centrum informatiebeveiliging en privacybescherming

Keten Service Library

Een naslagwerk voor veilige en robuuste dienstverlening in ketens

juni 2022 [versie 2.1 definitief]

© Centrum Informatiebeveiliging en Privacybescherming.
Voor dit werk geldt een Creative Commons Naamsvermelding GelijkDelen 4.0 licentie, verleend door het CIP. Zie https://creativecommons.org/licenses/by-sa/4.0/

Titel	Keten Service Library (KSL)
Datum	juni 2022
Status	Versie 2.1 definitief
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming
Regime	Becommentarieerde praktijk
Auteurs	CIP Keten Community
Reviewers	CIP Kernteam

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt.

Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Voorwoord

In de tegenwoordige 'vernetwerkte' wereld is er vaak een keten van partijen betrokken bij het leveren en in stand houden van kritische IT-diensten. Er is dan sprake van complexe afhankelijkheden en soms wisselende relaties tussen publieke en private partijen. In dergelijke situaties is het belangrijk om duidelijke afspraken te maken over het voorkomen en oplossen van incidenten in de keten. Want een organisatie kan het nog zo goed voor elkaar hebben, als dit bij een andere partij niet zo is, dan kan dat vervelende gevolgen hebben voor een van de partijen in de keten.
De visie van CIP is dat de complexiteit van de diverse netwerken of ketens dusdanig groot geworden is dat regie op een veilig en betrouwbaar end-to-endproces 'van invoer tot uitkomst' een achterhaald principe is. Andere ordeningsprincipes en besturingsarrangementen zijn nodig om ketens en partijen daarbinnen te ondersteunen bij het vormgeven van een robuuste vernetwerkte dienstverlening. Denk daarbij aan manieren voor:

1. het treffen van voldoende beveiligings- en privacy-maatregelen door de ketenpartijen op basis van geïdentificeerde risico's,
2. het benoemen en beleggen van de eind- en deelverantwoordelijkheden in de keten en binnen de eigen organisatie,
3. het maken van de afspraken die de verschillende ketenpartijen onderling moeten maken,
4. het toezien op de naleving van de afspraken,
5. de samenwerking en communicatie in de keten in het geval van een incident.

Deze voorliggende *Keten Service Library* biedt een verzameling van hulpmiddelen (best practices, tools, methodieken) die een netwerkorganisatie of ketenpartij kan inzetten bij het vormgeven van robuuste vernetwerkte dienstverlening. Wij hopen dat dit document houvast geeft aan betrokkenen in de diverse functieniveaus van ketenorganisaties en inspiratie biedt om er actief mee aan de slag te gaan.

Managementsamenvatting

Dit rapport biedt een aanzet tot een Keten Service Library voor mensen die op zoek zijn naar hulpmiddelen voor het realiseren van veilige en robuuste dienstverlening in ketens. De hulpmiddelen voor ketenbeheersing variëren van normenkaders naar best practices, van methodieken naar tools en richten zich op het creëren van beveiliging, transparantie, besturing, risicobeheersing en incident management. Ze bieden houvast en inspiratie voor verschillende functies binnen organisaties die in ketens actief zijn (bestuurders, security officers, risico managers, IT-beheerders, auditors, etc.).

Inhoudsopgave

Voorwoord		3
Managementsamenvatting		4
Inhoudsopgave		5
1	Veilige en robuuste dienstverlening in ketens	8
1.1	Essentiele bouwstenen	8
1.1.1	Beveiliging en privacy	8
1.1.2	Risicobesef	8
1.1.3	Ketensturing	9
1.1.4	Transparantie	9
1.1.5	Incidentmanagement	9
1.2	Keten Service Library	9
1.3	Hulpmiddelen	10
1.4	Werkwijze	12
1.5	Leeswijzer	12
2	Positionering van hulpmiddelen	13
2.1	Beveiliging en privacy	13
2.1.1	Baselines als startpunt	13
2.1.2	Identity & Access Management in ketens	14
2.1.3	SLA	16
2.1.4	Verwerkingsovereenkomst	16
2.1.5	Privacy	16
2.1.6	Cloud Computing	18
2.1.7	Contractmanagement	18
2.2	Risicobesef	18
2.2.1	Best practices	18
2.2.2	Methodieken en modellen	18
2.2.3	Gaming	19
2.2.4	PIA	19
2.2.5	Bewustzijn	20
2.3	Besturing	20
2.3.1	Inrichting en besturing	20
2.3.2	Kaders, afspraken en verantwoordelijkheden	22

2.4	Transparantie	25
2.4.1	Verantwoording	25
2.4.2	Baselines	26
2.4.3	Inkoopvoorwaarden	26
2.4.4	Logging en monitoring	26
2.4.5	Audits of assessments	27
2.5	Incident management	27
2.5.1	Alarmeren	27
2.5.2	Signaleren	27
2.5.3	Afhandelen	28
Appendix A. Naslagwerk Hulpmiddelen		29
2.6	Classificatie van hulpmiddelen	29
2.7	Overzicht van hulpmiddelen	29
2.8	Baselines informatiebeveiliging	31
2.9	Ketenafspraken en –kaders	32
2.10	Authenticatieniveaus	33
2.11	Authenticatie-architectuur	34
2.12	Ketenautorisatie	35
2.13	Keten Service Level Agreements	36
2.14	Berichtstandaardisatie	37
2.15	Doelbindingstoetsen	38
2.16	Filters	39
2.17	Privacy-by-design	40
2.18	NOREA Audit Alert Keteninformatisering	41
2.19	NISTIR 7622	42
2.20	Advanced Risk Management (ARM)	43
2.21	TTISC	44
2.22	TMAP NEXT Ketentest	45
2.23	C4-model	46
2.24	Privacy Impact Assessment (PIA)	47
2.25	Bewustzijnscampagne Suwinet	49
2.26	NORA Ketens de Baas	50
2.27	NORA Katern Verbinden	51

2.28	Handboek ketens VNG	52
2.29	Ketenoverleg	53
2.30	Beveiligings- en privacy-rapportages	54
2.31	Lessen uit de keten van werk en inkomen	55
2.32	Wetgeving	56
2.33	Keten DAP	57
2.34	Vervallen	58
2.35	Aansluitvoorwaarden	59
2.36	Monitoring Tool BKWI	60
2.37	Beveiligingsassessment DigiD	61
2.38	Vervallen	62
2.39	Leidraad responsible disclosure	63
2.40	Vervallen	64
2.41	Auditdienst Rijk over systeemverantwoordelijkheid	65
2.42	NOREA Keten-auditing	66
2.43	Secure Software Development (SSD)	67
2.44	Verwerkersovereenkomst	68
2.45	Cloud Computing	69
2.46	Contractmanagement	70
2.47	Inkoopvoorwaarden en informatiebeveiligingsdiensten	71
2.48	A3 jaarplan	72
2.49	Algemene beheersing van IT diensten	73
2.50	Netwerk game en Crisis game	74
2.51	Privacy-afspraken bij ketensamenwerking	75
2.52	Ketencommunicatie bij crises	76
2.53	KetenTestDorp	77

1 Veilige en robuuste dienstverlening in ketens

1.1 Essentiele bouwstenen

Samenwerking in ketens begint vaak bij een verwacht gezamenlijk voordeel of bij een dwingend wettelijk kader. Zo is de samenwerking in de Suwi-keten wettelijk bepaald, en spruit de samenwerking in het stelsel voor eHerkenning voort uit (o.a.) economisch voordeel. Veilige ketensamenwerking vraagt om afspraken tussen alle partijen, om te voldoen aan de wettelijke kaders of om voordelen te behalen. Met die afspraken wordt het vertrouwen tussen ketenpartijen geborgd, het risicobewustzijn vergroot, de informatiebeveiliging bevorderd, besturing georganiseerd, transparantie geboden en worden eventuele incidenten effectief opgelost.

De verantwoordelijkheid van organisaties voor een veilige informatievoorziening moet gericht zijn op het in gezamenlijkheid met andere ketenpartners realiseren van een veilige informatievoorziening van ketens. Dit vraagt van elke ketenpartij om vanuit keten breed risicobesef de voor hem geldende baseline informatiebeveiliging te implementeren en vanuit bewustzijn van de risico's aanvullende maatregelen te treffen en hierop te sturen. Deze sturing moet verankerd zijn in ieders reguliere planning-en-control-cyclus.

Het is daarbij wenselijk om collega-ketenpartijen of een eventueel keten breed toezichthoudend orgaan op de hoogte te houden over de inrichting en verankering van de beveiliging van ketenprocessen. In deze transparantie kan worden voorzien door het afleggen van een aan verantwoordingsverklaring vergelijkbare transparantieverklaring, bijvoorbeeld middels een periodieke externe audit of via rapportages. Een toezichthoudend orgaan kan een samenvatting maken van de rapportages en zo voor overzicht over de keten en zijn beveiliging zorgen.

Ondanks zulke inspanningen kunnen zich niettemin incidenten blijven voordoen. In zulke gevallen moeten de gevolgen voor andere ketenpartijen duidelijk worden, en ook wanneer, door wie en hoe ketenpartijen en de buitenwereld geïnformeerd worden. Daarnaast moet het incident in overleg met de andere ketenpartijen efficiënt opgelost worden en geleden schade hersteld worden.

De vijf aspecten die hierboven zijn geraakt komen hieronder in meer detail aan de orde: beveiliging en privacy, risicobesef, ketensturing, transparantie en incidentmanagement.

1.1.1 Beveiliging en privacy

Het afspreken en implementeren van een eenduidig en geharmoniseerd privacy- en beveiligingsbeleid biedt een fundament voor betrouwbare ketensamenwerking. Het implementeren van een baseline beveiliging binnen de eigen organisatie is daarbij een goede eerste stap.

Wel kan daarbij een spanningsveld ontstaan. Het voor de keten gewenste beveiligingsniveau kan immers andere, specifiekere eisen stellen dan welk met de eigen baseline voor een individuele organisatie gerealiseerd wordt. Een keten brede toezichthouder kan hierin het ketenbelang vertegenwoordigen.

1.1.2 Risicobesef

Risicobesef bij verschillende functies binnen ketenpartijen zorgt voor betrokkenheid en mitigerende beveiligingsmaatregelen. Net als in het geval van de baseline kunnen zulke maatregelen bij specifieke partijen specifieke invullingen krijgen, terwijl vanuit ketenperspectief meer of zwaardere eisen gesteld worden. Dat kan ertoe leiden dat hier en daar in de keten extra maatregelen getroffen moeten worden om ketenrisico's te beheersen.

Tot slot kan het zich voordoen dat risico's voor de ene ketenpartij ontstaan bij een andere, waarvoor de verantwoordelijke van eerstgenoemde dus geen verantwoordelijkheid kan dragen. Samenwerking met ketenpartners is dan noodzakelijk om die risico's voor eenieder passend het hoofd te bieden. Een ketenbrede autoriteit kan zorgen voor inzicht in en overzicht over ketenrisico's en hun mogelijke impact.

1.1.3 Ketensturing

Ketensturing borgt de onderlinge samenhang in het sturen, beheersen en toezicht houden in een keten, evenals het daarover open communiceren en verantwoorden, ten behoeve van alle belanghebbenden. Ketensturing is gericht op een efficiënte en effectieve verwezenlijking van veilige en robuuste dienstverlening.

Bij ketensturing spelen allerlei vraagstukken. Wie is verantwoordelijk? Hoe wordt verantwoording afgelegd? Wie monitort dit? Goede antwoorden daarop zijn voorwaarden voor het inrichten en beheersen van ketens en vernetwerking van ketens.

Hoe ketensturing ingevuld wordt hangt af van het type keten, het dominante ketenprobleem, de mate van vertrouwen tussen de partijen en de wettelijke kaders. Afhankelijk van het type keten zal er al dan niet een regisseur aanwezig zijn.

1.1.4 Transparantie

Transparantie over de gerealiseerde veiligheid en betrouwbaarheid van de dienstverlening is nodig voor vertrouwen tussen ketenpartijen en blootlegging van eventuele risico's. Er moet afgesproken worden waarover partijen elkaar precies informeren en hoe hierover verantwoording wordt afgelegd. Vaak rust de wijze van verantwoording op een wettelijke basis. Soms ook liggen hier contracten, afspraken, convenanten of gedragscodes aan ten grondslag. Verder kan een ketenregisseur of toezichthouder een rol spelen bij het creëren van transparantie en vertrouwen in de keten.

1.1.5 Incidentmanagement

Effectieve en gezamenlijke afhandeling van incidenten is essentieel om de schade te beperken. Niet elk incident wordt een crisis; goede incidentbehandeling kan een crisis voorkomen. Elke ketenpartij heeft daarvoor crisismanagement in de eigen organisatie ingericht. Hierbij is het verstandig om de gehele keten in ogenschouw te nemen, omdat een incident consequenties kan hebben voor andere ketenpartijen.

Bij het beheersen van ketenincidenten moet soms intensief worden samengewerkt. Beschikbaarheid van contactgegevens van ketenpartijen helpt daarbij. Bij die samenwerking is soms ook coördinatie nodig, waarbij een ketenautoriteit of één van de ketenpartijen een voortrekkersrol speelt. Tot slot vormt communicatie een belangrijk aspect van crisismanagement. Het kan veel onrust voorkomen als media, ketenpartijen en medewerkers tijdig en juist geïnformeerd worden.

1.2 Keten Service Library

Toenemende vernetwerking van ketens en de daardoor groeiende complexiteit maakt het niet eenvoudig invulling te geven aan deze vijf aspecten. Soms blijkt de huidige invulling achterhaald en zijn andere ordeningsprincipes en besturingsarrangementen nodig om ketens en partijen daarbinnen te ondersteunen bij het vormgeven van een robuuste vernetwerkte dienstverlening. Bij menige ketenpartij groeit de behoefte aan ondersteuning bij het grip houden op deze toenemende vernetwerking.

Een eerste stap in deze ondersteuning is het in kaart brengen van beschikbare hulpmiddelen bij de invulling van deze vijf aspecten. Deze *Keten Service Library* biedt een gestructureerd overzicht van hulpmiddelen waarmee op strategisch (richtinggevend), tactisch (sturend) en operationeel (uitvoerend) niveau invulling gegeven kan worden aan veilige en robuuste vernetwerkte dienstverlening.

De hulpmiddelen worden dus geordend langs twee assen, volgens de figuur hieronder.

Invulling van / op	Strategisch	Tactisch	Operationeel
Beveiliging en Privacy	Hulpmiddel A	Hulpmiddel F	
Risicobesef			Hulpmiddel C
Besturing		Hulpmiddel B	
Transparantie			Hulpmiddel E
Incident management	Hulpmiddel D		

De Keten Service Library biedt een gemeenschappelijk naslagwerk voor verschillende functies binnen netwerk- of ketenorganisaties bestuurders, security officers, IT-beheerders etcetera. Zij vinden daarin hulpmiddelen bij het vormgeven van een degelijke positie in keten(s).

1.3 Hulpmiddelen

Hulpmiddelen zijn er in soorten en maten: best practices, methodieken, tools, checklists en documenten. De focus daarbij ligt nadrukkelijk op hulpmiddelen die specifiek voor een keten of netwerk zijn ontwikkeld.

Voor het deelgebied risicobesef zijn bijvoorbeeld hulpmiddelen als A&K-analyse (afhankelijkheids- en kwetsbaarheidsanalyse), Sprint en IRAM (Integrated Risk Assessment Method) beschikbaar. Deze risico-analysehulpmiddelen, in dit geval methodieken, worden regelmatig door organisaties ingezet, vaak in de context van informatiebeveiliging. Deze methodieken zijn echter niet toegesneden op ketens. Beschikbare methodieken richten zich veelal op één organisatie en geven zo onvoldoende handvatten om de risico's van de keten inzichtelijk te maken, laat staan dat ze organisaties helpen ketenverantwoordelijkheid te nemen op dit gebied. Dergelijke hulpmiddelen vallen dus buiten de scope van de Keten Service Library.

Hetzelfde geldt voor de hulpmiddelen voor de deelgebieden transparantie en incidentmanagement. Het deelgebied besturing is specifieker voor ketens hoewel daar onderscheid gemaakt moet worden tussen intra-organisatie en organisatie-overstijgende afspraken en de verschillende hulpmiddelen daarvoor.

Vanzelfsprekend is elke keten uniek. Er bestaat geen vast recept, laat staan een standaard organisatie- of besturingsmodel voor ketens. Dit naslagwerk gaat ervan uit dat er geen 'beste oplossing' bestaat voor ketensamenwerking en –beveiliging, maar dat verschillende ketens verschillende vormen van organisatie, transparantie en besturing behoeven. Dit naslagwerk kan dus geenszins normatief zijn. Het is aan de ketens of de organisaties daarbinnen zelf om de voor hun bruikbare hulpmiddelen uit dit naslagwerk te selecteren en daarmee aan de slag te gaan.

Van elk van de opgenomen hulpmiddelen worden de volgende kenmerken beschreven:

Deelgebied	Eén of meerdere van de volgende vijf: beveiliging & privacy, transparantie, besturing, risicobesef of incidentmanagement
Soort hulpmiddel	Tool, best practice, methodiek, checklist, video, overeenkomst, normenkader…
Beschrijving	Korte beschrijving van het hulpmiddel en wat het beoogd te realiseren.
Doelgroep	Bestuurders, security officers, risico-managers en interne controllers, gegevensfunctionarissen, IT-beheerders, architecten, auditors,…
Inzetbaarheid / herkomst	In welke keten of welk domein wordt het ingezet? Is het breder inzetbaar? Zo niet, onder welke voorwaarden zou het dan wel succesvol ingezet kunnen worden?
Referenties	Verwijzing naar meer informatie, voorbeelden (denk hierbij aan een keten-SLA), contactpersonen en/of bedrijven die eigenaar of beheerder zijn van het hulpmiddel.
Overig	Specifieke opmerkingen over het hulpmiddel. Bijvoorbeeld verwijzingen naar andere hulpmiddelen.

Voor de classificatie van een hulpmiddel volgens de tabel in 1.2 worden iconen gebruikt, met het deelgebied in een blauwe band en daaronder een groene letter. Enkele voorbeeldiconen zijn:



Daarbij staat:

- S voor strategisch: hulpmiddelen die bestuurders en topmanagement helpen bij het invullen van ketenactiviteiten die richtinggevend en voor de lange termijn zijn.
- T voor tactisch: hulpmiddelen die het middenmanagement helpen bij het invullen van ketenactiviteiten die sturend en voor de middellange termijn zijn. De tactische activiteiten voeren een strategie uit. Voorbeelden van toepasselijke middenmanagementfuncties zijn de security officer, risk manager, gegevensfunctionaris en auditor.
- O voor operationeel: hulpmiddelen die het uitvoerend personeel helpen bij het invullen van ketenactiviteiten die operationeel en voor de korte termijn zijn. De operationele activiteiten voeren de tactiek uit. Voorbeelden van uitvoerende functies zijn de IT-beheerder en architect.

De Keten Service Library classificeert en beschrijft hulpmiddelen zo objectief mogelijk. Waardeoordelen zullen toegevoegd worden in het geval een hulpmiddel (nog) niet geheel toereikend is voor ketens, hulpmiddelen ontbreken of wanneer het gebruik van een hulpmiddel speciale aandacht vereist. Zulke waardeoordelen worden met het volgende icoon aangegeven:



1.4 Werkwijze

Initieel zijn de hulpmiddelen verzameld via bureau-onderzoek en met een beperkt aantal interviews met ketenpartijen. Daarnaast is input verkregen uit de verschillende ketenwerkgroepen binnen CIP. De belangrijkste bronnen van informatie zijn de Suwi-keten en verschillende stelsels voor federatief identiteitsmanagement. In mindere mate is inzicht gekregen in hulpmiddelen uit de loonaangifte- en strafrechtketen. In recentere versies van dit naslagwerk is gekeken naar de actualiteit van de links en zijn practices die via CIP worden beschikbaar gesteld toegevoegd.

1.5 Leeswijzer

Hoofdstuk 2 positioneert en beschrijft de verschillende hulpmiddelen per deelgebied. De namen van de hulpmiddelen zijn *onderlijnd en schuingedrukt* gezet. Daarnaast geeft een in de kantlijn geplaatst icoon aan of er sprake is van een strategisch, tactisch of operationeel hulpmiddel. De lezer kan dan eenvoudig beoordelen of het hulpmiddel bij zijn/haar functie of rol binnen de organisatie past. Het nummer achter de onderlijnde hulpmiddelen verwijst naar een uitgebreidere beschrijving en classificatie ervan in de Appendix.

2 Positionering van hulpmiddelen

Zoals een kaartenbak niet bedoeld is om door te lezen, zo is de gestructureerde en geclassificeerde beschrijving van hulpmiddelen in Appendix A dat ook niet. Voor wie toch een leesbaar overzicht zoekt, bevat dit hoofdstuk een overzicht over de hulpmiddelen in proza en in de context van veilige en robuuste dienstverlening in vernetwerkte ketens, zoals beschreven in het visiestuk van CIP.

2.1 Beveiliging en privacy

Een belangrijke stap voor het verbeteren van het niveau van de beveiliging in ketens is dat alle individuele ketenpartijen ervoor zorgen dat ze hun eigen huishouden hieromtrent op orde hebben. Dat wil zeggen dat ze de eigen informatiebeveiliging betreffende de vertrouwelijkheid (waarborgen dat informatie alleen toegankelijk is voor de degenen die hiertoe geautoriseerd zijn), integriteit (waarborgen van de correctheid en de volledigheid van informatie en verwerking) en de beschikbaarheid van gegevens geregeld hebben. Transparantie (zie 2.4) adresseert het vierde beveiligingsaspect: controleerbaarheid.

Binnen veel organisaties heeft informatiebeveiliging een bepaalde volwassenheid bereikt. Organisaties zijn zich bewust van de risico's, beleid is vastgesteld en verantwoordelijkheden zijn belegd. In een keten is echter meer nodig. De intensieve samenwerking en het uitwisselen van informatie betekent dat organisaties hun informatiebeveiliging niet (langer) 'op eigen houtje' kunnen inrichten. Zij moeten rekening houden met de extra eisen die samenwerking aan informatiebeveiliging stelt. Deze komen uit een keten brede risico analyse. Hulpmiddelen hiervoor zijn te vinden in 2.2.

2.1.1 Baselines als startpunt



Een goede samenwerking is alleen mogelijk als organisaties hun informatiebeveiliging op elkaar afstemmen en elkaar daarin ook vertrouwen. Een hiervoor goed in te zetten hulpmiddel is dat van een *security baseline* [2.8]. Een security baseline biedt bestuur en management een instrument waarmee ze in staat zijn om te bepalen of de organisatie 'in control' is op gebied van informatiebeveiliging. Er wordt zo een indruk opgedaan of informatiebeveiliging als zodanig aantoonbaar beheerst wordt tot op een niveau dat van de organisatie verwacht mag worden. Voorbeelden van dergelijke baselines is Baseline Informatiebeveiliging Overheid.



In een keten is het wenselijk dat er afspraken gemaakt worden over de te hanteren baseline om ervoor te zorgen dat er een eenduidig beeld over de beveiliging van de keten ontstaat. Ook zal het eenvoudiger zijn hierover te rapporteren richting de andere ketenpartijen. Het resultaat hiervan biedt nog geen garanties voor de realisatie van een keten brede baseline voor informatiebeveiliging. Het is denkbaar dat de implementatie van een baseline vanuit het risicobesef van een specifieke partij een eigen invulling krijgt, terwijl vanuit ketenperspectief toch zwaardere eisen gesteld worden. Dat kan ertoe leiden dat op plaatsen in de keten aanvullende maatregelen nodig zijn om de risico's in de keten het hoofd te bieden.



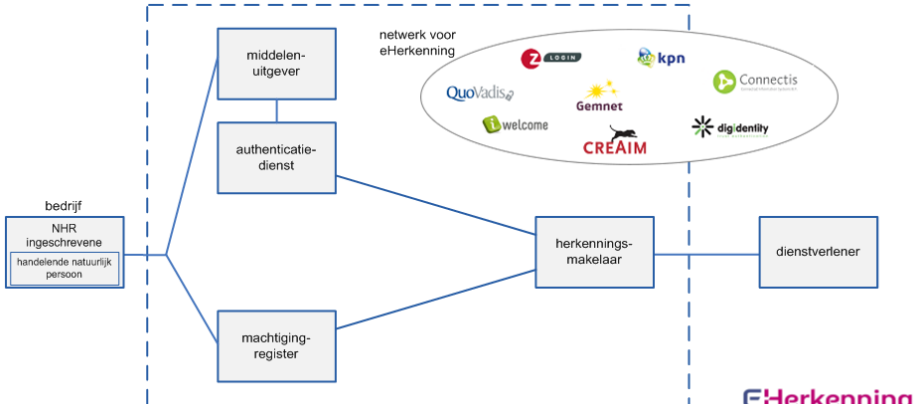
Het relatief generieke karakter van baselines is een ander aandachtspunt. Dit leidt er vaak toe dat additionele, keten specifieke beveiligingseisen nodig zijn. Dergelijke eisen zullen door de ketenpartijen geïdentificeerd en geïmplementeerd moeten worden om ervoor te zorgen dat ze hun beslag vinden in de keten en dat de ketenpartijen zich erover kunnen verantwoorden.



Afspraken hieromtrent vinden typisch hun beslag in *keten specifieke afsprakenkaders* 2.9]. Voorbeelden hiervan zijn het Normenkader voor Suwinet, de informatiebeveiligingsafspraken in de strafrechtketen en het Afsprakenstelsel eHerkenning.

eHerkenning

eHerkenning regelt de digitale herkenning (authenticatie) en controleert de digitale bevoegdheid (autorisatie) van personen die online een dienst willen afnemen. eHerkenning is ontstaan in een samenwerkingsverband tussen de overheid en het bedrijfsleven. De dienst eHerkenning wordt geleverd door erkende aanbieders die zijn verenigd in een netwerk. Zij werken samen volgens afspraken die gaan over het beheer, de ontwikkeling van nieuwe functionaliteiten, beveiliging en privacy. Het netwerk en de verschillende partijen daarin is hieronder geschetst.



2.1.2 Identity & Access Management in ketens

Een belangrijk onderdeel van een betrouwbare informatievoorziening in ketens is een goed ingerichte identity & acces management infrastructuur dat gebruikers op een gecontroleerde manier toegang tot informatie, diensten en systemen kan geven. Hier zijn verschillende hulpmiddelen voor in te zetten.

2.1.2.1 Betrouwbaarheidsniveau authenticatie



In eerste instantie zal de identiteit van de gebruiker die toegang wil tot bepaalde gegevens geverifieerd moeten worden: authenticatie. De betrouwbaarheid van de authenticatie dient gelijke tred te houden met de gevoeligheid van de gegevens of diensten. Hulpmiddelen hiervoor zijn handreikingen vanuit het Forum Standaardisatie en NICTIZ. Met deze handreikingen kan het vereiste *betrouwbaarheidsniveau van authenticatie* [2.10] worden bepaald in relatie tot de gevoeligheid van de persoonsgegevens die daarmee ontsloten worden. Sterke authenticatiemiddelen op basis van certificaten of een tweede factor zijn in sommige gevallen nodig om zeker(der) te zijn van de identiteit van de gebruiker en te voorkomen dat deze kan ontkennen bepaalde handelingen verricht te hebben. Afspraken over het vereiste niveau van authenticatie voor het verkrijgen van toegang tot diensten of gegevens zijn noodzakelijk. In eHerkenning zijn specifieke betrouwbaarheidsniveaus voor authenticatie vastgelegd in een normenkader. De dienstenaanbieder hoeft dan slechts aan te geven welke niveau gewenst is en hoeft zich niet te verdiepen in welke authenticatie-oplossing de gebruiker van een ketenpartner hiervoor gebruikt.

2.1.2.2 Authenticatie-architecturen



Een goede *authenticatie-architectuur* [2.11] voor de keten kan veel kosten en gebruikersergernis besparen. Het authentiseren van gebruikers kan door middel van een eigen oplossing of via een federatieve aanpak. Een voorbeeld van een eigen, centrale authenticatie-oplossing is te vinden bij Suwinet Inkijk waarvoor de centrale beheerder (BKWI) accounts uitgeeft en beheert. Gebruikers kunnen daarmee inloggen bij Suwinet Inkijk en gegevens over de klant raadplegen. Een dergelijke centrale oplossing is niet voor elke keten geschikt. Een alternatieve aanpak is gebruik te maken van federatieve authenticatie. In dat geval authentiseert iedere ketenpartij zijn eigen gebruikers, ook als deze toegang willen krijgen tot gegevens of diensten van andere ketenpartijen, of er is een centrale partij die het gezamenlijke identiteit-gebruik voor de keten regelt. Een decentrale federatieve oplossing is te vinden in het hoger onderwijs waar studenten met hun eigen universiteitsaccount kunnen inloggen bij tal van dienstenleveranciers. Voorbeelden van centrale federatieve oplossingen zijn DigiD en eHerkenning. Het voordeel van een federatieve aanpak is dat gebruikers slechts één account hebben (met bijbehorend wachtwoord) en dat de andere ketenpartijen hier geen beheerlasten van hebben. Wel dient er voldoende vertrouwen te zijn tussen de ketenpartijen en is het nodig overeenstemming te bereiken over de te garanderen betrouwbaarheidsniveaus.

Identiteitsfederatie SURFnet

De identiteitsfederatie voor het hoger onderwijs en wetenschappelijk onderzoek wordt beheerd door SURFnet. De federatie is opgezet volgens een hub-and-spoke-architectuur waarbij zowel dienstverleners als instellingen aansluiten op de hub bij SURFnet. Deze hub verzorgt de communicatie tussen de dienstverleners (SPs) en de instellingen (IdPs) waarbij de authenticatie-infrastructuur van de instellingen gebruikt kan worden om toegang te verlenen tot de diensten. Hierdoor hoeven medewerkers en studenten van de instellingen dus niet voor elke dienst een aparte gebruikersnaam en wachtwoord aan te vragen, maar hergebruiken ze hun instellingsaccount op een veilige manier.

2.1.2.3 Ketenautorisatie uniforme vastlegging van rollen of attributen



Als de identiteit van de gebruiker eenmaal bekend is, zal bepaald moeten worden wat hij/zij mag: autorisatie. Toegang is vaak gebaseerd op een toe te kennen rol. In toenemende mate is autorisatie ook gebaseerd op aangeleverde attributen (zoals leeftijd, lidmaatschap, KvK-nummer, functie, etc.). Voor ketenpartijen is het belangrijk om afspraken te maken over de rollen en attributen in de keten. *Uniforme vastlegging van rol- of attribuut-gebaseerde toegang* [2.12] maakt uitwisseling tussen verschillende zorgaanbieders en hun informatiesystemen mogelijk. Iedere partij in de keten kan rollen of attributen toekennen aan gebruikers op basis van hun functie in de organisatie. Dit dient met beleid te gebeuren om stapeling van bijvoorbeeld rollen te voorkomen.



In Suwinet zijn bijvoorbeeld enkele tientallen rollen gedefinieerd die toegang geven tot bepaalde gegevenssets. Voor de zorgsector beschrijft het NEN7521 normontwerp een mechanisme waarmee toegang tot patiëntgegevens, die berusten op een locatie (rol, instelling, praktijk enz.), kan worden verkregen vanaf een andere locatie en hoe de patiënt daarin zijn wil kan uiten. In de SURFnet federatie voor het hoger onderwijs wordt toegang gebaseerd op door de universiteit aangeleverde attributen, bijvoorbeeld de gevolgde studierichting. Ten opzichte van rol-gebaseerde toegang biedt attribuut-gebaseerde toegang meer mogelijkheden voor fijnmazige

autorisatie zonder dat dit gepaard gaat met een explosie van attributen (wat bij rollen wel het geval is als fijnmazigheid nodig is). eHerkenning maakt gebruik van attributen om aan te geven dat een gebruiker gemachtigd is om namens een bedrijf te handelen.

2.1.3 SLA

Met betrekking tot beschikbaarheid van gegevens worden Service Level Agreements (SLA's) ingezet.



Een *keten-SLA* [2.13] legt de wederzijdse resultaatverplichtingen over ICT-beheer, beschikbaarheid, integriteit en kwaliteit van de data, toegangsbeveiliging en incidenten- en risicobeleid vast. Een voorbeeld van een keten-SLA is die van Suwinet. Ook hier geldt dezelfde kanttekening als bij security baselines: de beschikbaarheid van de keten als geheel kan ertoe leiden dat de beschikbaarheid van de individuele ketenpartijen hoger zal moeten zijn dan strikt voor die partij noodzakelijk is. Dit kan extra kosten met zich meebrengen.

2.1.4 Verwerkingsovereenkomst

Er dient een verwerkingsovereenkomst [2.44] opgesteld te worden tussen partijen als een



verantwoordelijke partij persoonsgegevens laat verwerken door een bewerker. Elke keer dat een verantwoordelijke partij het verwerken van persoonsgegevens 'uitbesteedt' wordt een schriftelijke overeenkomst vereist. Een voorbeeld van een verwerkingsovereenkomst is die van de IBD gemeenten.

2.1.5 Privacy

Belangrijke aspecten van privacy zijn doelbinding en proportionaliteit van de gegevensverstrekking. De



realisatie ervan in ketens is echter niet triviaal. Om doelbinding te garanderen zijn er een aantal technische en organisatorische maatregelen te treffen. Daarnaast is het verstandig om een beroep te doen op het gedrag en de integriteit van de gebruiker.

Standaardisatie van de gegevensuitwisseling [2.14] is een maatregel om doelbinding en proportionaliteit te realiseren. Het Suwi-domein geeft hier invulling aan middels het Suwi Gegevensregister (SGR). Het SGR legt de structuur van de Suwinet gegevensuitwisseling vast in de vorm van definities, formaten en mogelijke waarden van het betreffende gegeven. In het kader van de Wet Eenmalige Uitvraag van gegevens (WEU) is een overzicht van SGR gegevens ten opzichte van de wettelijke grondslag beschikbaar. Dit met het doel voor zowel de burgers als de professionals de gegevensuitwisselingen binnen Suwinet zodanig transparant te maken dat inzichtelijk wordt op basis van welke wettelijke grondslag (doelbinding) welke gegevens (proportionaliteit) door wie (verantwoordelijke) aan wie (verwerker) worden geleverd en zodoende partijen aanspreekbaar te maken op naleving van de geldende privacy wetgeving AVG (Algemene Verordening Gegevensbescherming) en op eventuele keten-specifieke privacy afspraken en normen.

Aan het gebruik van gegevens voor een bepaald doel ligt vaak een wettelijke bepaling ten grondslag.



Het is daarom een vereiste dat, voordat een partij toestemming krijgt om bepaalde gegevens van een leverancier te mogen gebruiken, een toets plaatsvindt voor het bepalen van de wettelijke grondslag en de doelbinding. Dergelijke *doelbindingstoetsen* [2.15] worden ingezet in bijvoorbeeld de loonaangifteketen en de keten voor werk en inkomen.

Vooral betreffende de doelbinding voor het gebruik van gegevens treedt vaak een spanningsveld op met de efficiëntievoordelen, kostenbesparingen en betere dienstverlening die door (rijkere) gegevensuitwisseling te behalen zijn. De focus op doelbinding die per wet is vastgelegd leidt tot vaak starre aanpakken die de efficiëntie en meerwaarde van automatische verwerking van gegevens in de weg staan. Gegevens van bijvoorbeeld de RDW die voor een bijstandsaanvraag geleverd worden, mogen niet hergebruikt worden door de betreffende gemeente voor het verstrekken van een parkeervergunning. Vooral de afnemende partijen in de keten ervaren dit als een belemmerende en op onbegrip stuitende factor. Toezicht op het gebruik van gegevens is noodzakelijk om incidenten te voorkomen die het vertrouwen tussen de ketenpartijen en/of de reputatie van de keten kunnen schaden.



Om de proportionaliteit te garanderen kunnen *filtermechanismes* [2.16] worden ingezet waarmee de uit te wisselen gegevens kunnen worden beperkt tot de doelgroep. Dergelijke filters kunnen werken op basis van white- of blacklists. Zo bevat Suwinet bijvoorbeeld blacklists waarin VIPs, bekende Nederlanders of eigen collega's staan. Whitelists worden vaak gevuld op basis van werkvoorraad door de afnemer zelf. SURFnet, als beheerder van de identiteitsfederatie, maakt gebruik van zogenaamde "attribute release policies" om ervoor te zorgen dat alleen een vooraf bepaalde set van attributen doorgegeven wordt naar de dienstenaanbieder. De filters zijn te vergelijken met autorisatieregels die bepalen welke rechten een gebruiker heeft op basis van de aangeleverde rol of attribuutgegevens.



Filters kunnen worden aangebracht door de gegevensleverancier, door intermediairs en door de gegevens afnemende organisatie(s) en kunnen worden ingezet op de te leveren en de te ontvangen gegevens (informatiedoel), maar ook op gebruikersgroepen (voor autorisatiedoel).

Filtering kan ook helpen bij het verbeteren van de doelbinding door ze in te zetten bij monitoring. Actieve monitoring op de filters maakt het mogelijk om adequaat in te grijpen zodra een filter getriggerd wordt. De filters zorgen ervoor dat de gebruiker slechts de gegevens ziet die nodig zijn voor een bepaalde taak (need-to-know principe) en de monitoring erop draagt bij aan detecteren van mogelijk misbruik. De verantwoordelijkheden van de filters dienen duidelijk belegd te worden, inclusief wie verantwoordelijk is te acteren bij vermoeden van misbruik.



Naast het inzetten van filters is ontkoppeld koppelen of *privacy-by-design* [2.17] een in potentie minstens zo krachtige manier om invulling te geven aan het need-to-know principe. Daarmee wordt bedoeld dat de ontvanger niet een hele set aan gegevens ontvangt waaruit hij zelf de informatie moet afleiden die hij nodig heeft. In plaats daarvan wordt eerder in de keten deze informatie automatisch uit de gegevens gehaald. De gebruiker ontvangt dan alleen de afgeleide informatie, en niet de daaraan ten grondslag liggende gegevens. Een voorbeeld hiervan is terug te vinden in eHerkenning waarbij de identiteit van de gebruiker zelf niet bekend is, maar wel dat deze gemachtigd is om namens een bedrijf te handelen.





Een Privacy Self Assessment (PriSA) [2.24] kan organisaties ondersteunen om zicht te krijgen op het privacy volwassenheidsniveau van de organisatie en geeft handvatten om dit niveau te verhogen.

2.1.6 Cloud Computing



Cloud Computing [2.45] is relevant omdat het afnemen van Clouddiensten gevolgen heeft voor de plaats waar informatiebeveiligingsmaatregelen worden uitgevoerd. Hierbij is het van belang dat als een partij van Clouddiensten gebruik maakt, deze partij altijd verantwoordelijk blijft voor de juiste beveiliging van haar gegevens en ook de privacy waarborgt. Deze practice heeft een relatie met de verwerkersovereenkomst, zie 2.1.4

2.1.7 Contractmanagement

Wanneer organisaties contracten afsluiten met derden moet helder zijn welke informatiebeveiligingsmaatregelen hierin geadresseerd moeten worden [2.46].



2.2 Risicobesef

Om passende beveiligingsmaatregelen te kunnen treffen dient er allereest een besef van de risico's te zijn. Het participeren in een keten of een netwerk brengt additionele risico's met zich mee. In een keten kunnen bijvoorbeeld risico's ontstaan op een andere plek dan in de organisatie waar de betreffende bestuurder verantwoordelijkheid kan dragen.

2.2.1 Best practices



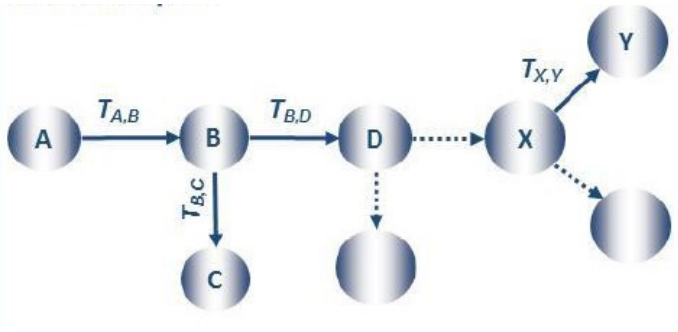
Voor bestuurders rijkt de NOREA, de beroepsorganisatie van IT-auditors (RE´s), vanuit de werkgroep Keten-auditing, best practices aan voor betrouwbare keteninformatisering. Door middel van deze *Alert* [2.18] wil NOREA de bestuurder op de hoogte brengen van de uitkomsten van haar onderzoek in de vorm van een aantal best practices. Deze best practices omvatten een negental maatregelen die bestuurders kunnen treffen om de risico's van keteninformatisering te mitigeren.



Het Amerikaanse standaardisatie-instituut *NIST heeft een aantal best practices verzameld voor risicobeheersing van informatiesystemen voor logistieke ketens* [2.19]. Naast deze 10 best practices geeft NIST ook handvatten voor rollen en verantwoordelijkheden rondom ICT in de logistieke keten en hoe de ICT te implementeren.

2.2.2 Methodieken en modellen

De bestaande methodieken voor risicoanalyse zijn veelal niet toegesneden op de complexiteit in ketens en leiden tot vaak zeer gedetailleerde analyses. De meeste analyses richten zich wel op de organisatie die deelneemt in een keten, maar geven onvoldoende handvatten om ketenrisico's inzichtelijk te maken. Risico-hulpmiddelen die wel oog hebben voor ketenaspecten zijn *Advanced Risk Management (ARM)* [2.20], *TTISC* [2.21] en *TMap Next* [2.22]. Deze hulpmiddelen richten zich vooral op het creëren van bewustzijn van ketenrisico's bij bestuurders. ARM is een hulpmiddel om ketenrisico's aan de bestuurstafel op een inzichtelijke wijze bespreekbaar te maken door verwachtingen en verplichtingen van ketenpartners te expliciteren. TTISC is gebaseerd op het principe dat het risico zich door de keten distribueert en dat hiervoor passende maatregelen nodig zijn en is sterk gericht op visualisatie. Een voorbeeld is het inzichtelijk maken van de beschikbaarheid van een ketensysteem en de verschillende lokale parameters vanuit de externe en interne keten (zie figuur hieronder).



TMap Next is een door Sogeti ontwikkelde methodiek voor het testen van ketens. De ketentest kent aspecten als een ketenrisicoanalyse, haalbaarheidsonderzoek en een draaiboek voor ketentesten. De ketentesten liggen op het snijvlak van business en IT.

CIP heeft een Keten Test Dorp ontwikkeld. Het KetenTestDorp (KTD) is een dataset die bedoeld is voor het ondersteunen van ketentests tussen verschillende organisaties. De gedachte: als iedere partij in een keten dezelfde testdata gebruikt bij de ketentest, dan bespaart dat veel tijd in het afstemmen van de ketentestdata. Doordat het gebruik van productiedata wordt vermeden, is er ook geen risico op datalekken. Deze testset is alleen bedoeld voor een functionele test en niet voor een performance of stress test(2.53).

Het *Chain Content, Context & Control (C4) model* [2.23] biedt een handvat om het totale speelveld van ICT-ketenbeheersing te overzien, hiaten hierin te identificeren en communicatie erover te vergemakkelijken. Het model is gericht op de te beheersen objecten in de keten (content), het perspectief van waaruit beheersing plaatsvindt (context) en de wijze waarop deze wordt vormgegeven (controle).

2.2.3 Gaming

Een relatief nieuwe aanpak om risicobesef te creëren is door gebruik te maken van *serious games* [2.50] en netwerkgame [2.50]. Dit zijn games waarbij de speler iets leert. Dit leren kan op bewust dan wel onbewust niveau gebeuren. Serious games kunnen op een computer, als bordspel of rollenspel gespeeld worden. Elk type game heeft zijn eigen voordelen en mogelijkheden. Een serious game heeft als voordeel dat de werkelijkheid van een spel niet de echte werkelijkheid is. Dit geeft dus mogelijkheden om situaties te oefenen die in het echt gevaarlijk of lastig te organiseren zijn zoals een ketenincident en zo het besef van de gevolgen ervan bij de verantwoordelijke persoon door te laten dringen.

2.2.4 PIA

Ketens die persoonsgegevens uitwisselen dienen specifieke maatregelen te treffen voor het borgen van de privacy. Een *Privacy Impact Assessment (PIA)* [2.24] is bij uitstek een hulpmiddel om inzicht te krijgen in de risico's van verwerking van persoonsgegevens. Wanneer die risico's bekend zijn, kunnen maatregelen worden genomen om deze te beheersen. Het inzicht geven in mogelijke mitigerende maatregelen is onderdeel van een goede PIA.



Nog op EU-niveau, noch in Nederland bestaat een algemeen aanvaard model of methodiek voor het uitvoeren van een PIA. In afgelopen jaren is naar aanleiding van een initiatief van het voomalig CBP, nu AP, gebleken dat de gedachten voor het ontwikkelen van een uniforme methodiek voor het uitvoeren van een PIA sterk uiteenlopen. Op internet zijn tal van voorbeelden en best practices van (D)PIA's te vinden.

2.2.5 Bewustzijn

Tot slot is het mogelijk om een *keten-brede bewustzijnscampagne* [2.25] onder de gebruikers te voeren. Het doel van de campagne is gebruikers van partijen in de keten bewust te maken van specifieke ketenrisico's. Een voorbeeld is de campagne "Zorgvuldig gebruik Suwinet" die in 2011-2012 gevoerd is op initiatief van het ministerie van SZW, Divosa, VNG, KING, het Inlichtingenbureau en het BKWI. Het doel van de campagne was het realiseren van een structurele inbedding van een zorgvuldig gebruik van Suwinet bij professionals. In de door BKWI in het hele land georganiseerde workshops "Zorgvuldig gebruik Suwinet" kregen gemeenten de mogelijkheid om vast te stellen hoe zorgvuldig zij met Suwinet omgaan. Daarnaast werd een handreiking geboden om knelpunten op te lossen.

2.3 Besturing

Waar organisaties in ketens samenwerken, moet ook de keten bestuurd worden. Dat is niet alleen nodig om ketenrisico's te beheersen, maar allereerst om de ketendoelstelling te realiseren en daartoe de ketenprocessen doeltreffend en doelmatig te laten verlopen. Het is daarom zaak dat de ketenpartijen de besturing van de keten in gezamenlijkheid vormgeven, passend bij de aard van de keten. Dat is geen sinecure, omdat vaak een balans gezocht moet worden tussen de organisatie-interne hiërarchische sturing en een meer horizontale sturing in ketens. Daar komt bij dat menige organisatie in meerdere ketens samenwerkt van uiteenlopende aard en samenstelling.



De verantwoordelijkheid van bestuurders voor een veilige informatievoorziening moet dan ook tevens gericht zijn op het in gezamenlijkheid met andere bestuurders realiseren van een veilige informatievoorziening van ketens. Het is aan bestuurders van betrokken ketenpartijen om een goede balans te vinden tussen enerzijds wat nodig is om in de eigen organisatie informatieveiligheid te borgen en anderzijds wat nodig is voor passende informatieveiligheid binnen de ketens.

Een integrale bestuurlijke aanpak voor het sturen op informatieveiligheid in ketens is niet voorhanden. Wel kan een beroep worden gedaan op verschillende hulpmiddelen die ketenbesturing in algemene zin bespreken en waarin informatieveiligheid als een besturingsaspect is ondergebracht.

2.3.1 Inrichting en besturing



2.3.1.1 Modellen

Het *NORA-katern "Ketens de Baas"* [2.26], bespreekt een bestuurlijk model voor ketenbesturing, met vier dimensies: inhoudelijk, relationeel, cultureel en procedureel. Het katern biedt bovendien een reeks van componenten waarmee de besturing van een keten kan worden ingericht. Hoewel het geboden model en de geboden besturingscomponenten vrij generiek zijn en wellicht niet alle componenten in alle ketens aan de orde zijn, is het goed mogelijk om het model en de componenten te gebruiken als checklist voor het sturen op

informatieveiligheid. Ook informatieveiligheid kent immers haar inhoudelijke, relationele, culturele en procedurele dimensies; en het merendeel van de geschetste besturingscomponenten zal informatieveiligheid ook tot zijn takenpakket moeten rekenen.

Een ander katern van de NORA heet *"Verbinden"* [2.27]. Ook dit katern is gericht op ketensamenwerking, maar kent een meer tactische oriëntatie, waar "Ketens de Baas" meer strategisch georiënteerd is. Het NORA-katern "Verbinden" kiest een architectuur-insteek, waarbij drie specifieke soorten van ketensamenwerking worden behandeld: front-offices, basisregistraties en e-dossiers. Voor elk van deze drie vormen biedt het katern een architectuurvisie en een reeks van architectuurprincipes. Deze principes hebben een weerslag op informatieveiligheid of gaan daar zelfs specifiek over. Deze elementen uit het katern zijn daarmee kandidaat om gebruikt te worden bij de tactische sturing van informatieveiligheid in ketens.



Het handboek van de Vereniging Nederlandse Gemeenten voor het inrichten van keten- en netwerksamenwerking [2.28] schetst een zestal basismodellen die gemeenten kunnen benutten om een keten of netwerk van organisaties in te richten ten behoeve van een maatschappelijk gewenste situatie. Daarnaast dienen drie kernvragen beantwoord te worden:



1. Wat is het motief voor het inrichten van een keten of netwerk? Wat wil je bereiken?
2. Hoe organiseer je het? Welk basismodel neem je als uitgangspunt?
3. Welke prikkels wil je in de samenwerking inbouwen?

Beveiliging en privacy aspecten worden slechts zijdelings aangestipt in het handboek.



Het A3 jaarplan [2.48] is een model om op strategisch niveau met alle betrokkenen in de organisatie het jaarplan uit te werken. Hierbij worden ook de partners en klanten geadresseerd, wat inzicht geeft in de partijen waarmee je afspraken moet maken.

Bij uitbesteding van IT dienstverlening en bij keteninformatisering is de diversiteit aan partijen groter dan bij interne automatisering en is de behoefte sterker aan een eenduidig, en vooral ook uniform, stelsel van beheersingscriteria.

De behoefte aan beheersing van IT-diensten doet zich in principe altijd voor, zowel bij interne als bij externe IT-dienstverlening. De klantorganisatie en de (interne of externe) service organisatie (IT-dienstverlener) hebben hierbij beiden belang bij eenduidige onderlinge afspraken over de criteria voor de beheersing van IT-diensten. Door Norea is, in samenwerking met PvIB, het studierapport "Algemene beheersing van IT-diensten" [2.49] opgeleverd.



2.3.1.2 Ketenoverleg

In verschillende ketens vindt regelmatig *overleg* [2.29] plaats tussen de ketenpartijen. In de domeingroep Privacy & Beveiliging van Suwinet worden allerlei zaken met betrekking tot deze onderwerpen besproken. De domeingroep is bijvoorbeeld verantwoordelijk voor het vaststellen van de Verantwoordingsrichtlijn en het Normenkader voor Suwinet. In eHerkenning vindt op strategisch, tactisch en operationeel niveau overleg plaats aangaande de besturing van het stelsel.



Rapportages [2.30] over het gebruik van ketendiensten op basis van log-informatie worden in dergelijke overlegbijeenkomsten gebruikt als stuurinformatie voor het verbeteren van de beveiliging. Over het algemeen wordt gerapporteerd over een vooraf bepaalde set van parameters zoals over het aantal gegevensuitwisselingen, het aantal logins en het aantal keer dat de toegang tot gegevens is geweigerd. De ketenpartijen zelf blijven verantwoordelijk voor de analyse van de rapportages teneinde (vermoedelijk) misbruik te kunnen detecteren.



2.3.1.3 Best practices

Naast de modellen, componenten en principes van de NORA-katernen, zijn ook best practices voorhanden, die opgetekend zijn op basis van ervaringen in de keten voor werk en inkomen. Deze lijst uit 2009 bespreekt *lessen die succesvolle ketensamenwerking bevorderen of bemoeilijken* [2.31]. Deze zijn:



1. Ketensamenwerking is een langdurig verbeterproces. Verzand niet in procesvereisten, maar blijf de inhoud – integrale dienstverlening aan de klant – centraal stellen.
2. Succesvolle ketensamenwerking valt of staat met personen. Zorg voor veel persoonlijk contact op alle niveaus van de keten, dit schept een basis voor vertrouwen en vergroot het lerend vermogen.
3. Denk voortdurend vanuit de klant en creëer binnen de betrokken organisaties de randvoorwaarden om daar naar te handelen.
4. Bepaal in samenspraak een heldere doelstelling en zorg ervoor dat de urgentie om tot gezamenlijke resultaten te komen bij alle betrokkenen wordt gevoeld. Door systematisch te denken en handelen vanuit het doel kunnen cultuurverschillen, organisatiebelangen en competentiestrijd worden overwonnen.
5. Ontwikkel eenvoudige, voor iedereen begrijpelijke prestatiemaatstaven en monitor de resultaten. Betrek de wensen en eisen van de klant bij het bepalen van ketenprestatie-indicatoren. Draag behaalde successen uit, dit inspireert en enthousiasmeert.
6. Er is geen blauwdruk voor ketensamenwerking. Samenwerking moet lokaal vorm krijgen en top-down worden gefaciliteerd, gelegitimeerd en gestimuleerd.
7. Geef medewerkers de ruimte om te experimenteren en beslissingen te nemen die passen bij de lokale mogelijkheden en omstandigheden.
8. Speur lokale best practices op en maak het mogelijk daarvan kennis te nemen en te leren.
9. Blijf continu zorgen voor politiek draagvlak, zowel op landelijk als op lokaal niveau.

Opnieuw geldt dat geen van deze best practices specifiek over informatieveiligheid gaat. Enkele ervan echter – vooral de eerste vijf – laten zich direct op informatieveiligheid toepassen. De best practices passen goed bij de inhoud van het NORA-katern "Ketens de Baas"; de schrijvers van het katern hebben deze best practices namelijk ook tot zich kunnen nemen. Wel bestaat een zekere spanning tussen de zesde best practice en de lijst van besturingscomponenten uit het katern.

2.3.2 Kaders, afspraken en verantwoordelijkheden

2.3.2.1 Wetgeving

Geen van voornoemde katernen en best practices is bindend. Het voordeel daarvan is dat zij zo ruimte geven aan de onvermijdelijke diversiteit, veranderlijkheid en complexiteit die aan ketens nog veel eigener is dan aan individuele organisaties. Wel bindend is *wetgeving* [2.32]. Met wetgeving kunnen taken, verantwoordelijkheden en verplichtingen worden benoemd en belegd. Informatieveiligheid zou, ook als dat niet expliciet genoemd wordt, een onvervreemdbaar



onderdeel van veel van deze verantwoordelijkheden moeten zijn. Een algemene "ketenwet" is er niet. Wel is ruimschoots sectorale wetgeving op dit terrein voorhanden. Bovendien is er de Algemene Verordening Gegevensbescherming (AVG) die regels stelt aan de bescherming van de privacy van de burger ook in ketenverband.

2.3.2.2 Ketenafspraken

Bindend, maar flexibeler, zijn afspraken tussen ketenpartijen over onderlinge verantwoordelijkheden.



Dergelijke *ketenafspraken* [2.9] worden vaak vastgelegd in convenanten, gedragscodes of normenkaders. Een voorbeeld is het Normenkader van Suwinet dat concrete aandachtsgebieden biedt, variërend van strategische tot operationele controlemaatregelen en die gebaseerd zijn op 'best practices' van informatiebeveiliging zoals de Code voor Informatiebeveiliging (ISO 27002). Een onderdeel van dit Normenkader is een jaarlijkse EDP-audit. Ook over de authenticatie van bedrijven via eHerkenning zijn afspraken gemaakt, op juridisch, technisch, organisatorisch en beveiligingsvlak.

2.3.2.3 Keten-SLA

Nog flexibeler zijn afspraken die tussen een kleine groep organisaties worden gemaakt, tot bilaterale



toe. Omdat ze tussen een relatief kleine groep organisaties worden gemaakt, kunnen afspraken ook concreter en specifieker gemaakt worden; zij hoeven minder variëteit te bedienen. Een *keten-SLA* [2.13 is een bruikbaar hulpmiddel voor het vastleggen van de afspraken. In een keten-SLA wordt bijvoorbeeld voor een specifieke ketendienst, afgesproken wat de prestatie-indicatoren en kwaliteitseisen zijn van de te leveren dienst of product om daarop later te kunnen toetsen. In een keten-SLA worden de rechten en plichten van de betrokken partijen omschreven. Een voorbeeld van een keten-SLA is die van Suwinet.



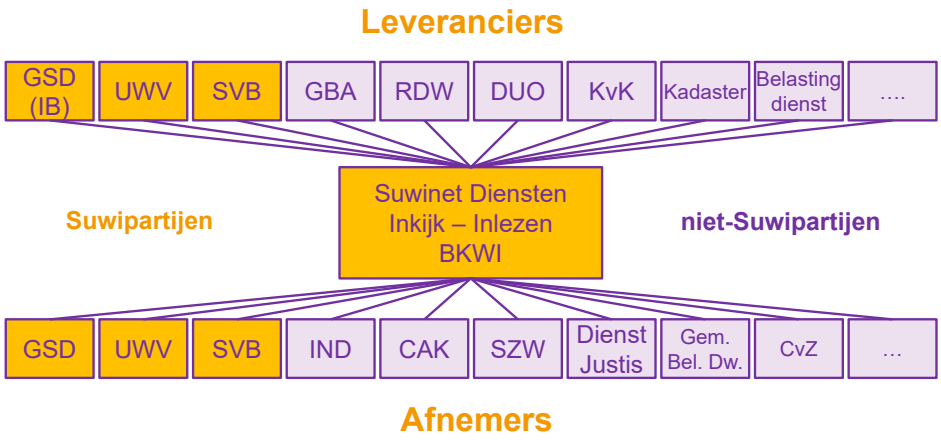
Bij het afsluiten van een SLA met andere ketenpartijen moet door een ketenpartij rekening gehouden worden met de SLA's die het met andere partijen is aangegaan in



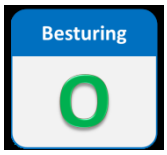
andere ketens, met interne onderdelen of met leveranciers. Het kan met name riskant of duur zijn om aan afnemers beduidend hogere dienstverleningsniveaus te beloven dan door de eigen leveranciers geboden wordt. Ook op tactisch niveau speelt de spanning tussen de veelal hiërarchische interne sturing en de meer horizontale sturing in ketens. Om dergelijke risico's af te wegen kan het *TTISC* [2.21] als hulpmiddel voor risicobesef ingezet worden.

Keten voor werk en inkomen: Suwinet

Suwinet is een gezamenlijke elektronische voorziening voor het uitwisselen van gegevens in het domein van werk en inkomen. Deze uitwisseling is in de wet SUWI geregeld. Bureau Keteninformatisering Werk en Inkomen (BKWI) beheert het Suwinet. Een belangrijke voorziening in Suwinet is de broker waarlangs al het berichtenverkeer gaat. BKWI biedt via de broker verschillende diensten aan en faciliteert en coördineert o.a. de beveiliging van Suwinet. Aangesloten op Suwinet zijn Suwi-partijen als SVB, UWV en gemeentelijke sociale diensten (GSDs), en niet Suwi-partijen als de Belastingdienst, DUO en gemeentelijke deurwaarders.



2.3.2.4 Keten-DAP



Waar SLA's gezien kunnen worden als een tactische afspraak, is het ook zaak om op operationeel niveau scherp te hebben welke afspraken en procedures aan de orde zijn. In een *keten Dossier Afspraken en Procedures (DAP)* [2.33] kunnen de afspraken en procedures voor het samenwerken aan geautomatiseerde systemen en ook de informatiesystemen of applicaties worden vastgelegd. Alle betrokken partijen behoren zich aan deze afspraken en procedures te houden, zodat goed samengewerkt kan worden en beveiliging en privacybescherming geborgd is. Een dergelijk dossier vormt een operationele aanvulling op de SLA. Daar waar het DAP en de SLA elkaar tegenspreken is de laatste over het algemeen leidend, tenzij expliciet staat aangegeven "in afwijking van". Logius hanteert bijvoorbeeld een DAP voor MijnOverheid. De onderwerpen hiervan zijn:

1. Verantwoordelijkheden;
2. Ingang voor meldingen;
3. Procedures voor incidentafhandeling;
4. Procedures voor wijzigingen;
5. Standaard overleggen;
6. Standaard afspraken over escalatie;
7. Algemene contactgegevens;
8. Algemene afspraken over (financiële) rapportages.

Alle betrokken personen bij een dergelijk systeem/keten zullen moeten samenwerken en zullen gebruik maken van de in het DAP beschreven afspraken en procedures. In het DAP wordt dus ook vastgelegd welke afspraken en procedures van belang zijn voor bepaalde rollen die personen in de organisatie hebben. Per rol is aangegeven welke taken, bevoegdheden en verantwoordelijkheden bij deze rol horen.

2.3.2.5 Aansluitvoorwaarden



Partijen die zich willen aansluiten bij bestaande ketens of netwerken moeten vaak voldoen aan zogenaamde *Aansluitvoorwaarden* [2.35]. Daarin zijn afspraken opgenomen over de looptijd van de aansluiting, eisen aan de informatiebeveiliging, verplichtingen zoals het inrichten van een helpdesk, beleid rondom het loggen van activiteiten en het doorgeven ervan richting ketenpartners, privacy, sancties zoals het opschorten van ketendiensten en eventuele aanvullende bepalingen zoals het overdragen van rechten/plichten/taken aan derden. De aanwezigheid van een aansluitprotocol helpt partijen om soepel aan te sluiten op de keten of het netwerk. Net als het DAP zijn ook de aansluitvoorwaarden vaak een operationele bijlage bij een SLA.

2.3.2.6 Grip op veilige ontwikkeling van diensten



Voor organisaties is het een uitdaging om als opdrachtgever van IT-projecten sturing te geven aan het ontwikkelen van veilige IT-diensten. Uitbesteding van ontwikkeling, onderhoud en beheer aan meerdere externe leveranciers maakt het sturingsvraagstuk extra complex. De *Secure Sofware Development (SSD) methode* [2.43] beschrijft hoe een opdrachtgever grip krijgt op het (laten) ontwikkelen van goed beveiligde software.

2.4 Transparantie

Voorwaarde van een goede sturing in de keten is dat er transparantie is over de uitgewisselde gegevens en de mate van beveiliging. Informatie hierover geeft bestuurders houvast om zaken bij te stellen of om tijdig in te grijpen. Verschillende hulpmiddelen worden daarbij ingezet.

2.4.1 Verantwoording



Een belangrijk element voor het bereiken van transparantie is hierover gezamenlijk een sluitend stel *spelregels af te spreken* [2.9]. Een voorbeeld van hoe dit te doen is de Verantwoordingsrichtlijn van Suwinet die aangeeft hoe de aangesloten organisaties invulling dienen te geven aangaande de transparantie over de beveiliging van de informatiehuishouding. Met deze transparantie bieden de aangesloten organisaties inzicht aan de registratiehouders en aan elkaar in hoeverre de beveiliging van Suwinet voldoet aan de gestelde eisen. Dit wordt in de vorm van een jaarlijkse verantwoordingsrapportage gedaan en draagt bij aan het onderling vertrouwen tussen de ketenpartijen.

Diverse professionals uit het CIP-netwerk hebben samen informatie aangedragen en bediscussieerd. Als product is het rapport "Privacy afspraken bij Ketensamenwerking" [2.51] ontstaan. Risico en aansprakelijkheid kun je onder de moderne wetgeving niet zomaar wegwerken door naar anderen te wijzen. Werken in ketens vereist afspraken met alle ketenbetrokkenen. En als je verstandig bent dan maak je die afspraken waterdicht.



Dit document gaat over dergelijke afspraken in het licht van de nieuwe Europese privacywetgeving. Het analyseert de privacy-problematiek in ketenstructuren en geeft mogelijke oplossingen, niet in de laatste plaats in de vorm van een opzet voor een modelovereenkomst.

Ketencommunicatie bij crisis [2.52]: als een incident zich voordoet, is het van groot belang een aantal zaken op orde te hebben. Vooral moeten dan de afhankelijkheden tussen systemen en organisaties, die inzicht verschaffen in de consequenties van verstoringen voor ketenpartners, afnemers etc., duidelijk zijn. Daarnaast is het van belang dat de verantwoordelijken voor de (crisis)communicatie binnen de organisaties elkaar snel weten te vinden. Dat gaat altijd gemakkelijker wanneer deze mensen elkaar al kennen (en dus ook samen regelmatig oefenen).



2.4.2 Baselines

Het gebruik van baselines [2.8] voor beveiliging vormt een grondslag voor een effectieve verantwoording over de beveiliging aan andere overheidsorganisaties en maakt een eenduidige, onafhankelijke toetsing mogelijk. Hierdoor ontstaat een grotere transparantie, die bijdraagt aan het beoogde onderlinge vertrouwen.



2.4.3 Inkoopvoorwaarden

Bij het verwerven van producten of diensten is het van belang om in een vroegtijdig stadium aan mogelijke leveranciers kenbaar te maken welke beveiligingseisen [2.47] de organisatie wenst te treffen, of door haar leverancier uitgevoerd wenst te zien. Dit voorkomt onenigheid en discussie achteraf.



2.4.4 Logging en monitoring



Een sterk middel voor het creëren van transparantie is logging en monitoring [2.30 en 2.36] van alle gegevensuitwisselingen in de keten en op basis hiervan te rapporteren. Voorwaarde hiervoor is wel dat de berichtdefinities voldoende handvatten bieden om keten-breed te kunnen loggen. De loggegevens geven een beter inzicht op naleving en faciliteren een betere sturing ervan. Daartoe kunnen op basis van de loggegevens rapportages opgesteld worden door de individuele ketenpartijen aan een centrale partij. Belangrijk is dus vast te leggen wie verantwoordelijk is voor het loggen en het opstellen van daaruit volgende de rapportages.

Een goed voorbeeld voor het creëren van transparantie is de BKWI Monitor Gebruik Suwinet welke inzage geeft in het onderhoud van accounts, toedeling van autorisaties, misbruik van Suwinet-Inkijk, en de aanlevering van gegevens.

BKWI voorziet haar ketenpartners ook van op logging en monitoring gebaseerde rapportages [2.30]. De rapportages bieden inzage in het gebruik van Suwinet door een partij en kunnen dienen als stuurmiddel voor het verder optimaliseren van de beveiliging van de keten.



2.4.5 Audits of assessments

Een andere manier om transparantie te creëren is partijen een *beveiligingsassessment* [2.37] te laten uitvoeren en hierover een verklaring te laten afgeven. Een voorbeeld hiervan is de DigiD beveiligingsassessment die partijen, die gebruik maken van de DigiD authenticatievoorziening, moeten laten uitvoeren. Een ander voorbeeld is de EDP-audit die niet-Suwi-partijen moeten laten uitvoeren als ze aan willen sluiten op Suwinet voor het afnemen van gegevens.



Tevens zijn er voor auditors handige leidraden voor het uitvoeren van een ketenaudit. De Audit Dienst Rijk heeft een leidraad voor *systeemverantwoordelijkheden* [2.41]. Ook NOREA heeft een *leidraad voor keten-auditing* [2.42].



2.5 Incident management

2.5.1 Alarmeren

Een IT-incident bij de ene ketenpartner kan een onvoorzien incident of een crisis bij de andere veroorzaken. Een IT-ketenincident is dus een IT-incident waarbij twee of meer ketenpartners betrokken zijn.

De interne alarmering van een IT-incident of crisis moet voor de bestuurder inhoudelijk direct voldoende duidelijk zijn. De impact voor de continuïteit, het imago en de kosten van de eigen organisatie moet snel bepaald kunnen worden, evenals de impact voor de ketenpartners. Het is dan zaak dat vanuit de interne incidentalarmering ook de ketenpartners snel geïnformeerd worden. Hulpmiddelen hiervoor zijn niet bekend.



De externe communicatie van het IT-incident naar ketenpartners moet duidelijk maken of sprake is van een keten-incident. De IT-afdelingen van de ketenpartners moeten hierover contact hebben met elkaar. Zodra mogelijk, moet bepaald worden of sprake is van een keten-incident/crisis. Onduidelijk is wie het besluit neemt tot opschaling naar 'ketencrisis' en hoe daar acties op worden gevolgd.

2.5.2 Signaleren

Om de gevolgen van een IT-incident zoveel mogelijk te beperken is snelle detectie ervan essentieel. Hiertoe loggen en monitoren de IT-afdelingen de eigen infrastructuur op ongewenste activiteiten. Daarnaast worden signalen van NCSC over cyberaanvallen ontvangen via www.veiliginternetten.nl.



Een nuttig hulpmiddel voor het signaleren van kwetsbaarheden en/of misstanden in de keten zijn *rapportages* [2.30] op basis van logging. Via rapportages kunnen ketenpartijen geïnformeerd worden over het gebruik van ketendiensten. Ook gaat er een preventieve werking van uit, omdat ketenpartijen van elkaar kunnen zien wie wat doet. De rapportagedienst van BKWI voor het gebruik van Suwinet is hiervan een goed voorbeeld.



Criminelen (intern en extern) zoeken veelal over een langere periode naar zwakheden in de IT-infrastructuur. Er is dan geen sprake van een ernstig IT-incident maar het kan daar wel toe leiden. Vaak proberen criminelen een zwakheid uit bij meerdere ketenpartijen. Het is dan zaak dat ketenpartijen dit van elkaar te horen krijgen. Onduidelijk is op welk moment en hoe dergelijke signalen door de IT-afdelingen gedeeld worden met ketenpartners.



In een vroegtijdig stadium moeten signalen, die de potentie hebben uit te groeien tot een ernstig IT-incident of een crisissituatie, breed worden besproken. Voorbeelden: een virusuitbraak bij de ene ketenpartner kan potentieel problemen veroorzaken bij de andere of vragen van het ministerie bij de ander tot gevolg hebben, etc.



De handreiking Ketencommunicatie bij crisis [2.52] kan hierbij behulpzaam zijn.

Er bestaan meerdere praktijken om kwetsbaarheden in informatiesystemen bekend te maken. Een voorbeeld hiervan is de zogeheten 'full disclosure', oftewel het volledig publiekelijk bekendmaken van een kwetsbaarheid. Vanuit ketenperspectief is dit een onwenselijke aanpak. Een meer verantwoorde wijze is *responsible disclosure* [2.39]. Het ministerie van Veiligheid en Justitie heeft een algemene leidraad om te komen tot responsible disclosure gepubliceerd. Deze leidraad helpt organisaties bij het opstellen van een eigen responsible disclosure beleid. Daarnaast geeft het melders een handreiking hoe te handelen bij het vinden en melden van een kwetsbaarheid. Ook ketenpartijen kunnen hier nuttig gebruik van maken.



2.5.3 Afhandelen

Ondanks alle getroffen maatregelen kan het toch voorkomen dat een incident resulteert in een crisissituatie voor de keten.

Elke ketenpartij heeft crisismanagement voor de eigen organisatie ingericht. In contactgegevens van derden is voorzien. In het bijzonder voor ketenincidenten is een intensieve samenwerking belangrijk, aangezien een incident – en ook het verhelpen ervan – consequenties kan hebben voor andere ketenpartners. De kosten voor het treffen van maatregelen die nodig zijn voor het bestrijden van het IT incident en die niet voor de eigen organisatie zijn maar voor een andere partij dienen in ogenschouw genomen te worden.

Voor het verhelpen van een ketenincident is soms samenwerking nodig. Bij de Diginotar affaire was het nodig om allemaal tegelijk Windows te updaten. Hiervoor is centrale regie nodig. Hoewel vaak onduidelijk is welke ketenpartij die centrale regie op zich moeten nemen zijn er toch uitzonderingen. In de voertuigketen vindt regelmatig overleg plaats tussen partijen uit die keten om problemen te bespreken en af te handelen. Een belangrijke partij in die keten, RDW, coördineert dergelijke vaak informele *keten-overleggen* [2.29]. Ook in de Suwi-keten is sprake van een dergelijke overlegstructuur. In de domeingroep Privacy & Beveiliging worden o.a. incidenten en passende maatregelen besproken.





Communicatie is een belangrijk aspect van crisismanagement. Het tijdig en juist informeren van de media, opdrachtgever, klanten en medewerkers kan veel onrust voorkomen. Afstemming van de communicatie bij de ketenpartijen is daarbij vereist om tegenstrijdige berichtgeving over de ketencrisissituatie voorkomen.

Door middel van *serious gaming* [2.50] kunnen incidenten en de afhandeling ervan eenvoudig nagespeeld worden. Hiermee doet een organisatie in een keten op een effectieve manier ervaring op met crisismanagement. Daarnaast zullen gedurende de game gebreken in de huidige organisatie van crisismanagement boven tafel komen.



Appendix A. Naslagwerk Hulpmiddelen

2.6 Classificatie van hulpmiddelen

De onderstaande structuur wordt gehanteerd om de verschillende hulpmiddelen te classificeren.

Deelgebied	Beveiliging & Privacy, Transparantie, Besturing, Risicobesef of Incident Management
Soort hulpmiddel	Tool, best practice, methodiek, checklist, video, overeenkomst, normenkader, richtlijn,…
Beschrijving	Korte beschrijving van het hulpmiddel en wat het beoogd te realiseren.
Doelgroep	Bestuurders, security officers, risico-managers en interne controllers, gegevensfunctionarissen, IT-beheerders, architecten, …
Inzetbaarheid / herkomst	In welke keten / domein wordt het hulpmiddel ingezet? Is het generiek inzetbaar? Als het niet generiek inzetbaar is, onder welke voorwaarden zou het dan wel succesvol ingezet kunnen worden?
Referenties	Naar meer informatie, voorbeelden (denk hierbij bijvoorbeeld aan een keten-SLA), contactpersonen en/of bedrijven.
Overig	Specifieke opmerkingen over het hulpmiddel. Bijvoorbeeld verwijzingen naar andere hulpmiddelen.

2.7 Overzicht van hulpmiddelen

Geïnventariseerde hulpmiddelen op dit moment:

1. Baselines informatiebeveiliging 2.8
2. Ketenafspraken en –kaders 2.9
3. Authenticatieniveaus 2.10
4. Authenticatie-architectuur 2.11
5. Ketenautorisatie 2.12
6. Keten Service Level Agreements 2.13
7. Berichtstandaardisatie 2.14
8. Doelbindingstoetsen 2.15
9. Filters 2.16
10. Privacy-by-design 2.17
11. NOREA Audit Alert Keteninformatisering 2.18
12. NISTIR 7622 2.19
13. Advanced Risk Management (ARM) 2.20
14. TTISC 2.21

15. TMAP NEXT Ketentest	2.22
16. C4-model	2.23
17. Privacy Impact Assessment (PIA)	2.24
18. Bewustzijnscampagne Suwinet	2.25
19. NORA Ketens de Baas	2.26
20. NORA Katern Verbinden	2.27
21. Handboek ketens VNG	2.28
22. Ketenoverleg	2.29
23. Beveiligings- en privacy-rapportages	2.30
24. Lessen uit de keten van werk en inkomen	2.31
25. Wetgeving	2.32
26. Keten DAP	2.33
27. Vervallen	
28. Aansluitvoorwaarden	2.35
29. Monitoring Tool BKWI	2.36
30. Beveiligingsassessment DIGID	2.37
31. Vervallen	
32. Leidraad responsible disclosure	2.39
33. Vervallen	
34. Auditdienst Rijk over systeemverantwoordelijkheid	2.41
35. NOREA Keten-auditing	2.42
36. Secure Software Development (SSD)	2.43
37. Verwerkersovereenkomst	2.44
38. Cloud Computing	2.45
39. Contractmanagement	2.46
40. Inkoopvoorwaarden en informatiebeveiligingseisen	2.47
41. A3 jaarplan	2.48
42. Algemene beheersing van IT diensten	2.49
43. Netwerk game en Crisis game	2.50
44. Privacy-afspraken bij ketensamenwerking	2.51
45. Ketencommunicatie bij crises	2.52
46. Keten Test Dorp	2.53

2.8 Baselines informatiebeveiliging

Deelgebied	Beveiliging en privacy, transparantie
Soort hulpmiddel	Normenkader, richtlijn
Beschrijving	Een goede samenwerking is alleen mogelijk als organisaties hun informatiebeveiliging op elkaar afstemmen en elkaar daarin ook vertrouwen. Afstemming bereiken over informatiebeveiliging is vaak makkelijker gezegd dan gedaan. Beveiligingsmaatregelen van organisaties wijken vaak zo van elkaar af dat barrières voor informatie-uitwisseling ontstaan. Baselines helpen bij het standaardiseren van de informatiebeveiliging in de organisatie en in de keten. Baselines beschrijven aan welke beveiligingseisen een keten of een partij daarin moet voldoen. De baseline vormt de grondslag voor een effectieve verantwoording over de beveiliging aan andere organisaties en maakt een eenduidige, onafhankelijke toetsing mogelijk. Hierdoor ontstaat een grotere transparantie, die bijdraagt aan het beoogde onderlinge vertrouwen.
Doelgroep	Bestuurders en security officers
Inzetbaarheid	Baselines zijn breed inzetbaar.
Referenties	Er zijn verschillende baselines: Het Voorschrift Informatiebeveiliging Rijksdienst (VIR) is een beperkte set van basisregels voor overheidsorganisaties. Het VIR is een doelstellende richtlijn, die veel overlaat aan de verantwoordelijke beheerders zelf. https://www.noraonline.nl/wiki/VIR_(Voorschrift_Informatiebeveiliging_Rijksdienst) Voor de behandeling van vertrouwelijke informatie bij de Rijksoverheid is een aanvullende set van maatregelen van toepassing: Het Voorschrift Informatiebeveiliging – Bijzondere Informatie (VIR-BI). https://wetten.overheid.nl/BWBR0033507/2013-06-01 De Baseline Informatiebeveiliging Overheid (BIO) is een overheid brede baseline op gebied van informatiebeveiliging. https://bio-overheid.nl/category/producten#BIO Bovengenoemde baseline zijn afgeleid van de Code voor Informatiebeveiliging (NEN ISO 27001 en 27002), dat geldt als een internationale standaard voor informatiebeveiliging in organisaties.
Overig	Let er op dat de implementatie van baselines bij alle individuele ketenpartijen nog geen garantie is voor een keten-brede baseline dat hetzelfde niveau kent als bij een individuele organisatie.

2.9 Ketenafspraken en –kaders

Deelgebied	Besturing
Soort hulpmiddel	Kader
Beschrijving	De ketenpartijen kunnen onderling afspraken maken over het niveau van beveiliging en de mate van verantwoording hierover. Deze afspraken worden typisch vastgelegd in convenanten, gedragscodes, normenkaders of verantwoordingsrichtlijnen.
Doelgroep	Bestuurders en security officers.
Inzetbaarheid	Het maken en vastleggen van afspraken over beveiliging- en privacy-maatregelen is een breed inzetbaar hulpmiddel. Over het algemeen zijn ze gebaseerd op basis van (generieke en sectorspecifieke) wettelijke voorschriften.
Referenties	Voorbeelden zijn het Normenkader en de Verantwoordingsrichtlijn Suwinet (zie https://www.bkwi.nl/producten/suwinet-services/suwinet-standaarden/privacy-beveiliging/. Deze documenten geven guidance voor toepassing van de BIO bij het gebruik van Suwinet en dan met name wat betreft de normen waarover afnemers van Suwinet zich moeten verantwoorden en hoe deze verantwoording moet plaatsvinden. Rondom het authentiseren van bedrijven via eHerkenning zijn op juridisch, technisch, organisatorisch en beveiligingsvlak afspraken gemaakt tussen de betrokken partijen onderling. Een beschrijving van het afsprakenstelsel eHerkenning is hier te vinden: https://www.eherkenning.nl/aansluiten-op-eherkenning/. Ook in de strafrechtketen zijn afspraken gemaakt over informatiebeveiliging. Deze afspraken bevatten een invulling van bestaande normen en afspraken voor het waarborgen van een adequaat niveau van beveiliging voor het uitwisselen van departementaal vertrouwelijk gerubriceerde informatie in de strafrechtketen tussen Politie, Ministerie Veiligheid & Justitie en Defensie (KMar) door middel van elektronisch berichtenverkeer. Zie https://www.noraonline.nl/wiki/Standaarden_informatievoorziening_strafrechtsketen.
Overig	Zie ook het hulpmiddel Wetgeving.

2.10 Authenticatieniveaus

Deelgebied	Beveiliging
Soort hulpmiddel	Richtlijn
Beschrijving	Authenticatie is noodzakelijk voor betrouwbare toegang tot diensten of gegevens. Afhankelijk van de gevoeligheid van de dienst of de gegevens is een bepaald niveau van authenticatie gewenst. Bijvoorbeeld, voor medische gegevens is een betrouwbaardere authenticatie vereist dan voor NAW gegevens. Omdat er tientallen verschillende authenticatie-oplossingen zijn, is het voor dienstenaanbieders of gegevensverstrekkers niet te doen om aan te geven welke passend zijn voor de toegangsbeheersing. Door verschillende niveaus van authenticatie te definiëren en hier oplossingen aan toe te kennen wordt het een stuk eenvoudiger. Men hoeft dan slechts aan te geven welk niveau vereist is. Standaard raamwerken voor authenticatieniveaus bestaan: STORK QAA niveaus, eHerkenning betrouwbaarheidsniveaus, ISO Quality Assurance Framework en NIST. Daarnaast zijn er voor dienstenaanbieders richtlijnen om het niveau van authenticatie te kunnen bepalen.
Doelgroep	Security officers, IT-beheerders, architecten
Inzetbaarheid	Het nut van authenticatieniveaus komt vooral tot uiting in federatieve omgevingen zoals eHerkenning. Het maakt het mogelijk om authenticatie uit te besteden aan derde partijen. Er wordt gebruik van gemaakt in de zorg, onderwijs en het overheidsdomein.
Referenties	Raamwerken: – eHerkenning: www.eherkenning.nl – NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf – ISO: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45138 Richtlijnen voor het bepalen van authenticatieniveaus: – Rijksoverheid: https://www.forumstandaardisatie.nl/sites/bfs/files/atoms/files/fs-guide-assurance-levels-v2-en.pdf / – Zorg: https://www.nictiz.nl/overig/handreiking-beis-deel-1-authenticatie-en-autorisatie/
Overig	-

m

2.11 Authenticatie-architectuur

Deelgebied	Beveiliging
Soort hulpmiddel	Architectuur
Beschrijving	Gebruikers en hun digitale identiteiten dienen eerst geauthentiseerd te worden op basis waarvan de toegangsrechten bepaald kunnen worden. In ketens zijn verschillende manieren beschikbaar om identity & access management in te richten: decentraal, centraal of federatief. Het decentrale model houdt in dat gebruikers accounts met bijbehorende rechten bij de andere ketenpartijen hebben. Het centrale model gaat uit van centrale verstrekking van identiteiten en rechten. In het federatieve model kan de gebruiker met zijn eigen accountgegevens inloggen in de systemen van ketenpartners.
Doelgroep	Security officers, IT-beheerders, architecten
Inzetbaarheid	De inzetbaarheid van de verschillende oplossingen hangt af van de besturing van de keten en het vertrouwen dat de ketenpartners in elkaar hebben. Het centrale model vereist een ketenregisseur of beheerder die identiteiten kan beheren en de toegangsrechten keten-breed kan standaardiseren. Het federatieve model vereist vertrouwen tussen de partijen. Het decentrale model is te allen tijde mogelijk maar schaalt erg slecht.
Referenties	Een voorbeeld van een centrale oplossing is Suwinet. Hier deelt BKWI accounts uit voor de toegang tot de Suwinet Inkijk dienst. Voorbeelden van federatieve oplossingen zijn de SURFnet federatie en eHerkenning.
Overig	-

2.12 Ketenautorisatie

Deelgebied	Beveiliging
Soort hulpmiddel	Best practice
Beschrijving	Toegang tot gegevens of diensten wordt bepaald aan de hand van rollen en/of attributen. In een keten is uniformering en eenduidigheid van de rollen en attributen belangrijk om consistente autorisatiebeslissingen te kunnen nemen.
Doelgroep	Security officers, IT-beheerders, architecten
Inzetbaarheid	De inzetbaarheid van de verschillende oplossingen hangt af van de besturing van de keten en het vertrouwen dat de ketenpartners in elkaar hebben. In een centraal model kan een ketenregisseur of beheerder de rollen/attributen bepalen. Ketenpartijen kunnen deze dan koppelen aan de functies van gebruikers binnen de eigen organisatie. Dit is bijvoorbeeld het geval in Suwinet. In een federatieve authenticatie-architectuur zullen attributen gebruikt worden voor toegang. Ook hier geldt dat er afspraken gemaakt moeten zijn over de te gebruiken attributen.
Referenties	Suwinet en GBA definiëren een autorisatiematrix voor toegang tot gegevens. Zie bijvoorbeeld http://www.bkwi.nl/producten/suwinet-services/suwinet-autorisatie/ handreiking autorisatie op Suwinet-Inkijk voor GSD. Standaarden voor attribuutschema's zijn OrgPerson, eduPerson en SCHAC (de laatste twee worden gebruik in de SURFnet federatie). Zie voor meer algemene schema's ook http://tools.ietf.org/html/rfc4519 en http://tools.ietf.org/html/rfc4524.
Overig	-

2.13 Keten Service Level Agreements

Deelgebied	Besturing
Soort hulpmiddel	Overeenkomst
Beschrijving	In een keten is het van belang dat afspraken worden gemaakt tussen alle partijen over de kwaliteit van de keten-brede dienstverlening. De afspraken hebben onder andere betrekking op: responsetijden van systemen, beschikbaarheid van systemen, de ondersteuning door de Servicedesk en de behandeling van incidenten en storingen. Dit wordt vastgelegd in een overeenkomst tussen de deelnemende partijen in de keten middels een Keten-SLA. De voordelen van een keten-SLA zijn dat aangesloten partijen weten wat zij op het niveau van dienstverlening van elkaar kunnen en mogen verwachten betreffende de verschillende onderdelen. Bovendien krijgen ze periodiek een beeld van de geleverde prestaties; zodat ze gericht kunnen bijsturen.
Doelgroep	Security officers, service level & contract managers en IT-beheerders.
Inzetbaarheid	SLA's zijn een algemeen en breed inzetbaar hulpmiddel. Bij het afsluiten van een keten-SLA dient rekening gehouden te worden met de beschikbaarheid van de eigen systemen en die van eventuele sub-contractors. Deze zal minimaal het niveau moeten hebben welke verwacht wordt door de ketenpartners.
Referenties	Voorbeeld van een keten-SLA is die van Suwinet waarin partijen als UWV, SVB, DUO en het Inlichtingenbureau gezamenlijk afgesproken hebben om middels een Service Level Rapportage maandelijks te rapporteren over de afgesproken prestatie-indicatoren zodat gerichte bewaking, sturing en verbetering van de dienstverlening mogelijk zijn. Deze SLA is hier te vinden: https://www.bkwi.nl/producten/suwinet-services/suwinet-standaarden/ketenafspraken-ict-beheer/gezamenlijke-elektronische-voorzieningen-gevs-suwi-keten-service-level-agreement-12-0/.
Overig	De vraag is vaak wie toeziet op het naleven van de keten-SLA. In het geval van Suwinet doet BKWI dat als beheerder van de generieke delen van de Suwinet infrastructuur. In ketens waar een dergelijke beheerder of regisseur ontbreekt, zal het toezicht op een andere manier ingevuld moeten worden. Afspraken hierover kunnen in de SLA meegenomen worden.

2.14 Berichtstandaardisatie

Deelgebied	Privacy
Soort hulpmiddel	Standaard
Beschrijving	Het standaardiseren van de uit te wisselen gegevens helpt bij het borgen van de doelbinding en proportionaliteit van de gegevensuitwisseling in ketens.
Doelgroep	Security officers, gegevensfunctionarissen, it-beheerders
Inzetbaarheid	Voor iedere keten waarin persoonsgegevens uitgewisseld worden.
Referenties	Het Suwi-Gegevens Register (SGR) is hiervan een voorbeeld. Zie http://www.bkwi.nl/producten/suwinet-services/suwinet-standaarden/suwi-gegevensregister-sgr/.
Overig	-

2.15 Doelbindingstoetsen

Deelgebied	Privacy
Soort hulpmiddel	Toets
Beschrijving	Gegevensverstrekking vindt soms plaats op basis van wettelijke verplichtingen en in overige gevallen op basis van leveringsovereenkomsten. De verstrekking is beperkt tot die taken waarvoor wettelijke grondslag en/of doelbinding van gegevensgebruik is vastgesteld. Voordat een organisatie toegang krijgt tot gegevens, vindt eerst een wettelijke toets plaats.
Doelgroep	Security officers, gegevensfunctionarissen
Inzetbaarheid	Voor iedere keten waarin persoonsgegevens uitgewisseld worden.
Referenties	Ketens waarin doelbindingstoetsen afgenomen worden zijn o.a. de loonaangifteketen en de Suwi-keten.
Overig	-

2.16 Filters

Deelgebied	Privacy
Soort hulpmiddel	Technologie
Beschrijving	Het inzetten van filters zorgt voor betere proportionaliteit doordat nadere technische invulling wordt gegeven aan het 'need-to-know' principe. Daarnaast kan het flinke efficiëntiewinst opleveren doordat onnodige informatie-uitwisseling wordt voorkomen. Zorgvuldigheid bij het aanbrengen van de filters is zeer belangrijk om te voorkomen dat de gegevensverstrekking te beperkt of te ruim wordt. Veelal zal de intelligentie in de filters aan de hand van de wettelijke kaders, het doel en de doelgroep van het primaire proces, en gezamenlijke afspraken tussen de stelselpartijen bepaald worden. De verantwoordelijkheden voor de filters dienen goed belegd te zijn.
Doelgroep	Security officers, gegevensfunctionarissen, IT-beheerders
Inzetbaarheid	Voor iedere keten waarin persoonsgegevens uitgewisseld worden.
Referenties	Als voorbeeld: BKWI biedt om de proportionaliteit te garanderen, een filtermechanisme aan als dienst waarmee de te raadplegen gegevens nader kunnen worden beperkt tot de doelgroep. Deze filters werken op basis van door de inlezende of inkijkende organisatie zelf opgestelde white- of blacklists. Zo zijn er bijvoorbeeld blacklists waarin VIPs, bekende Nederlanders of eigen collega's staan. Whitelists worden vaak gevuld op basis van werkvoorraad door de afnemer ketenpartijen zelf. Ook in de identiteitsfederatie voor het hoger onderwijs vindt (attribuut)filtering plaats. Door technische beperkingen leveren de universiteiten meer gegevens aan dan nodig is. De federatiebeheerder, SURFnet, filtert de overbodige gegevens weg.
Overig	-

2.17 Privacy-by-design

Deelgebied	Privacy
Soort hulpmiddel	Concept, methodiek
Beschrijving	Privacy-by-design gaat uit van het principe dat in een vroeg stadium nagedacht wordt over het goede gebruik van persoonsgegevens binnen een keten, de noodzaak van het gebruik van deze gegevens en de bescherming ervan. Door al bij het ontwikkelen van systemen privacy en bescherming van persoonsgegevens in te bouwen is de kans op het succes ervan het grootst.
Doelgroep	Security officers, IT-beheerders, architecten
Inzetbaarheid	Een voorbeeld van een privacy-by-design toepassing is het invullen van het 'need-to-know' principe door ontkoppeld koppelen. Daarmee wordt bedoeld dat de ontvanger niet een hele set aan gegevens ontvangt waaruit hij zelf de informatie moet afleiden die hij nodig heeft. In plaats daarvan wordt eerder in de keten deze informatie automatisch uit de gegevens gehaald. De gebruiker ontvangt dan alleen de afgeleide informatie en niet de daaraan ten grondslag liggende gegevens. Dit wordt ook wel dat-informatie genoemd (in plaats van de wat-informatie die veel privacygevoeliger is). Voorbeelden van ontkoppeld koppelen zijn het geven van een antwoord op de vraag of iemands loon hoger is dan een bepaalde grenswaarde (in plaats van het verstrekken van alle loongegevens), het bevestigen dat iemand ouder is dan 18 (in plaats van zijn geboortedatum te verstrekken), of het verstrekken van een indicatie dat sprake is van recidive (in plaats van het beschikbaar maken van alle fraudevorderingen).
Referenties	eHerkenning maakt gebruik van privacy-by-design door aan te geven dat iemand gemachtigd is om namens een bedrijf te mogen handelen zonder dat daarbij de naam van de persoon bekent wordt gemaakt. Methodiek: Privacy bescherming - cip-overheid - privacy baseline en Privacy bescherming - cip-overheid - Privacy by design
Overig	-

2.18 NOREA Audit Alert Keteninformatisering

Deelgebied	Besturing, risico management
Soort hulpmiddel	Best practice
Beschrijving	De NOREA, de beroepsorganisatie van IT-auditors (RE´s), houdt zich in de werkgroep Keten-auditing al lange tijd bezig met de gevolgen van keteninformatisering. Door middel van deze Alert wil NOREA de bestuurder op de hoogte brengen van de uitkomsten van haar onderzoek in de vorm van een aantal best practices. Deze best practices omvatten een negental maatregelen die bestuurders kunnen treffen om de risico's van keteninformatisering te mitigeren.
Doelgroep	Bestuurders
Inzetbaarheid	Als voorbeelden zijn grotendeels ketens vanuit de overheid genomen, deze zijn eenvoudig te projecteren op ketens in de zorg, betalingsverkeer, luchtvaart en industrie.
Referenties	NOREA, zie http://www.norea.nl/.
Overig	-

2.19 NISTIR 7622

Deelgebied	Risicobesef
Soort hulpmiddel	Best practice
Beschrijving 	Het Amerikaanse standaardisatie-instituut NIST heeft een aantal best practices verzameld voor risicobeheersing van informatiesystemen voor logistieke ketens. De best practices zijn: 1. Identificeer actoren, processen en functionele onderdelen in de keten op een unieke wijze. 2. Beperk de toegang tot en de zichtbaarheid van de keten. 3. Borg de herkomst van functionele onderdelen, processen en gegevens. 4. Beperk het delen van informatie zoveel mogelijk. 5. Zorg voor bewustzijn van ketenrisico's. 6. Hanteer een defensieve aanpak voor het ontwikkelen van functionele onderdelen en processen voor de keten. 7. Test, monitor en audit regelmatig. 8. Borg de performance van de keten. 9. Borg continuïteit van de keten. 10. Zie toe op betrouwbare uitfasering en/of vervanging van actoren, processen en functionele onderdelen in de keten. Naast deze 10 best practices geeft NIST ook handvatten voor rollen en verantwoordelijkheden rondom ICT in de logistieke keten en hoe de ICT te implementeren.
Doelgroep	Voornamelijk security officers
Inzetbaarheid	Hoewel NISTIR 7622 zich richt op logistieke ketens en de ICT-voorzieningen daarbinnen, zijn veel best practices goed van toepassing op ketens in andere domeinen.
Referenties	NISTIR 7622 (2012) is hier te vinden: http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf.
Overig	-

2.20 Advanced Risk Management (ARM)

Deelgebied	Transparantie en risicobesef
Soort hulpmiddel	Tool, methodiek, workshop, interviews
Beschrijving	Verwachtingen/verplichtingen van ketenpartners expliciteren. ARM is een hulpmiddel om ketenrisico's aan de bestuurstafel op een inzichtelijke wijze bespreekbaar te maken. ARM doet dit door in termen van 'verwachtingen' (wat verwacht ik van mijn ketenpartner op het gebied van informatieveiligheid) en 'verplichtingen' (aan welke verplichtingen rond informatieveiligheid moet mijn organisatie voldoen) de risico's vanuit het perspectief van bestuurders inzichtelijk te maken. Het resultaat is een verantwoorde prioritering van de te beheersen risico's die kunnen leiden tot het niet succesvol zijn. ARM is toepasbaar in combinatie met bestaande methodieken voor risico analyses en standaarden zoals de ISO 27000. ARM gaat o.a. in op de volgende onderwerpen: 1. Een visie op de veranderde context waarbinnen risicomanagement uitgevoerd moet kunnen worden. 2. Een aantal symptomen van falend risicomanagement. 3. De wijze waarop ARM aansluit bij huidige risicomanagement methoden.
Doelgroep	Bestuurders, security officers, risicomanagers.
Inzetbaarheid	ARM is goed inzetbaar om frictie in de samenwerking door onuitgesproken verplichtingen en verwachtingen tussen ketenpartners weg te nemen. Dit kan in allerlei ketens.
Referenties	TNO heeft in opdracht van BKWI deze methodiek in de Suwi keten toegepast. Het ARM handboek is te downloaden via de TNO website https://repository.tno.nl/islandora/object/uuid%3Aa0e3d385-6334-49b9-8686-a1b97f00415f.
Overig	-

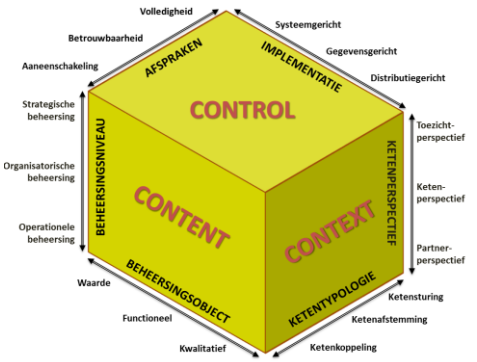
2.21 TTISC

Deelgebied	Risicobesef
Soort hulpmiddel	Tool, methodiek, interviews.
Beschrijving	TTISC is een methodiek gebaseerd op onderzoek dat door de RUG, LOGIUS en TNO is verricht. Het doel van dit onderzoek was om een wetenschappelijk framework voor Assurance in ICT service ketens op te stellen. TTISC = Towards Trustworthy ICT Service Chains. TTISC is gebaseerd op het principe dat het risico zich door de keten distribueert en dat hiervoor passende controle maatregelen voor moeten worden genomen. TNO heeft deze principes gebruikt om een methodiek af te leiden. Deze methodiek bestaat uit een vragenlijst/self assessment om in de risicodistributie vanuit het oogpunt van een keteninitiator overzicht en inzicht te bieden. De resultaten worden gevisualiseerd.
Doelgroep	Bestuurders, security officers, IT-beheerders
Inzetbaarheid	In allerlei ketens. De nadruk ligt momenteel op integriteit van data in de keten en de beschikbaarheid van de applicaties in de keten. Momenteel zijn er verkenningen in de loonaangifte keten, SBR en safe Sea net om deze methodiek te valideren.
Referenties	TF BID, Logius en TNO werken aan TTISC
Overig	Er zijn een aantal wetenschappelijke artikelen gepubliceerd over TTISC. Het ARM [2.20] hulpmiddel kan gezien worden als aanvulling op TTISC.

2.22 TMAP NEXT Ketentest

Deelgebied	Risicobesef
Soort hulpmiddel	Methodiek
Beschrijving	Sogeti heeft een testmethodiek ontwikkeld voor het testen van ketens. De aanpak voor ketentesten is gebaseerd op TMap NEXT, de standaard testmethode van Sogeti. De ketentest kent verschillende aspecten zoals: 1. een ketenrisicoanalyse, waarbij de faalkansen in de keten en het schadeaspect aan het eindpunt van de keten gemeten worden; 2. een haalbaarheidsonderzoek, uitgevoerd over alle ketenpartijen en betrokken systemen heen; 3. technieken voor het specificeren van ketentestgevallen voor ketentesten, waarbij wordt gewerkt met ketenproducten die aan het einde van de keten ontstaan en een methode waarop ketentestgevallen kunnen worden samengesteld uit eerder gemaakte testgevallen; 4. een draaiboek voor ketentesten, waarbij het vooral gaat om de juiste mensen, op het juiste moment de juiste acties uit te laten voeren. Het doel is te komen tot meer robuuste ketens. De ketentesten liggen op het snijvlak van business en IT en dat leidt tot de inzet van multidisciplinaire teams bij de uitvoering van ketentesten. Deze multidisciplinaire aanpak biedt ook voordelen; vanaf het inventariseren van de testbasis, het specificeren van testgevallen tot het uitvoeren van ketentesten.
Doelgroep	Security officers en ontwikkelaars van software.
Inzetbaarheid	Breed inzetbaar.
Referenties	Er is ook een boek over deze methodiek beschikbaar: Testen van ketens met TMap NEXT®, ISBN nummer: 9789072194954.
Overig	-

2.23 C4-model

Deelgebied	Risicobesef
Soort hulpmiddel	Model
Beschrijving	Het Chain Content, Context & Control (C4-) model is een model en hulpmiddel voor de beheersing en controle van ICT-ketens. Het model bestaat uit drie delen: 1. de content, gericht op wat het te beheersen object in de ICT-keten inhoudt; 2. de context, gericht op het perspectief van waaruit beheersing (of beoordeling) van de ICT-ketens plaatsvindt; 3. de control, gericht op de wijze waarop beheersing in ICT-ketens wordt vormgegeven. 
Doelgroep	Bestuurders, security officers en auditors.
Inzetbaarheid	Dit model geeft een handvat om het totale speelveld van ICT-ketenbeheersing te overzien, hiaten hierin te identificeren en communicatie hierover te vergemakkelijken. Daarbij kan het model tevens dienen om de scope van ICT-ketenaudits te bepalen. De sterkte van het model is dat het vanuit zowel een content, context als control perspectief is vormgegeven, waardoor het de grote diversiteit aan en invalshoeken voor ICT-ketens afdekt.
Referenties	Meer informatie over het C4-model is hier te vinden: https://www.deitauditor.nl/wp-content/uploads/2014/07/ITA-12-04-Eenmodel.pdf Of hier: https://c4model.com/.
Overig	Zie ook de beschrijving van TTISC [2.21] waaraan het C4 model gerelateerd is.

2.24 Privacy Impact Assessment (PIA)

Deelgebied	Risicobesef
Soort hulpmiddel	Methodische handreiking, toetsmodel
Beschrijving	Een Privacy Impact Assessment (PIA) biedt inzicht in de hoge risico's van een verwerking van persoonsgegevens. Wanneer die risico's bekend zijn, kunnen maatregelen worden genomen om deze te beheersen. Het inzicht geven in mogelijke mitigerende maatregelen is onderdeel van een goede PIA.
Doelgroep	Bestuurders, Security & Privacy officers en betrokken uitvoerende functies, bedrijfsjurist
Inzetbaarheid	In het regeerakkoord wordt aangegeven dat standaard een PIA moet worden uitgevoerd bij de bouw van systemen en bij de aanleg van databestanden met hoog risico verwerkingen. Tot voor kort bestond noch op EU-niveau, noch in Nederland een vaststaand model of algemeen aanvaarde methodiek voor het uitvoeren van PIA. Onlangs heeft de Rijksoverheid hiervoor een toets model geïntroduceerd. Ook vanuit NOREA is een handreiking voor het uitvoeren van een PIA gepubliceerd. Deze PIA richtsnoeren richten zich voornamelijk op bedrijfsinterne systemen en applicaties; er is minder aandacht voor gegevensuitwisseling tussen bedrijven in ketens/netwerken. De PIA dient voor deze laatstgenoemde situaties rekening te houden met aspecten als ketenintegratie, ketengovernance en ketentransparantie die stuk voor stuk van invloed kunnen zijn op de privacy van de gegevensuitwisseling. Merk op dat ook binnen organisaties samenhangende ketens van afhankelijkheden bestaan. Gebrek aan integratie kan potentieel leiden tot complexe ketens met grote kans op fouten en met gaten in de beveiliging van de gegevens, gebrek aan toezicht resulteert in gebrekkige privacy-handhaving en slap ingrijpen in het geval van een calamiteit, gebrek aan transparantie kan het vertrouwen ondermijnen. Deze aspecten dient de uitvoerende van een keten-brede PIA zelf toe te voegen.
Referenties	Model gegevensbeschermingseffectbeoordeling of Data Protection Impact Assessment (DPIA) Rijksdienst https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia. NOREA Privacy Impact Assessment, zie https://www.norea.nl/nieuws/8151/nieuwe-norea-handreiking-data-protection-impact-assessment of https://www.deitauditor.nl/nieuws/versie-1-1-privacy-impact-assessment-pia-gepubliceerd/
Overig	Vanuit het Europese Privacy Impact Assessment Framework project zijn aanbevelingen gedaan voor een PIA raamwerk. Nuttige informatie hierover is verder te vinden in een van de rapporten van het project, zie https://piafproject.files.wordpress.com/2018/03/piaf_d3_final.pdf. PRIvacy Self Assessment: Privacy bescherming - cip-overheid - Privacy Self Assessment (PriSA)

	Om op een eenvoudige wijze vast te stellen of een PIA gemaakt moet worden heeft CIP een Quick Scan PIA gemaakt. Aan de hand van een korte controlelijst kan dit vastgesteld worden. Privacy bescherming - cip-overheid - Pre-scan DPIA

2.25 Bewustzijnscampagne Suwinet

Deelgebied	Risicobesef
Soort hulpmiddel	Campagne door middel van workshops
Beschrijving	Om het zorgvuldig gebruik van Suwinet te bevorderen is in de nazomer van 2011 de campagne "Zorgvuldig gebruik Suwinet" gestart, die tot september 2012 doorliep. De initiatiefnemers voor deze campagne waren het ministerie van SZW, Divosa, VNG, KING, het Inlichtingenbureau en het BKWI. Het doel van de campagne was het realiseren van een structurele inbedding van een zorgvuldig gebruik van Suwinet bij professionals. In de door BKWI in het hele land georganiseerde workshops "Zorgvuldig gebruik Suwinet" hebben gemeenten de mogelijkheid om vast te stellen hoe zorgvuldig zij met Suwinet omgaan. Daarnaast werd een handreiking geboden om knelpunten op te lossen.
Doelgroep	Bestuurders, security officers en gebruikers.
Inzetbaarheid	Bewustwordingscampagnes kunnen te allen tijde worden ingezet. Gewaakt dient te worden voor verzadiging bij de doelgroep wat ten koste kan gaan van de effectiviteit van de campagne.
Referenties	Een presentatie over het zorgvuldig omgaan met persoonsgegevens uit Suwinet is hier te vinden: https://www.youtube.com/watch?v=xhbRa-n8MuY. Tips over het zorgvuldig en veilig gebruik van Suwinet zijn hier te vinden: https://www.bkwi.nl/veilig-suwinet/10-tips-voor-veilig-gebruik-suwinet/ en https://vng.nl/files/vng/nieuws_attachments/2013/20131202-veilig-suwinet.pdf.
Overig	Zie ook de Monitor Gebruik Suwinet [2.36] wat als bewustzijns-verhogend hulpmiddel hiervoor ingezet kan worden.

2.26 NORA Ketens de Baas

Deelgebied	Besturing
Soort hulpmiddel	Best practice
Beschrijving 	Het dossier 'Ketens de Baas' geeft een op de praktijk gestoelde visie op het inrichten van organisatie-overstijgende samenwerking. Het biedt principes en handvatten welke toepasbaar zijn in situaties waarin organisaties op gelijkwaardig niveau samenwerken. Het beoogd antwoorden te geven op vragen als: • Welke uitgangspunten zijn bijvoorbeeld van belang voor een succesvolle ketensamenwerking? • Hoe wordt voorkomen dat de individuele organisatiebelangen de horizontale samenwerking blokkeren? • Welke rollen en competenties zijn nodig? • Wat betekent dit voor bestuurders, managers en medewerkers? • Welke voorwaarden zijn van belang voor implementatie van een bestendige ketensamenwerking?
Doelgroep	'Ketens de baas' is in eerste instantie bestemd voor bestuurders, maar kan ook voor andere betrokkenen bij de ontwikkeling en werking van een keten een rol spelen.
Inzetbaarheid	Het leidende gezichtspunt van Ketens de Baas is dat de 'hardware' binnen ketens niet gevormd wordt door computers, maar door de 'soft skills' van de ketenspelers. Het zijn hun vaardigheden en kwaliteiten die doorslaggevend zijn voor het ontstaan van succesvolle ketensamenwerking, en niet de technologie. Het dossier wil vanuit dit gezichtspunt de ketenpartijen ondersteunen bij het inrichten van ketensturing. Het stuk is gebaseerd op overheidsorganisaties maar geeft ook handreikingen voor de besturing van niet-overheidsketens.
Referenties	Het dossier Ketens de Baas is hier te vinden: Download Ketens de Baas 2e druk (PDF, 11,78 MB)
Overig	Zie ook het NORA katern Verbinden (2.27).

2.27 NORA Katern Verbinden

Deelgebied	Besturing
Soort hulpmiddel	Best practice
Beschrijving	Het NORA katern "Verbinden" is een visiedocument dat samenwerkingsprincipes op drie aspecten beschrijft: proces, informatie en technologie. Deze principes beschrijven een raamwerk of afsprakenstelsel, waarbinnen een publieke organisatie vorm kan geven aan zijn verbinding met burgers en bedrijven en met andere (publieke) organisaties. De principes zijn tot stand gekomen langs de lijn vertrekpunt, architectuurvisie en architectuurprincipes. Het vertrekpunt beschrijft relevante beleidslijnen en maatschappelijke ontwikkelingen. De architectuurvisie vertaalt deze ontwikkelingen naar een visie op de inrichting van de processen en de informatievoorziening. Vervolgens geven de architectuurprincipes invulling aan de architectuurvisie door het formuleren van richtinggevende uitspraken voor realisatie.
Doelgroep	Architecten en bestuurders
Inzetbaarheid	Het katern is gedefinieerd voor overheidsdiensten. Erkend wordt dat de inrichtingsvarianten voor organisatie-overstijgende overheidsdiensten een breed spectrum zullen bestrijken. Bij bepaalde diensten zal een traditioneel, soms misschien nog wel papieren, formulier centraal staan in de administratieve afhandeling. Anderen zijn geschoeid op het concept van een informatiepositie, waar de burger of het bedrijf actueel inzicht in zijn gegevens heeft, en de overheid actief informeert over de gevolgen en mogelijkheden daarvan. De afspraken in het katern bieden de helpende hand om diensten in de overheid aan beide kanten van dit spectrum te adresseren.
Referenties	Meer informatie over het katern is hier te vinden: https://www.noraonline.nl/wiki/Katern_Verbinden
Overig	Zie ook NORA De Keten de Baas [2.26].

2.28 Handboek ketens VNG

Deelgebied	Besturing
Soort hulpmiddel	Handboek
Beschrijving	Het handboek voor het inrichten van keten- en netwerksamenwerking schetst een zestal basismodellen die gemeenten kunnen benutten om een keten of netwerk van organisaties in te richten die gezamenlijk aan een maatschappelijk gewenste situatie gaan werken. Daarnaast dienen drie kernvragen beantwoord te worden: 1. Wat is het motief voor het inrichten van een keten of netwerk? Wat wil je bereiken? 2. Hoe organiseer je het? Welk basismodel neem je als uitgangspunt? 3. Welke prikkels wil je in de samenwerking inbouwen? Beveiliging en privacy aspecten worden slechts zijdelings aangestipt in het handboek.
Doelgroep	Bestuurders.
Inzetbaarheid	Algemeen.
Referenties	Meer informatie over het handboek is hier te vinden:https://www.vng.nl/files/vng/szm-handreiking_keten-_en_netwerksamenwerking_inrichten_def.pdf en http://www.vng.nl/files/vng/szm-9_sept-handreiking_inrichten_ketensamenwerking.pdf
Overig	Ook de NORA Ketens de Baas [2.26] geeft een overzicht van verschillende keteninrichtingen.

2.29 Ketenoverleg

Deelgebied	Besturing en incident management
Soort hulpmiddel	Fysiek overleg tussen ketenpartijen
Beschrijving	Een mooi voorbeeld van informeel overleg is te vinden in de voertuigketen. Het overleg in de voertuigketen is naar aanleiding van een werkcongres in 2009 tot stand gekomen. In deze overleggen worden de casussen van probleemgevallen besproken. De deelnemers aan deze overleggen zijn business managers die ook betrokken zijn bij het ontwerpen van werkprocessen. De overleggen leiden altijd tot een oplossing. Wat belangrijk is, is dat er bestuurlijke dekking is: de bestuurlijke wil om probleemgevallen op te lossen. Casussen worden ingebracht in het overleg op basis van vakmanschap van de deelnemers van de ketenpartners. Ook wordt daar kennis gedeeld. Een ander voorbeeld betreft de verschillende domeingroepen binnen Suwinet. Zo komen vertegenwoordigers van de Suwi-partijen regelmatig bij elkaar in de domeingroep Privacy & Beveiliging. BKWI coördineert de bijeenkomsten en zit deze ook voor. De verantwoordelijkheden van de domeingroep Privacy en Beveiliging zijn o.a. het vaststellen van de Verantwoordingsrichtlijn en het Normenkader voor Suwinet.
Doelgroep	Bestuurders en security officers.
Inzetbaarheid	Dergelijke structurele overlegstructuren zijn inzetbaar voor iedere keten.
Referenties	-
Overig	-

2.30 Beveiligings- en privacy-rapportages

Deelgebied	Transparantie, besturing en risicobesef
Soort hulpmiddel	Rapportages
Beschrijving	Via rapportages kunnen ketenpartijen geïnformeerd worden over het gebruik van ketendiensten of -informatie. Rapportages worden over het algemeen samengesteld uit log-gegevens. Rapportages kunnen ingezet worden als een instrument om misbruik te detecteren. Ook gaat er een preventieve werking van uit omdat ketenpartijen van elkaar kunnen zien wie wat en wanneer doet. Rapportages bieden ook stuurinformatie om de beveiliging in de keten, indien wenselijk, verder te optimaliseren.
Doelgroep	Bestuurders en security officers.
Inzetbaarheid	Het inzetten van rapportages als hulpmiddel vereist vertrouwen, coördinatie en discipline. Afgesproken dient te worden over welke gegevens gerapporteerd gaat worden. De privacy van gebruikers dient in ogenschouw genomen te worden. In ketens met een regisseur of coördinator is het vaak eenvoudiger om het rapportagemiddel in te zetten.
Referenties	De rapportagedienst van BKWI rondom het gebruik van Suwinet is een goed voorbeeld https://www.bkwi.nl/producten/suwinet-services/suwinet-rapportages. Op basis van log-gegevens voorziet BKWI partijen van generieke en specifieke (op verzoek) rapportages. Ook dienen op Suwinet aangesloten partijen zich jaarlijks te verantwoorden richting de security officer van BKWI over hun beveiliging. De BKWI security officer stelt hiervan een zogenaamde samenvattende rapportage op voor de Minister en Inspectie SZW.
Overig	Zie ook het hulpmiddel Ketenafspraken [2.9] en met name de Verantwoordingsrichtlijn van Suwinet waarin aangegeven staat hoe partijen zich dienen te verantwoorden.

2.31 Lessen uit de keten van werk en inkomen

Deelgebied	Besturing
Soort hulpmiddel	Best practice
Beschrijving	Welke factoren en omstandigheden bevorderen of bemoeilijken succesvolle ketensamenwerking? Vanuit de keten van werk en inkomen zijn de ervaring hiermee in 2009 op papier gezet. Deze zijn: 1. Ketensamenwerking is een langdurig verbeterproces. Verzand niet in procesvereisten, maar blijf de inhoud – integrale dienstverlening aan de klant – centraal stellen. 2. Succesvolle ketensamenwerking valt of staat met personen. Zorg voor veel persoonlijk contact op alle niveaus van de keten. Dit schept een basis voor vertrouwen en vergroot het lerend vermogen. 3. Denk voortdurend vanuit de klant en creëer binnen de betrokken organisaties de randvoorwaarden om daar naar te handelen. 4. Bepaal in samenspraak een heldere doelstelling en zorg ervoor dat de urgentie om tot gezamenlijke resultaten te komen bij alle betrokkenen wordt gevoeld. Door systematisch te denken en handelen vanuit het doel kunnen cultuurverschillen, organisatiebelangen en competentiestrijd worden overwonnen. 5. Ontwikkel eenvoudige, voor iedereen begrijpelijke prestatiemaatstaven en monitor de resultaten. Betrek de wensen en eisen van de klant bij het bepalen van ketenprestatie-indicatoren. Draag behaalde successen uit. Dit inspireert en enthousiasmeert. 6. Er is geen blauwdruk voor ketensamenwerking. Samenwerking moet lokaal vorm krijgen en top-down worden gefaciliteerd, gelegitimeerd en gestimuleerd. 7. Geef medewerkers de ruimte om te experimenteren en beslissingen te nemen die passen bij de lokale mogelijkheden en omstandigheden. 8. Speur lokale best practices op en maak het mogelijk daarvan kennis te nemen en te leren. 9. Blijf continu zorgen voor politiek draagvlak, zowel op landelijk als op lokaal niveau. 10. Elke fase van de ketensamenwerking vereist andere instrumenten en stelt andere eisen aan de organisatie van het proces.
Doelgroep	Bestuurders
Inzetbaarheid	De lessen komen uit de keten van werk en inkomen, ze zijn echter voldoende generiek om ook van toepassing te zijn op ketens in andere domeinen.
Referenties	NORA, zKetensturing/voorbeelden/in dossier: https://www.nyfer.nl/documents/lessenuitdeketen.pdf. Ketensturing/voorbeelden/in dossier - NORA Online
Overig	-

2.32 Wetgeving

Deelgebied	Besturing
Soort hulpmiddel	Wet- en regelgeving
Beschrijving	Via wet- en regelgeving kunnen verantwoordelijkheden en verplichtingen tussen ketenpartijen expliciet vastgelegd worden.
Doelgroep	Bestuurders, informatie managers, security en privacy officers.
Inzetbaarheid	Vaak is sprake van sectorspecifieke wetgeving welke de verantwoordelijkheden van de keten(partijen) bepaalt. Dit kan zijn in termen van afnemer, leverancier of bewerker van gegevens. In algemene zin is de Algemene Verordening Gegevensbescherming van toepassing als het gaat om het borgen van de privacy van de burger in de keten.
Referenties	In art. 62.1 wet Suwi is vastgelegd dat UWV, SVB en de colleges van burgemeester en wethouders (de Suwi-partijen) elkaar de gegevens verstrekken die nodig zijn voor de uitvoering van de opgedragen wetten (voor gemeenten de WWB, IOAW, IOAZ). In art. 62.2 is bepaald dat zij gezamenlijk zorg dragen voor de instandhouding van een elektronische voorziening voor de verwerking van die gegevens. In art. 62.3 is bepaald dat UWV en colleges van B&W gezamenlijk verantwoordelijk zijn in de zin van de Wbp voor de gegevensverwerking op de werkpleinen. De Regeling Suwi bevat een uitwerking van de elektronische voorziening (het stelselontwerp, bijlage I), de beveiliging, de toegang van niet-Suwi-partijen (bijlage III, het Aansluitprotocol) en het principe van de eenmalige uitvraag (de Wet Eenmalige Uitvraag). Het melding maken van onjuistheden in persoonsgegevens door afnemende partijen aan de Gemeentelijke Basis Administratie (GBA) is een wettelijke verplichting.
Overig	Zie ook het hulpmiddel Ketenafspraken [2.9] waarin wetgeving vertaald kan worden in praktische afspraken tussen ketenpartijen.

2.33 Keten DAP

Deelgebied	Besturing
Soort hulpmiddel	Procedure
Beschrijving	Dossier Afspraken en Procedures (DAP) beschrijft afspraken en procedures voor het samenwerken aan geautomatiseerde systemen, ook informatiesystemen of applicaties genoemd. Alle betrokken partijen behoren zich aan afspraken en procedures te houden, zodat goed samengewerkt kan worden. Zo'n dossier kan gezien worden als een operationele aanvulling op een SLA. Daar waar het DAP en de SLA elkaar tegenspreken is de laatste over het algemeen leidend, tenzij expliciet staat aangegeven "in afwijking van". De onderwerpen van zo'n dossier zijn: 1. verantwoordelijkheden; 2. ingang voor meldingen; 3. procedures voor incidentafhandeling; 4. procedures voor wijzigingen; 5. standaard overleggen; 6. standaard afspraken over escalatie; 7. algemene contactgegevens; 8. algemene afspraken over (financiële) rapportages. Alle betrokken personen bij een dergelijk systeem zullen moeten samenwerken en zullen gebruik maken van de in het DAP beschreven afspraken en procedures. In het DAP ligt dus ook vast welke afspraken en procedures van belang zijn voor bepaalde rollen die personen in de organisatie hebben. Per rol is aangegeven welke taken, bevoegdheden en verantwoordelijkheden bij deze rol horen.
Doelgroep	Security officers, service level & contract managers en IT-beheerders.
Inzetbaarheid	Een DAP is een algemeen en breed inzetbaar hulpmiddel.
Referenties	Logius hanteert bijvoorbeeld een dergelijk dossier voor MijnOverheid: https://www.logius.nl/sites/default/files/public/bestanden/diensten/MijnOverheid/DAP%20MijnOverheid%20-%20Afnemers%202020.pdf .
Overig	De vraag is vaak wie toeziet op het naleven van het Keten-DAP. Afspraken hierover kunnen in het DAP worden meegenomen.

2.34 Vervallen

2.35 Aansluitvoorwaarden

Deelgebied	Besturing, risicobesef
Soort hulpmiddel	Methodiek
Beschrijving	Voordat organisaties 'mee kunnen doen' in ketens voor gegevensuitwisseling ten behoeve van dienstverlening dient soms voldaan te worden aan bepaalde voorwaarden. In zogenaamde aansluitvoorwaarden wordt dan kenbaar gemaakt waaraan een organisatie moet voldoen. Deze voorwaarden kunnen voortkomen uit vigerende wetgeving (bv WBP, AVG of sectoriele wetgeving) of eisen die vanuit de keten zelf gesteld worden (bv baseline beveiliging). Door middel van aansluitvoorwaarden wordt een bepaald level playing field voor beveiliging gecreëerd.
Doelgroep	Security officers, operationele mensen
Inzetbaarheid	Aansluitvoorwaarden zijn nuttig als er vanuit wetgeving en beveiliging specifieke eisen gesteld worden aan de organisaties in de keten.
Referenties	Enkele voorbeelden van aansluitvoorwaarden zijn: Digikoppeling: https://www.logius.nl/diensten/digikoppeling.. Suwinet: https://www.bkwi.nl/producten/suwinet-services/suwinet-inlezen. Kennisnet federatie voor het onderwijs: https://www.kennisnet.nl/fileadmin/kennisnet/dienst/entree_federatie/aansluitvoorwaarden-idp-22.pdf.
Overig	-

2.36 Monitoring Tool BKWI

Deelgebied	Transparantie
Soort hulpmiddel	Tool
Beschrijving 	BKWI heeft voor de controle van zorgvuldig gebruik van Suwinet-Inkijk een monitor ontwikkeld, die op basis van kleuren een indicatie geeft hoe het met de beveiliging is gesteld. Onderdelen waarop gemonitord wordt, zijn: 1. onderhoud van accounts; 2. gerichte toedeling van autorisaties; 3. analyse van het gebruik; 4. controle op misbruik; 5. planmatige aanpak beveiliging; 6. optimaal gebruik Suwinet-Inkijk; 7. de aanlevering van gegevens. Input voor de monitor vormen de log-gegevens van Suwinet-Inkijk. BKWI logt de volgende gegevens over het gebruik van Suwinet-Inkijk: 1. iedere al dan niet geslaagde aan- en afmeldpoging; 2. de identiteit of naam van degene die aanmeldt respectievelijk afmeldt; 3. het tijdstip van iedere aan-, afmeldpoging of (trans)actie; 4. elk BSN (of andere zoeksleutel) op basis waarvan gegevens worden opgevraagd; 5. elke (trans)actie, zoals bekeken kolom- of overzichtspagina's. Het primaire doel van dit tool is het kunnen controleren en mogelijk tegengaan van onrechtmatige of doel-overschrijdende verwerking. Blijkt uit de monitor dat er maar een laag percentage actieve accounts ten opzichte van het aantal geregistreerde accounts is, dan maken de klantmanagers van het BKWI een afspraak met de betreffende gemeenten. In het gesprek wordt gelijk ook gekeken naar het proces van toekennen en intrekken van autorisaties, de meest actieve gebruiker en de inlogpogingen buiten kantoortijd. Ook wordt aandacht besteed aan het beveiligingsplan en de rol van de security officer. De BKWI klantmanager belt de betreffende gemeente na enkele maanden terug om op de voortgang toe te zien. De Suwi-partijen zelf blijven verantwoordelijk voor de analyse van de rapportages teneinde (vermoedelijk) misbruik te kunnen detecteren.
Doelgroep	Security officers
Inzetbaarheid	De tool is op maat gemaakt op basis van de logging capaciteiten van BKWI als broker in Suwinet en voor de door BKWI beheerde Suwinet-Inkijk dienst.
Referenties	Meer informatie over de tool is hier te vinden: www.bkwi.nl/uploads/media/Voorbeeld_monitor_gebruik_Suwinet__BKWI_2011_.pdf
Overig	-

2.37 Beveiligingsassessment DigiD

Deelgebied	Transparantie en risicobesef
Soort hulpmiddel	Norm
Beschrijving	Alle organisaties die DigiD gebruiken, moeten voldoen aan een beveiligingsnorm. Via een ICT-beveiligingsassessment moeten zij dit vervolgens laten toetsen. De norm is gebaseerd op de ICT-beveiligingsrichtlijnen voor webapplicaties van NCSC. De norm is vastgesteld door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties in overleg met Logius, Rijksauditdienst en NCSC. Nadat organisaties hebben vastgesteld dat de noodzakelijke maatregelen zijn getroffen om aan de norm te voldoen, moeten zij een toetsing (IT-audit) laten doen door een Register EDP-auditor. De scope van de toetsing is "de internet-facing webpagina's, systeemkoppelingen en infrastructuur die met DigiD gekoppeld zijn en betrekking hebben op het proces". Met systeemkoppelingen wordt met name de system-to-systemkoppeling (authenticatieverzoek en uitwisselen DigiD Request IDentifier (RID) en verificatieverzoek van webdienst) bedoeld.
Doelgroep	Security officers
Inzetbaarheid	De norm bestaat uit de richtlijnen met de hoogste impact op de veiligheid van DigiD. De onderliggende beveiligingsrichtlijnen van NCSC zijn breed toepasbaar voor ICT-oplossingen die gebruikmaken van webapplicaties.
Referenties	De Norm ICT-beveiligingsassessments DigiD: https://www.logius.nl/diensten/digid/ict-beveiligingsassessments .
Overig	-

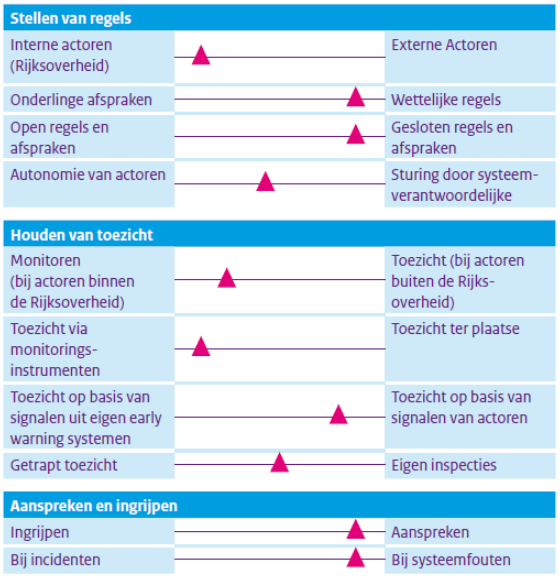
2.38 Vervallen

2.39 Leidraad responsible disclosure

Deelgebied	Incident management
Soort hulpmiddel	Leidraad
Beschrijving	Responsible disclosure kan een goede bijdrage leveren aan het verhogen van de veiligheid van informatiesystemen en (software)producten. Aan het opstellen van het kader heeft het ministerie van Veiligheid en Justitie samengewerkt met NCSC en publieke en private organisaties. De leidraad is een handreiking voor organisaties en melders voor het op een verantwoordelijk wijze melden en afhandelen van kwetsbaarheden in informatiesystemen en (software)producten. Met de handreiking kunnen organisaties een eigen responsible disclosure policy opstellen. De veiligheid van een informatiesysteem en (software)producten is primair de verantwoordelijkheid van organisaties. Melders hebben echter ook verantwoordelijkheden, waaronder het wachten met publicatie totdat de organisatie het probleem heeft verholpen.
Doelgroep	Security officers, IT-beheerders
Inzetbaarheid	De leidraad is een generiek hulpmiddel en is niet opgesteld vanuit het oogpunt van ketens. De leidraad kan wel houvast bieden voor ketens die werk willen gaan maken van incident management.
Referenties	Zie de website van het Nationaal Cyber Security Centrum (NCSC): https://www.ncsc.nl/security
Overig	Het NCSC heeft, waar nodig, een rol in het bij elkaar brengen van partijen en het delen van informatie over kwetsbaarheden met andere partijen zodat ook zij maatregelen kunnen nemen en lering kunnen trekken uit meldingen. Handreiking van CIP: https://www.cip-overheid.nl/category/producten/awareness#responsible-disclosure

2.40 Vervallen

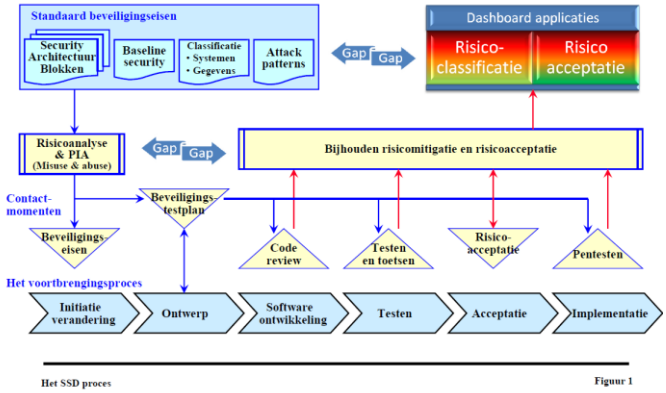
2.41 Auditdienst Rijk over systeemverantwoordelijkheid

Deelgebied	Besturing
Soort hulpmiddel	Best practices
Beschrijving	Na een korte inleiding over systeemverantwoordelijkheid worden op basis van een aantal voorbeelden gemeenschappelijke elementen afgeleid voor systeemverantwoordelijkheid. Deze elementen zijn: 6. Het stellen van regels (kaders) voor de inrichting van het systeem 7. Het houden van toezicht (monitoren) op de goede uitvoering door actoren in het systeem 8. Aanspreken actoren op hun verantwoordelijkheden en zo nodig en mogelijk ingrijpen in het systeem 9. Periodieke evaluatie van het systeem
Doelgroep	Bestuurders
Inzetbaarheid	De auditdienst Rijk merkt op dat bij het inrichten van een systeem keuzes gemaakt moeten worden, die het functioneren van een systeem beïnvloeden. Het is belangrijk dat deze keuzes bewust gemaakt worden om tot een optimale inrichting en werking te komen. In onderstaand schema zijn ter illustratie een aantal wezenlijke keuzes gegroepeerd voor een systeem voor financieel en materieel beheer. 
Referenties	https://platformoverheid.nl/artikel/systeemverantwoordelijkheid-is-gedeelde-verantwoordelijkheid/
Overig	-

2.42 NOREA Keten-auditing

Deelgebied	Risicobesef
Soort hulpmiddel	Leidraad
Beschrijving	NOREA geeft aandachtspunten voor de IT-auditor voor het uitvoeren van een ketenaudit. De volgende aspecten komen aan de orde: 10. De mate van samenwerking tussen de auditdiensten van de ketenpartijen. 11. Aandachtspunten voor het management zoals draagvlak, taken en verantwoordelijkheden. 12. Aandachtspunten voor de IT auditor zoals het benoemen van de opdrachtgever, het samenstellen van het ketenaudit team, de samenwerking binnen het team en het afstemmen van de interne en externe belangen.
Doelgroep	De keten-auditing leidraad is bedoeld als concrete hulp voor de auditor bij het uitvoeren van keten-audits, maar kan ook van nut zijn voor het management.
Inzetbaarheid	Een keten-audit is een onderzoek dat moet leiden tot een gefundeerd oordeel of advies over de beheersing van een keten als geheel ten aanzien van een gekozen object van onderzoek. De keten-audit richt zich alleen op dát aspect of onderdeel van zelfstandige organisaties dat bijdraagt aan het gemeenschappelijke doel en de beheersing van de gehele keten.
Referenties	Zie https://www.deitauditor.nl/wp-content/uploads/2014/09/2005-3-Ketenauditing-in-de-publieke-sector-complex-en-daarom-spannend.pdf
Overig	-

2.43 Secure Software Development (SSD)

Deelgebied	Besturing
Soort hulpmiddel	Handreiking/receptuur
Beschrijving	Voor organisaties is het een uitdaging om als opdrachtgever van IT-projecten sturing te geven aan het ontwikkelen van veilige IT-diensten. Uitbesteding van ontwikkeling, onderhoud en beheer aan meerdere externe leveranciers maakt dit sturings-vraagstuk extra complex. Over en weer zijn er onuitgesproken verwachtingen rondom informatiebeveiliging en privacybescherming. De opdrachtgever verwacht dat de leverancier deskundig is en spontaan de juiste maatregelen treft. Daarentegen verwacht de leverancier dat de opdrachtgever precies specificeert wat er moet gebeuren. Door het ontbreken van expliciete afspraken worden systemen opgeleverd met kwetsbaarheden die niet of te laat worden ontdekt De SSD-methode beschrijft hoe een opdrachtgever grip krijgt op het (laten) ontwikkelen van goed beveiligde software. De drie pijlers daarbij zijn standaard beveiligingseisen, contactmomenten en het inrichten van SSD-processen. De laatstgenoemde zijn processen voor onder meer het bijhouden van risico's en standaard beveiligingseisen, en het laten groeien van de organisatie naar hogere volwassenheidsniveaus. Voor de definitie van de normen is een nieuwe, fundamentele beschrijvingswijze gehanteerd, met zeggingskracht voor zowel managers als securityspecialisten. Het SSD proces is hieronder weergegeven. 
Doelgroep	De handreiking Grip op Secure Software Development (SSD) is opgezet vanuit het perspectief van een opdrachtgever die regisseert en stuurt op de ontwikkeling van gebruikersvriendelijke en veilige applicaties, zonder in te willen breken in het voortbrengingsproces van interne en externe softwareleveranciers.
Inzetbaarheid	SSD is inzetbaar door opdrachtgevers die te maken krijgen met het laten ontwikkelen van software door interne of externe dienstverleners.
Referenties	Zie Secure Software - cip-overheid
Overig	-

2.44 Verwerkersovereenkomst

Deelgebied	Beveiliging
Soort hulpmiddel	Overeenkomst
Beschrijving	De verwerkersovereenkomst is een overeenkomst/afspraak tussen de verantwoordelijke en bewerker van persoonsgegevens in de zin van de AVG. In een verwerkersovereenkomst wordt vastgelegd hoe de bewerker met de persoonsgegevens dient om te gaan
Doelgroep	Security officers, service level & contract managers en IT-beheer-ders.
Inzetbaarheid	Er dient een verwerkersovereenkomst opgesteld te worden tussen partijen indien een verantwoordelijke partij (gemeente) persoonsgegevens laat verwerken door een bewerker. Elke keer als een verantwoordelijke partij (gemeente) het verwerken van persoonsgegevens 'uitbesteedt' wordt een schriftelijke overeenkomst vereist.
Referenties	Een voorbeeld van een verwerkersovereenkomst: de Gebruikersvereniging Centric heeft met Centric overeenstemming bereikt over de standaard verwerkersovereenkomst van Centric voor gemeenten. Op verzoek van de gebruikersvereniging heeft de IBD bij dit proces geadviseerd. https://www.ibdgemeenten.nl/index.php?s=verwerkersovereenkomst
Overig	-

2.45 Cloud Computing

Deelgebied	Beveiliging
Soort hulpmiddel	Overeenkomst
Beschrijving	Wanneer een organisatie gebruik maakt van Cloud Computing heeft dit gevolgen voor de plaats waar informatiebeveiligingsmaatregelen worden uitgevoerd. Een organisatie die gebruik maakt van Clouddiensten blijft altijd verantwoordelijk voor de juiste beveiliging van haar gegevens en dat ook de privacy waarborgt.
Doelgroep	Security officers, service level & contract managers en IT-beheerders.
Inzetbaarheid	Overeenkomsten inzake cloud computing zijn van belang voor opdrachtgevers die te maken krijgen met clouddiensten en -applicaties.
Referenties	In de loop van 2022 verschijnt een herziene formulering van het rijksbrede cloudbeleid.
Overig	Sinds augustus 2016 moeten Amerikaanse bedrijven zich aanmelden voor het Privacy Shield programma. Bij uitwisseling van persoonsgegevens met een gecertificeerd bedrijf is het niet meer nodig een Europees Modelcontract af te sluiten. https://www.privacyshield.gov/Program-Overview Er is een Privacy Shield lijst met deelnemers: https://www.privacyshield.gov/list. Dit lijkt op de oude Safe Harbor lijst, alleen is het geen zelfregulering maar vinden er controles plaats. Er wordt vastgelegd hoe men Europese data behandelt en hoe het doorgeven ervan moet plaatsvinden. Doorgifte naar derde bedrijven is alleen onder strenge verplichtingen mogelijk. Bedrijven die non-compliant zijn, worden van de lijst verwijderd.

2.46 Contractmanagement

Deelgebied	Beveiliging
Soort hulpmiddel	Overeenkomst
Beschrijving	Voorafgaand aan een aanbesteding moeten veiligheidsrisico's worden onderkend die op een product of dienst inwerken. Daarmee wordt de basis gelegd voor beveiligingseisen en -wensen die op een bepaalde plaats in de contractdocumenten weer aan bod moeten komen. Hierover moeten afspraken worden vastgelegd in de overeenkomst/het contract. Contractmanagement moet op de hoogte zijn van derden werking.
Doelgroep	Contract managers en IT-beheerders.
Inzetbaarheid	Dit document gaat uit van de rol contractmanager. Niet iedere organisatie heeft hiervoor een aparte functionaris in dienst, echter kunnen vergelijkbare taken ook door een andere functionaris worden uitgevoerd. De contracten kunnen ook worden beheerd binnen de ICT-afdeling, door een financiële afdeling of bijvoorbeeld door een afdelingshoofd.
Referenties	Een voorbeeld daarvan is dat vooraf vastgesteld wordt of er (bijzondere/gevoelige)persoonsgegevens, waar de organisatie zeggenschap over heeft, in systemen bij een derde partij terecht kunnen komen. https://www.pianoo.nl/nl/document/13782/contractmanagement-bij-informatiebeveiligingsmaatregelen http://www.uwwet.nl/wetten-en-regelingen/privaatrecht/handelsregisterwet/3-gebruik-gegevens-handelsregister-en-derden.htm Belangrijke zaken waar een inkoper of contractmanager rekening mee dient te houden voor het verwerken van persoonsgegevens bij de uitvoering van een overeenkomst: https://www.ubrijk.nl/documenten/factsheet/2021/07/20/handreiking-wat-doe-je-als-inkoper-of-contractmanager-bij-verwerking-van-persoonsgegevens ICO-Wizard (ICO = Inkoopeisen Cybersecurity Overheid) is te gebruiken voor het samenstellen van eisenpakketten die passen bij de producten/diensten die aanbesteed worden. Al of niet aangepast n.a.v. risicoanalyse, kunnen deze eisen overgenomen worden in de RFP en het contract. https://www.bio-overheid.nl/category/ico-producten/#ICO
Overig	Contracten kunnen een sterke relatie hebben met verwerkersovereenkomsten (zie [2.44] hierboven).

2.47 Inkoopvoorwaarden en informatiebeveiligingsdiensten

Deelgebied	Transparantie
Soort hulpmiddel	Procedure, norm
Beschrijving	Bij het verwerven van producten en diensten is het van belang om in een vroegtijdig stadium aan mogelijke leveranciers kenbaar te maken welke beveiligingseisen de organisatie wenst te nemen, of door haar leverancier uitgevoerd wenst te zien, zodat hier achteraf geen discussie over kan ontstaan. Het vroegtijdig aangeven van beveiligingseisen zorgt ervoor dat leveranciers hier ook tijdig op in kunnen spelen. De verantwoordelijkheid voor informatiebeveiliging kan niet zomaar bij een leverancier worden belegd, neem bijvoorbeeld het outsourcen van ICT-services, Cloud Computing of het bewerken van persoonsgegevens.
Doelgroep	Inkopers, contract managers en IT-beheerders.
Inzetbaarheid	De inkoopcontracten kunnen bestaan uit een aantal documenten, zoals algemene voorwaarden en het contract. De algemene voorwaarden zijn standaardcontracten die een organisatie richting meerdere partijen hanteert. Daarin staan dus de algemene afspraken die richting verschillende partijen gehanteerd kunnen worden. Daarnaast worden in een specifiek contract de afspraken tussen twee specifieke partijen geregeld. In dit contract zijn de wensen en eisen nader gespecificeerd, en de concrete beveiligingseisen uitgewerkt. Het is niet voldoende om hier willekeurig de bestaande beveiligingsbeleidsdocumenten te gebruiken, die zijn vaak niet zondermeer geschikt voor een leverancier.
Referenties	Gemeenten hanteren vaak eigen Algemene Inkoopvoorwaarden (AIV) voor het afnemen van producten en/of diensten. In deze inkoopvoorwaarden moet ook rekening gehouden worden met de BIO-beveiligingseisen en het daarvan afgeleide gemeentelijk informatiebeveiligingsbeleid. https://www.informatiebeveiligingsdienst.nl/?s=inkoopvoorwaarden CIP heeft een algemenere methodiek uitgewerkt: https://www.cip-overheid.nl/media/1130/20141007_grip-op-beveiliging-in-inkoopcontracten-een-prestatiegerichte-aanpak_v1_0.pdf Bovendien heeft CIP een wizard ontwikkeld die helpen bij het stellen van scherpe eisen betreffende de veiligheid bij het aanbesteden en inkopen. Met de ICO Wizard selecteer je eisenpakketten die passen bij de producten/diensten die je aanbesteedt en die je meegeeft aan de inschrijvers. https://www.bio-overheid.nl/category/ico-producten/#ICO
Overig	-

2.48 A3 jaarplan

Deelgebied	Besturing
Soort hulpmiddel	Model
Beschrijving	Het A3 jaarplan is een model om op strategisch niveau met alle betrokkenen in de organisatie het jaarplan uit te werken. Hierbij adresseer je ook je partners en klanten. Dit geeft inzicht in de ketenpartijen waarmee je afspraken moet maken
Doelgroep	Alle medewerkers binnen de organisatie die betrokken zijn bij het management van de organisatie
Inzetbaarheid	Het A3 managementgesprek is een gesprek tussen collega's uit twee verschillende managementlagen die op open wijze bespreken of de organisatie of het project op koers ligt met het behalen van resultaten. Het A3 jaarplan vormt het uitgangspunt van dit gesprek.
Referenties	http://www.a3methodiek.nl/a3methodiek.aspx
Overig	-

2.49 Algemene beheersing van IT diensten

Deelgebied	Besturing
Soort hulpmiddel	Model, normen
Beschrijving	Bij uitbesteding van IT dienstverlening en bij keteninformatisering is de diversiteit aan partijen groter dan bij interne automatisering en is de behoefte sterker aan een eenduidig, en vooral ook uniform, stelsel van beheersingscriteria. In dit studierapport is een methodiek uitgewerkt om op basis van risicobenadering te bepalen wat de kritische componenten zijn voor een bepaalde organisatie en welke eisen vanuit beveiligingsoptiek aan deze componenten gesteld moeten worden. Deze methodiek geeft handvatten aan auditors, architecten en informatiebeveiligers om gericht tot goede keuzes te komen in de context van een willekeurige organisatie.
Doelgroep	Auditors, architecten en informatiebeveiligers
Inzetbaarheid	Dit studierapport is een uitbreiding en herziening van het studierapport "Normen voor de beheersing van uitbestede ICT beheerprocessen" uit 2007.Het bevat een herziening van het stelsel van uniforme beheersingscriteria voor beheerprocessen en is uitgebreid met een stelsel van uniforme beheersingscriteria voor technische instellingen van IT-middelen. Door deze uitbreiding omvat het stelsel nu zowel de technische als procesmatige aspecten van de "general IT-controls".
Referenties	https://www.norea.nl/handreikingen
Overig	-

2.50 Netwerk game en Crisis game

Deelgebied	Risicobesef, incident management
Soort hulpmiddel	Serious game
Beschrijving	Serious games zijn games waarbij de speler iets leert. Dit leren kan op bewust dan wel onbewust niveau gebeuren. Serious games kunnen op een computer, als bordspel of rollenspel gespeeld worden. Elk type heeft zijn eigen voordelen en mogelijkheden. Een serious game heeft als voordeel dat de werkelijkheid van een spel niet de echte werkelijkheid is. Dit geeft dus mogelijkheden om situaties te oefenen die in het echt gevaarlijk of lastig te organiseren zijn zoals een ketenincident. De games hebben als doel deelnemers kennis en ervaring op te laten doen met vraagstukken op het gebied van informatie- en privacybescherming en de rol van ketens en netwerken. Het gaat om de bewustwording dat informatie- en privacybescherming niet iets is dat je alleen binnen je eigen organisatie regelt, maar dat het vaak je eigen organisatie overstijgt. Met netwerkpartners (de keten) kijk je naar preventieve maatregelen en bereid je je voor op mitigerende en corrigerende maatregelen. Met een (gelegenheids-)crisisteam proberen een crisis te bestrijden. De game beoogt die bewustwording te creëren in een fictieve setting.
Doelgroep	Netwerk game: teams die met elkaar in ketensituaties samenwerken en samen tot inzicht en oplossingen moeten komen als het fout gaat. Crisis game: crisisteam Ook kan de game ingezet worden als teambuildingsoefening voor een afdeling of een managementteam.
Inzetbaarheid	Deze games zijn goed inzetbaar als teambuildingsoefening voor een afdeling of een managementteam.
Referenties	Workshops en serious games - cip-overheid
Overig	-

2.51 Privacy-afspraken bij ketensamenwerking

Deelgebied	Transparantie, verantwoording
Soort hulpmiddel	Handreiking
Beschrijving	Risico en aansprakelijkheid kun je onder de moderne wetgeving niet zomaar wegwerken door naar anderen te wijzen. Werken in ketens vereist daarom afspraken met alle ketenbetrokkenen. Het is verstandig deze afspraken vooraf waterdicht te maken. Dit document gaat over dergelijke afspraken in het licht van de nieuwe Europese privacywetgeving. Het analyseert de privacy problematiek in ketenstructuren en geeft mogelijke oplossingen, niet in de laatste plaats in de vorm van een opzet voor een modelovereenkomst.
Doelgroep	Ketenregisseur
Inzetbaarheid	Bij het maken van afspraken over privacy in ketens
Referenties	Keten producten - cip-overheid- Privacy afspraken in ketens
Overig	-

2.52 Ketencommunicatie bij crises

Deelgebied	Transparantie, verantwoording
Soort hulpmiddel	Handreiking
Beschrijving	Als een incident zich voordoet, is het van groot belang een aantal zaken op orde te hebben. Vooral moeten dan de afhankelijkheden tussen systemen en organisaties duidelijk zijn, die inzicht verschaffen in de consequenties van verstoringen voor ketenpartners, afnemers, etc. Daarnaast is het van belang dat de verantwoordelijken voor de (crisis)communicatie binnen de organisaties elkaar snel weten te vinden. Dat gaat altijd gemakkelijker wanneer deze mensen elkaar ook kennen (en dus ook samen regelmatig oefenen).
Doelgroep	Crisisorganisatie
Inzetbaarheid	Deze handreiking biedt een generieke opzet voor een ketencommunicatieprotocol bij crisis. De organisaties kunnen de handreiking invullen en aanvullen met proces-eigen kenmerken. Zo ontstaat een communicatieprotocol dat kan worden gebruikt voor de communicatie met keten/netwerkpartners en overige stakeholders. Als alle keten-/netwerkpartners dit hanteren (en er ook mee oefenen), ontstaat grotere transparantie en eenduidigheid in de onderlinge communicatie en in de communicatie met klanten, burgers, media, etc.
Referenties	Keten producten - cip-overheid- Ketencommunicatie bij crises
Overig	-

2.53 KetenTestDorp

Deelgebied	Risicobesef
Soort hulpmiddel	Best practice, methodiek
Beschrijving	Het KetenTestDorp (KTD) is een set met gefingeerde data die door diverse organisaties gebruikt kan worden om een ketentest uit te voeren, Het gebruik van deze test set heeft een aantal voordelen: 1. Veiliger: het gaat om gefingeerde data; 2. Goedkoper: deze gegevens kunnen herhaaldelijk gebruik worden 3. Sneller: tijdwinst bij het overleg over de inhoud van de ketentest tussen diverse organisaties. Iedere organisatie kan zijn specifieke data voor de ketentest in een apart tabblad opslaan. Het KTD is alleen bedoeld om een functionele test is de keten uit te voeren. Het aantal testgevallen wordt zo klein mogelijk gehouden om het beheer te aan te kunnen.
Doelgroep	Testmanagers, testers
Inzetbaarheid	Het KTD is vooral bedoeld voor ketentesten tussen meerdere overheidsinstanties. Het idee van een KTD kan in private ketens gebruikt worden.
Referenties	Keten producten - cip-overheid - KetenTestdorp
Overig	-