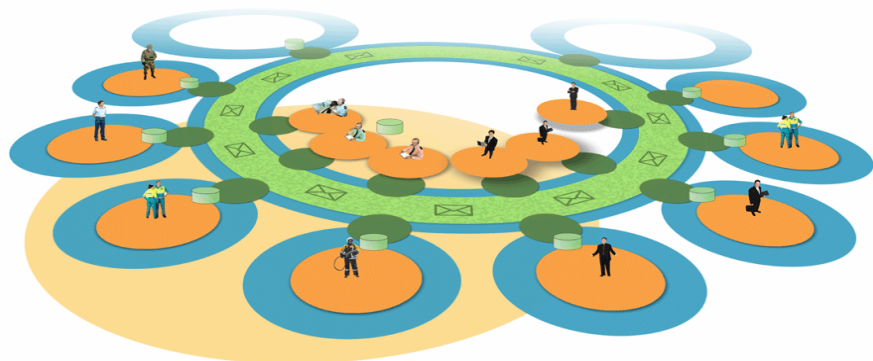


Zelfevaluatie

Zelf beoordelen van uw initiatief of projectvoorstel op het voldoen aan A-IBV uitgangspunten

Deze handreiking is één van de resultaten van het project “Architectuur Informatie Basisvoorziening Veiligheid”.

Inlichtingen: Dhr. Dick Kaas, dirk.kaas@isc.nl



De samenleving eist van de hulpverleningsdiensten adequaat optreden, zowel regulier als bij crises. Daarvoor zijn mensen, middelen en informatie nodig. Steeds blijkt dat de coördinatie en samenwerking gehinderd worden door lacunes in het hebben en delen van informatie. Informatievoorziening in de veiligheidssector moet en kan beter. Alle in-ieder-geval benodigde gegevens zijn immers ergens aanwezig.

Er gebeurt lokaal, regionaal en landelijk veel om de juiste gegevens te ontsluiten. In de honderden initiatieven ontbreekt vooralsnog de samenhang. De initiatieven uiten zelf de behoefte aan landelijke kaders en standaarden. De Minister van BZK en de Raad MIV trekken hiertoe inmiddels gezamenlijk op in het beleidsprogramma Informatie Basisvoorziening Veiligheid (kortweg IBV).

De informatievoorzieningen van de Informatie Basisvoorziening Veiligheid (hierna te noemen: "IBV", het beleidskader van het ministerie van BZK voor informatievoorziening in de veiligheidssector) komen samen met partijen uit het veld tot stand. Informatievoorzieningen dienen te voldoen aan de uitgangspunten van A-IBV, de Architectuur Informatie Basisvoorziening Veiligheid.

Om aan deze uitgangspunten te kunnen voldoen, heeft u een "checklist" nodig om de opzet van (nieuwe) initiatieven te kunnen toetsen aan de uitgangspunten van A-IBV. Dit document biedt die checklist in de vorm van een zelfevaluatie.

Aan de hand van de toets in dit document kunt u zelf nagaan in hoeverre uw initiatief of project voldoet aan de belangrijkste uitgangspunten van A-IBV. Het is bedoeld als hulpmiddel om uw projectvoorstellen te verbeteren, samenhang in het veld te bevorderen en kosten te reduceren.

De toets beschrijft geen referentiestandaarden. De referentiestandaarden vindt u op de apart verkrijgbare poster "Referentiestandaarden van de Informatie Basisvoorziening Veiligheid"². Die poster kan wel van nut zijn bij de zelfevaluatie.

Deze zelfevaluatie is een product van het project "Architectuur Informatie Basisvoorziening Veiligheid" (A-IBV). Zie ook www.a-ibv.nl (account vereist).

De zelfevaluatie bestaat uit vier onderdelen:

- 1. Het eerste onderdeel is informatief, niet evaluatief. U vult er de belangrijkste gegevens over uw initiatief of projectvoorstel in.*
- 2. Onderdelen 2, 3 en 4 vormen de zelfevaluatie. Met onderdeel 2 toetst u uw initiatief aan bestuurlijk-organisatorische uitgangspunten.*
- 3. Met onderdeel 3 beschrijft u de informatiekundige uitgangspunten van uw initiatief of projectvoorstel.*
- 4. Met onderdeel 4 beschrijft u de technologische uitgangspunten van uw initiatief of projectvoorstel.*

In de bijlagen van deze zelfevaluatie vindt u verwijzingen naar documenten die u kunnen helpen bij het invullen van deze toets.

Voor overige vragen over deze zelfevaluatie kunt u terecht bij Dhr. Dick Kaas, projectmanager A-IBV, dirk.kaas@isc.nl.

Meer informatie over A-IBV vindt u op de website www.a-ibv.nl (account vereist)

¹ "Partijen uit het veld": denk aan, de NVBR, NICTIZ, VNG, Raad MIV; gemeenten, veiligheidsregio's, regionale brandweerkorpsen, de VtS-Politie Nederland.

² De A-IBV uitgangspunten zijn beschikbaar op posterformaat bij de Afdeling Informatiebeleid van het DG Veiligheid van BZK. Contactpersoon: Dhr. Erik Kroon, of op de A-IBV wiki: www.a-ibv.nl, onderdeel "downloads".

1.1

Werktitel
Van initiatief of project

1.2

Contactpersoon
(Naam, organisatie, email)

Over de terminologie “Initiatief / project”

Deze zelfevaluatie is bruikbaar voor vele typen ontwikkelingen rondom informatie-management en informatievoorziening.

In principe kunt ude zelfevaluatie toepassen op:

- 1. Programma's of projecten rondom het verbeteren van informatie-hebben-en-informatie-delen.*
- 2. Bestaande gegevensverzamelingen met beheerders en afnemers.*
- 3. Bestaande of nieuwe technologische voorzieningen (ICT), informatievoorzieningen, applicaties en infrastructurele voorzieningen.*

In de vragenlijsten op de volgende pagina's wordt de term “initiatief” gebruikt. Hieronder kunt u dus alle bovengenoemde betekenissen verstaan.

2

Bestuurlijk/organisatorisch

2.1

IBV initiatieven zijn voor meer dan één discipline inzetbaar. Voor welke disciplines of partijen is uw initiatief toepasbaar?

 ++
 +
 -
 --

2.2

Welke samenwerkingsverbanden tussen twee of meer partijen, bijvoorbeeld twee of meer veiligheidsregio's of gemeenten kent uw initiatief?

 ++
 +
 -
 --

2.3

Welke afspraken maakt u met de betrokken partijen over levering en gebruik van gegevens en kennis van elkaar? Denk ook aan het gebruik van gegevens uit landelijke voorzieningen voor basisregistraties.

 ++
 +
 -
 --

2.4

IBV initiatieven benoemen vroegtijdig welke partijen mee weten, wie mee denken, en wie mee beslissen (wie waar over gaat). Hoe organiseert u dit voor uw initiatief?

 ++
 +
 -
 --

2.5

IBV initiatieven benoemen duidelijk hoe de financiering en mede-financiering tot stand komt, inclusief gebruik van andermans middelen en personeel. Hoe organiseert u dit voor uw initiatief?

 ++
 +
 -
 --

2.6

IBV initiatieven besteden aandacht aan de bestuurlijke borging van de resultaten: de resultaten worden door bevoegd gezag vastgesteld en hebben status. Hoe organiseert u dit voor uw initiatief?

 ++
 +
 -
 --

2.7

IBV initiatieven zorgen voor afstemming met relevante trajecten in de eigen regio, met andere regio's, en waar nodig ook landelijk. Hoe borgt u deze afstemming van uw initiatief?

 ++
 +
 -
 --

2.8

IBV initiatieven beschrijven duidelijk de verschillende belangen van de betrokken betrokkenen. Hoe organiseert u dit voor uw initiatief?

 ++
 +
 -
 --

2.9

Hoe organiseert u voor uw initiatief de nodige promotie en communicatie, zowel intern (directe eigen omgeving) alsook extern (veiligheidssector of zelfs breder)?

 ++
 +
 -
 --

Overige opmerkingen over bestuurlijk – organisatorische uitgangspunten:

Bronnen

3.1

IBV initiatieven betrekken gegevens uit landelijke basisregistraties waar mogelijk. Hoe organiseert u dit voor uw initiatief? Geef ook aan met welke basisregistraties uw initiatief geholpen zou zijn.

 ++
 +
 -
 --

3.2

IBV initiatieven betrekken overige bronnen zoveel mogelijk uit bronnen die regionaal dan wel landelijk beschikbaar zijn, bijvoorbeeld risico-gegevens van het Interprovinciaal Overleg (IPO). Hoe organiseert u dit voor uw initiatief?

 ++
 +
 -
 --

3.3

IBV initiatieven besteden aandacht aan de borging van gegevenskwaliteit, bijvoorbeeld door bij twijfel aan juistheid van verkregen gegevens, dit terug te melden aan de bronhouder. Hoe organiseert u dit voor uw initiatief?

 ++
 +
 -
 --

3.4

Hoe borgt u de kwaliteit van de eigen gebruikte gegevens op de kenmerken actualiteit, beschikbaarheid, betrouwbaarheid, compleetheid, context-beschrijving en authenticiteit (d.w.z. registers met enig gezag, bijv. de Kerndataset).

 ++
 +
 -
 --

3.5

Op welke wijze heeft u het gebruik van gegevens beschreven in een informatiebehoefte overzicht en een informatie-aanbod overzicht (voor gebruikers en afnemers van gegevens)?

 ++
 +
 -
 --

3.6

Hoe organiseert u de beveiliging van gegevens in de zin van het omgaan met exclusiviteitsaspecten, beschikbaarheidseisen, authenticatie en autorisatievraagstukken? Welk instrumentarium gebruikt u voor het realiseren van de gewenste beveiligingsniveaus?

 ++
 +
 -
 --

3.7

IBV initiatieven hanteren als uitgangspunt dat de gegevens beveiligd dienen te worden in plaats van de netwerkinfrastructuur. Hoe organiseert u dit voor uw initiatief?

 ++
 +
 -
 --

3.8

IBV initiatieven hanteren een strikte scheiding tussen gegevensopslag, gegevensverwerking en gegevenstransport (zie ook bijlage B). Hoe organiseert u dit voor uw initiatief?

 ++
 +
 -
 --

3.9

IBV initiatieven hanteren XML-gebaseerde mechanismen voor het structureren van de gegevens (Zie de referentie-standaarden in bijlage B). In hoeverre sluit uw initiatief hier bij aan?

 ++
 +
 -
 --

Overige opmerkingen over inhoudelijke uitgangspunten:

Kwaliteit

Beveiliging

Gegevensstructurering

4

Technologisch

4.1

IBV initiatieven betrekken authentieke gegevens ofwel direct (real-time) uit basisregistraties, en/of bewaren deze tijdelijk in een interne cache (zonder lokale mutaties).
Hoe organiseert u dat voor uw initiatief?

 ++
 +
 -
 --

4.2

Hoe maakt uw initiatief (her)gebruik van reeds beschikbare toegevoegde waarde diensten of voorzieningen, of draagt uw initiatief bij aan het ontstaan daarvan? (Zie www.a-ibv.nl voor een overzicht van reeds bestaande diensten en bijlage C voor de lijst van IBV voorzieningen)

 ++
 +
 -
 --

4.3

IBV initiatieven baseren gegevenstransport en gegevenspresentatie (user interface) op internettechnologie (webtechnologie; zie ook bijlage B).
Hoe organiseert u dat voor uw initiatief?

 ++
 +
 -
 --

4.4

IBV initiatieven baseren keuzes in netwerk-infrastructuur, en koppelingen met andere netwerken of applicaties of registers, op basis van de referentiestandaarden in bijlage B volgens het principe: eerst hergebruik, dan connectie, dan pas maatwerk. Hoe organiseert u dat voor uw initiatief?

 ++
 +
 -
 --

4.5

In IBV voorzieningen zijn koppelingen met informatiesystemen service georiënteerd (zie bijlage A) en besteden aandacht aan beveiliging, maar altijd volgens het principe "eenvoud als uitgangspunt".
Hoe organiseert u dit voor uw initiatief?

 ++
 +
 -
 --

4.6

IBV initiatieven benoemen kwaliteitskenmerken van leveranciers, zoals afspraken over levering, continuïteit en datakwaliteit.
Hoe organiseert u dit voor uw initiatief?

 ++
 +
 -
 --

4.7

IBV initiatieven organiseren de verwerking van gegevens op basis van service georiënteerde architectuurprincipes, zoals beschreven in NORA (zie bijlage A en B).
Hoe organiseert u dit voor uw initiatief?

 ++
 +
 -
 --

4.8

Geef aan hoe uw initiatief informatie beveiligt en hoe de applicatie en gebruiker de toegang regelen tot informatie input en output.

 ++
 +
 -
 --

4.9

IBV initiatieven baseren het beheer van informatiesystemen op ITIL, met een SMART gedefinieerde Quality of Service (QoS) overeenkomst (zie ook bijlage B).
Hoe organiseert u dit voor uw initiatief?

 ++
 +
 -
 --

Overige opmerkingen over technologische uitgangspunten:

Hier volgt een extract uit de beleidsuitgangspunten die NORA stelt voor gegevens-uitwisselingsdiensten tussen overheidspartijen onderling en tussen overheid en burgers en bedrijf.

1. Diensten worden zoveel mogelijk via Internettechnologie aangeboden.
2. Bestaande kanalen van dienstverlening blijven beschikbaar.
 - Wanneer een dienst via meerdere kanalen wordt geleverd, moet het mogelijk zijn om bij elk interactie moment tussen overheid en dienst afnemer het optimale kanaal te kiezen.
 - Semantische modellen zijn technologie-neutraal.
 - Dienstverleningskanalen zijn ingericht vanuit het perspectief van de gebruiker.
 - Diensten van de overheid die via verschillende kanalen worden geleverd moeten hetzelfde resultaat voor de afnemer van de dienst opleveren.
 - Content wordt kanaalafhankelijk opgezet.
3. Diensten worden aangeboden in voor de klant logische bundels per (soort) gebeurtenis.
 - Overheidsorganisaties werken samen aan diensten aan burgers en bedrijven op basis van een service georiënteerde architectuur.
 - Overheidsorganisaties maken afspraken over het verlenen van services.
 - Diensten kunnen ook in combinatie geleverd worden: combinatiediensten.
 - Dienstverlening gaat over organisatiegrenzen heen.
4. Dienstverlening is pro-actief, niet reactief.
 - Een verandering in de administratieve werkelijkheid wordt ter attentie gebracht van alle partijen die daar belang bij hebben.
 - Organisaties in het publieke domein attenderen burgers en bedrijven op voor hen relevante diensten (pro-actieve dienstverlening).
5. Eénmalig uitvragen van gegevens, meermalen gebruiken.
 - Informatie wordt éénmalig uitgevraagd.
 - Documenten die gebruikt worden door meerdere overheidsorganisaties of door burgers en bedrijven kunnen worden geraadpleegd, worden in een elektronisch archiefsysteem opgeslagen.
 - Overheidsorganisaties maken gebruik van (landelijke) basisregistraties.
 - Binnen de e-overheid worden metagegevens geregistreerd op het moment dat belangrijke proceswijzigingen optreden. Bij voorkeur gebeurt dit automatisch.
 - Gegevensverzamelingen die eigendom zijn van een overheidsorganisatie worden - met in achtname van nadere wettelijke regels - ter beschikking gesteld van de gehele overheid.
 - Gegevens, documenten en berichten worden voorzien van metagegevens ten behoeve van ontsluiting informatie.
 - Inkomende en uitgaande formele communicatie met klanten wordt gearchiveerd.
6. Dienstverleners verschaffen inzicht in de status van het dienstverleningsproces.
 - Samenwerkende organisaties organiseren de vastlegging van relevante gebeurtenissen (event logging, audit logging) met een organisatieoverschrijdend karakter op een inhoudelijk samenhangende wijze.
 - Klanten hebben de mogelijkheid zich op de hoogte te stellen van de stand van zaken van de uitvoering van de dienstverlening.
 - Overheidsorganisaties betrachten maximale transparantie voor de betrokkenen wat betreft de op hen betrekking hebbende verwerking van persoonsgegevens en verstrekkingen aan derden van die persoonsgegevens. Zij streven daarom naar inzage langs elektronische weg voor die betrokkenen.
7. De kwaliteit van het dienstverleningsproces wordt verantwoord.
 - Tot de kwaliteitsindicatoren van een (combinatie)dienst horen ten minste: juistheid, volledigheid, doorlooptijd, rechtmatigheid.
 - Diensten worden SMART beschreven.
 - Per dienst wordt een normbepalingstijd en een daarvan afgeleide kostprijs vastgesteld.
 - Van geleverde gegevens is de kwaliteit bekend
 - De eigenaar van een gegeven is verantwoordelijk voor de kwaliteit (actualiteit, betrouwbaarheid) van een gegeven.
8. Taken, besluiten, gegevens en werkwijze zijn zichtbaar binnen overheidsorganisaties.
9. Organisaties in het publieke domein geven een helder, vindbaar beeld van de diensten die burgers, bedrijven en maatschappelijke organisaties afnemen.
10. Waar mogelijk worden generieke bouwstenen gebruikt en hergebruikt.
 - Front Office applicaties kennen een beperkte controletaak op de kwaliteit van de gegevens.
 - Dienstverleningskanalen sluiten waar mogelijk aan op de generieke componenten van de e-overheid.
 - Applicaties voeren services van slechts één functioneel domein uit.
 - Sectorale en de nationale servicebussen kennen een hoge betrouwbaarheid en zijn 7*24h beschikbaar.
 - Het berichtenverkeer binnen de e-overheid ontwikkelt zich in de richting van een naadloos op elkaar aangesloten hiërarchie van samenwerkende servicebussen.
 - Communicatie tussen overheidsorganisaties verloopt via of besloten, separate netwerken of door middel van een virtual private network verbinding via netwerken van particuliere bedrijven.

Referentiestandaarden* van de Informatie Basisvoorziening Veiligheid

Versie 0.5, 17 september 2007. CONCEPT. Redactie: Dick Kaas en Jan-Willem van Aalst. Eindredactie: Erik Kroon, Directie Strategie, DG Veiligheid, Ministerie van BZK.

DE VRIJBLIJVENDEHOED VOORBIJ

- Nieuwe initiatieven worden door BZK goetoezt met een lijst criteria op 'IBV'-compliance. Dit overzicht van referentiestandaarden is daar maar één onderdeel van.
- Gebruik dit overzicht als hulpmiddel bij het kiezen van standaarden voor nieuwe ICT initiatieven, indien u zoveel mogelijk IBV compliant wilt opereren.

Algemeen geldende referentiekaders IBV

- Aan het gedeelde informatiegebruik tussen de veiligheidspartners gaat de afsluiting van een overeenkomst over gebruiksvoorwaarden vooraf.
- Veiligheidspartners die met hun ICT initiatieven IBV compliant willen zijn respecteren de regierollen van de Minister van BZK en van het Veiligheidsberaad/MIV.
- Projecten voor gegevensuitwisseling tussen ketenpartners baseren zich zoveel mogelijk op principes van de Nederlandse Overheid Referentie Architectuur.
- Nieuwe ICT initiatieven maken gebruik van het stelsel van basisregistraties voor het hebben, delen en behouden van authentieke gegevens.
- Vernieuwing van ICT wordt gebaseerd op bestaande afspraken tussen veiligheidspartners, als dit draagt aan samenwerking, en ICT-versnippering tegengaat.
- Vernieuwing van ICT sluit aan bij het goede bestaande, maakt optimaal hergebruik van best practices. Benutten van bestaande producten gaat voor koop (pakketten) of ontwikkeling van nieuwe producten (maatwerk).
- Gebruik van open standaarden gaat voor gebruik van specifieke (proprietary) gesloten standaarden, dit om interoperabiliteit van ICT te bevorderen.
- Vernieuwing van ICT wordt liefst landelijk of regionaal opgezet tbv schaalgroefvoordeel en harmonisatie.
- Vernieuwing van ICT gebeurt gefaseerd en in kleine hapklare brokken, die aansluitbaar zijn op het bestaande ("Modulair opgezette ICT").
- ICT projecten hanteren strikte scheiding van functionaliteit en gegevensopslag.
- De beschikbare gegevens zijn betekenisvol voor de partij die ze gebruikt.
- Er komen alleen de voor de rol relevante gegevens beschikbaar. Die zijn beschikbaar wanneer nodig.
- De gegevens zijn verifieerbaar, juist en actueel.
- De gegevens zijn alleen beschikbaar voor degene waar ze voor zijn bedoeld.
- Informatievoorzieningen dienen zoveel mogelijk in bijzondere en reguliere situaties bruikbaar te zijn. Informatievoorzieningen dienen ook bovenregionaal bruikbaar te zijn.

Relativerende wenk: geen enkele standaard is statisch. Indien deze poster ouder is dan zes maanden na de hierboven vermelde statusdatum, raden wij u aan om de poster te vervangen door een nieuwe. Deze kunt u downloaden vanaf www.a-ibv.nl of bestellen bij het Ministerie van BZK, Dhr. Rijn Gooskens, rijn.gooskens@minbzk.nl.

IBV Standaarden voor bedrijfsprocessen:

- Van elk proces zijn de informatie-producten opgenomen in het IBV informatiebehoefteboek en -aanbod-boek, zie www.a-ibv.nl.
- NORA principes t.a.v. ketenprocessen zijn leidend en worden gevolgd.
- Van elk proces is middels een afhankelijkheids- en kwetsbaarheidsanalyse bekend wat de afhankelijkheid is van de kwaliteit van onderstaande lagen

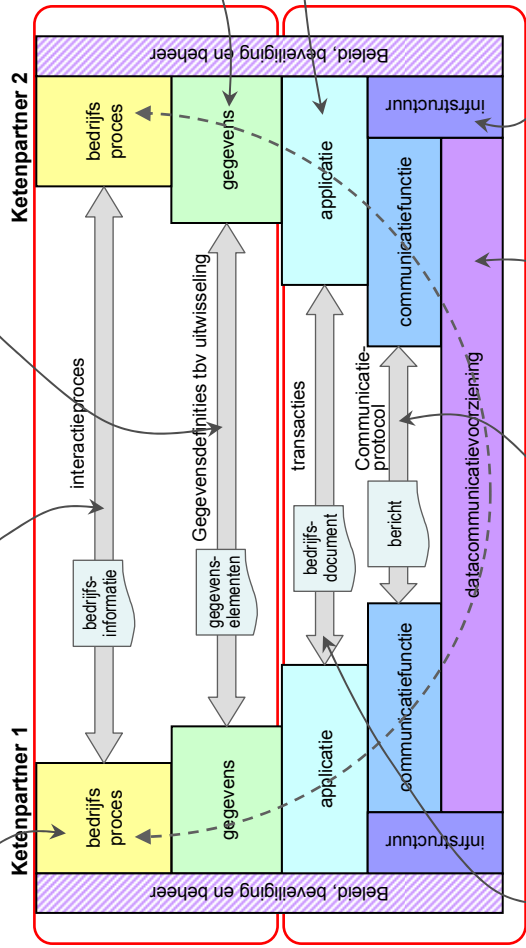
IBV Standaarden in interactieprocessen:

- De concepten situationaal awareness en 'Netcentric' zijn uitgangspunt voor interactie in de repressiefase.
- Alle partijen moeten gemachtigd zijn de betreffende informatie uit te wisselen.
- Partijen kunnen zich abonneren op informatie of op een gebeurtenis.
- Beveiligingsarchitectuur OOV ICT is van toepassing op interactieprocessen.

IBV Standaarden voor gegevensdefinities:

- Definities voor gegevensuitwisseling zijn opgenomen in Gegevenswoordenboeken Veiligheid (www.a-ibv.nl). Deze worden toegepast in de berichtenboeken per ketenproces.
- Er worden geen nieuwe gegevens-elementen bedacht als die al beschikbaar zijn via de Gegeve.wrd.bkn Veiligheid.
- Vastlegging van gegevendefinities gebeurt zoveel mogelijk met XML. Gerelateerde standaarden, zoals UBL en NDR (ebXML). Geo-standaarden liggen bij GDI / G1 beaad.
- Gegevens-elementen passen binnen de definities in de IBV almanak op www.a-ibv.nl.

Kijk ook op www.a-ibv.nl om zelf bij te dragen aan de continue evolutie van de IBV standaarden!



IBV Standaarden voor gegevens:

- Authentieke gegevens halen bij de bron.
- Erkende gegevensleveranciers: gemeente, provincie, IPO, Waterschap, Kadaster, RDW, KVK, RVM, Dataland, TNO.
- Stelselhandboek basisregistraties is leidend voor authentieke gegevens.
- Gegevensmanagement is waar mogelijk ingericht volgens het beheermodel BISL (zie nl.wikipedia.org/wiki/BISL).

IBV Standaarden voor applicaties:

- Applicatie-architectuur volgens Service Gerichte Architectuur (NORA v1.9, p.66 e.v.)
- Beheer van applicaties volgens Application Services Library (ASL, zie nl.wikipedia.org/wiki/ASL-beheermethodiek)
- User interface in web browser
- Open standaarden waar mogelijk; voor Geo vanuit Open Geospatial consortium

IBV Standaarden voor infrastructuur:

- Beheer volgens ITIL methodiek met City of Service (zie nl.wikipedia.org/wiki/ITIL)
- Beveiliging/privacy volgens PKI, DigiD (zie NORA v1.9, p.39 e.v.), usename, wachtwoord, geen (na afdoende motivatie) Steluitgifte: **nog niet vastgesteld**
- Sectorale knooppunten: **nog niet vastgesteld**.

IBV standaarden voor datacommunicatie:

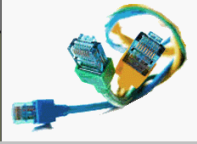
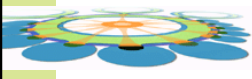
- Verbinding: via glas, koper of wireless (vooralnag niet nader gespecificeerd)
- Toegestane voorzieningen: GEMnet, NAFIN, Politie Nuisvoorziening, C2000, Noodnet, Haagse Ring. "Specials" zoals GSM en Internet zijn toegestaan na afdoende motivatie: o.a. exclusiviteit en authenticatie moeten gewaarborgd zijn.

IBV standaarden communicatieprotocol:

- Standaardprotocol voor data: TCP/IP (zie nl.wikipedia.org/wiki/TCP/IP)
- Standaardprotocol voor spraak mobiel in extern gerichte primaire processen: TETRA (zie nl.wikipedia.org/wiki/TETRA)
- Standaardprotocol voor spraak overig: **nog niet vastgesteld**
- Client-applicaties zijn "LDAP-aware".

IBV standaarden voor berichttransacties:

- Transacties op basis van servicebus, zoals beschreven in NORA v1.9, §2.2 e.v.
- Protocollen: ISO-15000-2-eb-XML en Web-service gebaseerd (zie www.iso.org)
- Transacties reliable messaging: JAB 2.0 uit ePV (zie www.e-pv.nl) of Berichtenstandaard SBG/OBS (z.Stelselhandboek)
- Transactiestandaard realtime bevragingen: **nog niet vastgesteld**



1. IBV communicatienetwerk

Om informatie te kunnen hebben en delen, moeten de gegevens ter plekke komen via een betrouwbaar netwerk (zowel via een vaste als een draadloze verbinding). Deze voorziening vult dat in. Een belangrijk onderdeel van de vaste verbinding is de Nutsvoorziening Veiligheid.



2. Toegangsportaal met poortwachter

Gegevens mogen alleen beschikbaar zijn voor diegenen die daartoe gerechtigd zijn. Met deze voorziening kunnen verschillende domeinen zoals politie, brandweer, gemeenten, etc. veilig gekoppeld worden, met gedegen authenticatie en autorisatie.



3. Berichtenmakelaar met postkantoor

Om berichten naar partners te sturen en gegevens met anderen te kunnen delen, is een routeringsmechanisme nodig dat voor gebruikers onzichtbaar is. Deze voorziening vult dat in. Veiligheidspartners kunnen berichten en gegevens afgeven aan het "IBV postkantoor".



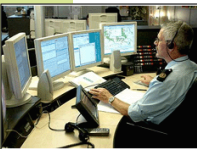
4. Ontsluiting van basisregistraties

Het gebruik van basisregistraties voor authentieke gegevens over personen, gebouwen, adressen, bedrijven, percelen en kaartmateriaal is wettelijk verplicht. Om er winst mee te behalen zijn goede ontsluitingsmogelijkheden onontbeerlijk. Deze voorziening vult dat in.



5. Borging van gegevenskwaliteit

In alle primaire processen van het veiligheidswerk is het hebben en delen van juiste, actuele en relevante gegevens en metadata van het grootste belang. Veredeling van oude gegevens is vaak geautomatiseerd mogelijk. Deze voorziening ondersteunt daarbij.



6. Generieke en gemeenschappelijke toepassingen

Dit zijn toepassingen voor het hebben en kunnen delen van informatie, die zich in een gemeenschappelijk domein bevinden. Hieronder vallen o.a. GMS, Geografische Informatiesystemen, en toepassingen die gegevens ontsluiten richting mobiele devices zoals PDA's.



7. Crisisplein: voorziening voor crisiscoördinatie

In crisissituaties moet er een (virtuele) ontmoetingsplaats zijn waar coördinatoren gestructureerd en op basis van goede gegevens de juiste beslissingen kunnen nemen. Deze CMIS voorziening ondersteunt daarbij. Dit is niet één toepassing, maar een stelstel van ict-modules.



8. Dossiermanagement

Deze voorziening ontsluit, als ware het een papieren dossier, alle relevante gegevens van een object, subject of locatie en houdt tegelijk de historie, de afhandeling en bewerking van het dossier bij. Dit zit dicht tegen werkstroombeheersing en document management aan.



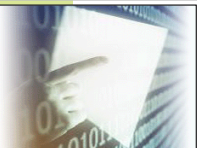
9. Integrale zoekfunctionaliteit

Voor de veiligheidspartners is het van belang om benodigde informatie op een snelle en intuïtieve wijze (à la "Google") te kunnen vinden. Daarbij moet over alle deelnemende domeinen kunnen worden gezocht. Deze voorziening vult dat in.



10. Ketenbrede coördinatie

De veiligheidsketen blijft zich evolueren. Op strategisch en tactisch niveau moet de samenhang in informatie-uitwisseling en informatievoorzieningen geborgd blijven. Deze voorziening (en aanpak) ondersteunt daarbij, vooral op bestuurlijk niveau.



11. Informatiebehoefteboek

Informatie hebben en kunnen delen, kan alleen realiteit worden als bekend is wie behoefte heeft aan welke informatie, waar en wanneer, en in welke vorm. Deze voorziening biedt daar continu inzicht in.



12. Veiligheidsloket voor burger en bedrijf

Een belangrijke taak van de veiligheidspartners bestaat uit voorlichting richting burger en bedrijf, zowel in reguliere als bijzondere omstandigheden. Deze voorziening ondersteunt daarbij.