ISO 27001:2005 beheersdoelstellingen en beheersmaatregelen binnen de scope van eHerkenningsdiensten, - aktiviteiten, -objecten en -informatie.		relevant voor het	rol	rol	rol	rol	BO	Toelichting selectie of uitsluiting	Opmerkingen t.a.v. deelnemers en Beheerorganisatie	Toelichting / referenties
Nr	**Beheersdoelstellingen en beheersmaatregelen**	**Stelsel eHerk**	**MU**	**AD**	**MR**	**HM**				**Afsprakenstelsel**
4.	Risicobeoordeling en risico behandeling								De basis voor de inrichting van een ISMS (Information Security Management System) wordt gevormd door een risico-analyse. Op grond hiervan worden maatregelen geselecteerd en ingevoerd. Dit houdt derhalve in dat iedere deelnemer en de BO deze aktiviteiten moet hebben uitgevoerd. De keuze voor de methode van risico-analyse bijv. SPRINT, Haagse Methode) is in beginsel vrij. Herhaalde uitvoering van de risico-analyse gebeurt in het kader van een goede vergelijkbaarheid in principe met dezelfe methode. Risico-analyse is altijd een verplicht onderdeel van het ISMS (ISO27001:2005, par. 4.2.1) en formeel genomen geen te selecteren maatregel uit de Appendix van ISO27001. Vanwege het belang van de risico-analyse is dit toch opgenomen in het gemeenschappelijk normenkader.	
4.1	Beoordelen van beveiligingsrisico's	S	Sv	Sv	Sv	Sv	Sv		Beheerorganisatie dient een proces in te richten om periodiek, tenminste eenmaal per jaar of bij belangrijke gebeurtenissen, de stelselrisico's te herijken. Dit is een onderdeel van de risico-analyse. Deelnemers betrekken de stelselrisicoanalyse in hun eigen risicoanalyse.	In samenwerking tussen BO en deelnemers is een stelsel risicoanalyse voor het netwerk eHerkenning opgesteld. De risicoanalyse is beschikbaar gesteld aan de deelnemers. Deze risicoanalyse vormt input voor de door deelnemer uit te voeren risicoanalyse in het kader van de ISO certificering.
4.2	Behandelen van beveiligingsrisico's	S	Sv	Sv	Sv	Sv	Sv		Beheerorganisatie dient een proces in te richten om periodiek de risicobeperkende stelselrelevante maatregelen te herijken waaronder dit normenkader. Dit is een onderdeel van de risico-analyse. Deelnemers richten hun eigen risicomanagement in.	Het normenkader wordt tenminste eenmaal per jaar of bij belangrijke gebeurtenissen herijkt.
A.5	Beveiligingsbeleid									
A.5.1	Informatiebeveiligingsbeleid	Doelstelling: Directie richting en ondersteuning bieden voor informatiebeveiliging overeenkomstig de bedrijfsmatige eisen en relevante wetten en voorschriften.								
A.5.1.1	Beleidsdocument voor informatiebeveiliging	S	Sv	Sv	Sv	Sv	Sv		Iedere deelnemer en de BO stelt een eigen beleidsdocument voor informatiebeveiliging op waarin rekening wordt gehouden met het beleidsdocument voor informatiebeveiliging dat voor het Netwerk c.q. het stelsel van eHerkenning is opgesteld.	De beheerorganisatie beheert het beleidsdocument voor informatiebeveiliging namens het Netwerk. Dit beleidsdocument bestaat uit dit normenkader inclusief de procedureafspraken die uit de normen voortvloeien en de afspraken of standaarden waarnaar in dit normenkader wordt verwezen. Zie in Afsprakenstelsel document: Afsprakenstelsel eHerkenning - Informatiebeveiliging
A.5.1.2	Beoordeling van het informatiebeveiligingsbeleid	S	Sv	Sv	Sv	Sv	Sv		Deelnemers en de BO beoordelen regelmatig de werking van het informatiebeveiligingsbeleid en leveren hierover input t.b.v. de beoordeling op stelselniveau.	Informatiebeveiligingsbeleid wordt periodiek beoordeeld met input van de beoordelingen van de deelnemers en de BO. Dit is onderdeel van de jaarlijkse beoordeling van het stelsel. Zie in Afsprakenstelsel document: Afsprakenstelsel eHerkenning - Informatiebeveiliging

A.6	Organisatie van informatiebeveiliging									
A.6.1	Interne organisatie	Doelstelling: Beheren van de informatiebeveiliging binnen de organisatie.							Er dient per deelnemer en beheerorganisatie een interne organisatie te zijn t.b.v. het beheren van de informatiebeveiliging binnen de organisatie.	
A.6.1.1	Betrokkenheid van de directie bij informatiebeveiliging	S	v	v	v	v	S			Lees voor directie: besturend orgaan van het stelsel, t.w. de Stelselraad (zie document Juridisch Kader)
A.6.1.2	Coördinatie van de informatiebeveiliging	S	v	v	v	v	S			Beheerorganisatie coördineert tbv het stelsel. Concreet door het beheren van de Stelselrisicoanalyse en het Gemeenschappelijk Normenkader Informatiebeveiliging, alsmede door het faciliteren en het organiseren van het Security officers overleg.
A.6.1.3	Toewijzing van verantwoordelijkheden voor informatiebeveiliging	S	v	v	v	v	S			Beheerorganisatie coördineert tbv het stelsel. Concreet door toewijzing van de rollen van security officer en riskmanager.
A.6.1.4	Goedkeuringsproces voor IT-voorzieningen	S	v	v	v	v	S		Vooralsnog zijn er geen - op stelselniveau - gemeenschappelijke IT-voorzieningen. Wel zijn er testtools en simulator software die ten behoeve van andere partijen door de Beheerorganisatie beschikbaar worden gesteld. Changes in die tools vinden plaats naar aanleiding van changes in bijv. functionaliteit.	In het geval dat er - op stelselniveau - gemeenschappelijke IT voorzieningen zijn dan moeten veranderingen hierin die direct ingrijpen op het Netwerk een goedkeuringsproces op stelselniveau doorlopen. Zie procedure WAR.
A.6.1.5	Geheimhoudingsovereenkomst	S	S	S	S	S	S		Uit risico-analyse zal moeten blijken dat toegang tot bepaalde gegevens extra aandacht voor of eisen ten aanzien van de geheimhoudingsplicht zal vereisen.	Het betreft tenminste die gegevens die persoons- en bedrijfsgevoelige elementen bevatten zoals: bij MU: persoonsgegevens, bij AD: persistent pseudoniem, authenticatiecredentials bij MR: persoonsgegevens bij BO: commerciële informatie deelnemers. Geheimhoudingsovereenkomsten (non-disclosure agreements) worden geacht de eisen ten aanzien van deze gegevens te reflecteren.
A.6.1.6	Contact met overheidsinstanties	S	v	v	v	v	S			De BO zal op stelsel niveau contact met overheidsinstanties onderhouden (Govcert, EL&I, BZK)
A.6.1.7	Contact met speciale belangengroepen	S	v	v	v	v	S			Op stelsel niveau zal de BO contact onderhouden met speciale belangengroepen bijv ivm europese ontwikkelingen (bijv. STORK).
A.6.1.8	Onafhankelijke beoordeling van informatiebeveiliging	S	S	S	S	S	S		Voor de deelnemers en de Beheerorganisatie gaat het om het laten uitvoeren van (interne en externe) audits en reviews. Onderdeel van de ISO 27001 certificering is het periodiek/jaarlijks uitvoeren van een controleaudit door de certificerende organisatie.	Afspraken over de stelselaudit en het Gemeenschappelijk Normenkader Informatiebeveiliging staan beschreven in het document: Afsprakenstelsel eHerkenniong - Informatiebeveiliging.
A.6.2	Externe partijen	Doelstelling: Beveiligen van de informatie en IT-voorzieningen van de organisatie handhaven waartoe externe partijen toegang hebben of die door externe partijen worden verwerkt of beheerd, of die naar externe partijen wordt gecommuniceerd.								
A.6.2.1	Identificatie van risico's die betrekking hebben op externe partijen	v	v	v	v	v	v			Maakt onderdeel uit van de risicoanalyse voor de BO.
A.6.2.2	Beveiliging behandelen in de omgang met klanten	S	S	v	S	S	S		Voor deelnemers gaat het om Dienstverleners. De vereisten aan beveiliging op het koppelvlak tussen Deelnemer en Dienstverlener zijn in het afsprakenstelsel opgenomen. Onderdeel van de afspraken tussen deelnemers en dienstverlener/klant zijn de Gebruikersvoorwaarden.	Zie: Document "Koppelvlakspecificatie DV (dienstverlener) en HM (herkenningsmakelaar)". De Beheerorganisatie beheert de autorisaties van deelnemers op het documentenbeheerssysteem (Confluence).
A.6.2.3	Beveiliging behandelen in overeenkomsten met een derde partij.	S	Sv	Sv	Sv	Sv	Sv		Bij uitbesteding (deel) van de rol/activiteiten aan een onderaannemer, dienen de stelselspecifieke (beveiligings)eisen doorvertaald te worden, de opdrachtgever (deelnemer/BO) blijft verantwoordelijk.	Iedere overeenkomst met een derde dient, gebaseerd op een risicoanalyse, een paragraaf/onderdeel te bevatten over eisen ten aanzien van informatiebeveiliging.

A.7	Beheer van bedrijfsmiddelen									
A.7.1	Verantwoordelijkheid voor bedrijfsmiddelen	Doelstelling: Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.								
A.7.1.1	Inventarisatie van bedrijfsmiddelen	v	v	v	v	v	v	Het stelsel eH beschikt niet over gemeenschappelijke middelen.		Vooralsnog zijn er geen gemeenschappelijke middelen onderkend. Indien dit wel het geval zou worden, is de Beheerorganisatie verantwoordelijk voor het bijhouden van de inventarisatie.
A.7.1.2	Eigendom van bedrijfsmiddelen	v	v	v	v	v	v			idem
A.7.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	v	v	v	v	v	v			idem
A.7.2	Classificatie van informatie	Doelstelling: Bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt.								
A.7.2.1	Richtlijnen voor classificatie	S	S	S	S	S	S			Zie document: Afsprakenstelsel eHerkenning - Informatiebeveiliging (Richtlijnen voor classificatie informatie eHerkenning)
A.7.2.2	Labeling en verwerking van informatie.	S	v	v	v	v	S			idem
A.8	Beveiliging van personeel									
A.8.1	Voorafgaand aan het dienstverband	Doelstelling: Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij worden overwogen en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.								
A.8.1.1	Rollen en verantwoordelijkheden	S	v	v	v	v	Sv			BO dient dit proces in te richten voor de BO medewerkers die voor het stelsel worden ingezet.
A.8.1.2	Screening	S	S	S	S	S	S		Uit de risico-analyse (bijv. via "misbruik-scenario's") kan blijken dat per rol en evt. per betrouwbaarheidsniveau onderscheid moet worden gemaakt in het niveau van screening.	Zie document: Afsprakenstelsel eHerkenning - Informatiebeveiliging (Procedure screening)
A.8.1.3	Arbeidsvoorwaarden	v	v	v	v	v	v		Bijv. in de vorm van een ondertekend arbeidscontract of vergelijkbaar alternatief. Zie bijv. ook onder A.8.2.2	
A.8.2	Tijdens het dienstverband	Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen en het risico van een menselijke fout te verminderen.								
A.8.2.1	Directieverantwoordelijkheid	S	Sv	Sv	Sv	Sv	Sv		Management dient personeel dat een taak/activiteit verricht ten behoeve van een rol in het stelsel, o.m. op de hoogte te stellen van de relevante eisen uit het afsprakenstelsel en bijbehorende procedures	
A.8.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	v	v	v	v	v	v		Zie ook A.8.2.1	

A.8.2.3	Disciplinaire maatregelen	S	v	v	v	v	v		Voor deelnemers en Beheerorganisatie is de maatregel bedoeld voor werknemers die inbreuk op de beveiliging hebben gepleegd. Iedere organisatie binnen het stelsel bepaalt zelf of daartoe een formeel disciplinair proces moet worden vastgesteld.	Op stelselniveau is een zogenaamd "nalevingsbeleid" geformuleeerd. Zie document: Afsprakenstelsel eHerkenning - Juridisch kader.
A.8.3	Beëindiging of wijziging van dienstverband	Doelstelling: Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers ordelijk de organisatie verlaten of hun dienstverband wijzigen.								
A.8.3.1	Beëindiging van verantwoordelijkheden	v	v	v	v	v	Sv		BO dient dit proces in te richten voor de BO medewerkers	
A.8.3.2	Retournering van bedrijfsmiddelen	v	v	v	v	v	Sv		BO dient dit proces in te richten voor de BO medewerkers	
A.8.3.3	Blokkering van toegangsrechten	v	v	v	v	v	Sv		BO dient dit proces in te richten voor de BO medewerkers	
A.9	Fysieke beveiliging en beveiliging van de omgeving									
A.9.1	Beveiligde ruimten	Doelstelling: Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatievan de organisatie.								
A.9.1.1	Fysieke beveiliging van de omgeving	v	v	v	v	v	v			
A.9.1.2	Fysieke toegangsbeveiliging	v	v	v	v	v	v			
A.9.1.3	Beveiliging van kantoren, ruimten en facilitetien	v	v	v	v	v	v			
A.9.1.4	Bescherming tegen bedreigingen van buitenaf	v	v	v	v	v	v			
A.9.1.5	Werken in beveiligde ruimten	v	v	v	v	v	v			
A.9.1.6	Openbare toegang en gebieden voor laden en lossen	v	v	v	v	v	v			
A.9.2	Beveiliging van apparatuur	Doelstelling: Het voorkomen van verlies, schade, diefstal of compromittering en onderbreking van de bedrijfsactiviteiten.								
A.9.2.1	Plaatsing en bescherming van apparatuur	v	v	v	v	v	v			
A.9.2.2	Nutsvoorzieningen	v	v	v	v	v	v			
A.9.2.3	Beveiliging van kabels	v	v	v	v	v	v			
A.9.2.4	Onderhoud van apparatuur	v	v	v	v	v	v			
A.9.2.5	Beveiliging van apparatuur buiten het terrein	v	v	v	v	v	v			
A.9.2.6	Veilig verwijderen en hergebruiken van apparatuur	S	Sv	Sv	Sv	Sv	Sv		Belangrijk hierbij is dat wanneer apparatuur wordt verwijderd/hergebruikt of anderszins er gecontroleerd moet worden dat gevoelige gegevens (bijv. persoonsgegevens, metagegevens, routeringstabellen, etc.) onleesbaar worden gemaakt.	
A.9.2.7	Verwijdering van bedrijfseigendommen	v	v	v	v	v	v			
A.10	Beheer van communicatie- en bedieningsprocessen									
A.10.1	Bedieningsprocedures en verantwoordelijkheden	Doelstelling: Bewerkstelligen van een correcte en veilige bediening van IT-voorzieningen.								
A.10.1.1	Gedocumenteerde bedieningsprocedures	S	v	v	v	v	S			Het gaat om procedures die betrekking hebben op het stelsel. De BO beheert deze procedures, instructies, e.d.
A.10.1.2	Wijzigingsbeheer	S	S	S	S	S	S			BO is verantwoordelijk voor de wijzigingsprocessen op stelselniveau. Alle wijzigingen worden behandeld conform de change en release procedure. Zie document: Afsprakenstelsel eHerkenning Operationeel Handboek
A.10.1.3	Functiescheiding	S	Sv	v	v	v	v		Voor MU al standaard bij PKI. Zo mogelijk moet functiescheiding worden toegepast. Waar dit voor kleine organisaties niet mogelijk is moeten compenserende maatregelen worden genomen (bijv. audtitrails).	Zwaarte van de maatregelen moet in relatie staan tot de geleverde betrouwbaarheidsniveaus van de dienst.

A.10.1.4	Scheiding van faciliteiten voor ontwikkeling, testen en productie.	S	S	S	S	S	S		BO is verantwoordelijk voor de coördinatie van de testen bij wijzigingen en nieuwe toetreders in het netwerk met behulp van de simulatietool. Eenieder heeft een A(cceptatie)-omgeving.	Het stelsel hanteert een O, TA en P omgeving. Omtrent de beschikbaarheid en inrichting van de Test/Acceptatie omgeving zijn eisen gesteld. Zie: Afsprakenstelsel eHerkenning Operationeel Handboek
A.10.2	Beheer van dienstverlening door een derde partij	Doelstelling: Geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij.								
A.10.2.1	Dienstverlening	Sv	Sv	Sv	Sv	Sv	Sv		Bij uitbesteding (deel) van de rol/activiteiten aan een onderaannemer, dienen de stelselspecifieke eisen doorvertaald te worden, de opdrachtgever blijft verantwoordelijk.	
A.10.2.2	Controle en beoordeling van dienstverlening door een derde partij	v	v	v	v	v	v			
A.10.2.3	Beheer van wijzigingen in dienstverlening door een derde partij	v	v	v	v	v	v			
A.10.3	Systeemplanning en -acceptatie	Doelstelling: Het risico van systeemstoringen tot een minimum beperken.								
A.10.3.1	Capaciteitsbeheer	S	v	v	v	v	v		Maatregel moet gezien worden in het kader van de SLA.	Zie document: Afsprakenstelsel eHerkenning Service Level
A.10.3.2	Systeemacceptatie	S	v	v	v	v	v		Bij wijzigingen, onderhoud en verstoringen dienen stelselspecifieke afspraken gevolgd te worden.	Zie document: Afsprakenstelsel eHerkenning Service Level
A.10.4	Bescherming tegen virussen en 'mobile code'	Doelstelling: Beschermen van de integriteit van programmatuur en informatie.								
A.10.4.1	Maatregelen tegen virussen	S	Sv	Sv	Sv	Sv	Sv		Iedere organisatie neemt adequate maatregelen tegen virussen. Bij 'doorbraken' dient onderzocht te worden wat de impact op het netwerk is.	
A.10.4.2	Maatregelen tegen 'mobile code'	S	Sv	Sv	Sv	Sv	Sv		Iedere organisatie neemt adequate maatregelen tegen 'mobile code' Bij 'doorbraken' dient onderzocht te worden wat de impact op het netwerk is.	
A.10.5	Back-up	Doelstelling: Handhaven van de integriteit en beschikbaarheid van informatie en IT-voorzieningen.								
A.10.5.1	Reservekopieën maken (back-ups)	S	Sv	Sv	Sv	Sv	Sv		Back-up strategie moet minimaal de SLA ondersteunen. Additioneel afspraken over: - "dienst" zoals benoemd in SLA: inclusief gegevens die met de dienst beheerd worden, - maximaal dataverlies - afspraken m.b.t. classificatie van gegevens (7.2.1) hebben tevens betrekking op de back-up	Back-up strategie moet minimaal de SLA ondersteunen. De BO is verantwoordelijk voor de back-up van voor het stelsel gemeenschappelijke informatie (bijv. Metadata, catalogi, berichtenspecs.)
A.10.6	Beheer van netwerkbeveiliging	Doelstelling: Bewerkstelligen van de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur.								
A.10.6.1	Maatregelen voor netwerken	S	S	S	S	S	S		Netwerkverkeer tussen deelnemers onderling, tussen deelnemers en dienstverleners en tussen deelnemers en dienstafnemers.	Netwerkverkeer tussen deelnemers onderling, tussen deelnemers en dienstverleners en tussen deelnemers en dienstafnemers. Zie: Koppelvlakdocumenten Afsprakenstelsel

A.10.6.2	Beveiliging van netwerkdiensten	S	S	S	S	S	S		Beheerorganisatie is verantwoordelijk voor doorvertaling maatregelen naar onderlinge afspraken in het afsprakenstelsel. Zie ook 6.2.3 voor doorvertaling naar onderaannemers van de deelnemers.	Beheerorganisatie is verantwoordelijk voor doorvertaling maatregelen naar onderlinge afspraken in het afsprakenstelsel. Zie ook A.6.2.3 voor doorvertaling naar onderaannemers van de deelnemers. Maatregelen moeten SLA ondersteunen.

A.10.7	Behandeling van media	Doelstelling: Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten.								
A.10.7.1	Beheer van verwijderbare media	v	v	v	v	v	v		Alleen specifiek: zorgvuldig beheer van verwijderbare media die drager zijn van persoonsgegevens en metagegevens. Zie ook 9.2.6 en 9.2.7	
A.10.7.2	Verwijdering van media	S	Sv	Sv	Sv	Sv	Sv		Media waar archiveringsgegevens zijn opgeslagen. Media waar persoonsgegevens zijn opgeslagen Media waar metadata is opgeslagen	De BO is verantwoordelijk voor het verwijderen van media van het stelsel. Deelnemers moeten te verwijderen media waarop stelselinformatie is opgenomen adequaat behandelen.
A.10.7.3	Procedures voor de behandeling van informatie	v	v	v	v	v	v		Procedure behorend bij classificatie, zie 7.2	Procedure behorend bij classificatie, zie 7.2
A.10.7.4	Beveiliging van systeemdocumentatie	v	v	v	v	v	v			BO beheert stelselspecifieke documentatie.
A.10.8	Uitwisseling van informatie	Doelstelling: Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met enige externe entiteit.								"Kern van het bestaan van eHerkenning"
A10.8.1	Beleid en procedures voor informatie-uitwisseling	S	S	S	S	S	S			Beleid, procedures en afspraken met betrekking tot de uitwisseling van informatie en programmatuur tussen deelnemers en BO is vastgelegd in het Afsprakenstelsel.
A.10.8.2	Uitwisselingsovereenkomsten	S	S	S	S	S	S			Betreft overeenkomsten tussen deelnemers en alle externe partijen waarbij sprake is van uitwisseling van informatie en programmatuur. Idem voor de BO.
A.10.8.3	Fysieke media die worden getransporteerd.	v	v	v	v	v	v			
A.10.8.4	Electronische berichtuitwisseling	S	S	S	S	S	S			Conform koppelvlak documenten
A.10.8.5	Systemen voor bedrijfsinformatie	S	v	v	v	v	S		Gaat met name over het beschermen van de metadata en de archieven waarin de commerciële contracten worden beheerd.	BO: Maatregelen voor beheer en beveiliging van gevoelige stelselinformatie zoals contracten, metagevens, commerciële informatie van deelnemers etc.
A.10.9	Electronic Commerce Services	Doelstelling: Bewerkstelligen van de beveiliging van diensten voor e-commerce en veilig gebruik ervan.								
A.10.9.1	E-commerce	-	v	v	v	v	-	nvt, informatie wordt niet via openbare netwerken = niet beveiligde verbindingen uitgewisseld		
A.10.9.2	Online transacties	S	S	S	S	S	S		Implementatie conform de relevante koppelvlakdocumenten.	Zie de actuele documenten HM-AD, HM-MR, DV-HM, waarbij te allen tijde de versie geïmplementeerd dient te zijn/worden die vanuit het afsprakenstelsel wordt toegestaan
A.10.9.3	Openbaar beschikbare informatie	S	v	v	v	v	S			BO is verantwoordelijk voor het beheer van de openbaar beschikbare informatie van het stelsel eHerkenning. Van belang is bijv dat informatie over het stelsel juist is en consistent is met de informatie die deelnemers openbaar maken.

A.10.10	Controle	Doelstelling: Ontdekken van onbevoegde informatieverwerkingsaktiviteiten.								
A.10.10.1	Aanmaken audit logbestanden	S	S	S	S	S	S			Zie document: Afsprakenstelsel eHerkenning Informatiebeveiliging
A.10.10.2	Controle van systeemgebruik	v	v	v	v	v	v		Constateren afwijkingen in gebruik door deelnemer zelf Controleren naleven afspraken door deelnemer zelf	
A.10.10.3	Bescherming van informatie in logbestanden	S	S	S	S	S	S		Dient aan te sluiten op de vereiste historie voor b.v. fraudeonderzoek (geen relatie met archivering), b.v. passend bij 6 maanden periode voor terugzoeken transacties en handelingen op kritieke systemen	Zie document: Afsprakenstelsel eHerkenning Informatiebeveiliging
A.10.10.4	Logbestanden van administrators en operators	v	v	v	v	v	v			
A.10.10.5	Registratie van storingen	S	S	S	S	S	S		Netwerkbrede afspraken nodig zodanig dat netwerkbreed vastlegging van storingen plaatsvindt ten behoeve van storingsoplossing met bredere impact dan één deelnemer Voorkeur: centrale coördinerende rol beheerorganisatie	Zie document: Afsprakenstelsel Operationeel Handboek - Proces Incidentmanagement Zie ook A.13 Beheer van informatiebeveiligingsincidenten
A.10.10.6	Synchronisatie van systeemklokken	S	S	S	S	S	v		Noodzakelijk voor goede berichtenafhandeling, er dient een eenduidige tijdsbron te worden gedefinieerd en gebruikt	Afspraken omtrent tijdsynchronisatie zijn opgenomen in de koppelvlakspecificaties.
A.11	Toegangsbeveiliging									
A.11.1	Bedrijfseisen ten aanzien van toegangsbeheersing	Doelstelling: Beheersen van de toegang tot informatie								
A.11.1.1	Toegangsbeleid	S	S	S	S	v	S		Toegangsbeveiligingsbeleid in overeenstemming met de classificatie	Zie: Document Betrouwbaarheidsniveaus
A.11.2	Beheer van toegangsrechten van gebruikers	Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen.								
A.11.2.1	Registratie van gebruikers	S Sv	S Sv	S Sv	S Sv	S Sv	S Sv		Specificatie (S) bedoeld voor de registratie van externe gebruikers i.c. bedrijven/klanten van deelnemers. Voor interne gebruikers (medewerkers van deelnemers) bepaalt de deelnemers zelf de invulling (Sv).	Met name voor MU,MR: Procesbeschrijvingen en registratie moeten voldoen aan de beschrijving van de betrouwbaarheidsniveaus voor het verkrijgen van middelen en registraties van bevoegdheden.
A.11.2.2	Beheer van speciale bevoegdheden	S	Sv	Sv	Sv	Sv	Sv			
A.11.2.3	Beheer van gebruikerswachtwoorden	S	Sv	Sv	Sv	Sv	Sv		MU en/of AD t.b.v. hergebruik van middelen.	
A.11.2.4	Beoordeling van toegangsrechten van gebruikers	S	Sv	Sv	Sv	Sv	Sv			
A.11.3	Verantwoordelijkheden van gebruikers	Doelstelling: Voorkomen van onbevoegde toegang door gebruikers en van beschadiging of dienstal van informatie en IT-voorzieningen.								
A.11.3.1	Gebruik van wachtwoorden	S	Sv	Sv	Sv	Sv	Sv		Opmerking: het gaat hier om het gebruik van wachtwoorden door eindgebruikers.	Gebruikers worden geacht een goede beveiligingspraktijk te hanteren bij het selecteren en gebruik van wachtwoorden.
A.11.3.2	Onbeheerde gebruikersapparatuur	v	v	v	v	v	v			
A.11.3.3	"Clear desk" and "Clear screen" - beleid	v	v	v	v	v	v			
A.11.4	Toegangsbeheersing voor netwerken	Doelstelling: Het voorkomen van onbevoegde toegang tot netwerkdiensten.								
A.11.4.1	Beleid ten aanzien van het gebruik van netwerkdiensten	S	S	S	S	S	v			Zie: Koppelvlak documenten HM-DV, MR-HM, AD-HM
A.11.4.2	Authenticatie van gebruikers bij externe verbindingen	S	S	S	S	S	v			Bijv. van toepassing indien een gebruiker zelf machtigingen gaat beheren. Hierbij gelden de afspraken over toepassen betrouwbaarheidsniveaus.
A.11.4.3	Identificatie van netwerkapparatuur	S	S	S	S	S	v			Zie: Koppelvlak documenten HM-DV, MR-HM, AD-HM

A.11.4.4	Bescherming op afstand van poorten voor diagnose en configuratie	S	Sv	Sv	Sv	Sv	Sv		Relevant voor het stelsel. De wijze van invulling wordt bepaald door de deelnemer zelf.	
A.11.4.5	Scheiding van netwerken	v	v	v	v	v	v			
A.11.4.6	Beheersmaatregelen voor netwerkverbindingen	S	S	S	S	S	S			Zie: Koppelvlak documenten HM-DV, MR-HM, AD-HM

A.11.4.7	Beheersmaatregelen voor netwerkroutering	S	S	S	S	S	S			Conform vastgelegde afspraken in de koppelvlak documenten
A.11.5	Toegangsbeveiliging voor besturingssystemen	Doelstelling: Voorkomen van onbevoegde toegang tot besturingssystemen.								
A.11.5.1	Beveiligde inlogprocedures	v	v	v	v	v	v			
A.11.5.2	Gebruikersidentificatie en -authenticatie	v	v	v	v	v	v			
A.11.5.3	Systemen voor wachtwoordbeheer	v	v	v	v	v	v			
A.11.5.4	Gebruik van systeemhulpmiddelen	v	v	v	v	v	v			
A.11.5.5	Time-out van sessies	v	v	v	v	v	v			
A.11.5.6	Beperking van verbindingstijd	v	v	v	v	v	v			
A.11.6	Toegangsbeheersing voor toepassingen en informatie	Doelstelling: Voorkomen van onbevoegde toegang tot informatie in toepassingssystemen.								
A.11.6.1	Beperking van toegang tot informatie	S	v	v	Sv	v	v			Indien het elektronische registratie van machtigingen betreft dan moet aan deze maatregel worden voldaan.
A.11.6.2	Isolatie van gevoelige systemen	v	v	v	v	v	v			
A.11.7	Draagbare computers en telewerken	Doelstelling: Waarborgen van informatiebeveiliging bij het gebruik van draagbare computers en faciliteiten voor telewerken.								
A.11.7.1	Draagbare computers en communicatievoorzieningen	v	v	v	v	v	v		Mogelijk ontstaat vanuit bestaande normenkaders (hogere betrouwbaarheidsniveaus) een beperking op de mogelijkheid om werkzaamheden via mobiele apparatuur uit te voeren.	Indien het informatiebeveiligingsbeleid het gebruik van draagbare computers en communicatievoorzieningen ten behoeve van het beheer van eHerkenning toestaat dienen hierbij passende maatregelen te worden genomen op basis van een daarop gerichte risicoanalyse.
A.11.7.2	Telewerken	v	v	v	v	v	v		Mogelijk ontstaat vanuit bestaande normenkaders (hogere betrouwbaarheidsniveaus) een beperking op de mogelijkheid om werkzaamheden via mobiele apparatuur uit te voeren.	Indien het informatiebeveiligingsbeleid het gebruik van draagbare computers en communicatievoorzieningen ten behoeve van het beheer van eHerkenning toestaat dienen hierbij passende maatregelen te worden genomen op basis van een daarop gerichte risicoanalyse.
A.12	Verwerving, ontwikkeling en onderhoud van informatiesystemen.									
A.12.1	Beveiligingseisen voor informatiesystemen	Doelstelling: Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.								
A.12.1.1	Analyse en specificatie van beveiligingseisen	v	v	v	v	v	v			
A.12.2	Correcte verwerking in toepassingen	Doelstelling: Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen.								
A.12.2.1	Validatie van invoergegevens	S	S	S	S	v	S			Conform de procedure-afspraken voor het uitgeven van middelen en registratie van machtigingen. Deelnemers en Beheerorganisatie: van toepassing voor het beheren van metadata en dienstencatalogi. Zie procedure hiervoor in document: Afsprakenstelsel eHerkenning Operationeel Handboek.
A.12.2.2	Beheersing van interne gegevensverwerking	S	Sv	Sv	Sv	Sv	Sv		Essentieel voor de juiste en betrouwbare werking van het netwerk. Bewaken integriteit berichtenuitwisseling op netwerkniveau. Bewaken correct functioneren verschillende gegevensverwerkingen.	Het gaat hier om applicaties/informatiesystemen die in eigen ontwikkeling zijn. Voor de BO zijn dit bijv de simulatietool, testtool en de specificaties van de eHerkenningsberichten.
A.12.2.3	Integriteit van berichten	S	S	S	S	S	S			Conform vastgelegde afspraken in de koppelvlak documenten
A.12.2.4	Validatie van uitvoergegevens	S	v	v	S	v	S		BO: Denk aan oa. metagegevens en catalogi	Conform vastgelegde afspraken in de koppelvlak documenten

A.12.3	Cryptografische beheersmaatregelen	Doelstelling: Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen.								
A.12.3.1	Beleid voor het gebruik van cryptografische beheersmaatregelen	S	S	S	S	S	S			Conform afsprakenstelsel (cryptosleutels, -algoritmen, PKIoverheid toepassing)
A.12.3.2	Sleutelbeheer	S	S	S	S	S	S			Conform afsprakenstelsel (cryptosleutels, -algoritmen, PKIoverheid toepassing)

A.12.4	Beveiliging van systeembestanden	Doelstelling: Beveiliging van systeembestanden bewerkstelligen.								
A.12.4.1	Beheersing van operationele programmatuur	v	v	v	v	v	v			
A.12.4.2	Bescherming van testdata	S	Sv	Sv	Sv	Sv	S			Document Operationeel handboek par. 4.1.3.3 Document Testen voor deelnemers par. 2.1 en achterliggende testcases
A.12.4.3	Toegangsbeheersing voor broncode van programmatuur	S	Sv	Sv	Sv	Sv	S		Voor de integriteit van het Netwerk is specifieke aandacht nodig voor bescherming tijdens de projectfasen voorafgaande aan in productname.	De BO is verantwoordelijk voor de bescherming van broncode van software gebruikt ten behoeve van het stelsel.
A.12.5	Security in Development & Support Processes	Doelstelling: Beveiliging van toepassingsprogrammatuur en -informatie handhaven.								
A.12.5.1	Procedures voor wijzigingsbeheer	S	S	S	S	S	S			Wijzigingsbeheer staat onder "Proces change en release" beschreven in het document: Afsprakenstelsel eHerkenning - Operationeel Handboek.
A.12.5.2	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem	v	v	v	v	v	v		Van belang voor betrouwbaarheid netwerk. Specifiek wordt van Deelnemers en Beheerorganisatie een zorgvuldig proces verwacht ten aanzien van wijzigingen in relatie tot de andere partijen en adequaat patch- en updatebeleid.	
A.12.5.3	Restricties op wijzigingen in programmatuurpakketten	S	S	S	S	S	S			Wijzigingsbeheer staat onder "Proces change en release" beschreven in het document: Afsprakenstelsen eHerkenning - Operationeel handboek. Restricties kunnen volgen uit de besluiten van het Tactisch Overleg.
A.12.5.4	Uitlekken van informatie	S	S	S	S	S	S			Zie documenten Afsprakenstelsel eHerkenning - koppelvlakdocumenten. Zie Penetratietesten in document Afsprakenstelsel eHerkenning - Operationeel handboek.
A.12.5.5	Uitbestede ontwikkeling van programmatuur	S	Sv	Sv	Sv	Sv	Sv		Bij uitbesteding (deel) van de ontwikkelwerkzaamheden aan een onderaannemer, dienen de stelselspecifieke eisen ten aanzien van het te ontwikkelen product doorvertaald te worden	
A.12.6	Beheer van technische kwetsbaarheden	Doelstelling: Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.								
A.12.6.1	Beheersing van technische kwetsbaarheden	S	Sv	Sv	Sv	Sv	S		Er wordt een hoog niveau van beveiliging verwacht. Specifiek wordt van de deelnemer verwacht dat deze zelf de ontwikkelde informatiesystemen test op alle bekende technische kwetsbaarheden in de broncode (test/audittools) en werking van het informatiesysteem (penetratietesten). Daarnaast dient conform de afspraken in het afsprakenstelsel periodiek, op initiatief van de beheerorganisatie, een penetratietest te worden uitgevoerd op het netwerk en de specifieke systemen van een deelnemer.	Zie document: Afsprakenstelsel eHerkenning - Informatiebeveiliging

A.13	Beheer van informatiebeveiligingsincidenten									
A.13.1	Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken	Doelstelling: Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.								
A.13.1.1	Rapportage van informatiebeveiligingsgebeurtenissen	S	S	S	S	S	S		Deelnemers dienen zelf een registratie van beveiligingsincidenten met betrekking tot de door hen geleverde dienst(en) binnen eHerkenning bij te houden.	Zie Procesbeschrijving Incidentmanagement in document: Afsprakenstelsel eHerkenning - Operationeel handboek.
A.13.1.2	Rapportage van zwakke plekken in de beveiliging	S	S	S	S	S	S		Kwetsbaarheden die mogelijk kunnen leiden tot een beveiligingsincident dienen gemeld te worden bij de BO voor zover: 1. deze een netwerkbrede impact hebben of 2. door de melder niet bepaald kan worden of en op welke individuele deelnemer een kwetsbaarheid betrekking heeft of 3. de kwetsbaarheid met grote kans op korte termijn tot een beveiligingsincident kan leiden. Het signaleren en melden van zwakke plekken is voor ieder van belang.	Zie Procesbeschrijving Incidentmanagement in document: Afsprakenstelsel eHerkenning - Operationeel handboek.
A.13.2	Beheer van informatiebeveiligingsincidenten en verbeteringen	Doelstelling: Bewerkstelligen dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.								
A.13.2.1	Verantwoordelijkheden en procedures	S	S	S	S	S	S		Er dient per deelnemer een contactpersoon te zijn voor coördinatie van beveiligingsincidenten (kan dezelfde persoon zijn als benoemd in 6.1.2) De centrale coördinatie wordt gedaan door de beheerorganisatie.	Zie Procesbeschrijving Incidentmanagement in document: Afsprakenstelsel eHerkenning - Operationeel handboek.
A.13.2.2	Leren van informatiebeveiligingsincidenten	S	S	S	S	S	S		Iedere organisatie dient de beveiligingsincidentregistraties en -rapportages te evalueren op trends en verbeterpunten	Zie Procesbeschrijving Incidentmanagement in document: Afsprakenstelsel eHerkenning - Operationeel handboek.
A.13.2.3	Verzamelen van bewijsmateriaal	S	S	S	S	S	S		Bij aanleiding tot onderzoek (intern het stelsel of op verzoek van opsporingsinstanties) dient relevante informatie voor een transactie door de keten van de deelnemers heen verzameld te kunnen worden.	Zie document: Afsprakenstelsel eHerkenning - Informatiebeveiliging.
A.14	Bedrijfscontinuïteitsbeheer									
A.14.1	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	Doelstelling: Onderbreken van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.								
A.14.1.1	Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer	S	Sv	Sv	Sv	Sv	S		Alle Rollen en BO: Bedrijfscontinuïteit is van belang voor het imago van het netwerk. In te vullen n.a.v. risicoanalyse voor het halen van de service levels. Ook aandacht besteden aan maatregelen voor herstel van de dienstverlening na een calamiteit.	Zie document Afsprakenstelsel eHerkenning - Service Level.

A.14.1.2	Bedrijfscontinuïteit en risicobeoordeling	S	Sv	Sv	Sv	Sv	S		Alle rollen en BO: idem	Deelnemers en de BO nemen maatregelen op basis van een risicobeoordeling en de eHerkenning SLA. Op stelselniveau wordt de bedrijfscontinuïteit gemonitord door de BO.

A.14.1.3	Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging	S	Sv	Sv	Sv	Sv	S		Alle rollen en BO: idem	
A.14.1.4	Kader voor de bedrijfscontinuïteitsplanning	S	Sv	Sv	Sv	Sv	S		Alle rollen en BO: idem	
A.14.1.5	Testen, onderhoud en herbeoordelen van continuïteitsplannen	S	Sv	Sv	Sv	Sv	S		Alle rollen en BO: idem	
A.15	Naleving									
A.15.1	Naleving van wettelijke eisen	Doelstelling: Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen en van enige beveiligingseisen.								
A.15.1.1	Identificatie van toepasselijke wetgeving	S	S	S	S	S	S			Zie document: Afsprakenstelsel eHerkenning - Juridisch Kader
A.15.1.2	Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)	S	S	S	S	S	S		Additioneel specifiek: waar de beheerorganisatie in het kader van toetreding over informatie komt te beschikken waar intellectueel eigendom op rust, dient geheimhouding gewaarborgd te zijn	Zie document: Afsprakenstelsel eHerkenning - Juridisch Kader
A.15.1.3	Bescherming van bedrijfsdocumenten	S	S	S	S	S	S		Geheimhouding door de beheerorganisatie van deelnemerspecifieke informatie (zie ook 15.2.2) Vertrouwelijke omgang met stelselspecifieke informatie.	Zie document: Afsprakenstelsel eHerkenning - Juridisch Kader Zie document: Afsprakenstelsel eHerkenning - Operationeel Handboek
A.15.1.4	Bescherming van gegevens en geheimhouding van persoonsgegevens	S	S	S	S	S	S		Er behoort door de Deelnemers en de BO een beleid voor bescherming van persoonsgegevens te worden ontwikkeld en ingevoerd. Dit beleid behoort te worden gecommuniceerd naar alle personen die betrokken zijn bij het verwerken van persoonsgegevens.	Zie ook: A.7.2 Classificatie Zie: document Juridisch Kader
A.15.1.5	Voorkoming van misbruik van IT-voorzieningen	S	v	v	v	v	S			
A.15.1.6	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	S	S	S	S	S	S			Zie document: Afsprakenstelsel eHerkenning - Juridisch Kader. Zie documenten m.b.t. Koppelvlakspecificaties.
A.15.2	Naleving van beveiligingsbeleid en -normen en technische naleving	Doelstelling: Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie.								
A.15.2.1	Naleving van beveiligingsbeleid en -normen	S	v	v	v	v	S		Opstellen en uitvoeren van een controleplan op basis waarvan procedures regelmatig worden gecontroleerd op naleving	De stelselaudit is beschreven in het document: Handboek beheer Stelselaudit en gemeenschappelijk normenkader informatiebeveiliging.
A.15.2.2	Controle op technische naleving	S	v	v	v	v	S		Opstellen en uitvoeren van een controleplan op basis waarvan informatiesystemen regelmatig worden gecontroleerd op de implementatie van beveiligingsstandaards	Wordt o.a. getoetst door periodieke pentetratietest. Zie document: Afsprakenstelsel eHerkenning Operationeel handboek.
A.15.3	Overwegingen bij audits van informatiesystemen	Doelstelling: Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren.								
A.15.3.1	Beheersmaatregelen voor audits van informatiesystemen	S	v	v	v	v	S		Hantering additionele normenkader eHerkenning (voorliggend kader) Formele audits worden conform het afsprakenstelsel uitgevoerd door een gecertificeerde auditor.	De BO organiseert en coördineert de stelselaudit en rapporteert daarover. De stelselaudit is beschreven in het document: Handboek beheer Stelselaudit en gemeenschappelijk normenkader informatiebeveiliging.
A.15.3.2	Bescherming van hulpmiddelen voor audits van informatiesystemen	S	v	v	v	v	S			