Toezicht C2000 stand van zaken 2005-2006

Inspectie
OPENBARE ORDE
EN VEILIGHEID

Toezicht C2000
stand van zaken 2005-2006

Inspectie Openbare Orde en Veiligheid

Den Haag

juli 2007

INSPECTIE OPENBARE ORDE EN VEILIGHEID

Inspectie Openbare Orde en Veiligheid (Inspectie OOV)
Bezoekadres: Juliana van Stolberglaan 148, 2595 CL Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
Telefoon: (070) 426 62 61
Telefax: (070) 426 69 90
Website: www.ioov.nl

COLOFON

Uitgave: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Inspectie Openbare Orde en Veiligheid
Lay out: Grafisch Buro van Erkelens
Fotografie cover: Fons Sluiter fotografie
Drukwerk: drukkerij Hega, Den Haag

ISBN 978-90-5414 -135-8

juli 2007

Inhoudsopgave

Onze missie

De Inspectie OOV levert een bijdrage aan de veiligheid van de samenleving. Zij oefent daartoe toezicht uit op besturen en organisaties die verantwoordelijk zijn voor de openbare orde en veiligheid en stelt hen daarmee in staat de veiligheid te verbeteren.

De Inspectie OOV houdt, onder de verantwoordelijkheid van de ministers van BZK en van Justitie, toezicht op de kwaliteit van de taakuitvoering van zowel de verantwoordelijke bestuursorganen als de operationele diensten die op de verschillende onderdelen van het OOV-terrein actief zijn (politie, brandweer, GHOR).

De Inspectie OOV laat zich leiden door enerzijds de inschatting van maatschappelijke veiligheids-risico's en anderzijds door de vraag waar zij met haar toezicht maximaal kan bijdragen aan het realiseren van beoogde beleidseffecten. In haar werkplannen, jaarverslagen en rapportages worden de gemaakte keuzes en gevolgde werkwijzen verantwoord.

Het oordeel van de Inspectie OOV komt onafhankelijk tot stand.

De Inspectie OOV draagt haar bevindingen actief uit. Zij geeft daarmee de ministers en de onder toezicht staande organisaties inzicht in hun bijdragen aan de kwaliteit van het veiligheidsniveau en de praktische uitwerking van het gevoerde beleid. De Inspectie OOV beoogt daarmee bij betrokkenen een oriëntatie op permanente aandacht voor verbetering tot stand te brengen.

De Inspectie OOV zoekt actief samenwerking met andere partijen van beleid, uitvoering en toezicht, zowel op het OOV-domein als op aanverwante terreinen.

De Inspectie OOV weet wat er leeft en toetst of het werkt.

Inleiding

DOELSTELLING RAPPORTAGE

De Inspectie Openbare Orde en Veiligheid (Inspectie OOV) wil rapporteren over de door haar in het kader van toezicht C2000 uitgevoerde activiteiten. Daarbij maakt zij onderscheid tussen de periode tot oktober 2006[1] (afronding landelijk C2000 project) en de periode daarna. Het in 2004 bijgestelde Beveiligingsbeleid C2000 is daarbij het vertrekpunt. De Inspectie OOV geeft een beeld weer van de wijze van naleving van het Beveiligingsbeleid op basis van twee regionale pilot onderzoeken. Tevens geeft de Inspectie aan welke activiteiten zij oppakt.

WAT IS C2000?

C2000 is sinds juni 2004 hét landelijke digitale netwerk voor mobiele communicatie voor hulpverleningsdiensten. Het systeem maakt communicatie mogelijk met meerdere disciplines tegelijk. Het gesloten en beveiligde netwerk is zowel geschikt voor spraak als voor datacommunicatie. Doordat C2000 is gebaseerd op de Europese TETRA-standaard is communicatie met buitenlandse hulpverleners over de landgrenzen mogelijk, zodra de buurlanden ook feitelijk met dezelfde standaard werken. Momenteel wordt er nog gewerkt met tussenoplossingen.

De algemene doelstelling van het C2000 systeem is:
De openbare orde en veiligheid diensten (OOV-diensten) brandweer, ambulancediensten, politie en Koninklijke Marechaussee in staat te stellen de hulpverlening aan de burgers snel en effectief te kunnen uitvoeren en de veiligheid van de hulpverlener te kunnen waarborgen[2]

C2000, BETROUWBAARHEID EN RISICO'S

Betrouwbaar systeem

De OOV-diensten zijn sterk afhankelijk van een betrouwbaar C2000 syteem. Valt bijvoorbeeld C2000 uit, dan hebben zowel meldkamer(s) alsmede een grote groep politie-, brandweer- en ambulancepersoneel (en daaraan gelieerden) daar last van. Het landelijke Beveiligingsbeleid definieert betrouwbaarheid in termen van de volgende vijf kwaliteitsaspecten: vertrouwelijkheid, integriteit, beschikbaarheid, controleerbaarheid en beheersbaarheid. Uit de gehanteerde definitie blijkt dat betrouwbaarheid meer omvat dan alleen beschikbaarheid.

1 Algemeen overleg met de minister van Binnenlandse Zaken en Koninkrijksrelaties d.d. 22-09-2006 over:
- de brief d.d. 19 april 2006 met de voortgangsrapportage C2000 (25 124, nr. 48)
- de brief d.d. 21 juni 2006 met het rapport Eindevaluatie groot project C2000 (25 124, nr. 49).

2 Uit Beveiligingsbeleid C2000, december 2004.

Zowel in alledaagse situaties als in rampen- en crisissituaties is communicatie essentieel. Daarom heeft de politiek destijds gekozen voor een communicatienetwerk dat specifiek bedoeld is voor de OOV-diensten. De minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is eindverantwoordelijk voor de betrouwbaarheid van C2000 en stelt daartoe eisen aan gebruikersorganisaties en een keur van overige organisaties (leveranciers, beheerorganisaties en onderhouds-organisaties). Deze eisen staan verwoord in het periodiek bij te stellen Beveiligingsbeleid C2000, omdat beveiliging om (procesmatige) risicobeheersing draait en niet is op te vatten als eenmalige actie.

Voorbeelden van wat er fout kan gaan

De natuur dan wel de omgeving kan bijvoorbeeld tegenwerken. Denk daarbij aan schade door stormen, overstromingen, brand, elektriciteitsuitval en kabelverwoestende graafmachines. Ook kunnen er zich storingen voordoen in apparatuur en programmatuur. Apparatuur kan verdwijnen door verlies of diefstal. De huidige encryptie technieken kunnen verouderd raken waardoor gevaar voor afluisteren dreigt. Gebruikers- en beheerorganisaties kunnen geen greep op de beveiliging van C2000 krijgen/houden.

Beheersmaatregelen

Bij beveiliging C2000 draait het om een samenhangend pakket van maatregelen en procedures die ervoor zorgt dat C2000 betrouwbaar werkt. Verschillende partijen moeten daar aan bijdragen. Het draait hierbij om het beheersen van risico's en het zo nodig treffen van maatregelen. Beheersen impliceert periodiek analyseren, plannen, uitvoeren, toetsen en zonodig bijstellen.

ORIËNTATIEFASE

De Inspectie OOV heeft bij de inrichting van toezicht op C2000 gekozen voor een gefaseerde aanpak. Deze eerste fase behelst een oriëntatie op C2000. Doel van de oriëntatiefase is het verkrijgen van inzicht in de stand van zaken met betrekking tot de implementatie (en mogelijke knelpunten bij implementatie) van het Beveiligingsbeleid, waarbij de focus met name is gericht op gebruikersorganisaties met zijdelingse aandacht voor de centrale beheerorganisatie. Op basis van documentenstudies, interviews, het volgen van ontwikkelingen in brede zin en het uitvoeren van een tweetal pilot onderzoeken in de regio heeft de Inspectie OOV een indruk verkregen over het operationaliseren en beveiligen van C2000. Ter afsluiting van de oriëntatiefase heeft zij deze indruk, inclusief aandachtspunten, vastgelegd in een rapportage.

LEESWIJZER

Het eerste hoofdstuk beschrijft de aanleiding voor toezicht op C2000, de positionering tussen beleid, uitvoering en toezicht, de C2000 activiteiten die de Inspectie OOV heeft uitgevoerd en gesignaleerde aandachtspunten in relatie tot de Projectdirectie C2000 en de beleidsdirectie Strategie van BZK. Hoofdstuk twee, de feitelijke praktijkoriëntatie, bevat een toelichting op het systeem C2000 en haar omgeving, de bij het systeem betrokken partijen en een samenvatting, inclusief aandachtspunten, van de in de regio uitgevoerde pilot onderzoeken. Hoofdstuk drie gaat nader in op (mogelijke) vervolg-onderzoeken en/of vervolgacties.

Oriëntatie op C2000

1

AANLEIDING

Ingebruikname

De minister van BZK heeft de C2000 infrastructuur aangewezen als vitale infrastructuur en onderschrijft daarmee het belang van dit systeem voor de OOV-diensten. Met de ingebruikname van C2000 is ook beveiliging in de praktijk in beeld. Een betrouwbaar C2000 systeem staat of valt met de daadwerkelijk getroffen beveiligingsmaatregelen.

Naleving beleid

De Staat is eigenaar van C2000, waarbij de minister van BZK - in de rol van strategisch beheerder - eindverantwoordelijk is voor de beveiliging van het C2000 systeem.
Het door de minister van BZK vastgestelde Beveiligingsbeleid C2000 bevat de grondslagen en hoofdlijnen voor de integrale beveiliging van (het gebruik en beheer van) het C2000 systeem met als doel een betrouwbaar systeem te verkrijgen en te behouden. Dit Beveiligingsbeleid is gebaseerd op het Voorschrift Informatiebeveiliging Rijksdienst (VIR). Het voeren van beleid impliceert toets op naleving. De minister van BZK heeft de Inspectie OOV aangewezen om de rol van 'onafhankelijke deskundige C2000' uit te oefenen.

ROL VAN DE INSPECTIE

Beschreven

De rol van de Inspectie OOV ten aanzien van C2000 staat beschreven in het Beveiligingsbeleid C2000. Deze rol komt neer op:

- Het beoordelen van de werking, de opzet en het bestaan van de interne controle en beveiligingsmaatregelen.
- Het beoordelen van de beveiligingsbeheersorganisatie.
- Het toetsen van de toereikendheid van het Beveiligingsbeleid.

Specifieke taken

Een aantal specifieke taken is in het Beveiligingsbeleid nader benoemd, waaronder het beoordelen van de 'op beveiligingsbewustzijn gerichte communicatieplannen' en het beoordelen van de beveiligingsplannen op hun implementatie en werking.

MEERWAARDE VAN TOEZICHT

Schakel

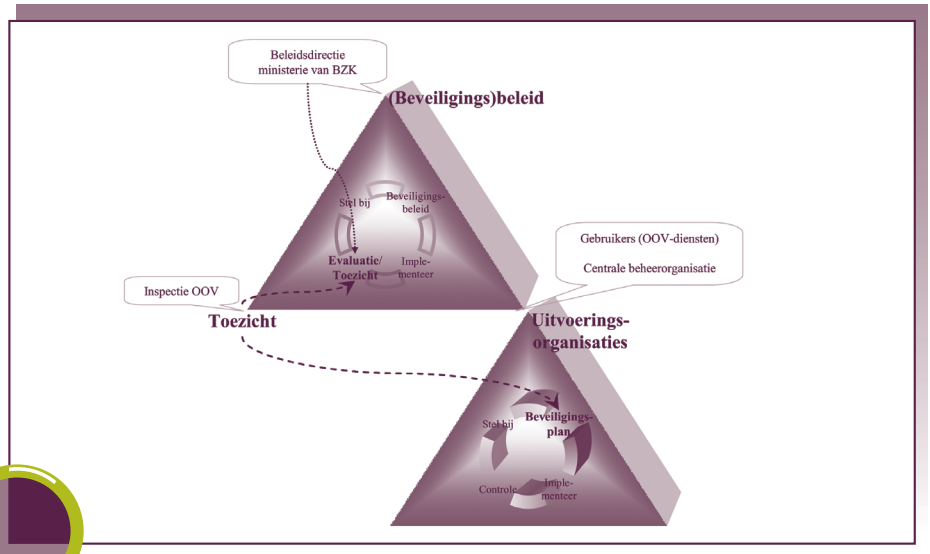
Toezicht is, evenals evaluatie van het beleid door de beleidsdirectie, een onderdeel van de beleidscyclus. De positionering tussen beleid, uitvoering en toezicht is in figuur 3

weergegeven. Op basis van de informatie die het toezicht levert over de uitvoering, kan bestaand beleid worden aangepast of nieuw beleid worden geïnitieerd. Daarnaast kan met de informatie die een toezichthouder beschikbaar stelt de uitvoering worden verbeterd.

Input op drie fronten

Door toezichtinformatie te leveren over de uitvoering van het Beveiligingsbeleid C2000 voorziet de Inspectie OOV in input op drie fronten:

- Input voor de verantwoordelijke beleidsdirectie Strategie van BZK voor de cyclische bijstelling van het Beveiligingsbeleid C2000.
- Input voor de centrale beheerorganisatie (C2000 infrastructuur) voor het waarborgen van het vereiste beveiligingsniveau.
- Input voor de OOV-diensten en de daaraan gelieerde organisaties voor de periodieke bijstelling van de beveiligingsplannen en vereiste rapportages.



Figuur 1

In bovenstaande figuur is weergegeven hoe de beleidsdirectie van het ministerie van BZK, OOV-diensten en de Directie Mobiele Diensten (onderdeel van de voorziening tot samenwerking Politie Nederland) en de Inspectie OOV (toezicht) ten opzichte van elkaar zijn gepositioneerd.
Uitvoeringsorganisaties rapporteren periodiek intern - als onderdeel van interne controle maatregelen - en aan de Directie Mobiele Diensten over beveiliging C2000 (stand van zaken beveiligingsplannen en incidenten-rapportages).
Uitvoeringsorganisaties zijn zelf verantwoordelijk voor het uitvoeren, onderhouden en controleren van beveiligingsplannen.

Uit Beveiligingsbeleid C2000, december 2004:

'Op basis van deze eisen dient per organisatie een beveiligingsplan te worden opgesteld waarin alle vereiste beveiligingsmaatregelen zijn opgenomen in een samenhangend geheel. Zowel het vastleggen van de (beveiligings)-verantwoordelijkheden van leidinggevenden als het bevorderen van het beveiligingsbewustzijn wordt daarbij als essentieel beschouwd. Ter controle op de uitvoering dient door de leidinggevenden periodiek over de status van de beveiliging te worden gerapporteerd aan de Directie Mobiele Diensten. De Directie Mobiele Diensten geeft deze informatie door aan het ministerie van BZK alsmede aanvullende gegevens over de C2000 infrastructuur. Deze werkwijze bevordert een uniforme aanpak zodat het vereiste basis-beveiligingsniveau van het C2000 Systeem als geheel kan worden gewaar-borgd. Voor specifieke bedrijfsprocessen kunnen additionele maatregelen worden getroffen om een hoger niveau van beveiliging te bereiken. Op diverse terreinen zijn beveiligingseisen nader uitgewerkt in meer gedetail-leerde voorschriften.'

ONTWIKKELING TOEZICHTINSTRUMENT

Focus gebruikersorganisaties

De Inspectie OOV heeft een toezichtinstrument ontwikkeld. Een eerste stap daarin was het richten van de focus op de gebruikersorganisaties, dus op de hulpverlenings-diensten. De centrale beheerorganisatie Directie Mobiele Diensten (DMD) was geen object van onderzoek, omdat tot oktober 2006 een aparte verantwoordingsstructuur bestond voor het project C2000 waar de Directie Mobiele Diensten onderdeel van uit maakte. Wel heeft de Inspectie OOV ontwikkelingen bij de centrale beheerorganisatie gevolgd.

Referentiekader[3] gericht op gebruikersorganisaties

Vanwege bovengenoemde focus heeft de Inspectie OOV - met gebruikmaking van algemeen aanvaarde standaarden - een referentiekader opgesteld voor het toetsen op naleving van het Beveiligingsbeleid specifiek gericht op gebruikersorganisaties. Dit referentiekader kan met enkele aanpassingen ook voor het toetsen van de centrale beheerorganisatie worden ingezet.

Pilotregio's

Aan de hand van het referentiekader heeft de Inspectie OOV bij een tweetal pilotregio's onderzoek uitgevoerd. Daarbij was de focus van het onderzoek voornamelijk gericht op de dienst digitale spraak, omdat de dienst dataverkeer via dataterminals nog in ontwikkelingsfase verkeert. Het zwaartepunt van het onderzoek lag voornamelijk bij het organisatieonderdeel meldkamer, omdat maatregelen uit beveiligingsplannen met name betrekking hebben op objecten in de meldkamer. De resultaten uit de twee pilotonderzoeken komen later in dit document terug.

3 Zie bijlage 'Referentiekader C2000 Aangewezen Gebruiker en Gelieerden'.

RELATIE MET DE PROJECTDIRECTIE C2000/DMD

Eerste indrukken

Tijdens het volgen van de ontwikkelingen bij de Directie Mobiele Diensten (als onderdeel van de Projectdirectie C2000), heeft de Inspectie OOV in maart 2006 eerste indrukken over C2000 gedeeld met de Projectdirectie C2000 en de DMD. Daarbij heeft de Inspectie OOV specifiek aandacht gevraagd voor het verder bestrijden van kwaadaardige software en voor de onderwerpen dienstenniveaubeheer en (het ontbreken van) Service Level Agreements (SLA's), accreditatie van externe koppelingen, (mandatering) cryptobeheer en het testen door gebruikers. Daarnaast vond een gedachtewisseling plaats over beleids- en beheeraspecten voor Special Coverage Locations, waarbij tevens het Agentschap Telecom (gebruik frequenties) en de mogelijke toezichtrol van dit agentschap ter sprake kwam.

Indrukken DMD medio 2006

Het onderzoek bij twee pilot regio's heeft geleid tot het signaleren van de volgende aandachtspunten aan de Directie Mobiele Diensten. Aangezien de DMD nog geen object van onderzoek was, zijn deze punten in de vorm van het delen van eerste indrukken richting Projectdirectie C2000 en DMD gecommuniceerd:

- Het ontbreken van een overkoepelend (DMD) architectuur- en beveiligingsdocument voor de C2000 systemen maakt externe beoordeling lastig en kan tot misverstanden leiden bij de verdere verbetering van het beveiligingsniveau.
- Op technisch gebied is een aantal maatregelen het overwegen waard. Dit varieert van het inzetten van een extra firewall tot het automatiseren van verschillende controle activiteiten en het verder bestrijden van kwaadaardige software.
- Vanwege activiteiten met een hogere urgentie heeft de Directie Mobiel Diensten een aantal accreditaties van koppelingen nog niet afgerond. De audits in het kader van cryptobeheer moeten eveneens nog door de Directie Mobiele Diensten worden uitgevoerd.

RELATIE MET DE BELEIDSDIRECTIE

De Inspectie OOV heeft bij de verantwoordelijke beleidsdirectie Strategie onder andere het volgende onder de aandacht gebracht.

Beheerovereenkomst

Het tactisch en operationeel beheer van de C2000 infrastructuur maakte tot september 2006 onderdeel uit van het ministerie van BZK[4]. Daarna is een nieuwe situatie ontstaan. Tactisch en operationeel beheer C2000 - lees Directie Mobiele Diensten - bevindt zich in een transitieproces naar de voorziening tot samenwerking Politie Nederland (vtsPN). De minister van BZK is contractpartij in de beheerovereenkomst met vtsPN en blijft contractpartij in de contracten met Tetraned, Defensie Telematica Organisatie en

overige leveranciers.
De inspanningen om te komen tot de beheerovereenkomst met vtsPN hebben op 16 april 2007 nog niet geleid tot een ondertekende overeenkomst[5]. Een getekende overeenkomst is van groot belang, omdat de daarin geformuleerde afspraken de basis vormen voor de door de centrale beheerorganisatie op te stellen verantwoording en de toets op naleving. Alleen al uit oogpunt van continuïteit van dienstverlening is een getekende overeenkomst noodzakelijk.

Vraagorganisaties (gebruikers)

Vanuit gebruikersperspectief is er sprake van uitbesteding van diensten. Bij uitbesteding blijft de verantwoordelijkheid voor informatiebeveiliging bij de uitbestedende organisatie – de vraagorganisatie. Ten tijde van het C2000 project waren gebruikers vertegenwoordigd in het Operationeel Bestuurlijk Overleg (OBO) dat onderdeel was van de projectorganisatie. Met de opheffing van het project was de projectorganisatie overbodig en verdween het gremium waarin vraagzijde en aanbodzijde onderling overleg voerden over de dienstverlening (inclusief de beveiliging daarvan). Wanneer de koppelvlakken tussen gebruikersorganisaties en (strategisch) beheerder niet goed op elkaar aansluiten, is de beveiliging van C2000 beperkt geborgd. De Inspectie OOV volgt daarom aandachtig de ontwikkelingen met betrekking tot de beoogd[6] opvolger van OBO: de Raad voor de Multidisciplinaire Informatievoorziening Veiligheid.

(Ontbreken) Normenkader en verantwoordingsrichtlijn

C2000 is ontworpen als een gesloten systeem voor de OOV-diensten (en gelieerden). De aard van het systeem - communicatiemiddel voor de hulpverleningsdiensten - stelt eisen aan de wijze van beveiliging. Het Beveiligingsbeleid C2000 geeft op hoofdlijnen de kaders aan waaraan de verschillende organisaties moeten voldoen. Tot op heden ontbreekt het aan een vanuit strategisch beheer met de centrale beheerorganisatie en gebruikersorganisaties afgestemd normenkader en bijbehorende verantwoordingsrichtlijn. Dit draagt bij aan een ondoorzichtige situatie ten aanzien van de borging van de beveiliging van C2000.

5 Toevoeging juli 2007:
Met genoegen stelt de Inspectie vast dat op 7 juni 2007 ondertekening van de beheerovereenkomst C2000 met de vtsPN heeft plaatsgevonden.

6 Toevoeging juli 2007:
Twee citaten uit de 'Brief uitvoering kabinetsstandpunt ACIR', d.d. 26 januari 2007, kenmerk 2007-0000011242:
'Voor de multidisciplinaire vraagorganisatie speelt de Raad MIV een belangrijke rol, in ieder geval tot het moment waarop deze rol ingevuld kan worden vanuit de taken en bevoegdheden van de Veiligheidsregio's, benoemd in de Wet op de Veiligheidsregio's.'
'Op 5 juli jl. heeft bestuurlijk overleg plaatsgevonden tussen mij en bestuurders uit de Raad voor Multidisciplinaire Informatievoorziening Veiligheid (MIV) over de taken en formalisering van de Raad. Gesteld is dat de Raad MIV een formele status nodig heeft om de taken goed uit te kunnen voeren. Er is een verkennend onderzoek uitgevoerd naar de mogelijkheden van de formalisering van de Raad MIV. Afgesproken is om de formalisering te regelen door middel van bestuurlijke convenanten. De Raad kan dan besluiten nemen binnen het mandaat dat tot stand komt door de convenant structuur. Deze constructie kan tevens bijdragen aan de versterking van de adviesrol van de Raad MIV, met name ook als het gaat om de onderwerpen C2000 en GMS.'

RELATIE MET DE AUDITDIENST BZK

Mogelijke samenwerking

De Auditdienst BZK voert onderzoeken uit bij agentschappen van BZK, waaronder het Korps landelijke politiediensten. Gedurende het C2000 verantwoordingstraject heeft de Auditdienst het grote project C2000 conform de vereisten van de Procedureregeling Grote Projecten beoordeeld. De Inspectie OOV heeft in brede zin met de Auditdienst BZK van gedachten gewisseld over mogelijke samenwerking en afstemming over parallelle activiteiten. Dit heeft geleid tot concrete activiteiten in het kader van C2000. Daarnaast heeft de Auditdienst BZK in 2006 onderzoeksuren aan de Inspectie OOV ter beschikking gesteld voor een technisch deelonderzoek C2000.

De beveiliging van C2000 in de praktijk

2

VAN VERLEDEN NAAR HEDEN

Analoge tijdperk

Ruim vijftien jaar geleden startte een aantal politiekorpsen een onderzoek naar de mogelijkheden van een nieuw communicatiesysteem. Niet alleen de politie was toe aan een nieuw communicatiesysteem, ook brandweer en ambulancezorg wilden af van de beperkingen van hun (oude) analoge radionetwerken. In die tijd maakten de hulpverleningsdiensten gebruik van een honderdtal afzonderlijke analoge netwerken. Dit had zo zijn nadelen. Onderlinge communicatie tussen de verschillende disciplines was niet mogelijk. De radionetwerken hadden een beperkte gesprekscapaciteit, bovendien was het voeren van vertrouwelijke gesprekken niet mogelijk aangezien iedereen via een scanner kon meeluisteren.

Multidisciplinair project C2000

Ooit begonnen als project Politie Communicatie Systeem 2000 ging dit project in 1997 over in het multidisciplinaire project C2000 met de minister van BZK in de rol van opdrachtgever. Doel van het project: het realiseren van één landelijk dekkend netwerk voor politie, brandweer en ambulancehulpverleningsdiensten. In 2003 werd binnen het ministerie van BZK de Projectdirectie C2000 opgericht, die belast werd met de verdere uitvoering van het project.

Van implementatie naar gebruik & beheer fase

In 2004 heeft leverancier Tetraned het C2000 netwerk opgeleverd. Vervolgens waren de gebruikersorganisaties aan zet. Tot in 2006 rolden de regionale en landelijke hulpverleningsdiensten onder eigen verantwoordelijkheid C2000 uit. Deze uitrol vond plaats via afzonderlijke (regionale) projecten, met ondersteuning van de projectdirectie C2000. In juni 2006[7] heeft de projectdirectie C2000 haar taken afgerond dan wel overgedragen. Taken op het gebied van strategisch beheer zijn overgedragen aan een van de beleidsdirecties Strategie binnen het Directoraat Generaal Veiligheid (DGV), binnen BZK. Taken van de Directie Mobiele Diensten, als onderdeel van de projectdirectie C2000, zijn in een beheerovereenkomst beschreven. C2000 is geïmplementeerd, er is zicht op een nieuwe fase: de gebruik & beheer fase.

Beveiliging

Naast eisen aan de functionaliteit van C2000 - wat moet het systeem kunnen - zijn er destijds ook eisen aan de betrouwbaarheid ervan geformuleerd[8]. De hulpverleningsdiensten zijn immers afhankelijk van een adequaat werkende portofoon en mobilofoon

7 Formeel is de projectdirectie C2000 per 1 juli 2006 opgeheven.
8 betrouwbaarheid in termen van de kwaliteitsaspecten exclusiviteit, integriteit en beschikbaarheid (zie bijlage I).

(en toekomstige dataterminal). Het gaat hierbij onder andere om het niet afluisterbaar zijn van gesprekken (en dataverkeer), afgeschermde gespreksgroepen en optimale verbindingen. Hiervoor moeten bij de verschillende partijen beveiligingsmaatregelen worden getroffen en daar is beveiligingsbeleid voor nodig.

Beveiligingsbeleid

In februari 2001 heeft de staatssecretaris van BZK de eerste versie van het landelijke Beveiligingsbeleid C2000 vastgesteld. Eind 2004 heeft de minister van BZK de tweede geactualiseerde versie vastgesteld. Deze versie bevatte enkele kleine aanpassingen. Uit het Beveiligingsbeleid volgt dat zowel de centrale beheerorganisatie als de gebruikersorganisaties een beveiligingsplan dienen te hebben waarover zij periodiek rapporteren. Het ministerie van BZK heeft voor het opstellen van een beveiligingsplan een handreiking in de vorm van een format opgesteld.

PARTIJEN

Bij (de beveiliging van) C2000 draait het om het digitale netwerk, de diensten die over dit netwerk gaan, het gebruik van deze C2000 diensten en om randapparatuur. Verschillende partijen werken samen en er zijn meerdere afhankelijkheidsrelaties in het kader van de beveiliging.
In het landelijke Beveiligingsbeleid spelen de volgende partijen een rol:

Eigenaar en opdrachtgever

De Staat is eigenaar van C2000 met als opdrachtgevende departementen: BZK, VWS en Defensie. De minister van BZK is eindverantwoordelijk voor de beveiliging van C2000. Binnen het DGV van BZK heeft de Directie Strategie/Informatiebeleid C2000 beleidstaken in portefeuille.

Onafhankelijke deskundige

De Inspectie OOV is belast met de beoordeling van de toereikendheid van het Beveiligingsbeleid en de daaruit voortvloeiende organisatorische, technische en procedurele beheersmaatregelen.

Centrale beheerorganisatie (ICT-dienstenleverancier)

De Directie Mobiele Diensten[9], vroeger onderdeel van het ministerie van BZK, is de centrale beheerorganisatie die het tactische en operationele beheer van de C2000 infrastructuur uitvoert. Deze dienst onderhoudt contacten op operationeel niveau met leveranciers en met de C2000 gebruikers.

Gebruikersorganisaties

De besloten groep C2000 gebruikers bestaat uit politie, brandweer, ambulancediensten en de Koninklijke Marechaussee – de openbare orde en veiligheidsdiensten – en de daar-

9 DMD -> ITO per 01-07-2006; ITO -> vtsPN per 01-08-2006.

aan gelieerde organisaties. Voorbeelden van gelieerden zijn: bedrijfsbrandweer, GHOR, gemeenten, huisartsenpost en het Explosieven Opruimingscommando.
OOV-diensten en gelieerden gebruiken het C2000 systeem binnen bepaalde spelregels en voeren lokaal beheer C2000 uit. Deze spelregels staan op hoofdlijnen beschreven in het landelijke Beveiligingsbeleid C2000.

Derden

De C2000 infrastructuur is zodanig opgezet dat voor de ondergrondse lijnen deels gebruik wordt gemaakt van infrastructuur van derden[10]. Ook het technisch onderhoud van de opgeleverde C2000 infrastructuur (zendmasten en componenten) is uitbesteed. Meldkamers kunnen kiezen voor het al of niet uitbesteden van technische beheer aan derden. Voor aankoop, beheer en onderhoud van randapparatuur hebben gebruikersorganisaties ook te maken met derden. Het landelijke Beveiligingsbeleid verwijst naar uitvoeringsrichtlijnen die ook betrekking hebben op derden.

Objecteigenaren (van special coverage locations)

Voor binnenhuisdekking heeft de minister van BZK 'Special Coverage Location' beleid geformuleerd. Eigenaren van objecten waar binnenhuisdekking voor moet worden geregeld kunnen door de lokale overheid worden aangesproken om hiervoor voorzieningen te treffen. Eisen ten aanzien van special coverage locations zijn beschreven in het landelijke Beveiligingsbeleid C2000.

COMPLEXE OMGEVING

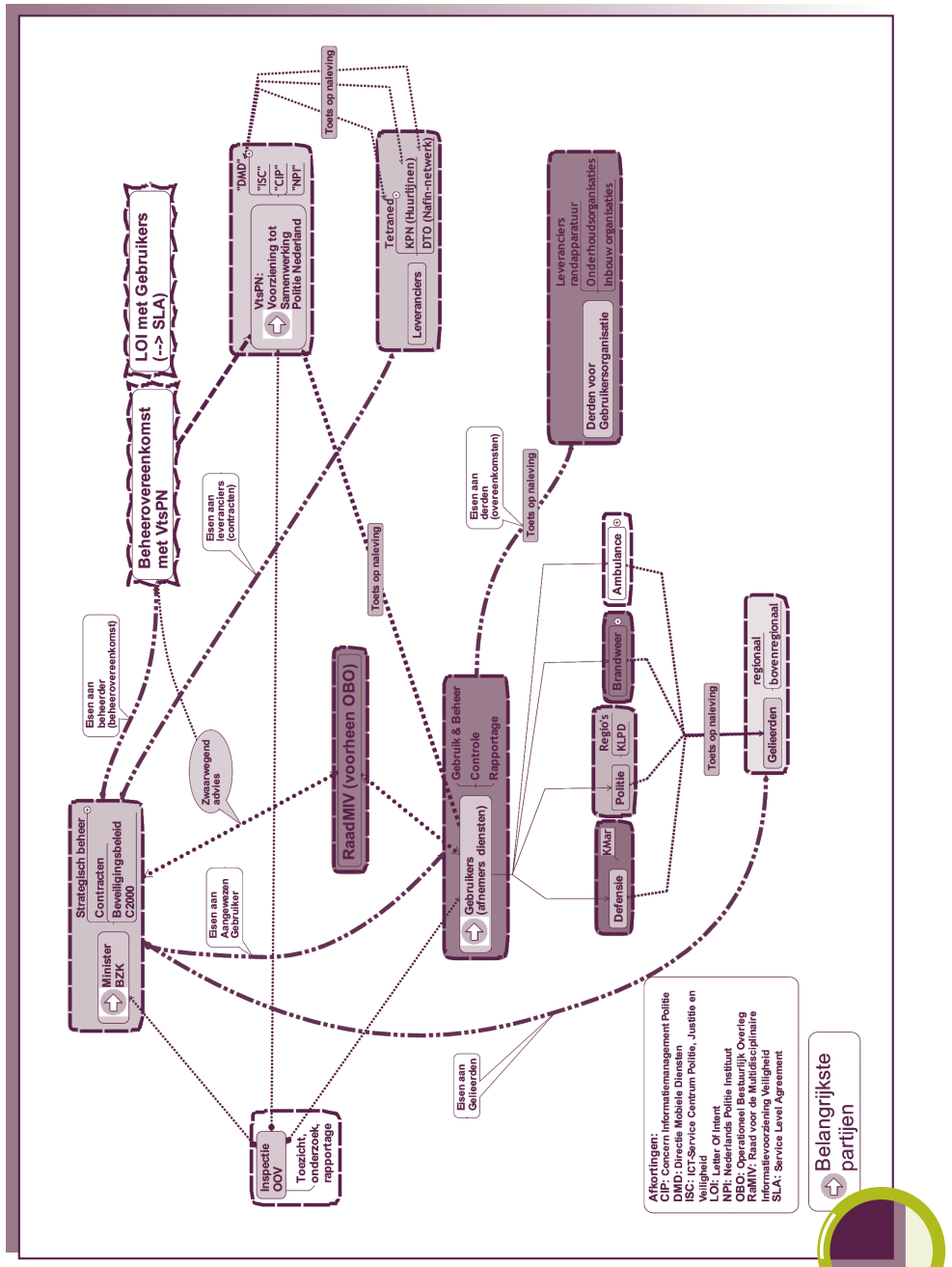
Definitie kwestie

De omgeving waarbinnen C2000 functioneert is complex. De Koninklijke Marechaussee, politie, brandweer en ambulancezorg (en daaraan gelieerden) vormen een diverse gebruikersgroep die een onderlinge afhankelijkheidsrelatie met elkaar hebben. De relatie tussen deze gebruikersgroep en strategisch beheerder BZK wijkt af van de standaard 'leverancier-klant' verhouding. In een dergelijke omgeving ligt spraakverwarring tussen verschillende partijen op de loer bij het hanteren van containerbegrippen en niet eenduidige begrippen.

Omgeving in beweging/ontwikkelingen

De omgeving van C2000 draagt het karakter van een sterk bewegend veld. Zo zijn veiligheidsregio's in ontwikkeling[11], wordt ambulancezorg op regionaal niveau georganiseerd. met een centrale rol voor de zorgverzekeraars[12] en zijn er ontwikkelingen rond de meldkamer (opvolger voor Gemeenschappelijk Meldkamer Systeem, referentiekader meldkamer). Bij de dienstenleverancier Directie Mobiel Diensten is er sprake van een veranderende organisatorische inbedding.

10 Zie bijlage I, Leveranciers en derden.
11 Concept wetsvoorstel op de veiligheidsregio's.
12 Nieuwe Wet ambulancezorg.



Figuur 2

C2000 moet betrouwbaar functioneren in een complexe omgeving. In bovenstaande figuur zijn de belangrijkste elementen van deze complexe omgeving in beeld gebracht: partijen, documenten (contracten en afspraken), eisen aan partijen en samenspraak tussen strategisch beheerder en overleg-orgaan gebruikers.

Directie Mobiele Diensten uit het ministerie van BZK

Tot juli 2006 maakt de Directie Mobiele Diensten onderdeel uit van de Projectdirectie C2000 en dus van het ministerie van BZK[13]. Met de overheveling van de Directie Mobiele Diensten naar de voorziening tot samenwerking Politie Nederland ontstaat er een (nieuwe) situatie. Inzicht in juridische, organisatorische en personele factoren dragen bij tot beheersing van de uitbesteding. De aansturing[14] van een externe ICT-diensten-leverancier vanuit het ministerie van BZK vergt specifieke deskundigheid, evenals het bepalen van de benodigde herkenbaarheid van de Directie Mobiele Diensten in de nieuwe situatie.

Meldkamers in de regio

Binnen de regio ligt de verantwoordelijkheid voor het uitdragen van het landelijke Beveiligingsbeleid en het opstellen van beveiligingsplannen bij de korpsbeheerders van de politie en de regionale bestuursvoorzitters van brandweer en ambulance voorzieningen. Beveiligingsplannen bevatten een samenhangend stelsel maatregelen en procedures op operationeel niveau. De regio's zijn vrij in het al of niet kiezen voor een multidisciplinaire benadering. Ook het eventueel uitsplitsen naar beveiligingsplannen voor meldkamer en randapparatuur is een keuzevrijheid van de regio. De wijze waarop meldkamers organisatorisch zijn opgehangen in een regio is niet uniform. Ook de wijze van multidisciplinaire samenwerking binnen een regionale meldkamer verschilt. Dit varieert van gecoloceerde meldkamer (politie, brandweer, ambulancedienst delen dezelfde huisvesting) tot geïntegreerde meldkamer (meldkamerprocessen van de drie disciplines zijn in elkaar verweven). Aan gebruikerszijde ligt veel van de C2000 techniek in de meldkamers. C2000 is verder gekoppeld aan het gemeenschappelijke meldkamersysteem (GMS). Op landelijk niveau zijn ontwikkelingen gaande voor de inrichting van een C2000 overstijgende uitwijkvoorziening voor de meldkamer. Immers, bij uitwijk zal niet alleen voor C2000 wat geregeld moeten worden, maar ook voor andere systemen binnen de meldkamer. Daarnaast spelen er - in het kader van (accreditatie) C2000 koppelingen - ontwikkelingen rond een Nieuw Meldkamer Systeem (NMS).

13 DMD -> ITO per 01-07-2006; ITO -> vtsPN per 01-08-2006.

14 Toevoeging juli 2007:
In juni 2007 is de uitbesteding van tactisch en operationeel beheer van C2000 aan vtsPN bekrachtigd in een ondertekende beheerovereenkomst. Omdat de Staat eigenaar is van C2000 en omdat strategisch beheer C2000 tot de verantwoordelijkheid van de minister van BZK behoort, zal binnen BZK professioneel opdrachtgeverschap geborgd moeten zijn. VtsPN gaat in opdracht van BZK projecten in het kader van C2000 uitvoeren. Professioneel opdrachtgeverschap houdt in dat er in ieder geval aandacht is voor risicomanagement en waarborgen voor de kwaliteit van de te leveren producten en of diensten, draagvlak creëren voor het eindproduct bij de belangrijkste interne en externe belanghebbenden, voldoende sturing en beheersing van het project, voldoende informatievoorziening tijdens het project, managen van verwachtingen betreffende de verwachte resultaten van complexe projecten.

Beveiligingsbeheer C2000

Beveiligingsbeheer gaat over het in de greep houden van risico's. In het landelijke Beveiligingsbeleid zijn de kaders van beveiligingsbeheer beschreven. De organisatie van beveiligingsbeheer is verspreid over verschillende partijen: de strategisch beheerder, de centrale beheerorganisatie en de gebruikersorganisaties (en de daaraan gelieerde organisaties). Tot augustus 2006 bestuurde de minister van BZK de beheerder van de C2000 infrastructuur - Directie Mobiele Diensten - ten behoeve van de opdrachtgevende departementen van BZK, van VWS en van Defensie. Bij overheveling van de Directie Mobiele Diensten naar de voorziening tot samenwerking Politie Nederland ging besturen over in aansturen via een beheerovereenkomst.
De relatie tussen de minister van BZK en de OOV-diensten heeft een ander karakter. Enerzijds dienen de OOV-diensten zich door tussenkomst van de Directie Mobiele Diensten te verantwoorden over de beveiliging van C2000. Anderzijds kunnen deze diensten hun C2000 wensen via het Operationeel Bestuurlijk Overleg - later via de Raad voor Multidisciplinaire Informatievoorziening Veiligheid - kenbaar maken aan de minister van BZK.

Centraal beheer C2000 versus lokaal beheer C2000

C2000 is een complex verhaal, zoveel (keten)partijen met even zoveel discussies. Waar het feitelijk om gaat is dat de communicatie via portofoon en andere randapparatuur het gewoon zou moeten doen. De hulpverleningsdiensten zijn daar in de dagelijkse praktijk immers sterk van afhankelijk. Een van de pijlers van een betrouwbaar systeem is adequaat beheer. Beheer ligt niet bij één partij maar ligt verspreid over meerdere partijen. Centraal beheer heeft betrekking op de C2000 infrastructuur. Strategisch (centraal) beheer ligt bij de beleidsdirectie Strategie van BZK. Tactisch en operationeel (centraal) beheer ligt bij de centrale beheerorganisatie Directie Mobiele Diensten.
Lokaal Beheer heeft betrekking op de meldkamers en randapparatuur en ligt bij de gebruikersorganisaties. Een heldere scheidslijn tussen centraal beheer en lokaal beheer is een noodzakelijke randvoorwaarde voor de invulling van adequaat beheer door de verschillende partijen.

Twee perspectieven: Gebruik en beheer

Via het project C2000 is de levenscyclus van het C2000 systeem gestart. Vanuit automatiseringsperspectief is C2000 na de ontwikkel- en invoeringsfase terecht gekomen in de beheer- en onderhoudsfase. Vanuit perspectief van de gebruikers van C2000 is er sprake van de gebruik fase en loopt de communicatie (met de meldkamer) nu via de nieuwe portofoons en mobilofoons. De gebruikersorganisaties dragen in 2005 t/m 2007 voor 71% bij in de financiering van C2000 (voornamelijk beheer- en exploitatiekosten). Gebruikersorganisaties maken niet alleen gebruik van C2000, maar hebben daarnaast ook een beheertaak, namelijk lokaal beheer (meldkamer, randapparatuur). Beveiliging en onderlinge afstemming op de koppelvlakken tussen dienstverlener en gebruikersorganisaties is vanuit beide perspectieven een belangrijk aspect.

Aanschaf randapparatuur door gebruikers

Destijds is ervoor gekozen om de aanschaf van randapparatuur bij de gebruikersorganisaties neer te leggen. Binnen de ruimte die de richtlijn Landelijke Aanbesteding Randapparatuur (LARA) biedt zijn de OOV-diensten vrij te kiezen. Zelf aanschaffen betekent onder andere ook zelf zorgdragen voor het beheer ervan, en het veilig maken en veilig houden van de randapparatuur.

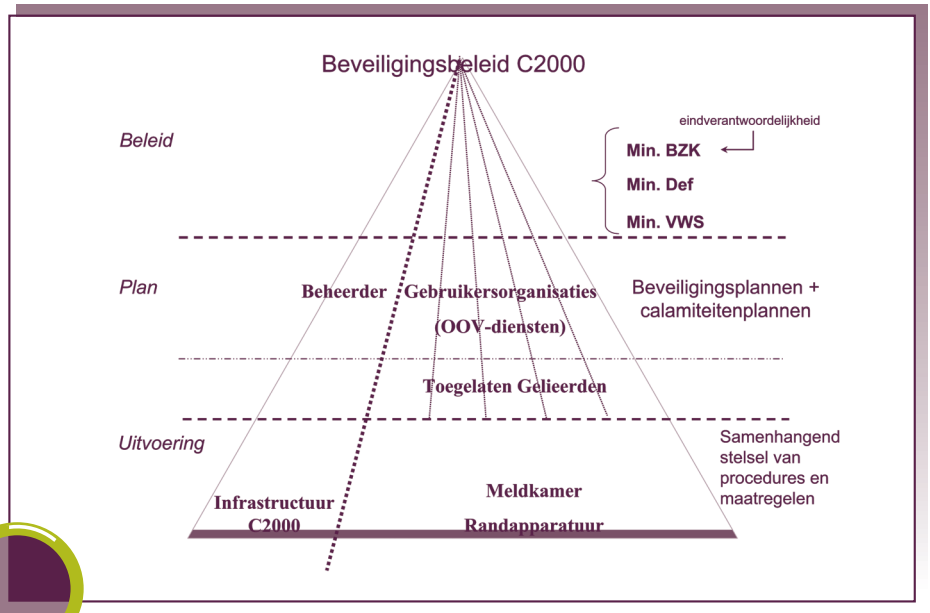
BEVEILIGINGSBELEID

Doelstelling C2000 systeem en Beveiligingsbeleid[15]

Beveiliging van C2000 is geen doel op zich. Het gaat om het borgen van de benodigde betrouwbaarheid van C2000. Ook het C2000 systeem is geen doel op zich maar het is een ondersteunend systeem voor de primaire bedrijfsprocessen van de OOV-diensten.

De algemene doelstelling van het C2000 systeem is:
De voor een noodzakelijke ondersteuning van de bedrijfsprocessen van de OOV-diensten benodigde betrouwbaarheid van het C2000 systeem op een zo doeltreffend en doelmatig mogelijke wijze te waarborgen.'

15 Uit Beveiligingsbeleid C2000, december 2004.



Figuur 3

In bovenstaande figuur is de onderlinge samenhang tussen beleid, plan en uitvoering tot uiting gebracht. Beleid moet leiden tot plannen, die op hun beurt moeten leiden tot een samenhangend pakket maatregelen en procedures op operationeel niveau.
De beheerder van de infrastructuur - links van de stippellijn - opereert op tactisch en operationeel niveau en verleent ICT-diensten aan gebruikersorganisaties - rechts van de stippellijn.
De beveiligingsplannen van beheerder en gebruikersorganisaties moeten op elkaar aansluiten.

Beleid en implementatie (beveiligingsplannen)

Beveiligingsbeleid speelt zich af op diverse niveaus bij diverse organisaties. In het overkoepelende landelijke Beveiligingsbeleid staat beschreven wat er moet gebeuren. Hoe het moet gebeuren – in termen van een samenhangend stelsel van concrete maatregelen op operationeel niveau - staat in opzet beschreven in de beveiligingsplannen van de verschillende organisaties (centrale beheerorganisatie, gebruikersorganisaties en daaraan gelieerden). Via de implementatie van deze beveiligingsplannen binnen de bijbehorende organisaties wordt vorm gegeven aan de implementatie van het landelijke Beveiligingsbeleid.

Interpretatie document Beveiligingsbeleid

Om een betrouwbaar C2000 systeem te kunnen realiseren heeft BZK tijdens het landelijke C2000 project landelijk Beveiligingsbeleid geformuleerd. Dit beleid bevat de grondslagen en hoofdlijnen voor de integrale beveiliging van (het gebruik en beheer van) het C2000 systeem en is hiervoor richtinggevend en bepalend. Het Beveiligingsbeleid C2000 is geschreven met een sterke ICT-insteek bezien vanuit de invalshoek van het aanbieden van ICT-diensten (IT-beheer) met consequenties voor het gebruik ervan. De wereld van IT-beheer is een andere wereld dan de wereld van openbare orde en veiligheid. Een risico bij een dergelijke aanpak is dat door de verschillende partijen bij de implementatie eigen interpretaties worden gegeven aan dit beleid, waardoor het vereiste beveiligingsniveau niet is geborgd.

Naleving Beveiligingsbeleid en rapportage

In de aanbiedingsbrief bij het Beveiligingsbeleid C2000 (editie 2004) schrijft de minister van BZK:
'...Het document beschrijft net als de editie 2001 beveiligingseisen voor C2000. En heeft als doelstelling een betrouwbaar C2000 systeem te waarborgen. Op basis van de beveiligingseisen dient per organisatie een plan opgesteld te worden volgens aangegeven richtlijnen. Dit geldt ook voor een toegelaten gelieerde.
Aangezien de naleving in het belang is van u allen dient er ter controle op de uitvoering door de leidinggevenden periodiek over de status van de beveiliging te worden gerapporteerd. Tevens is met de Inspectie OOV afgesproken te controleren of een dergelijk plan aanwezig is en of er periodiek gerapporteerd wordt.'

Controle op implementatie binnen een organisatie

Het landelijke Beveiligingsbeleid stelt dat zowel de centrale beheerorganisatie als de gebruikersorganisaties regelmatig (interne) controles dienen uit te laten voeren door een (informatie)beveiligingsfunctionaris betreffende de implementatie van het Beveiligingsbeleid en de in het beveiligingsplan concreet benoemde maatregelen.

Beveiliging C2000 is ketenprobleem

Ook voor C2000 geldt dat de beveiliging zo sterk is als de zwakste schakel. Zo is C2000 een gesloten netwerk. Wanneer in een van de meldkamers (onbedoeld) een achterdeurtje wordt opengezet via een (niet geaccrediteerde) koppeling, dan kan dit impact hebben op het hele land. Een ander voorbeeld heeft te maken met randapparatuur. Wanneer een randapparaat (onbedoeld) in verkeerde handen komt, worden (zonder repressieve maatregelen) de voor dat randapparaat gedefinieerde gespreksgroepen afluisterbaar.

TWEE PILOTONDERZOEKEN IN DE REGIO

Aard van de onderzoeken

De Inspectie OOV heeft - vanwege de complexe omgeving – aan twee regio's gevraagd medewerking te verlenen aan een pilotonderzoek om te kunnen komen tot nadere concretisering van een gestructureerde aanpak van toezicht op C2000. Tevoren is met deze regio's afgesproken dat de pilot niet het karakter van een beoordeling heeft. Wel heeft de Inspectie OOV in een pilotverslag haar bevindingen en aandachtspunten teruggekoppeld naar de regio's. De Inspectie OOV heeft in beide regio's veel medewerking gekregen bij het uitvoeren van het onderzoek. Ook de centrale beheerorganisatie Directie Mobiele Diensten heeft welwillend en open gereageerd op een technisch verzoek van de Inspectie OOV.

Gecombineerde benadering

Bij de pilotonderzoeken heeft de Inspectie OOV zowel een top down als een bottom up benadering gehanteerd. De top down benadering - gebaseerd op het eerder genoemde referentiekader - richt zich vooral op de 'opzet' van maatregelen. Bij het uitgevoerde ondersteunende technische deelonderzoek is de bottom up benadering gekozen waarbij de aandacht meer naar het 'bestaan' van beveiligingsmaatregelen is uitgegaan.

Overall beeld

Beide regio's hebben volgens een pragmatische benadering multidisciplinaire beveiligingsplannen opgesteld en hebben daarin concrete beveiligingsmaatregelen benoemd. Zij missen echter een landelijke richtlijn voor het opstellen van een beveiligingsplan, waardoor onduidelijk is wanneer een beveiligingsplan aan de daaraan te stellen eisen voldoet. Beide regio's werken voor de meldkamer aan een verdere invulling van C2000 continuïteitsvoorzieningen.
De regionale projecten C2000 - die zorg dragen voor het operationaliseren van C2000 in de regio - zijn nog niet formeel afgerond en nog niet (geheel) overgedragen aan de lijn. Dit zou een gedeeltelijke verklaring kunnen zijn waarom beide regio's nog geen invulling hebben gegeven aan de vereiste periodieke rapportages. De Inspectie OOV neemt deze bevinding mee als aandachtspunt bij haar geplande onderzoek naar beveiligingsplannen en rapportages.

Centraal en lokaal beheer

Bij de pilots is gebleken dat er een grijs gebied bestaat tussen centraal en lokaal beheer. Waar centraal beheer eindigt en lokaal beheer begint (en vice versa) is niet eenduidig vastgelegd.
Ten aanzien van lokaal beheer van randapparatuur blijken de generieke C2000 cryptografische eisen voor het versleutelen van gegevens (gesprekken) niet overal aan te sluiten op de binnen de regio's gehanteerde praktijk. Waar het aan ontbreekt is een vanuit strategisch beheer (door het ministerie van BZK) concreet geformuleerde set van eisen.

Aandachtspunten

De Inspectie heeft naar aanleiding van het onderzoek in beide regio's specifiek aandacht gevraagd voor:

- Overdracht van taken en verantwoordelijkheden aan de lijn bij afronding van het regionale C2000 project.
- Het opstellen van de vereiste periodieke rapportages in het kader van monitoring en naleving.
- Het toewerken naar een landelijk geaccepteerde richtlijn voor het opstellen van een beveiligingsplan, inclusief normenkader basisbeveiligingsniveau met specifieke aandacht voor de generieke crypto-eisen.
- Het toewerken naar een formele procedure gebruikersacceptatietest voor het accepteren van wijzigingen.
- Het vastleggen van heldere afspraken met de DMD over de afbakening (in termen van taken, verantwoordelijkheden, bevoegdheden) tussen centraal en lokaal beheer.
- Het zorgdragen voor een Service Level Agreement met de Directie Mobiele Diensten inclusief beveiligingsparagraaf.
- Registratie van beveiligingsincidenten bij de korpsen en standplaatsen, mede ten behoeve van risicobeheersing.

Ontwikkelpunten, vervolgonderzoeken

3

GEPLANDE ONDERZOEKEN

De Inspectie OOV heeft te maken met een relatief groot, complex veld en is qua toerusting beperkt. Dat leidt ertoe dat er ook voor het toezicht op C2000 jaarlijks keuzes gemaakt moeten worden. De ruimte waarbinnen de Inspectie OOV keuzes kan maken wordt begrensd door de verantwoordelijkheden van de minister van BZK voor de beveiliging van C2000. Deze ruimte stelt eisen aan de benodigde capaciteitsinzet en competenties voor C2000 onderzoeken.
De Inspectie zal in 2007 twee onderzoeken uitvoeren in het kader van C2000[16]. Een onderzoek richt zich op de vereiste beveiligingsplannen en rapportages bij de gebruikers - de OOV-diensten en gelieerden - en bij de centrale beheerder Directie Mobiele Diensten. Deze plannen en rapportages vormen het fundament voor het geïmplementeerd zijn van beveiligingsbeleid. Met dit onderzoek geeft de Inspectie OOV invulling aan de met de minister van BZK overeengekomen afspraak[17] om hierop te controleren. Het tweede onderzoek richt zich op een specifiek onderdeel van een beveiligingsplan, namelijk beveiligd gebruik, opslag, programmering (inclusief encryptie) en registratie van randapparatuur. Tijdens de pilotonderzoeken kwam bij beide regio's naar voren dat een aantal eisen ten aanzien van randapparatuur verduidelijking behoefde aan de kant van de gebruikersorganisaties. Ook bleken door de centrale beheerorganisatie nog geen audits in het kader van cryptobeheer te zijn uitgevoerd. Daarom wil de Inspectie OOV onderzoek doen naar de wijze waarop partijen invulling hebben gegeven aan de vereiste beveiliging van randapparatuur.

TOEZICHTVISIE C2000

Samenspraak

De Inspectie OOV wil in 2007 haar visie op toezicht C2000 verder ontwikkelen om op gestructureerde en systematische wijze invulling te geven aan de taak van Onafhankelijk Deskundige. De Inspectie OOV zal in goed overleg met directie Strategie en de Auditdienst BZK hier vorm aan geven. De Inspectie OOV heeft met de raad voor Multidisciplinaire Informatievoorziening Veiligheid contact, omdat zij een brug naar de gebruikersorganisaties vormt.

In verdere visie-ontwikkeling schenkt de Inspectie OOV in ieder geval aandacht aan de volgende onderwerpen.

16 Werkplan IOOV 2007.
17 Aanbiedingsbrief bij het Beveiligingsbeleid C2000 (editie 2004).

Normenkader en verantwoordingsrichtlijn

Noodzakelijke voorwaarde voor het uitvoeren van toezicht op C2000 is de aanwezigheid van een normenkader en een verantwoordingsrichtlijn die met het veld zijn afgestemd. De directie Strategie heeft daarin een voortrekkersrol.

Metatoezicht

Naast het uitvoeren van reguliere onderzoeken op basis van risicoanalyse onderzoekt de Inspectie OOV de mogelijkheid tot metatoezicht. De idee achter metatoezicht komt neer op het enkelvoudig uitvoeren van onderzoek, met als bijkomend voordeel het beperkt houden van toezichtslast. Daar waar verantwoordingsinformatie van de centrale beheerorganisatie en gebruikerorganisaties aanwezig is kunnen toezicht-activiteiten in eerste instantie beperkt worden tot review activiteiten ter verificatie van de verantwoordingsinformatie. Review activiteiten leiden na analyse en beoordeling eventueel tot aanvullend onderzoek.

Audit activiteiten Auditdienst BZK

De Inspectie OOV heeft oog voor samenloop in activiteiten met de Auditdienst BZK. Daarom vindt afstemming plaats over de respectievelijke jaarplannen.

Third party mededelingen

Ook third party mededelingen spelen een rol bij metatoezicht. Een third party mede-deling is een mededeling die wordt afgegeven door een onafhankelijke derde partij die een oordeel kan afgeven over het niveau van beveiliging bij een ICT-dienstverlener. Deze mededeling is bedoeld voor de klanten van de ICT-dienstenleverancier opdat zij inzicht hebben in het beveiligingsniveau bij de ICT-dienstenleverancier zonder dat zij zelf onderzoek ter plaatse (laten) uitvoeren.
In het kader van C2000 kan voor het beperken van toezichtactiviteiten en het verkrijgen van assurance (naar de toekomst toe) gedacht worden aan het opvragen van third party mededelingen voor KPN (vast KPN-netwerk) en DTO (Nafin-netwerk). Hetzelfde geldt voor de voorziening tot samenwerking Politie Nederland (vtsPN/DMD).

AANDACHTSPUNTEN UIT DE ORIËNTATIEFASE

Projectdirectie/DMD

De Inspectie OOV heeft op basis van haar werkzaamheden bij de directeur van de Projectdirectie C2000 en de directeur van de Directie Mobiele Diensten aandacht gevraagd voor de volgende onderwerpen:

- Het opstellen van een overkoepelend (DMD) architectuur- en beveiligingsdocument voor de C2000 systemen.
- Het afsluiten van service level agreements met de regio's.
- Het afronden van de accreditaties van externe koppelingen.

- Het verder bestrijden van kwaadaardige software.
- In het kader van Change Management door gebruikers laten uitvoeren van gebruikersacceptatietesten.
- Het uitvoeren van audits in het kader van mandatering cryptobeheer en het verduidelijken van generieke cryptografische eisen.

Beleidsdirectie Strategie

De Inspectie OOV vraagt, naast de hierboven genoemde punten (Projectdirectie/DMD), bij de directie Strategie aandacht voor de volgende twee onderwerpen:

- Het zorgen voor een getekende beheerovereenkomst met de voorziening tot samenwerking Politie Nederland[18].
- Het zorgen voor een met de gebruikersorganisaties afgestemd normenkader en bijbehorende verantwoordingsrichtlijn.

Regio's

De Inspectie vraagt aan de gebruikersorganisaties aandacht voor de volgende onderwerpen:

- Het zorgen voor overdracht van taken en verantwoordelijkheden aan de lijn bij afronding van het regionale project C2000.
- Het bijdragen aan een landelijk gedragen heldere scheidslijn tussen centraal beheer en lokaal beheer.
- Het bijdragen aan een landelijk gedragen richtlijn beveiligingsplan.
- Het binnen de kolommen (bij korpsen en standplaatsen) bijhouden van een registratie beveiligingsincidenten.

Voornoemde aandachtspunten neemt de Inspectie OOV mee bij het bepalen en afbakenen van vervolgonderzoeken.

18 Ondertekening van de beheerovereenkomst C2000 heeft plaats gevonden op 7 juni 2007. De beheerovereenkomst geldt met terugwerkende kracht vanaf 1 augustus 2006.

Bijlage: Begrippenlijst

ACIR

Actieprogramma Coördinatie Informatievoorziening Rampenbestrijding.
De minister van BZK heeft aan de Tweede Kamer toegezegd halfjaarlijks over de uitvoering van het kabinetsstandpunt ACIR te informeren. De kern van dit kabinetsstandpunt is het creëren van meer eenheid in de informatievoorziening ten behoeve van het grootschalig gezamenlijk optreden.

A&K analyse

Afhankelijkheids- en kwetsbaarheidsanalyse. De A&K analyse maakt onderdeel uit van risico beheersing.

Betrouwbaarheid

(Uit: Hoofdstuk 5 Beveiligingsbeleid C2000, versie december 2004)
'Om tot een adequate invulling van de beveiliging van het C2000 systeem te komen, worden betrouwbaarheidseisen gesteld op het gebied van fysieke, personele, technische en organisatorische beveiligingsaspecten. Deze eisen zijn van dien aard dat, bij gemeenschappelijke invulling van deze eisen, een basisbeveiligingsniveau van het C2000 systeem wordt bereikt. Het kunnen vaststellen van het basisbeveiligingsniveau vereist een inzicht in zowel de bedrijfsprocessen die gebruik maken van het C2000 systeem als in de afhankelijkheid van deze bedrijfsprocessen van het C2000 systeem. Uit de afhankelijkheid van de bedrijfsprocessen van het C2000 systeem volgen de betrouwbaarheidseisen die aan het C2000 systeem dienen te worden gesteld. De betrouwbaarheidseisen betreffen met name eisen op het gebied van beschikbaarheid, integriteit en exclusiviteit van het C2000 systeem. Er wordt uitgegaan van de volgende indeling van de betrouwbaarheidseisen:

- Beschikbaarheid: De mate waarin een systeem in bedrijf is op het moment dat de gebruikers het nodig hebben.
- Integriteit: De mate waarin een systeem zonder fouten is.
- Exclusiviteit: De mate waarin de toegang tot een systeem en/of verantwoordelijkheidsgebied en kennisname van de informatie daarin is beperkt tot een gedefinieerde groep van gerechtigden.'

Het aspect controleerbaarheid speelt een belangrijke rol bij het afleggen van verantwoording. Beheersbaarheid gaat over aansturing en bijsturing zodanig dat bij voortduring aan de gestelde eisen wordt/kan worden voldaan.

Centraal beheer

Het centraal beheer betreft met name het technisch beheer van de zgn. 'vitale C2000 infrastructuur'. Hieronder wordt verstaan het samenstel van vitale onderdelen van de C2000 infrastructuur bestaande uit schakelnodes, C2000 basisstations, vaste verbindingen (waaronder het NAFIN-netwerk), radiobediensystemen, alarmeringsbediensystemen, radiofrequenties en de zgn. 'vitale' Special Coverage Locations.

COBIT

Control Objectives for Information and related Technology.
COBIT is een procesgericht managementinstrument voor de beheersing van de volledige IT-omgeving, en dekt alle aspecten van informatie en de ondersteunende technologie af.

DGV

Directoraat Generaal Veiligheid, onderdeel van BZK.

DMD

Directie Mobiele Diensten. Vroeger onderdeel van het ministerie van BZK. (Projectdirectie C2000, per 01-07-2007 terug naar BZK-agentschap Informatie- en communicatieTechnologie Organisatie (ITO). Per 01-08-2006 onderdeel uitmakend van de voorziening tot samenwerking Politie Nederland.

GMS

Gemeenschappelijk Meldkamer Systeem (zie NMS).

Informatiebeveiliging

Informatiebeveiliging is het inrichten en onderhouden van een stelsel van maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en informatiesystemen te waarborgen (ISO, 2005).

LARA

Landelijke aanbesteding randapparatuur.

Leveranciers en derden

Tetraned, Motorola, Defensie Telematica Organisatie (DTO) en KPN vallen onder technische infrastructuur. Tetraned heeft medio 2004 het netwerk opgeleverd aan de minister. Zij voert tevens onderhoud uit op contractbasis. De C2000 software is afkomstig van Motorola. Voor een deel maakt C2000 gebruik van het door DTO beheerde Nafinnetwerk en van een aantal door KPN beheerde vaste lijnen.
Voor de gebruikers spelen leveranciers van randapparatuur, onderhouds- en inbouworganisaties een rol.

LOI

Letter of Intent. Het betreft een voornemen tot afspraken.

Lokaal beheer

Lokaal beheer betreft voornamelijk functioneel beheer (subscribermanagement) van een deel van het C2000 systeem. Dit is een verantwoordelijkheid van de gebruikersorganisatie die het functionele beheer uitvoert.

Het beheer van de randapparatuur wordt uitgevoerd door de Aangewezen Gebruikersorganisaties. Zij hebben deze apparatuur aangeschaft en is in gebruik bij hun organisatie of bij de aan hen gelieerde organisaties.

NAFIN

Het Netherlands Armed Forces Integrated Network is een zwaar beveiligd glasvezelnetwerk van het ministerie van Defensie.

NMS

Nieuw Meldkamer Systeem. Beoogd opvolger van het huidige Gemeenschappelijke Meldkamer Systeem (GMS).

OBO

Operationeel Bestuurlijk Overleg. Het OBO was destijds het overleg tussen het gebruikersveld en de directeur Projectdirectie C2000. In het OBO participeerden vertegenwoordigers van de koepels van politie, brandweer, ambulancediensten, Koninklijke Marechaussee en het Korps landelijke politiediensten, evenals een delegatie van voorzitters van de regionale Stuurgroepen en de VNG.

Raad MIV

Raad voor de Multidisciplinaire Informatievoorziening Veiligheid. De Raad MIV is beoogd opvolger van het Operationeel Bestuurlijk Overleg (OBO).

SLA

Service Level Agreement. Concrete afspraken in de vorm van een overeenkomst.

Special Coverage Location

Een Special Coverage Location is (in bestuurlijke zin) een object, waarvoor door het bevoegd gezag (bijv. burgemeester of minister) is bepaald door middel van een schriftelijke aanwijzing dat om reden van openbare orde en veiligheid binnenhuisdekking noodzakelijk is.

TETRA

Een standaard voor digitale radiocommunicatie: Terrestrial Trunked Radio.

VIR

Voorschrift Informatiebeveiliging Rijksoverheid.

vtsPN

De voorziening tot samenwerking Politie Nederland (zie tevens DMD) is een ICT-dienstenleverancier.

Bijlage: 'Referentiekader C2000 Aangewezen Gebruiker en Gelieerden'

Versie juni 2006

II

HOOFDVRAAG

Wordt het Beveiligingsbeleid C2000 (versie december 2004) nageleefd door de daarvoor aangewezen verantwoordelijken.

Deze hoofdvraag is opgesplitst in de volgende deelvragen met gebruikmaking van het referentiemodel Cobit[19]. Bij het opsplitsen in deelvragen is de indeling van het IT-domein in vier subdomeinen gevolgd.

- **Planning & Organisatie.** Voldoet het beveiligingsplan C2000 aan de daaraan te stellen eisen en vindt kwaliteitsborging van het gebruik van C2000 plaats?
- **Verwerving & Implementatie.** Worden wijzigingen en onderhoudsactiviteiten op C2000 objecten beheerst?
- **Beschikbaarheidsstelling & Ondersteuning.** Zijn de in het beveiligingsplan benoemde maatregelen geoperationaliseerd?
- **Monitoring.** Heeft de Aangewezen Gebruiker aantoonbaar zicht op beveiligd gebruik van het C2000 systeem?

II.1 PLANNING & ORGANISATIE

Voldoet het beveiligingsplan C2000 aan de daaraan te stellen eisen en vindt kwaliteitsborging van het gebruik van C2000 plaats?
Deze vraag wordt beantwoord aan de hand van de volgende drie Cobit-processen:

- Voldoen aan externe eisen.
- Uitvoeren risicoanalyse.
- Kwaliteitsmanagement.

Voldoen aan externe eisen

Is bij de Aangewezen Gebruiker (dan wel Gelieerden) invulling gegeven aan het opstellen van een beveiligingsplan dat is afgeleid van het geaccordeerde Beveiligingsbeleid C2000[20]?

19 Cobit = Control Objectives for IT and related technology.
20 Versie december 2004.

Is daarbij sprake van door de organisatie gedragen adequaat beleid en planning ten aanzien van:

- Fysieke beveiliging?
- Logische toegangsbeveiliging?
- Testen van applicatiesoftware, de technische infrastructuur, de organisatorische procedures en de documentatie?
- Storingen en wijzigingen?
- Calamiteiten, reconstructie, virusbestrijding en dergelijke?
- Beheer randapparatuur?
- Cryptomanagement?

Is specifiek aandacht geschonken aan awareness, rapportages en accreditatie conform het Beveiligingsbeleid C2000?

- Zijn alle met de bevordering van het beveiligingsbewustzijn verband houdende activiteiten vastgelegd in een communicatieplan en zijn alle opleidingen ten behoeve van het bevorderen van de deskundigheid op het gebied van beveiliging vastgelegd in een opleidingsplan?
- Wordt voldaan aan de in het Beveiligingsbeleid C2000 genoemde rapportages richting de centrale beheerorganisatie?
- Wordt de (her-)accredatie procedure voor externe koppelingen met het C2000 systeem nageleefd?
- Wordt de accreditatie procedure Gelieerden nageleefd?

Uitvoeren risicoanalyse

Worden risico's toegespitst op het C2000 systeem in beeld gebracht. Worden hiertoe afhankelijks- en kwetsbaarheids analyses uitgevoerd voor het benoemen van (aanvullende) beheersmaatregelen in het van het Beveiligingsbeleid C2000 afgeleide beveiligingsplan C2000?

Kwaliteitsmanagement

Voldoet het communicatieplan ter bevordering van awareness aan de daaraan te stellen eisen?

Is er sprake van adequaat ingericht relatiebeheer met third party leveranciers?

Voorziet het testproces in voldoende waarborgen voor de exclusiviteit, beschikbaarheid, integriteit en controleerbaarheid van het C2000 systeem en de voorgeschreven randapparatuur? De daaraan te stellen eisen betreffen:

- De implementatie van het testbeleid dient de exclusiviteit, beschikbaarheid, integriteit en controleerbaarheid van het C2000 systeem en randapparatuur te waarborgen.
- Er dient sprake te zijn van adequate registratie van het testen testdocumentatie.

II.2 VERWERVING & IMPLEMENTATIE

Worden wijzigingen en onderhoudsactiviteiten op C2000 objecten beheerst?

Deze vraag wordt beantwoord aan de hand van het Cobit-proces:

- Wijzigingenbeheer.

Wijzigingenbeheer

Is er sprake van een beheerst proces Wijzigingenbeheer (change- en (incident/)problem management) toegespitst op het C2000 systeem, waarbij het change- en problem management de exclusiviteit, integriteit, controleerbaarheid en beschikbaarheid van het C2000 systeem waarborgt? De daaraan te stellen eisen betreffen:

- De implementatie van het storings- en wijzigingsbeleid dient de exclusiviteit, integriteit, controleerbaarheid en beschikbaarheid van de resources in voldoende mate te waarborgen.
- Er dient een adequate registratie en controle te zijn van de met het storings- en wijzigingsbeheer samenhangende handelingen.

II.3 BESCHIKBAARHEIDSSTELLING & ONDERSTEUNING

Zijn de in het beveiligingsplan benoemde maatregelen geoperationaliseerd?

Deze vraag wordt beantwoord aan de hand van de volgende vijf Cobit-processen:

- Beheren third party diensten (uitbesteding).
- Verzekeren van continuïteit dienstverlening.
- Beveiligen van systemen.
- Gegevensbeheer.
- Beheer faciliteiten.

Beheren third party diensten (uitbesteding)

Worden de met dienstenleveranciers voor het C2000 systeem gemaakte afspraken en procedures, zoals vastgelegd in contracten en SLA's, nageleefd?

- ICT-dienstenleverancier DMD(/ITO)?
- Onderhoudsorganisaties (randapparatuur)?

Verzekeren van continuïteit dienstverlening

Zijn er voldoende waarborgen voor de beschikbaarheid van het C2000 systeem voor tijdige en adequate afhandeling van productieverstoringen in termen van backup, recovery en uitwijk? De daaraan te stellen eisen betreffen:

- Implementatie van backup, recovery en uitwijkbeleid, alsmede het beleid ter zake van virusbestrijding dient de beschikbaarheid in voldoende mate te waarborgen.
- Er dient een adequate registratie te zijn van backup, recovery, uitwijk en virus bestrijdingsactiviteiten.

Beveiligen van systemen

Zijn er voor het C2000 systeem voldoende waarborgen getroffen voor exclusiviteit, integriteit, en controleerbaarheid? De daaraan te stellen eisen betreffen:

- Logische toegangsbeveiliging.
- Cryptomanagement.
- Beheer randapparatuur.
- Externe koppelingen.
- Gegevensbeheer.
- Beheer faciliteiten.

Gegevensbeheer

Zijn er voldoende beheersmaatregelen getroffen ter waarborging van de integriteit van de Fleetmap (C2000 configuratie bestanden; functioneel beheer) binnen de meldkamer?

Beheer faciliteiten

Zijn er voor de meldkamer- en apparatuurruimte voldoende beheersmaatregelen getroffen ter waarborging van de exclusiviteit, integriteit, controleerbaarheid en beschikbaarheid van het C2000 systeem? De daaraan te stellen eisen betreffen:

- De implementatie van het fysieke beveiligingsbeleid dient de exclusiviteit van de resources in voldoende mate te waarborgen.
- Er dient een adequate registratie te zijn van en adequate controle op de wijze waarop het fysieke beveiligingsbeleid in de organisatie wordt uitgevoerd.

II.4 MONITORING

Heeft de Aangewezen Gebruiker aantoonbaar zicht op beveiligd gebruik van het C2000 systeem?

Deze vraag wordt beantwoord aan de hand van de twee Cobit-processen:

- Volgen en bewaken processen.
- Vaststellen toereikendheid interne controle.

Volgen en bewaken processen

Worden de relevante C2000 processen adequaat gevolgd en bewaakt?

Vaststellen toereikendheid interne controle

Is er sprake van een toereikende interne controle op het gebruik van het C2000 systeem?

Inspectie
OPENBARE ORDE
EN VEILIGHEID