Projectvoorstel

Landelijke aanpak informatiebeveiliging

Relatie IOOV audit 2007

Titel	:	Projectvoorstel
Project	:	Landelijke aanpak informatiebeveiliging
Documentnummer	:	xxxx
Datum	:	20 oktober 2009
Versie	:	1.0
Status	:	Ter vaststelling
Opdrachtgever	:	A. Rietstra portefeuillehouder IB RHC
Projectleider	:	G. Alberts, H.P.G. Janssen.
Opsteller(s)	:	G. Alberts, H.P.G. Janssen.

Inhoudsopgave

1 Projectvoorstel

1.1 Plaats document

De bron van dit document is te vinden in:
F:\RBB\Proces projecten\Formats documenten\Projectvoorstel.dot

1.2 Versie geschiedenis

Versiedatum	Veranderingen	Markering/wijzigingen
31-03-2009	Eerste uitgave	

1.3 Goedkeuring

Dit document is geldig indien goedgekeurd en ondertekend door:

Naam	Handtekening	Functie	Datum	Versie
A. Rietstra		Ptfh. I RHC		
H.P.G. Janssen		Ptfh InformatieBeveiliging landelijk CIO-overleg		

1.4 Verspreiding

Dit document wordt gestuurd naar:

Naam	Functie	Datum	Versie
Leden RHC	Beleidsverantwoordelijke korps		
Directeur vtsPN	Beleidsverantwoordelijke vtsPN		
CIO's	Aanspreekpunt IV korps		

1.5 Begrippenlijst

Beveiliging is het treffen van maatregelen om een te beveiligen doel te beschermen tegen schadelijke invloeden.

BBNP
Basis Beveiligingsniveau Nederlandse Politie. Dit omvat een set van minimale beveiligingsmaatregelen op technisch en organisatorisch gebied.

Informatiebeveiliging is het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, exclusiviteit en integriteit van alle vormen van informatie binnen een organisatie of een maatschappij garanderen, met als doel de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.

Op basis van een risicoanalyse wordt het gewenste niveau van beveiliging bepaald. Daarbij wordt in de regel een BIV-klasse beschikbaarheid, integriteit (=betrouwbaarheid) en vertrouwelijkheid (=exclusiviteit) bepaald, vaak uitgebreid met een indicatie voor controleerbaarheid (het belang om achteraf toegang en transacties te kunnen verifiëren).

Informatiebeveiliging is een onderwerp dat goed verankerd moet zijn in het topmanagement van de organisatie en is deels gebaseerd op het creëren van draagvlak bij gebruikers. Een bewustwordingsprogramma moet dan ook de invoering van de beveiligingsmaatregelen ondersteunen.

Beschikbaarheid bevat de garanties voor het afgesproken niveau van dienstverlening gericht op de beschikbaarheid van de dienst op de afgesproken momenten (bedrijfsduur, waarbij rekening wordt gehouden met uitvalstijden, storingen en incidenten).

Integriteit is het kwaliteitsbegrip dat juistheid, volledigheid, tijdigheid en geautoriseerdheid van de transacties omvat.

Vertrouwelijkheid is het kwaliteitsbegrip waaronder privacybescherming maar ook de exclusiviteit van informatie gevangen kan worden. Het waarborgt dat alleen geautoriseerden toegang krijgen en dat informatie niet kan uitlekken.

Toezicht vindt plaats vanuit de IT-audit discipline en vanwege diverse wettelijke toezichthouders. Door middel van het uitvoeren van IT en privacy-audits kan worden vastgesteld of het overeengekomen niveau van beveiliging is gerealiseerd. Ook kan een organisatie worden gecertificeerd op basis van de Code voor Informatiebeveiliging, de Nederlandse versie van de BS 7799 en tegen de internationale standaard ISO 27001.

RIP
In 1997 stelden de ministers van BZK en Justitie de Regeling Informatiebeveiliging Politie (RIP) vast. In de RIP werd de verantwoordelijkheid van de korpsbeheerders om een beveiligingsbeleid te formuleren en beveiligingsplannen op te stellen verwoord. De drie politieberaden (OM-Politieberaad, Korpsbeheerdersberaad en de Raad van Hoofdcommissarissen) onderschreven destijds de Regeling Informatiebeveiliging Politie (RIP) en gaven opdracht voor de ontwikkeling van een Stelsel voor Informatiebeveiliging. Ook gaven ze aan dat een en ander door de korpsen in 2005 geïmplementeerd zou moeten zijn.

Inspectie OOV
Inspectie Openbare Orde en Veiligheid

IBF (IBF-er)
Informatie Beveiliging Functionaris

2 Inleiding

2.1 Doel van dit document

Dit document is bedoeld om:
- er zeker van te zijn dat de noodzakelijke autoriteiten bestaan en zijn benoemd;
- er genoeg basisinformatie is om het project te starten;
- het werk in de volgende (initiatie-)fase te plannen;
- de organisatie op de hoogte te brengen van het project.

Het opstartproces heeft tot doel inzicht te verschaffen in de aanleiding, de projectdefinitie, de hoofdlijnen van de projectaanpak en voorstellen te doen voor de mogelijke samenstelling van het projectmanagement.
De belangrijkste redenen voor gebruik van dit document zijn om te dienen als basisdocument op grond waarvan de Stuurgroep de start van het project kan autoriseren.

2.2 Achtergrondinformatie

2.2.1 De context van het project

Informatiebeveiliging gaat over de zorg voor de betrouwbaarheid van informatie:
- integriteit: dat informatie juist, volledig en actueel is,
- exclusiviteit: dat informatie terecht komt bij degene die er recht op heeft en niet bij iemand anders,
- beschikbaarheid: dat informatie beschikbaar is op het moment dat en de plaats waar de informatie nodig is.

Het zou misschien beter zijn te spreken over “betrouwbaarheidszorg” maar informatiebeveiliging is nu eenmaal ingeburgerd.

Er zijn goede redenen informatiebeveiliging, de zorg voor de betrouwbaarheid van informatie, serieus te nemen.
- De politie verzamelt en beschikt over gigantische hoeveelheden informatie. Die informatie komt uit de administratie (de aangiften, verhoren, verificaties, etc), uit het actief verzamelen via uitluisteren, informanten en bronnenonderzoek en is afkomstig van externe partijen. De informatie gaat over mensen en aan de hand van die informatie kunnen mensen worden beschreven, tot in de finesses. Het is daarom vanzelfsprekend, in een rechtstaat, dat de uiterste zorg wordt besteed aan de zorg voor de betrouwbaarheid (integriteit, exclusiviteit, beschikbaarheid) van die informatie. Door onbetrouwbare informatie kan schade ontstaan aan de belangen van burgers en kunnen burgers in de uitoefening van hun rechten belemmerd worden.
- Voor de politie is informatie onontbeerlijk. De politie kan zonder informatie haar werk niet uitvoeren in de straat en de buurt, bij de criminaliteitsbestrijding, bij de advisering aan bestuurders. Informatie is ook cruciaal voor het sturen van het werk; niet voor niets wordt gesproken over “informatiegestuurde politie”. Als de politie zichzelf en haar werk serieus neemt, dan draagt zij zorg voor integriteit, exclusiviteit

en beschikbaarheid van de informatie waarmee ze werkt. In onderzoeken van de inspectie OOV, onder meer in "De politiële jeugdtaak" en "Opsporing gevonden", wordt informatiebeveiliging als kritische succesfactor beschreven. De prestaties in het operationele vlak worden sterk beïnvloed door het "cijfer" voor informatiebeveiliging.

- De politie deelt steeds vaker en steeds meer informatie met elkaar en met derden, nationaal en internationaal. Verzamelen en gebruiken van informatie ligt steeds minder in één hand. Verzamelaars en gebruikers, verstrekkers en afnemers zijn anoniem voor elkaar, maken deel uit van ketens, zijn partijen op een markt van bovenregionale, nationale en soms zelfs globale betekenis. En dan is het cruciaal dat er zekerheden zijn ingebouwd, via afspraken en maatregelen, dat de verstrekte informatie voldoet aan vastgestelde kwaliteitsnormen en slechts gebruikt wordt voor overeengekomen doelen.

Het belang van adequate beveiliging van de politiële informatievoorziening is vastgelegd in wet- en regelgeving. In navolging van het Voorschrift Informatiebeveiliging Rijksdienst werd voor het politiedomein de Regeling Informatiebeveiliging Politie opgesteld en in maart 1997 van kracht verklaard. De regeling heeft een sterk "hoe"-karakter: legt de nadruk op toedeling van verantwoordelijkheden voor de informatievoorziening, wijst een methode aan voor het bepalen van de noodzakelijke beveiligingsmaatregelen en bepaalt dat afspraken gemaakt moeten worden over de betrouwbaarheid van informatie bij uitwisseling. In 2004 is de regeling aangevuld met de normstelling voor de inrichting van de interceptiefaciliteiten. Ter ondersteuning van de uitvoering van de regeling werd in 1997 het Expertisecentrum Informatiebeveiliging Nederlandse Politie opgericht voor een periode van vijf jaren. Het Expertisecentrum heeft een volledig instrumentarium opgeleverd voor de toepassing van de regeling in de politiepraktijk, het Stelsel voor Informatiebeveiliging.

Op 1 januari 2008 [1] is de Wet Politiegegevens van kracht geworden die de Wet op de Politieregisters vervangt. Die wet benadrukt het belang van grip op het informatievoorzieningsproces, geeft daarvoor aanwijzingen, benoemt de noodzaak van informatiebeveiliging en schrijft de inrichting van een autorisatiefunctie voor. Het bijzondere, en van de Wet Bescherming Persoonsgegevens afwijkend regime van de Wet Politiegegevens, vindt zijn oorsprong in de overweging dat politiegegevens (nogal eens) zonder medeweten en instemming van de betrokkene worden opgeslagen en verwerkt.

2.2.2 Aanleiding tot het project

Door de Inspectie voor Openbare Orde en Veiligheid is een onderzoek uitgevoerd naar de informatiebeveiliging bij de Nederlandse politie. De rapportage van dat onderzoek is in maart 2007 verschenen onder de titel "Samen werken, samen beveiligen". Met die titel geeft de inspectie aan dat beveiliging een kwestie is van "samen" en randvoorwaardelijk voor "samen werken". Het rapport schetst een niet heel rooskleurig beeld van de stand van zaken met betrekking tot informatiebeveiliging bij de Nederlandse politiekorpsen. Voor alle duidelijkheid: het rapport constateert niet dat de Nederlandse politie een acuut beveiligingsprobleem heeft,

[1] *Bij het noemen van maatregelen in het BBNP is) uitgegaan van de toen vigerende WBP. (Zie de inleiding BBNP)*

in de zin van informatielekken of verkeerd handelen als gevolg van onbetrouwbare informatie. Dat kan de inspectie niet weten want daar is nog nooit systematisch politiebreed onderzoek naar gedaan. Het rapport constateert dat het schort aan de randvoorwaarden voor betrouwbare informatievoorziening.

Het beleid, voor zover er beleid met betrekking tot informatiebeveiliging is geformuleerd, is vaak verouderd, niet aangepast aan de veranderde situatie. Impliciet is daarmee aangegeven dat het beleid niet of in onvoldoende mate van papier tot uitvoering is gekomen. Niet in elk korps is een informatiebeveiligingsfunctionaris (IBF) aangesteld. In sommige korpsen, waar ooit een functionaris is aangesteld, is de functie weer verdwenen[2]. Maatregelen zijn min of meer hapsnap genomen, naar de waan van de dag. Verantwoordingsinformatie van de implementatie – is de maatregel op papier ook tot uitvoering gekomen? – ontbreekt. De stand van zaken met betrekking tot informatiebeveiliging is bij vrijwel geen korps geëvalueerd en dus onduidelijk. De inspectie constateert verder dat het stelsel voor informatiebeveiliging en de daarbij behorende opleidingen niet zijn onderhouden. De constatering heeft vooral betrekking op de leidraad Basisbeveiliging Nederlandse Politie (BBNP) en ook op de handreiking Organisatie van de Informatievoorziening. Overigens bevat het rapport ook lichtpuntjes. Er zijn nogal wat "best practices" ontwikkeld en "lessons learned".

De inspectie constateert dus dat de politie de afspraken die vervat zijn in de Regeling Informatiebeveiliging Politie niet is nagekomen, inclusief de later daaraan toegevoegde normstelling voor interceptie, en ook niet de afspraak is nagekomen die zij met zichzelf heeft gemaakt ten aanzien van het basisbeveiligingsniveau. De inspectie constateert dat de politie onvoldoende grip op het proces, het informatieproces heeft, in afspraken en maatregelen.

Belangrijk, met het oog op de toekomst, is dat ook het Stelsel voor Informatiebeveiliging niet is onderhouden. Dat constateert de inspectie met name ten aanzien van de leidraad Basisbeveiligingsniveau Nederlandse Politie (BBNP) en ten aanzien van de handreiking Organisatie van de informatievoorziening. Revisie van het Stelsel is absoluut noodzakelijk wil de politie ook in de toekomst kunnen beschikken over een gemeenschappelijk en geaccepteerd instrumentarium.

---

[2] *Het belang van een hulporganisatie en van een informatiebeveiligingsfunctionaris als spil daarvan blijkt uit de bevindingen: korpsen die een hulporganisatie hebben ingericht en een IBF hebben aangesteld komen verder. De hoogst scorende korpsen Amsterdam - Amstelland en Noord en Oost Gelderland geven daarvan blijk.*

3 Projectdefinitie

3.1 Projectdoelstellingen

Het doel van het project om de situatie op het gebied van informatiebeveiliging politiebreed op het voorgeschreven niveau te brengen en in het resultaat een evenwichtige balans te ontwikkelen tussen de aandacht voor techniek en gedrag. Het overgrote deel van de informatiebeveiligingssituatie is intussen afhankelijk van gedrag van medewerkers. Het project kent als zwaartepunt het homogeniseren van de business op het stuk van risicoherkenning, duiding en aanpak. In dit kader is het van groot belang om draagvlak te ontwikkelen voor de landelijke ontwikkelingen bij alle politiemedewerkers door middel van een structurele communicatiedraaggolf als basis voor concrete implementatie.

3.2 Bereik (Scope)

Het bereik van het project is het door de raad van hoofdcommissarissen vastgestelde Basisbeveiligingsniveau Nederlandse Politie (BBNP) te implementeren binnen de korpsen en binnen de VtS-verzorgingsgebieden. De implementatie van het BBNP wordt beschouwd als minimale zekerstelling voor betrouwbare uitwisseling van informatie tussen de korpsen en gezamenlijk gebruik van informatiesystemen. Uitgangspunt is dat de korpsen met betrekking tot de betrouwbaarheidseisen en maatregelen een zo uniform mogelijk niveau bereiken, als bedoeld in artikel 5 van de Regeling Informatiebeveiliging Politie ’97.

Het voorgestelde informatiebeveilingsproject moet niet alleen vanuit het IOOV standpunt, maar ook vanuit bedrijfsvoeringsoptiek opbrengsten opleveren. Tot op heden heeft de beveiligingsaanpak sterk in het teken van de kosten en belemmeringen in het werk gestaan, maar is in de planvorming onvoldoende aandacht geschonken aan revenuen van een landelijke aanpak.

De context van het project zal derhalve aanvullend op de opdracht om te komen tot de invoering van het BBNP tevens bestaan uit de aanpak van de hierna genoemde onderdelen:

a. De realisatie van eenduidige gebruikersopleidingen;
b. Onderzoek naar de mogelijkheid om te komen tot de invoering van een eenduidige en internationaal erkende beveiligingscode en toepassing daarvan;
c. Herziening van het normenkader voor audits en de mogelijkheden van koppeling aan het standaard auditproces in het kader van INK en WPG;
d. Onderzoek naar mogelijkheden op het gebied van landelijke benchmarking;
e. Invoeging van het onderwerp informatiebeveiliging in jaarlijkse accountancy verklaring.

3.3 Op te leveren producten en diensten

Het project zal de navolgende producten opleveren:

Normenkader:
Er wordt een document opgeleverd, waarin de volgende elementen aan de orde komen:

Sturing:	Periodieke risico-afwegingen op hoofdlijnen Beleidsvaststelling, inclusief kwaliteitsaspecten en afbreukrisico's (op processen, dataverzamelingen, informatiesystemen en infrastructurele voorzieningen) Verantwoordelijkheidstoedeling
Richtlijnen:	Ontwikkeling en onderhoud systemen Toegang tot het gebruik Personele maatregelen (waaronder screening) Privacywaarborgen Toets fysieke maatregelen
Toezicht:	Hoe verantwoording wordt afgelegd Onafhankelijke controles

Beleid:
- een generieke beschrijving van de risico's, die samenhangen met politie-informatie
- een gestandaardiseerd beveiligingsplan, implementeerbaar per korps, inhoudende tenminste:
  - hoe systeemontwikkeling en -onderhoud plaats heeft
  - hoe toegang en gebruik tot gegevens is geregeld
  - welke personele maatregelen worden genomen
  - hoe privacy wordt gewaarborgd
  - welke fysieke maatregelen worden genomen
- een gestandaardiseerd calamiteitenplan, implementeerbaar per korps

Toezicht:
- de wijze waarop inzicht in het korps wordt geborgd
- de inbedding van de beveiligingsaudits in de INK-audticylcus
- hoe onafhankelijke controles worden uitgevoerd

3.4 Afbakening

Het onderwerp informatiebeveiliging heeft een relatie met het project "WPG implementatie". Waar op personen herleidbare gegevens immers ten dienste van de politie een bijzondere categorie vormen, maken zij onverminderd deel uit van de te beschermen informatie. Ook die -hoewel onder een specifiek stuk wetgeving ressorterende- gegevens interacteren immers met onderwerpen als personeel, facilities en IT-communicatie. Binnen het landelijke project informatiebeveiliging zullen intussen geen onderwerpen worden uitgevoerd die onderdeel zijn in het WPG implementatieproject.

Met klem wordt benadrukt dat de noodzaak om politiebreed tot een eenduidig niveau van beveiliging te komen (als voorgeschreven in de Regeling Informatiebeveiliging Politie) alleen maar bereikt kan worden door middel van een gezamenlijke aanpak, die als volgt vorm zal krijgen:

1. Voor de regie zal een slanke projectgroep te worden samengesteld, die functioneert met intensieve participatie van de community van Informatiebeveiligingsfunctionarissen van de politieregio's, het Korps Landelijke PolitieDiensten en de VtSPN. Deze projectgroep is verantwoordelijk voor de organisatie van de landelijk afstemming en de ontwikkeling van diensten en producten die noodzakelijk zijn voor lokale implementatie. Hierin wordt ook begrepen de organisatie van vakinhoudelijke en fysieke ondersteuning van de lokale informatiebeveiligingsfunctionaris.
2. De feitelijke realisatie van invoering van de organisatorische BBNP maatregelen op korpsniveau zal een verantwoordelijkheid blijven van het lijnmanagement van het korps, zoals benoemd in het "Stelsel voor informatiebeveiliging Nederlandse Politie". De technische maatregelen zullen (mede) door VtsPN verzorgd moeten worden.

3.5 Randvoorwaarden

De harde condities waaronder het project moet worden uitgevoerd zijn als volgt beschreven:

1. Expliciete instemming van de betrokken autoriteiten is een absolute noodzaak.
2. De doorlooptijd van het landelijk project wordt gesteld op maximaal 2½ jaar na de feitelijke start.
3. Korpsen die gebruik willen maken van de producten en ondersteuning van de landelijke projectgroep dienen te voldoen aan een nader te omschrijving instapniveau.
4. Het landelijk project dient de beschikking te hebben over de benodigde middelen in geld, projectruimte en benodigde middelen op gebied van kantoorautomatisering, vervoer etc.
5. De participatie van de informatiebeveiligingsfunctionarissen, van de korpsen, het korps Landelijke Politiediensten en VtSPN, in het landelijk project dient gegarandeerd te zijn.
6. De balans tussen (het tempo en) de realisatie van organisatorische en technische maatregelen en voorzieningen dient door de stuurgroep te worden bewaakt.

3.6 Relaties met andere projecten

Het onderwerp informatiebeveiliging heeft een relatie met het project "WPG implementatie". Onder "3.4 Afbakening" is hierover een opmerking vermeld. Voorts zijn er relaties met de onderstaande projecten:

C2000.
Het C2000 communicatienetwerk is het mobiele communicatie- en alarmeringsnetwerk ten behoeve van de Openbare Orde en Veiligheid (OOV) diensten binnen Nederland.

Voor dit netwerk is qua beleid gekozen de methodiek van de norm NEN-ISO/IEC 27001 (Managementsystemen voor informatiebeveiliging) te volgen, zoals ook is geadopteerd in het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR2007). Hierin staat het proces van informatiebeveiliging beschreven, dat wordt aangestuurd vanuit een managementsysteem dat Information Security Management System (ISMS) wordt genoemd. Dit systeem heeft als doel dat op systematische en adequate wijze beveiligingsmaatregelen worden toegepast. Deze beveiligingsmaatregelen staan beschreven in een andere norm NEN-ISO/IEC 27002:2007 ('Code voor Informatiebeveiliging').

ICT-strategie.
De Voorziening tot samenwerking Politie Nederland, vtsPN, is met betrekking tot informatievoorzieningen en ICT, mede verantwoordelijk voor het gezamenlijke informatiemanagementproces en de aansluiting daarvan op de lokale informatiemanagementprocessen, Op basis van haar strategie worden gerealiseerd: ID-management, waaronder Autorisatiebeheerserver en Single Sign On; Visieontwikkeling Identitymanagement en worden er producten opgeleverd. Dezen zijn vermeld in een zogenaamde "roadmap".

Project Kaders bedrijfsarchitectuur Nederlandse politie (BaNp).
De BaNp geldt primair voor ICT, maar zij raakt zowel het fysiek en organisatorisch aspect, teneinde de ICT-maatregelen überhaupt te laten renderen. Een voorbeeld is het uitgifte proces en beheerproces van tokens of het vereisen van een beveiligingsorganisatie binnen korpsen, waar sleutelbeheer is belegd. De resultaten van dit project zijn in hoofdlijnen: visie, uitgangspunten en de belangrijkste principes voortkomende uit de onderstaande hoofdlijnen.

4 Globale Business Case

4.1 Redenen om het project te starten

Het doel van het project is de situatie op het gebied van informatiebeveiliging politiebreed op het voorgeschreven niveau te brengen en in het resultaat een evenwichtige balans te ontwikkelen tussen de aandacht voor techniek en gedrag.
De kern van het project wordt gevormd door de implementatie van de maatregelen genoemd in het BBNP. Het uniformeren en verbeteren van de situatie op informatiebeveiligingsgebied binnen Politie Nederland zal leiden tot vermindering van het aantal informatiebeveiligings-incidenten, tot vergroting van het vertrouwen van de burgers in de politie, en tot een veiliger uitwisseling van informatie tussen de korpsen en partners c.q. derden.

4.1.1 Huidige werkwijze

De huidige werkwijze wordt gekenmerkt door een individuele aanpak per korps, waardoor per korps ook een verschillend niveau van beveiliging is gerealiseerd. De uitkomst van de genoemde IOOV audit toont dit in alle duidelijkheid.

4.1.2 Toekomstige werkwijze

De toekomstige werkwijze kent in de projectfase een landelijke regie, die zal leiden tot concrete aanpak van invoering van maatregelen, gebaseerd op landelijke besluitvorming en de realisatie van een eenduidig niveau van beveiliging in de korpsen. In de eindfase zal sprake zijn van een benoemde beveiligingsautoriteit, die beleid aan de hand van genormeerde kaders monitort, stuurt en waar nodig ondersteunt en die keuzen voor de Nederlandse politie maakt.

4.2 Opties

In de aanloop naar het project zijn naar aanleiding van de uitkomsten van de IOOV audit "Samen werken Samen beveiliging", en naar aanleiding van besluitvorming in het Korpsbeheerdersberaad en de Raad van Hoofdcommissarissen verschillende opties in overweging genomen. Deze zijn als volgt te omschrijven:.

a. De aanpak van informatiebeveiliging per regio individueel, zonder landelijke projectgroep en landelijke regie.
b. Aanpak met een relatief omvangrijke landelijke projectgroep, met daaraan verbonden kosten.
c. Aanpak met een kleine projectgroep die de verantwoordelijkheid krijgt voor regie en landelijke afstemming en betrokkenheid van de IBF community, met daaraan verbonden beperkte kosten.

Deze projectbrief gaat uit van een projectmatige aanpak als bedoeld onder "C".
De onderbouwing voor deze keuze is als volgt:

1. De conclusie is getrokken dat landelijke eenduidigheid niet kan zonder landelijke regie.
2. In het gekozen model is er sprake van een verantwoordelijkheidsdefinitie die geen afbreuk doet aan de uitgangspunten van het "Stelsel voor informatiebeveiliging Nederlandse Politie".
3. Het gekozen model geeft optimale participatiemogelijkheden van de IBF community en zal draagvlak en persoonlijke ontwikkeling met zich brengen.
4. De kosten voor de voorgestelde aanpak zijn relatief laag in relatie tot het beoogde resultaat.

4.3 Fasering en Tijdschema

Een eerste aanzet voor een globale planning van de verschillende managementfasen.

FASE	PRODUCTEN	DATUM GEREED
Initiëren project (IP)		**……**
	Vastgestelde projectopdracht	Januari 2010
	Benoemde projectleider	Januari 2010
	Opgesteld Plan van Aanpak	Februari 2010
	Goedgekeurd Plan van Aanpak	April 2010
	Benoemde projectorganisatie	April 2010
Inhoud van het project (realisatie)		**……**
	Implementatie instructie per korps en landelijke afstemming	Vanaf najaar 2010
	Communicatie project	periodiek
	Start Communicatie awareness	najaar 2010
	Monitoring en rapportage voortgang project	periodiek
	Beschrijving audit als sytematiek binnen INK-model	Einde project
	Architectuuroplossingen VtsPN	Eind 2010/begin 2011
	Voortgangsrapportage	maandelijks
	Samenkomsten IB-gemeenschap best practices /lessons learned.	3x per jaar
	Invoeren rubriceringsregeling	2011
	Harmonisatie met projecten/ jaarplannen VtsPN	Vanaf 2011
	Opleidingen	Vanaf 2011
	Fase eindrapport	Voorjaar 2012
Afsluiten van het project		**……**
	Eindrapportage	Voorjaar 2012
	Aanbevelingen en borging	Voorjaar 2012
	Decharge	Voorjaar 2012

4.4 Financiële baten en lasten

De projectkosten komen tot stand door het inzetten van menskracht. Het volgende wordt voorzien:

Rol	menskracht	Korps
Opdrachtgever	p.m.	NH-Noord
CSO	p.m.	vtsPN
Portefeuillehoudend CIO	50% fte	Limburg-Noord
Projectleider	100% fte	Nog te benoemen
Beleidsmedewerker	100% fte	Nog te benoemen
Secretariële ondersteuning	100% fte	Nog te benoemen
Sr. Beleidsmedewerker	p.m.	vtsPN
IBF	p.m.	Alle korpsen

De menskracht, aangevuld met materiële lasten, zijn, -over twee jaren projectlooptijd-, als volgt in kaart gebracht:

Omschrijving	Herkomst kosten	Bedrag
Salariskosten portefeuillehoudend CIO	Detachering bji vtsPN (sch 13)	€ 120.000,=
Salariskosten projectleider	Detachering bij vtsPN (sch 12)	€ 210.000,=
Salariskosten beleidsmedewerker	Detachering bij vtsPN (sch 10)	€ 180.000,=
Salariskosten sercretar(is) (esse)	Detachering bij vtsPN (sch 7)	€ 130.000,=
Communicatiekosten, themadagen, beveiligingscommunity	Ontwikkelen draaggolf	€ 200.000,=
Bureaukosten, vergaderen, vervoer,		
Onvoorzien, afronding		€ 60.000,=
Totaal		**€ 900.000,=**

De besomde projectkosten zijn bedoeld voor de organisatie van de het landelijke project wat noodzakelijk is voor eenduidige implementatie in de korpsen. Voor de toedeling van deze projectkosten aan de korpsen wordt de volgende optie aangeboden:

De helft van de projectkosten komt voor helft ten laste van het budget bovenregionale voorzieiningen en andere helft wordt aan de korpsen gefactureerd. De aan de korpsen te factureren bedragen zijn gerelateerd aan de uitkomsten van de IOOV-rapportage. Deze verdeling lijkt tegemoet te komen aan het gegeven dat er korpsen zijn, die al substantiële investeringen deden voor informatiebeveiliging. Deze korpsen blijven bovendien investeren doordien zij de IBF-er mee laten werken aan het realiseren van het project. De feitelijke implementatiekosten in de korpsen en de kosten in relatie tot de participatie van de

informatiebeveiligingsfunctionarissen in het landelijk project komen voor rekening van het eigen korps.

Voor de omvang van de communicatiekosten in relatie tot het ontwikkelen van een communicatie-draaggolf is aanvullend onderzoek noodzakelijk. Uitgaven van ditbudget alleen na uitdrukkelijke toestemming van de opdrachtgever.

4.5 Projectmanagementstructuur

Een effectieve organisatiestructuur is voor het project de voorwaarde voor succes. De structuur maakt communicatie met besluitvormende organen mogelijk. Het zijn de leden van de Stuurgroep, de Projectleider en het Programmabureau, die tezamen verantwoordelijk zijn voor het management van het project.

4.6 Rolbeschrijvingen

Stuurgroep
De stuurgroep die ten behoeve van het project "Landelijke aanpak Informatiebeveiliging" wordt ingericht bestaat uit:

portefeuillehouder IB RHC	(voorzitter)
Korpsbeheerder	(lid)
Korpsbeheerder Twente	(lid)
CIO, portefeuillehouder IB	(lid)
CSO, vtsPN	(lid)
Projectleider	(lid)

Proceseigenaar (Opdrachtgever)
Namens de Raad van Korpschefs is A. Rietstra portefeuillehouder IB RHC als opdrachtgever verantwoordelijk voor het 'Landelijk project Informatiebeveiliging" De opdrachtgever is gemandateerd om "zaken te doen" met de projectleider. De opdrachtgever fiatteert plannen van aanpak cq. de producten die binnen het project geproduceerd worden, enz.. Als opdrachtgever maakt zij deel uit van de stuurgroep. Zij rapporteert eens per kwartaal aan de RKC i.o.

De opdrachtgever is verantwoordelijk voor het faciliteren van het project zoals in het plan van aanpak omschreven. Hieronder wordt mede verstaan het ter beschikking stellen van mensen, middelen en financiën. Wanneer het verkrijgen van extra financiën, personeel dan wel een afwijking van de projectopdracht aan de orde is legt de opdrachtgever dit voor aan de voorzitter van de stuurgroep.

Projectleider (opdrachtnemer)
De projectleider is belast met de uitvoering van het project.
De projectleider:
- Geeft leiding aan de projectorganisatie.
- Stelt een plan van aanpak en de daarbij behorende planning en begroting op;

- Geeft uitvoering aan het vastgestelde plan van aanpak. Hij heeft hiertoe de beschikking over een projectorganisatie waarin de benodigde capaciteit en kwaliteit vertegenwoordigd is;
- Bewaakt de voortgang van het project.
- Rapporteert de opdrachtgever over de voortgang van het project, draagt zorg voor tijdige aanlevering van de afgesproken producten volgens de vooraf bepaalde kwaliteit. Hij pleegt zonodig tussentijds overleg;
- Stelt zonodig een afwijkingsrapport op. Dit ingeval zich ontwikkelingen voordoen die een succesvolle uitvoering van het project volgens de gemaakte afspraken in gevaar brengen. Hij brengt dit afwijkingsrapport in bij de opdrachtgever. Na besluitvorming binnen de stuurgroep past hij zonodig het plan van aanpak aan.
- Pleegt regelmatig afstemmingsoverleg met de projectleiders van de aan dit project gerelateerde deelprojecten;

De IBF-er:

In het korps is de IBF-er de verbindende schakel tussen project en korps.

- Participeert op tactisch niveau in de landelijke projectgroep
- Ontwikkelt een implementatieplan voor eigen organisatie
- Is verantwoordelijk voor implementatie van het plan in eigen organisatie.

5 Kwaliteitsverwachtingen

Het project moet voldoen aan de eisen die aan Prince2 compliant projecten mogen worden gesteld op het gebied van:

- Projectbeheersing
- Verdeling van verantwoordelijkheden
- Management van de project fase overgangen
- Gebruik van wijzigingsprocedures
- Auditeerbaarheid van de project processen

De borging in het project ontstaat door:
- de bijeenkomsten van de stuurgroep,
- de rapportages vanuit de stuurgroep aan de RKC,

Borging na het project vindt plaats door:
- de te houden audits,
- de verplichte opname in elke toekomstige PID van een hoofdstuk Informatiebeveiliging.

Voor de overige kwaliteitsverwachtingen wordt verwezen naar de beschrijving van de globale businesscase, zoals verwoord in hoofdstuk 4.1.

6 Risico's

Hieronder worden de belangrijkste directe en indirecte risico's aangegeven die mede de vervolgstappen bepalen. Risico's kunnen liggen in aantasting kwaliteit van producten of dienstverlening, op het vlak van uitwisseling van informatie/systemen, in de impact ervan op de organisatie en de mate van veranderingsbereidheid en de implementatiekracht. Geef aan de kans dat een risico zich kan voordoen en de impact daarvan. (geef aan op een schaal van 0 tot 5, waarbij 0 staat voor geen impact tot 5 hoge mate van impact).

Bedreiging	Tegenmaatregel	Kans	Effect	Risico	Risico-eigenaar
Project werkruimte komt niet beschikbaar	Ad-hoc werk en vergaderruimte organiseren	3	4	4	stuurgroep
Benodigde financiën niet beschikbaar t.b.v. landelijk project	Loyaliteits verzoek doen bij korpsen voor beschikbaar stellen van ruimte en middelen	4	4	5	stuurgroep
Korpsen voldoen niet aan instapniveau	Korpsen dienen eerst zelf de nodige maatregelen te nemen om dit niveau te bereiken	4	4	5	korpsen
Participatie IBF community niet gegarandeerd	Nieuwe keuze maken in aanpak. Onderdeel 4.2 keuze b volledig landelijk project	3	5	4	korpsen
Kennisniveau IBF's	Voorafgaande aan participatie eerst kennisontwikkeling op gewenst niveau	4	5	5	korpsen / projectleider
Acceptatie landelijke aanpak ontbreekt in korpsen	Communicatie impuls, intensiveren van overleg met verantwoordelijken	4	5	5	korpsen / projectleider