaande ontwikkelingen.
De (inter)departementale IT-auditoren kunnen wat betreft de keuze van maatregelen adviseren.

5.4 Methode voor concretiseren van eisen naar maatregelen

Volgens artikel 15 van het Vir-bi is de lijnmanager verantwoordelijk voor de implementatie van de beveiligingsmaatregelen. Die implementatie moet in overeenstemming zijn met de exclusiviteitseisen die artikel 13 stelt en geldt voor het onder zijn verantwoordelijkheid vallend informatiesysteem of verantwoordelijkheidsgebied. Het Vir-bi geeft daartoe in de bijlagen al een groot aantal voorgeschreven maatregelen. Voor het overige legt het voorschrift de verantwoordelijkheid bij het lijnmanagement. Het Vir-bi geeft niet aan hoe deze exclusiviteitseisen moeten worden geconcretiseerd naar die door de lijnmanager zelf te bedenken beveiligingsmaatregelen.
Een aantal geïnterviewden duidt aan dat de lijnmanagers van overheidsorganisaties kennis en kunde in huis zouden moeten halen om die vertaling van exclusiviteitseisen naar concrete maatregelen te kunnen maken. Dit baseren zij mede op hun ervaringen met de implementatie van het Vir.

Advies
Wij denken aan het ontwikkelen van een soort richtlijnenboek zoals het richtlijnenboek Informatiebeveiliging SUWI[6] gegevensuitwisseling. Dit document is ook opgesteld volgens de indeling van de Code voor Informatiebeveiliging (CvIB).
De CvIB bestaat uit twee delen: een norm (NEN ISO 27001, voorheen BS 7799-2) en een 'code of practice' (NEN ISO 17799:2005, deze gaat in de toekomst NEN ISO 27002 heten). Certificering gebeurt tegen de norm, de 'code of practice' geeft handreikingen voor de implementatie van maatregelen in de organisatie.
De CvIB geeft een indeling in een aantal beveiligingscategorieën met per beveiligingscategorie één of meer beheersdoelstellingen (objectives) die vermelden wat er moet worden bereikt. Daarnaast bevat de CvIB een inventarisatie van mogelijke maatregelen. Maatregelen die marktconform werken en beveiligen mogelijk maken, inclusief nadere informatie om de implementatie van de beheersmaatregelen te ondersteunen. Door de tweejaarlijkse update van de CvIB wordt het overzicht van maatregelen

[6] Wet Structuur Uitvoering Werk en Inkomen (SUWI)

aangepast aan voortschrijdend inzicht en de ontwikkelingen in de markt voor beveiligingsproducten.

Een werkgroep zoals de WBI zou zo'n richtlijnenboek kunnen ontwikkelen. Voor de beveiliging van gerubriceerde informatie van de NAVO, de EU en van het Galileo-project[7] is de National Security Authority (NSA) op nationaal niveau verantwoordelijk. In Nederland is het NSA-schap een verantwoordelijkheid van de ministers van defensie (de beveiliging van de militaire sector) en van BZK (de beveiliging van de civiele sector). Deze partijen zijn in de WBI vertegenwoordigd.

De IT auditor kan daarbij, op basis van zijn expertise en ervaring met bijvoorbeeld de CvIB, adviseren over te definiëren maatregelen.
Een van de beveiligingsmaatregelen is het uitvoeren van een periodieke audit door een onafhankelijke deskundige. En die rol kan een IT-auditor vervullen.

5.5 Exclusiviteit of vertrouwelijkheid?

Zoals uit de voorgaande paragrafen al bleek, gebruikt het Vir-bi de begrippen exclusiviteit en exclusiviteitseisen. Ook het Vir 1994, waarmee het Vir-bi onlosmakelijk verbonden is, gebruikt het begrip exclusiviteit. En definieert het als "de mate waarin de toegang tot en de kennisname van een informatiesysteem en de informatie daarin is beperkt tot een gedefinieerde groep van gerechtigden".
Het Vir-bi definieert exclusiviteit van de informatie als "de mate waarin de toegang is beperkt tot een gedefinieerde groep van gerechtigden".
In nationale en internationale literatuur, boekwerken en vaktaal over informatiebeveiliging wordt de term vertrouwelijkheid gebruikt in plaats van de term exclusiviteit. Dit is ook de term die wordt gebruikt in de CvIB (met edities uit onder andere 1995, 2000 en 2005).
CvIB definieert het begrip vertrouwelijkheid als de eigenschap dat informatie niet beschikbaar wordt gesteld of wordt ontsloten aan onbevoegde personen, entiteiten of processen.
Vergelijking van het Vir-bi met de Code leidt tot meer verschillen in gebruikte begrippen voor gelijke zaken, bijvoorbeeld rubriceren versus classificeren en merken versus labelen.
Een en ander kan tot begripsverwarring en -onduidelijkheden leiden bij het management en functionarissen die verantwoordelijk zijn voor de implementatie van het Vir-bi. Deze verwarring kan nog groter worden nu in het nieuwe Vir 2007 geen sprake meer is van het begrip exclusiviteit maar van het begrip vertrouwelijkheid. Waarbij het Vir 2007 verwijst naar de CvIB voor het begrippenkader.

Advies
We stellen voor om aan te sluiten op de termen in de CvIB en de term exclusiviteit niet meer te gebruiken. Ook zal het Vir-bi, na een evaluatie van dit voorschrift, in lijn gebracht moeten worden met het nieuwe Vir 2007.

5.6 Alleen aandacht voor het aspect Vertrouwelijkheid?

In het Vir-bi worden "exclusiviteits"-eisen gedefinieerd voor gerubriceerde informatie. (Vanaf nu gebruiken wij het begrip vertrouwelijkheid in plaats van exclusiviteit, zoals voorgaand onder 5.5 aangegeven).

---

[7] Galileo is het satellietnavigatiesysteem dat gebouwd wordt door de Europese Unie als aanvulling op het Amerikaanse Global Positioning System (GPS)

De kwaliteitseisen integriteit[8] en controleerbaarheid[9] zijn ook opgenomen in het Vir-bi. Echter beperkt en alleen voor zover zij voor het behalen van de vertrouwelijkheideisen van belang zijn.
Het Vir-bi vermeldt dat bij de beveiliging van bijzondere informatie zowel de regels van het Vir als die van het Vir-bi gevolgd moeten worden. Informatiebeveiliging volgens het Vir richt zich op de bescherming van integriteit, vertrouwelijkheid en beschikbaarheid van de informatie.
Het Vir-bi wil bijzondere informatie zwaarder tegen onbevoegde kennisname beschermen dan de overige informatie bij de rijksdienst. Daarom bevat het voorschrift, afhankelijk van de kwetsbaarheid van de informatie, eisen voor de vertrouwelijkheid. Die eisen gelden voor de gehele rijksdienst.
Met een aantal geïnterviewden vragen wij ons af of het wel terecht is dat beschikbaarheid en controleerbaarheid van staatsgeheime informatie in het voorschrift geen of nagenoeg geen aandacht krijgen. Daarbij wordt onder andere aangevoerd dat de eisen van vertrouwelijkheid de eisen van beschikbaarheid in de weg kunnen staan. Een aantal geïnterviewden noemt daarbij als voorbeeld het verloren gaan van staatsgeheimen, wat tot veel grotere gevolgen kan leiden dan het verloren gaan van niet gerubriceerde informatie. En dit terwijl op basis van het ‘need to know principe’ staatsgeheime informatie op zo min mogelijk plaatsen wordt opgeslagen. Als er dan om vertrouwelijkheideisen ook nog geen back-up gemaakt kan of mag worden, is de informatie niet meer (direct) beschikbaar in gevallen van bijvoorbeeld verlies of diefstal.
Dit is een reden te meer om de eisen voor vertrouwelijkheid en beschikbaarheid meer in hun samenhang te beschouwen.
Ook kan verwerking van niet-integere, gerubriceerde informatie tot grotere gevolgen leiden dan het verwerken van niet-integere, niet-gerubriceerde informatie. We denken hierbij aan bijvoorbeeld gevolgschade voor het verdere verloop en het succes van opsporing en vervolging van zware criminaliteit en terrorisme.
Ook het aspect controleerbaarheid van de bewerkingen en verstrekkingen van bijzondere informatie, weliswaar in de bijlagen van het voorschrift aangestipt, krijgt in het voorschrift zelf geen plaats. Voor controleerbaarheid moeten voldoende maatregelen zijn getroffen om de bewerkingen en verstrekkingen van bijzondere informatie te kunnen controleren. Geïnterviewden duiden aan dat aandacht voor de controleerbaarheid van bijzondere informatie in het voorschrift zelf te beperkt is.

Advies

Wij geven in overweging in het risicomanagementproces ook de kwaliteitseisen beschikbaarheid (inclusief reproduceerbaarheid), integriteit en controleerbaarheid te betrekken. Waarbij ook nadrukkelijk naar de samenhang tussen de betreffende eisen wordt gekeken. En op basis daarvan de zwaarte, de soort en de omvang van de benodigde maatregelen te bepalen.
Bovendien adviseren we de concretisering van die eisen naar maatregelen niet alleen te baseren op de in het Vir-bi vastgestelde rubricering. Dus niet alleen uit te gaan van de indeling naar omvang en soort schade voor de Staat. Vanuit de doelgroepen ook de aandacht vestigen op de waarde van de informatie voor de processen.
Wij geven in overweging het Vir-bi op dit punt uit te breiden. Het nieuwe

---

[8] Vir-bi : “Voor zover dat noodzakelijk is om de exclusiviteit te waarborgen zijn eisen met betrekking tot integriteit meegenomen.”

[9] Vir-bi : “Accounting (Vastleggen gebruikershandelingen); Er wordt voldoende informatie vastgelegd om een onderzoek van een (vermoed) incident mogelijk te maken”

Vir wil aansluiten op de CvIB. Een Vir-bi dat ook zal aansluiten op de CvIB is hierdoor een logische stap.

Voor de auditor zien we geen adviesrol weggelegd. Wel kan een auditor na incidenten meehelpen een incidentanalyse uit te voeren en op basis daarvan extra of vervangende maatregelen aanbevelen.
De keuze voor een interne of externe IT-auditor kan ingegeven worden door de mate van de ervaring met en de kennis van de bewuste doelgroep en informatieketen.

5.7 Draagvlak voor informatiebeveiliging-bijzondere informatie

De betrokkenheid van het management en het beveiligingsbewustzijn bij alle betrokken partijen zijn volgens de literatuur en ook de CvIB twee van de belangrijkste kritische succesfactoren voor een geslaagde implementatie van informatiebeveiliging.
Uit onze interviews blijkt dat de betrokkenheid van het management en het beveiligingsbewustzijn van de medewerkers binnen de organisaties kunnen verbeteren.
Een algemeen beeld dat tijdens de interviews werd geschetst was dat de informatie over het Vir-bi bij de introductie niet goed is geweest. Met name de informatievoorziening top down vanuit de BVA richting lijnmanagement van de dienstonderdelen wordt als gebrekkig ervaren. Hetzelfde wordt opgemerkt over de communicatie en informatie richting de informatiebeveiligings-coördinatoren van die dienstonderdelen. Geïnterviewden geven ook aan dat er nog te weinig wordt gedacht in ketens en evenmin aan het belang van de ketenpartners. Partners die betrokken zijn bij het genereren, het uitwisselen en verwerken van de bijzondere informatie.
Binnen het Vir-bi wordt volgens ons ook maar beperkt aandacht geschonken aan beveiligingsbewustzijn. In het Vir-bi wordt in bijlage 3 Matrix exclusiviteitseisen bij beveiligingseisen ten aanzien van Personeel, onder de noemer “Beveiligingsscholing en -training” één eis gedefinieerd: “De BVA zet een beveiligingsbewustzijnbevorderend programma op en zorgt voor uitvoer”. Hoe een dergelijk programma op te zetten en uit te voeren is niet aangegeven. Mogelijk dat het ontbreken van die informatie de reden is dat dergelijke bewustzijnbevorderende programma’s nog niet zijn ontwikkeld en uitgevoerd volgens de geïnterviewden.

Advies
Wij adviseren gebruik te maken van een door het Amerikaanse National Institute of Standards and Technology (NIST) uitgebrachte publicatie: *NIST Special Publication 800-50*. Deze publicatie gaat in op het stapsgewijze ontwikkelen en invoeren van een bewustzijnsprogramma voor informatiebeveiliging. Een programma waarbij een duidelijk onderscheid wordt gemaakt en uitgewerkt in bewustzijn, training en opleiding.
Het trainen in de NIST aanpak is gericht op het aanleren van vaardigheden die noodzakelijk zijn om bepaalde functies op een zo veilig mogelijke manier uit te voeren. Bij die training wordt voortgebouwd op de tijdens een bewustzijnscampagne opgedane kennis en wordt voorzien in functionele rollen en verantwoordelijkheden in relatie tot informatiebeveiliging.
Ook biedt de methode handvatten om het management te overtuigen van het nut en de noodzaak van een bewustzijnsprogramma. De kanttekening die hierbij uiteraard moet worden gemaakt is dat NIST een Amerikaans programma is wat zonodig moet worden aangepast aan de Nederlandse cultuur.
Om te voorkomen dat elke BVA een eigen programma gaat ontwikkelen

en uitvoeren, geven wij de voorkeur aan een door BZK centraal gecoördineerde ontwikkeling en uitvoering.

De (IT-)auditor kan vanuit zijn expertise en praktijkervaringen input leveren voor de opzet van de trainings- en opleidingsmodules.

5.8 Kennis en kunde informatiebeveiliging-bijzondere informatie

De geïnterviewden spreken op basis van hun eigen ervaringen over een algemeen gebrek aan (basis)kennis en kunde van informatiebeveiliging. En speciaal van beveiliging van bijzondere informatie bij het lijnmanagement binnen de rijksoverheid.
Het lijnmanagement kan voor de dagelijkse ondersteuning en advies voor informatiebeveiliging terecht bij de departementale beveiligingscoördinator. Volgens geïnterviewden wordt deze functie vaak vervuld door medewerkers uit het primaire proces of een staffunctie. Medewerkers die verantwoordelijkheden toegedeeld hebben gekregen voor informatiebeveiliging-bijzondere informatie. Mensen die hun werk gewoonlijk doen op basis van hun praktijkervaring met fysieke en personele veiligheidsmaatregelen. Slechts weinigen hebben een gerichte en specialistische opleiding in informatiebeveiliging genoten.

Advies
Er zijn master- en hbo-opleidingen ‘information security management’. Wellicht kan een nascholingstraject worden ontwikkeld door bijvoorbeeld de Rijksacademie voor Financiën en Economie voor de BVA’s en de beveiligingscoördinatoren. Hierdoor neemt de rijksoverheid haar verantwoordelijkheid voor informatiebeveiliging en professionaliseert zo het risicomanagement. Daarnaast krijgen de betrokken medewerkers meer greep op de informatiebeveiliging.
De IT-auditor kan een bijdrage leveren. Een aantal IT-auditoren is als docent verbonden aan genoemde opleidingen.

5.9 Verplichte screening en certificering door de AIVD

Volgens het Vir-bi dienen medewerkers van de departementen die omgaan met bijzondere informatie te zijn ‘gescreend’. Zo’n screening, een onderzoek naar de integriteit van de betreffende medewerkers, vindt plaats door de AIVD en in het geval van Defensiemedewerkers door de MIVD. Het onderzoek is ook verplicht voor medewerkers van ondernemingen, die bij hun dienstverlening aan het departement in aanraking komen met bijzondere informatie. De grondigheid van het (justitiële) antecedentenonderzoek is afhankelijk van de rubricering van de informatie waarmee deze mensen in aanraking komen.
Uit interviews en recente Kamerstukken blijkt dat er grote achterstanden bestaan in het uitvoeren van het grote aantal verzoeken om screening door de AIVD. Dit leidt volgens geïnterviewden tot situaties dat nog niet gescreende medewerkers omwille van de continuïteit van de bedrijfsvoering al inhoud geven aan de (nieuwe) functie.
Daarnaast meldden geïnterviewden dat na de eerste screening nog maar incidenteel, of alleen als daar er aanleiding toe is, een nieuw veiligheidsonderzoek plaatsvindt.
Juist een vertrouwensfunctionaris in functie kan echter vanwege de mogelijke toegang tot staatsgeheimen van waarde zijn voor vijanden van de staat. In zoverre is een mens, gescreend of niet, een mogelijk zwakke schakel in de informatiebeveiliging.
In het Vir-bi is ook aangeduid dat beveiligingsproducten gecertificeerd

dienen te worden door de afdeling NBV (Nederlands Bureau Verbindingsbeveiliging) van de AIVD. Deze verplichte certificering geldt al voor producten die ingezet worden ter beveiliging van de informatie met de rubricering Departementaal Vertrouwelijk. Volgens geïnterviewden blijkt dat er ook hier sprake is van tijdrovend onderzoek en vertragingen in de uitvoering. Men duidt daarbij op het reële risico van een situatie dat met achterhaalde of nog niet gecertificeerde producten wordt gewerkt.

Advies
Wij hebben geen onderzoek gedaan naar de mogelijke oorzaken van vertraging in de uitvoering van screening en certificeringen. Ook hebben we geen onderzoek gedaan naar de opzet van het proces van screening van personen respectievelijk het proces van certificering van beveiligingsproducten.
Wij stellen wel voor de gesignaleerde feiten mee te nemen bij een risicoanalyse. Wellicht moet er gezorgd worden voor aanvullende of vervangende beheersmaatregelen of noodprocedures.
Tot slot wijzen we op de gevolgen die ons advies in 5.2, het afschaffen van een aparte rubricering Departementaal Vertrouwelijk, kan hebben. Voor deze (vervallen) rubricering hoeft dan geen certificering van beveiligingsproducten meer plaats te vinden. Dit leidt tot het vrijkomen van onderzoekscapaciteit die ingezet kan worden voor de certificering van producten voor de beveiliging van staatsgeheime informatie.

5.10 Informatiebeveiliging en bedrijfsvoering

Naar de mening van de geïnterviewden maakt informatiebeveiliging op dit moment nog geen integraal onderdeel uit van de bedrijfsvoering bij de rijksoverheid. In Rijk verantwoord 2006, het rapport bij het Financieel jaarverslag van het Rijk 2006 wordt aandacht gevraagd voor de informatievoorziening. Namelijk om goede management- en beleidsinformatie voort te brengen. De managementverantwoordelijkheid zou in het managementcontrolsysteem nog voldoende verankerd moeten worden.

In de bedrijfsvoeringparagraaf van het jaarverslag van een ministerie verantwoordt de minister zich over de bedrijfsvoering. De bedrijfsvoering omvat alle processen die ervoor zorgen dat een ministerie kan functioneren. Daaronder vallen ook de processen voor materieelbeheer, informatievoorziening en -beveiliging.

In de jaarverslagen 2005 en 2006 van de departementen vonden wij maar heel beperkt en incidenteel verantwoordingsinformatie over informatiebeveiliging. Dit geldt voor informatiebeveiliging algemeen, maar zeker voor (de implementatie van) het Vir-bi. Een reden daarvoor kan zijn het moeilijk of niet kunnen vertalen van de waarde van bijzondere informatie naar financiële gevolgen.
Een andere reden kan liggen in het feit dat de bedrijfsvoeringparagraaf in het jaarverslag op dit moment alleen inzoomt op de uitzonderingen.

Advies
Wij stellen voor dat een werkgroep zoals WBI[10] of een werkgroep onder verantwoordelijkheid van de directie POIR[11] van BZK zich buigt over de opzet van de verantwoordingsrapportage in de lijn.
Vir-bi schrijft in art. 13 lid 2 voor dat de secretaris-generaal in het informatiebeveiligingsbeleid aangeeft op welke wijze de lijnmanager

[10] zie afkortingenlijst
[11] idem

rapporteert over de beveiliging van bijzondere informatie.
Modellen voor een dergelijke rapportage ontbreken nog. Wij geven de werkgroep in overweging de doelstellingen voor informatiebeveiliging (inclusief de doelstellingen voor het bewustzijnsbevorderend programma, opleidingen en trainingen) te vertalen naar meetbare normen (key performance indicators).
Deze normen kunnen dan element zijn van de managementinformatie-contracten en de periodieke verantwoordingsrapportages. Daardoor kan inzichtelijk worden gemaakt of organisatiedoelen voor informatiebeveiliging worden behaald of dat bijsturing noodzakelijk is.

Bovendien pleiten wij voor een verantwoordingsparagraaf over informatiebeveiliging in het jaarverslag van elk departement.
Zo'n paragraaf zou dan een vast onderdeel moeten uitmaken van de bedrijfsvoeringmededeling in het jaarverslag waarin niet alleen de uitzonderingen worden gemeld.
Daarbij kunnen de best practice bepalingen van de Code Tabaksblatt naar onze mening een goede leidraad zijn. Ook al geldt deze Code alleen voor de verantwoordingsinformatie in het jaarverslag van beursgenoteerde bedrijven, zij kan toch als voorbeeld dienen voor verantwoordingsinformatie in de jaarverslagen van de rijksoverheid. De Code Tabaksblatt wil immers dat verantwoording wordt afgelegd over interne risicobeheersing- en controlesystemen, in het bijzonder die systemen die betrekking hebben op operationele risico's en relevante wetgeving.
Het Referentiekader Mededeling over de bedrijfsvoering, dat door het Ministerie van Financiën is samengesteld, kan dan uitgebreid worden. De uitbreiding bestaat uit een door de werkgroep te ontwikkelen model waarin de principes voor een dergelijke verantwoordingsparagraaf informatiebeveiliging verder worden uitgewerkt.
In het informatiebeveiligingsbeleid moet opgenomen worden dat het informatievoorzieningbeleid (bijzondere informatie) wordt afgestemd met het informatiebeveiligingsbeleid (bijzondere informatie).

De IAD toetst of het beleid toereikend is en verricht onderzoek naar de bedrijfsvoeringmededeling. De IT-auditoren van een IAD zullen in ieder geval hiertoe gekwalificeerd zijn, echter zeker niet uitsluitend.

5.11 Antwoorden in hoofdlijnen op de onderzoeksvragen

5.11.1 Is er voldoende draagvlak voor het Vir-bi?

Wij concluderen dat er onvoldoende draagvlak bestaat voor het Vir-bi in zijn huidige vorm. Deze conclusie baseren we op de volgende elementen van onze analyse van de interviews en deskresearch:

- Het Vir-bi als voorschrift is op onderdelen niet duidelijk en schiet inhoudelijk tekort als goede leidraad voor het lijnmanagement. Er zijn vier rubriceringen bijzondere informatie geformuleerd waarbij richtlijnen om te rubriceren ontbreken. De tabel in bijlage 2 van het Vir-bi en de toelichting daarop geven voorbeelden die geen houvast bieden voor het maken van een navolgbare keuze. Hierdoor is ook het treffen van extra maatregelen voor de borging van de vertrouwelijkheid van gerubriceerde informatie arbitrair. Het voorschrift wordt ervaren als een sterke beperking van het eigen initiatief en de eigen verantwoordelijkheid van in het bijzonder de lijnmanager. De sterke rule-based benadering kan volgens geïnterviewden belemmerend werken op de procesgang en werkt kostenverhogend bij de inrichting. In het bijzonder lijnmanagers ervaren dit als een hindernis om marktconform te werken en te beveiligen. Het treffen van

maatregelen naast de door het Vir-bi voorgeschreven maatregelen wordt niet ondersteund met goede richtlijnen of methoden.
- Vraagtekens worden geplaatst bij de noodzaak en werkbaarheid van de rubricering “Departementaal Vertrouwelijk”. Er lijkt geen noodzaak voor een aparte rubricering die komt boven op de reguliere classificatie voor vertrouwelijke informatie zoals privacygevoelige gegevens;
- Het ontbreken van (voldoende) aandacht in het Vir-bi voor de risico’s van integriteit, beschikbaarheid en controleerbaarheid van gerubriceerde informatie;
- Informatiebeveiliging wordt nog niet als volwassen en integraal onderdeel van de bedrijfsvoering ervaren;
- Het (nog) ontbreken van een beveiligingsbewustzijnbevorderend programma voor verbetering van het draagvlak voor en betrokkenheid bij beveiliging van bijzondere informatie. De informatie en communicatie bij de introductie van het Vir-bi zijn niet goed verlopen;
- Er is sprake van een gebrek aan (basis)kennis informatiebeveiliging. Met name bij de staffunctionarissen die belast zijn met advisering van het verantwoordelijke lijnmanagement;
- Er zijn tegenstrijdigheden en/ of onduidelijkheden tussen enerzijds het Vir-bi en anderzijds het nieuwe Vir 2007 en de internationaal gebruikte CvIB.

5.11.2 Hoe kan de beveiliging van bijzondere informatie worden versterkt?

Op hoofdlijnen vatten wij onze voorstellen tot verbetering van de beveiliging bijzondere informatie als volgt samen.
In volgorde van prioriteit stellen wij voor:
- Het Vir-bi enten op de baselinebenadering en de risicoanalysemethode van de CvIB. Daarbij wordt rekening gehouden met alle relevante kwaliteitsaspecten zijnde vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid van de bijzondere informatie.
  Deze aspecten moeten in samenhang worden gezien.
- Alleen een of twee rubrieken staatsgeheim en geen rubricering departementaal vertrouwelijk.
  Voor staatsgeheime informatie worden doelgroepsgewijze, aanvullende en speciale maatregelen getroffen op basis van risicomanagement. Per doelgroep wordt daarbij gekeken naar het specifieke karakter en de waarde van de informatie voor zowel de interne processen als voor de keten; bovendien is daarbij aandacht voor de relevante wet- en regelgeving.
- Betrokkenheid van alle partijen (via een vertegenwoordiger) bij de opzet en het onderhoud van maatregelen; daarmee wordt een beter draagvlak voor en betrokkenheid bij het onderwerp informatiebeveiliging gecreëerd bij met name het lijnmanagement en medewerkers; zo wordt ook de eigen verantwoordelijkheid van het lijnmanagement benadrukt;
- De opzet en uitvoering van een op NIST Special Publication 800-50 gebaseerd beveiligingsbewustzijnbevorderend programma voor het lijnmanagement en de medewerkers betrokken bij bijzondere informatieverzorging;
- Het faciliteren van een nascholingstraject informatiebeveiliging voor informatiebeveiligingscoördinatoren en BVA’s die niet een Information Security Management opleiding hebben gevolgd;
- “Let CIA be the key”; goede Communicatie, Informatie en Advies (ook van de IT-auditor) zijn de sleutel voor een succesvolle borging van

Confidentiality, Integrity en Availability van bijzondere informatie;
- Na te denken over de wijze van rapporteren door lijnmanagers over informatiebeveiliging aan de secretaris generaal op het departement; daarbij in het managementcontract en de periodieke rapportages kpi's op te nemen;
- Na te denken over het opnemen van verantwoordingsinformatie over bijzondere informatiebeveiliging in de departementale jaarverslagen. Namelijk in een aparte verantwoordingsparagraaf over interne risicobeheersings- en controlesystemen, in het bijzonder die systemen die betrekking hebben op operationele beveiligingsrisico's en relevante wetgeving.

5.11.3 Hoe kan de IT-auditor vanuit zijn adviesrol bijdragen aan de naleving van het Vir-bi?

In de paragrafen 5.1 tot en met 5.10 hebben we onze adviezen tot verbetering van het draagvlak in detail beschreven. Daarbij hebben we vermeld welke rol de IT-auditor daarbij kan spelen.
Samengevat kan een IT-auditor een bijdrage leveren bij de totstandkoming van een goed pakket aanvullende maatregelen voor de beveiliging van bijzondere informatie (voor alle kwaliteitsaspecten). Hij kan dat doen vanuit een klankbordfunctie (consultatie of counseling) of als 'quality assurance' functionaris. Of als projectmanager in een project tot ontwikkeling van die aanvullende beveiligingsmaatregelen.
Wij adviseren hierbij ook vertegenwoordigers van externe partijen te betrekken, namelijk die partijen die ervaring hebben met de implementatie van de Code voor Informatiebeveiliging.
Een eveneens waardevolle bijdrage kan geleverd worden bij het doelgroepsgewijze uitbreiden van de baseline met aanvullende, specifieke maatregelen. Aanvullende specifieke maatregelen zoals Digital Rights Management, encryptie in de applicaties en dergelijke kunnen worden beoordeeld door de auditor.
Ook kan een IT-auditor materiaal ontwikkelen voor het programma gericht op het creëren van beveiligingsbewustzijn. Daarbij kan hij vanuit de eigen expertise en praktijkervaringen input leveren voor de opzet van de training- en opleidingsmodules. En tot slot kan hij als specialist / docent optreden tijdens een scholingscursus voor informatiebeveiligings-coördinatoren en BVA's.

6 Beveiliging bijzondere informatie en de assurancerol van de IT-auditor

Het Vir-bi schrijft in art. 13 lid 2 letter c dat het de verantwoordelijkheid van de secretaris-generaal binnen een ministerie is, dat het informatiebeveiligingsbeleid iedere twee jaar wordt geëvalueerd. Een evaluatie van het beleid voor de bijzondere informatie, voor het eerst in 2007, door een onafhankelijke deskundige. Het Vir-bi licht dit nader toe. "*De onafhankelijke deskundige beoordeelt in hoeverre de beveiliging van bijzondere informatie in overeenstemming is met de eisen van dit voorschrift".* En vult daarbij aan: "*De functie van onafhankelijk deskundige kan bijvoorbeeld worden vervuld door een EDP-auditor*".
De waarde van het oordeel van een onafhankelijke deskundige neemt nog toe gezien de inhoud van artikel 16 Vir-bi en de daarbij gegeven toelichting. Het betreffende artikel definieert de verantwoordelijkheid van de Minister van Binnenlandse Zaken voor bijzondere informatie binnen de rijksoverheid. "*De minister van Binnenlandse Zaken en Koninkrijksrelaties rapporteert eens in de twee jaar aan de ministerraad over de beveiliging van bijzondere informatie binnen de rijksdienst*". Dat wordt als volgt nader toegelicht. "*Voor deze rapportage kan onder meer gebruik worden*

gemaakt van de gegevens afkomstig uit de evaluatie als bedoeld in artikel 13, tweede lid onder c."

Naar aanleiding van deze artikelen in het Vir-bi hebben wij de volgende onderzoeksvragen gedefinieerd:

1. *wie zijn de stakeholders bij een goede beveiliging van bijzondere informatie?*
2. *hoe kunnen deze stakeholders zekerheid krijgen over een goede beveiliging van bijzondere informatie? Welke assurance kan een IT-auditor daarbij geven?*
3. *Wat is de rol van de IT-auditor bij het verkrijgen van die zekerheid?*

6.1 Stakeholders en zekerheid bij een goede beveiliging van bijzondere informatie

In deze paragraaf geven wij als antwoord op de eerste vraag een opsomming van de stakeholders en geven daarbij tegelijkertijd een antwoord op de vraag: *Hoe kunnen deze stakeholders zekerheid krijgen over een goede beveiliging van bijzondere informatie?*
Hierbij gebruiken wij een bottom-up benadering en onderkennen de volgende stakeholders:

1) De medewerkers op departementen en de daaronder vallende onderdelen van de rijksdienst. Het betreft hier in het bijzonder de functionarissen met screening A, B en C. Deze zijn belast met de verwerking van bijzondere informatie. Ook noemen we hier het lijnmanagement dat verantwoordelijk is voor die informatie-verzorging en een adequate beveiliging daarvan. Door middel van self-assessment controleert en rapporteert de verantwoordelijke functionaris (A, B, C) periodiek de kwaliteit van de beveiligings-maatregelen binnen het eigen verantwoordelijkheidsgebied.
   De verantwoordelijke lijnmanager kan de resultaten van het self-assessment door een interne audit laten toetsen.
   De BVA kan, namens de secretaris-generaal, bijvoorbeeld jaarlijks een onderzoek (laten) instellen naar de betrouwbaarheid van de door het lijnmanagement afgelegde verantwoording.
2) De ondernemingen en hun medewerkers. Ondernemingen die in verband met hun leveringen en diensten aan de rijksoverheid in aanraking komen met bijzondere informatie.
   De departementale auditor, de AIVD of een in te huren externe auditor zal in opdracht van de secretaris-generaal een onderzoek instellen bij die ondernemingen. De auditor zal daarbij moeten vaststellen dat de maatregelen voor beveiliging van bijzondere informatie zijn verwezenlijkt en worden nageleefd.
3) De Minister van Binnenlandse Zaken en Koninkrijksrelaties. Deze rapporteert eens in de twee jaar aan de ministerraad over de beveiliging van bijzondere informatie binnen de rijksdienst. Hij kan daartoe onder meer gebruik maken van de gegevens afkomstig van de evaluatie welke door de secretaris-generaal op elk departement is ingesteld. Daartoe kan deze minister de eigen auditor, de AIVD of een externe auditor inschakelen.
4) De Tweede Kamer. Deze zal door inschakeling van de Algemene Rekenkamer (AR) zekerheid wil verkrijgen over de beveiliging van bijzondere informatie. De AR kan daartoe gebruik maken van de werkzaamheden en rapportage van de departementale auditor. Ook kan men gebruik maken van de rapportage en werkzaamheden welke in opdracht van de Minister van Binnenlandse Zaken zijn uitgevoerd bij de tweejaarlijkse evaluatie.
5) De internationale partners in de EU, NAVO en het Galileo-project. Deze hebben behoefte aan assurance over de naleving van de internationale regels. De EU kan daartoe gebruik maken van de

Europese Rekenkamer. Audits kunnen assurance verschaffen; auditoren hebben de kennis en vaardigheden om zo'n audit uit te voeren. IT-auditoren hebben kennis van nieuwe technologie en zijn geschoold in het auditen van informatiebeveiliging. Daarom kunnen zij de genoemde onafhankelijke deskundige zijn.

6.2 Waarom de inzet van een IT-auditor?

De praktijk van hedendag leert dat de verwerking van bijzondere en staatsgeheime informatie onderdeel uitmaakt van de totale informatieverwerking van departementen. Daarbij neemt de inzet van informatietechnologie grote vormen aan. En ook de interdepartementale informatie-uitwisseling en het samenwerken in ketens met leveranciers en afnemers van informatie buiten het eigen departement verloopt via technologische middelen. De aan de inzet van informatietechnologie gerelateerde risico's pleiten voor de inzet van een IT-expert. De mens blijft echter de zwakste schakel in de informatiebeveiliging. De IT-auditor heeft in zijn studie geleerd dat de strategie, doelen, cultuur en kenmerken van de organisatie een rol spelen bij het classificeren van informatie. En als belangrijk of als bijzonder gelden bij het kiezen van de beveiligingsmaatregelen. Deze maatregelen moeten worden toegesneden op de organisatie. Een IT-auditor kan dus de genoemde onafhankelijke deskundige zijn, echter zeker niet bij uitsluiting van andere onderzoekers. Voor een audit naar informatiebeveiliging waarin IT een belangrijke component is, kan een IT-auditor in het auditteam niet ontbreken.

7 Randvoorwaarden bij werkzaamheden door de IT-auditor

In hoofdstuk 5 hebben wij aangegeven op welke wijze de IT-auditor vanuit een adviesrol kan bijdragen aan de totstandkoming van de beveiliging van bijzondere informatie.
In paragraaf 6.1 zijn we ingegaan op de diverse stakeholders en mogelijke assuranceopdrachten voor de IT-auditor.
Algemeen geldt dat de IT-auditor de werkzaamheden uitvoert in overeenstemming met de Code of Ethics en daarbij de fundamentele basisbeginselen in acht neemt:
- integriteit: eerlijk en oprecht optreden;
- objectiviteit: geen aantasting van het oordeel door vooroordeel, belangentegenstelling of ongepaste beïnvloeding door een derde;
- deskundigheid en zorgvuldigheid: rekening houden met actuele ontwikkelingen in de praktijk, wetgeving en vaktechniek en handelen in overeenstemming met vaktechnische en beroepsvoorschriften;
- geheimhouding: eerbiedig het vertrouwelijke karakter van verkregen informatie;
- professioneel gedrag: zich houden aan relevante wet- en regelgeving en het auditberoep niet in diskrediet brengen.

De fundamentele beginselen *objectiviteit* en *geheimhouding* willen wij hier nog extra belichten. Wat betreft het beginsel objectiviteit zal de IT-auditor moeten waken voor het collisiegevaar. Dit kan ontstaan indien hij zijn eigen werkzaamheden of het resultaat daarvan beoordeelt. Dus het beoordelen van de in hoofdstuk 5 genoemde werkzaamheden vanuit de adviesrol en de resultaten daarvan.
Het beginsel geheimhouding geldt heel nadrukkelijk daar de werkzaamheden betrekking hebben op de beveiliging van staatsgeheime informatie. Voor de auditrol zal naast een door de AIVD uit te voeren screening, het fundamentele basisbeginsel geheimhouding nog extra aandacht kunnen krijgen. Namelijk door goede aandacht te geven aan de

volgende artikelen in de Code of Ethics.
1. De IT-auditor overweegt de noodzaak de geheimhoudingsplicht in acht te nemen binnen de auditorganisatie waaraan hij is verbonden of waarbij hij werkzaam is of binnen de organisatie waarbij of ten behoeve waarvan hij werkzaam is (artikel A-140.4).
2. De IT-auditor treft de redelijkerwijs te nemen maatregelen om te waarborgen dat de voor hem geldende geheimhoudingsplicht in acht wordt genomen door personeelsleden die hiërarchisch aan hem ondergeschikt zijn en door personen aan wie hij om advies of ondersteuning vraagt. (artikel A-140.5)

8 Conclusie en aanbevelingen per verantwoordelijke

De conclusie van ons onderzoek is dat het Vir-bi geen helder voorschrift is en in de huidige vorm verwarring en onduidelijkheid met zich brengt. Het voorschrift bevat veel rubriceringen, maar schiet tekort in de uitleg hoe die rubriceringen toe te passen. Wanneer vertrouwelijke informatie ook ‘Departementaal Vertrouwelijke informatie’ is, is eveneens niet helder voor betrokkenen. Zij plaatsen nadrukkelijk vraagtekens bij de noodzaak van die rubricering.
De maatregelen die worden beschreven als passend bij de rubrieken bijzondere informatie worden niet als passende maatregelen gezien. De sterke rule-based benadering kan belemmerend werken op de procesgang en werkt kostenverhogend bij de inrichting van verwerking en beveiliging van bijzondere informatie.
De gedetailleerde benadering en beschrijving in de bijlagen van het voorschrift hebben als risico dat de voorgeschreven maatregelen niet meer passen in het tijdsgewricht.
Dit verklaart waarom er sprake is van een gebrekkig draagvlak voor het Vir-bi. Een gebrekkig draagvlak staat een succesvolle implementatie en toepassing van het voorschrift in de weg.

In paragraaf 5.11.3 hebben wij onze adviezen voor verbetering beschreven.
Op hoofdlijnen samengevat willen we onze adviezen richten aan:
1. de wetgever, in het bijzonder het ministerie van Binnenlandse Zaken en Koninkrijksrelaties als coördinerend ministerie waaronder ook de AIVD ressorteert,
2. de departementen, in het bijzonder de BVA’s die de bij hen aanwezige bijzondere informatie moeten beveiligen en
3. onze collega’s, de (interdepartementale en departementale) IT-auditoren.

1. Wij adviseren het ministerie van Binnenlandse Zaken en Koninkrijksrelaties:
   - De resultaten van ons onderzoek mee te nemen in de evaluatie van het Vir-bi. Deze evaluatie van het Vir-bi is aan de Tweede Kamer toegezegd bij de behandeling van de jaarverslagen 2006 op 16 mei 2007;
   - Op basis van onze bevindingen en argumenten te overwegen Vir-bi aan te passen respectievelijk te vervangen. En daarbij naast het aspect vertrouwelijkheid rekening te houden met de aspecten beschikbaarheid, integriteit en controleerbaarheid. De maatregelen die al getroffen moeten worden op basis van de Wbp kunnen worden aangevuld op basis van risicomanagement door de gebruikers van specifieke informatie (doelgroepen);
   - In het geval van handhaving van de drie rubriceringen

staatsgeheim na te denken over de ontwikkeling van rubriceringrichtlijnen, een beslissingstabel of questionnaire. In ieder geval een instrument waarmee het lijnmanagement veel beter dan nu uit de voeten kan met rubriceren van de informatie.
- Het Vir-bi in ieder geval in lijn te brengen met het in de CvIB opgenomen begrippenkader;
- Na te denken over de mogelijkheden om te stimuleren en uit te dragen dat informatiebeveiliging een integraal onderdeel is van de bedrijfsvoering. Een mogelijkheid hiertoe is om verantwoordings-informatie over de beheersing van informatiebeveiligingsrisico's een plaats te geven in de bedrijfsvoeringmededeling. Dit kan gebeuren op de wijze zoals de Code Tabaksblatt dat voorschrijft voor beursgenoteerde ondernemingen;
- Te overwegen middelen ter beschikking te stellen en de coördinatie op zich te nemen voor de opzet van een beveiligingsbewustzijnbevorderend programma en opleidingen.

2. Wij adviseren de departementen, in het bijzonder de BVA's:
   - Hun kennis en ervaring in te brengen, met name voor de binnen hun eigen departement aanwezige doelgroepen;
   - De opzet en uitvoering van een beveiligingsbewustzijn-bevorderend programma op te pakken. We geven daarbij in overweging dit programma te baseren op een door het Amerikaanse National Institute of Standards and Technology (NIST) uitgebrachte publicatie: *NIST Special Publication 800-50*. Deze publicatie gaat in op het ontwikkelen en invoeren van een bewustzijnsprogramma voor informatiebeveiliging.
   - "Let CIA be the key" . Goede Communicatie, Informatie en Advies kunnen de implementatie van een (vernieuwd) Vir-bi bevorderen. En daarmee de sleutel tot succes zijn voor een goed waarborgen van de Confidentiality, Integrity, Availability en Auditability van de bijzondere Informatie.

3. Tot slot wenden we ons tot onze collega's, de IT-auditoren. Hun deskundigheid en ervaring zijn gewenst, zowel voor het geven van advies als assurance. De uitdagingen voor het beroep liggen in het breed worden ingezet: zowel voor consultancy om het management te adviseren over het ontwikkelen van een beleid voor bijzondere informatiebeveiliging en een toegesneden normenkader, als voor het uitvoeren van brede of juist diepgaande onderzoeken naar de organisatorische en technische aspecten van de bijzondere informatiebeveiliging. Het is de uitdaging voor de IT-auditor om op alle niveaus een gesprekspartner te zijn met zijn kennis van (nieuwe) technologieën en organisaties. Taken die op zijn pad zouden kunnen liggen voor de invoering en naleving van het Vir-bi (of een nieuw Vir-bi) zijn:
   - De advisering bij het ontwikkelen van een samenstel van aanvullende beveiligingsmaatregelen voor bijzondere informatie. Een samenstel dat zoveel mogelijk aansluit bij de internationale standaarden en daarenboven wellicht gepaste maatregelen per te onderkennen doelgroep. De kennis die een IT-auditor heeft van de Code van Informatiebeveiliging kwalificeert hem hiervoor.
   - Het ontwikkelen van materiaal voor het programma gericht op het creëren van beveiligingsbewustzijn. Een IT-auditor kan vanuit de eigen expertise en praktijkervaringen bijdragen aan de opzet van opleidingsmodules.
   - Als specialist / docent fungeren in een scholingstraject voor

informatiebeveiligingscoördinatoren en BVA's;
- Het geven van zekerheid aan zowel nationale als internationale stakeholders, die betrokken zijn of belang hebben bij de verwerking en beveiliging van bijzondere informatie. Zekerheid over een adequate verwerking en beveiliging van die informatie. De interne, departementale IT-auditor is daarbij een schakel in de keten van government governance van het departement. En geeft die zekerheid binnen het departement en voor de bestuurder. Voor de overige nationale en de internationale stakeholders zal een (inter-)departementale IT auditor of externe IT-auditor onderzoek kunnen verrichten om de gewenste assurance te geven.

In hoofdstuk 7 'Randvoorwaarden bij werkzaamheden door de IT-auditor' hebben wij een aantal aandachtspunten beschreven. Daarbij duiden we aan dat naast de aspecten objectiviteit en geheimhouding die voor iedere auditor gelden een screening vereist is. Een systeem dat bijzondere informatie bevat, mag alleen door een gescreende auditor worden onderzocht.

Bijlagen

Bijlage 1 Lijst met gebruikte afkortingen

AIVD	Algemene Inlichtingen en Veiligheidsdienst
AR	Algemene Rekenkamer
BVA	Beveiligingsambtenaar
BZ	Buitenlandse Zaken
BZK	Binnenlandse Zaken en Koninkrijksrelaties
CvIB	Code voor Informatiebeveiliging
Dept.	Departementaal
EDP	Electronic Data Processing
EU	Europese Unie
FIOD-ECD	Fiscale Inlichtingen- en Opsporingsdienst - Economische Controledienst
IAD	Interne Auditdienst
IT	Informatie Technologie
MIVD	Militaire Inlichtingen en Veiligheidsdienst
NAVO	Noord-Atlantische Verdragsorganisatie (Engelse afkorting: NATO)
NSA	National Security Authority
POIR	directie Personeel, Organisatie en Informatie Rijk van het ministerie van BZK
Stg.	Staatsgeheim
SUWI	Wet Structuur Uitvoering Werk en Inkomen
Vir	Voorschrift informatiebeveiliging rijksdienst
Vir-bi	Voorschrift informatiebeveiliging rijksdienst-bijzondere informatie
WBI	Werkgroep Bijzondere Informatiebeveiliging
Wbp	Wet bescherming persoonsgegevens

Bijlage 2 Lijst met definities van gebruikte begrippen en bronvermelding

A-functies: Functies waarin werkzaamheden worden verricht met betrekking tot zeer geheim en lager gerubriceerde informatie (bron Vir-bi)

Baseline informatiebeveiliging: een (samengestelde) lijst van minimale beveiligingsmaatregelen (security controls), waarmee een basisbeveiligingsniveau (security baseline) kan worden bereikt (bron Portaal Informatiebeveiliging)

Bedrijfsmiddel: alles dat waarde heeft voor de organisatie (bron CvIB)

Beschikbaarheid: kenmerk dat iets toegankelijk en bruikbaar is op verzoek van een bevoegde entiteit (bron CvIB)

Beveiligingsambtenaar: een door de secretaris generaal aangewezen ambtenaar die belast is met de integrale beveiliging van organisatie, medewerkers, materieel, informatiesystemen, gebouwen en overige objecten (bron Beveiligingsvoorschrift Rijksdienst 2005)

B-functies: Functies waarin werkzaamheden worden verricht met betrekking tot geheim en lager gerubriceerde informatie (bron Vir-bi)

C-functies: Functies waarin werkzaamheden worden verricht met betrekking tot confidentieel gerubriceerde informatie (bron Vir-bi)

Departementaal Vertrouwelijke Informatie: overige (bijzondere) informatie waarvan kennisname door niet-gerechtigden nadelige gevolgen kan hebben voor de belangen van een of meer ministeries (bron Vir-bi)

Informatiebeveiliging: behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie; daarnaast kunnen ook andere eigenschappen, zoals authenticiteit, verantwoording, onweerlegbaarheid en betrouwbaarheid hierbij een rol spelen (bron CvIB)

Integriteit: eigenschap dat de nauwkeurigheid en volledigheid van bedrijfsmiddelen wordt beveiligd (bron CvIB)

Risicomanagement: gecoördineerde activiteiten om een organisatie sturing te geven en te bewaken met betrekking tot risico's (bron CvIB)

Staatsgeheim: bijzondere informatie waarvan kennisname door niet-gerechtigden nadelige gevolgen kan hebben voor de belangen van de Staat en / of van zijn bondgenoten. Er zijn drie categorieën staatsgeheimen: Zeer geheim (ernstig schade), Geheim (schade) en Confidentieel (nadeel). (bron Vir-bi)

Vertrouwelijkheid: eigenschap dat informatie niet beschikbaar wordt gesteld of wordt ontsloten aan onbevoegde personen, entiteiten of processen (bron CvIB)

Bijlage 3 Deskresearch en literatuurstudie

Deskresearch en literatuurstudie
1. **Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie 2004**
2. **Besluit Voorschrift informatiebeveiliging rijksdienst 1994** *Besluit van 22 juli 1994, nr. 94/M004882, Stcrt. 173*
3. **Besluit Voorschrift informatiebeveiliging rijksdienst 2007**
4. **Beveiligingsvoorschrift rijksdienst 2005**
5. **Wet Bescherming staatsgeheimen**, *Wet van 5 april 1951, houdende nadere voorzieningen met betrekking tot de bescherming van gegevens, waarvan de geheimhouding door het belang van de Staat wordt geboden*
6. **Wet Veiligheidsonderzoeken** *Wet van 10 oktober 1996, houdende regelen inzake het verrichten van veiligheidsonderzoeken*
7. **Inbreng bij wijziging van de Wet veiligheidsonderzoeken** *ChristenUnie, Arie Slob, 25 oktober 2006*
8. **Wet op de inlichtingen- en veiligheidsdiensten 2002**
9. **De Comptabiliteitswet**
10. **Code of Ethics voor IT-auditoren (Norea)** *Vervanging van het Reglement Gedrags- en Beroepsregels Register EDP-Auditoren, geldt met ingang van 14 juli 2006*
11. **Handboek Vir-bi bevordering, deel 1** *Het handboek is een product van de afdeling Beleid en Expertise van de directie Beveiliging van de AIVD* *handboek d.d. 21-11-2005; bevindt zich nog in concept status*
12. **NEN-ISO/IEC 17799** Informatietechnologie – Beveiligingstechnieken – Code voor Informatiebeveiliging **NEN-ISO/IEC 27001** Informatietechnologie – Beveiligingstechnieken – Informatiebeveiliging - Eisen
13. **Beveiliging van persoonsgegevens, Achtergrondstudies en Verkenningen 23 (www.cpb.nl),** *uitvoeringsmaatregelen in het licht van de Wet Bescherming persoonsgegevens*
14. **NIST Special Publication 800-50** (www.nist.gov)
15. **Instructie ICT/Informatiebeveiliging, deel Vir-bi;** *instructie onderzoek Algemene Rekenkamer d.d. 24-11-2006* *onderzoek AR om na te gaan of er zekerheid is dat 'bijzondere' informatie rijksbreed goed en consistent beveiligd is tegen kennisname door onbevoegde personen. AR bekijkt hiertoe hoe het staat met het verschaffen van een rijksbreed beeld hiervan door BZK aan de ministerraad*
16. **Algemeen beleidsplan beveiliging Ministerie van Financiën** *ultimo 2005; auteur BVA Ministerie van Financiën*
17. **Voorstel inventarisatie Bijzondere informatie Belastingdienst** *Voorstel van departement aan Belastingdienst (Tafel ARGI, Aandacht*

Risicobeheersing, Gegevensbeveiliging en Integriteit), d.d 15 augustus 2005
18. Convenant inzake informatie-uitwisseling tussen de Belastingdienst en de Algemene Inlichtingen- en Veiligheidsdienst *convenant nr. 2459337/01, d.d. 2 november 2005*
19. Werkinstructie uitwisselen van operationele informatie op verzoek *bijlage bij Convenant inzake informatie-uitwisseling tussen de Belastingdienst en de Algemene Inlichtingen- en Veiligheidsdienst; convenant nr. 2459337/01, d.d. 2 november 2005*
20. Werkinstructie spontane informatieverstrekking door Belastingdienst *bijlage bij Convenant inzake informatie-uitwisseling tussen de Belastingdienst en de Algemene Inlichtingen- en Veiligheidsdienst; convenant nr. 2459337/01, d.d. 2 november 2005*
21. Richtlijnen behandeling staatsgeheimen en BZ-(personeels)-vertrouwelijke informatie *Een handleiding; uitgave van Ministerie van Buitenlandse Zaken, december 2005*
22. MP1010, *Voorschriften van het ministerie van Defensie over omgaan met gerubriceerde informatie*
23. Omgaan met gerubriceerde en kwetsbare informatie, Aanwijzingen voor de beveiliging van staatsgeheimen en vitale onderdelen bij de rijksdienst, Merkingsregeling, *brochures en handleidingen van het ministerie van BZK*
24. Handboek EDP-auditing
25. Handboek Informatiebeveiliging Rijksdienst, opgesteld door het ACIB, 1995
26. Afhankelijkheids- en Kwetsbaarheidsanalyse; brochure deel I-II; opgesteld door het ACIB, 1994
27. Jaarverslagen 2005 en 2006 van de AIVD
28. Tweede Kamer, vergaderjaar 2006-2007, 31 031, nr. 2 Rijk verantwoord 2006 en 31 031 VII, nr. 2 Jaarverslag en slotwet ministerie van BZK 2006
29. Waardevol maakt kwetsbaar, *Het belang van informatiebeveiliging, oratie van Marcel Spruit, 3 december 2003*
30. Aanpassing Voorschrift Informatiebeveiliging Rijksdienst, *Sven Planken, Marcel Spruit en Wilbert Vrouwenvelder, Informatiebeveiliging oktober 2005*
31. Informatiebeveiliging onder controle, 2e editie, *P. Overbeek, E.Roos Lindgreen, M. Spruit*
32. NOREA Geschrift No 1, getiteld 'IT-auditing aangeduid', uit 1998
33. Artikelen over het VIR: Aanpak Pragmatische invoering Vir; Zin en onzin van het Vir, Kennisbank ZBC Consultants BV
34. Diverse krantenartikelen en daaruit voortvloeiende Kamervragen http://www.aivd.nl http://www.minbzk.nl/onderwerpen/veiligheid/algemene/kamerstukken?ActItmIdt=80965 http://www.minocw.nl/documenten/brief2k-2005-doc-26809.pdf