

Versie 21 mei 2021 CBR - Levering van tolkdiensten
1.0

* Voor de meest rechter kolom (kolom H) geldt dat met het voldoen aan ISO 27001 binnen een periode van maximaal twee jaar na de start van de overeenkomst (zie paragraaf 4.2 van het programma van eisen) wordt voldaan aan de minimumeisen van het CBR op het gebied van privacy en informatiebeveiliging

[illegible]

6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging: Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	1			x	
		1	6.1.1.1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	x	
		1	6.1.1.2	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten	nice to have	
		1	6.1.1.3	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	nice to have	
		1	6.1.1.4	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	nice to have	
6.1.2	Scheiding van taken: Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	1			nice to have	
		1	6.1.2.1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	nice to have	
6.1.3	Contact met overheidsinstanties: Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.	2			nice to have	
		2	6.1.3.1	Er is door de organisatie uitgewerkt wie met welke (overheids)instanties en toezichhouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.	nice to have	
		2	6.1.3.2	Het contactoverzicht wordt jaarlijks geactualiseerd.	nice to have	
6.1.4	Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.	2			nice to have	
6.2 Mobiele apparatuur en telewerken						
6.2.1	Beleid voor mobiele apparatuur: Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	1			nice to have	
		2	6.2.1.1	Mobiele apparatuur is zo ingericht dat geen bedrijfsinformatie onbewust wordt opgeslagen ('zero footprint'). Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die gegevens. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn.	nice to have	

		2	6.2.1.2	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: a) in bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde; b) het device maakt onderdeel uit van patchmanagement en hardening; c) het device wordt waar mogelijk beheerd en beveiligd via een MDM Mobile Device Management (MDM)-oplossing; d) gebruikers tekenen een gebruikersovereenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen. Deze verklaring heeft betrekking op alle mobiele apparatuur die de medewerker zakelijk gebruikt; periodiek wordt getoetst of de punten in lid b), c) en d) worden nageleefd.	nice to have	
6.2.2	Telewerken: Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.	2			nice to have	
7. Veilig personeel						
7.1 Voorafgaand aan het dienstverband						
7.1.1	Screening: Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.	1			x	
		1	7.1.1.1	Bij indiensttreding overleggen alle medewerkers (intern en extern) een specifiek voor de functie verstrekte Verklaring Omtrent het Gedrag (VOG).	x	
7.1.2	Arbeidsvoorwaarden: De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	1			x	
		1	7.1.2.1	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.	x	
7.2 Tijdens het dienstverband						
7.2.1	Directieverantwoordelijkheden: De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	1			x	

		1	7.2.1.1	Er is aansluiting bij de interne klokkenluidersregeling, zodat iedereen in staat is om anoniem en veilig beveiligingsissues te kunnen melden.	nice to have	
7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging: Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	1			x	
		1	7.2.2.1	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen	x	
		1	7.2.2.2	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen- en diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.	nice to have	
		1	7.2.2.3	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij haar medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.	x	
7.2.3	Disciplinaire procedure: Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	1			x	
7.3 Beëindiging of wijziging van dienstverband						
7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband: Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht.	1			x	
8. Beheer van bedrijfsmiddelen						
8.1 Verantwoordelijkheid voor bedrijfsmiddelen						
8.1.1	Inventariseren van bedrijfsmiddelen: Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.	1			nice to have	

8.1.2	Eigendom van bedrijfsmiddelen: Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.	1			nice to have	
8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen: Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	1			x	
		1	8.1.3.1	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen	x	
		1	8.1.3.2	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel in het contract vastgelegd overeenkomstig de huisregels of gedragsregels	x	
8.1.4	Teruggeven van bedrijfsmiddelen: Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven.	1			nice to have	
8.2 Classificatie van informatie						
8.2.1	Classificatie van informatie: Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	1			nice to have	
		1	8.2.1.1	De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.	nice to have	
8.2.2	Informatie labels: Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	1			nice to have	
8.2.3	Behandelen van bedrijfsmiddelen: Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	1			nice to have	
8.3 Behandelen van media						
8.3.1	Beheer van verwijderbare media: Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	1			nice to have	
		1	8.3.1.1	Er is een verwijderinstructie waarin is opgenomen dat van herbruikbare media die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd (ISO27002 – implementatierichtlijn 8.3.1.a).	nice to have	

		2	8.3.1.2	De wijze waarop vertrouwelijke of hoger geclassificeerde informatie is opgeslagen, voldoet aan de eisen van het NBV.	nice to have	
8.3.2	Verwijderen van media: Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	2			x	
		2	8.3.2.1	Media die vertrouwelijke informatie bevatten zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden.	x	
		2	8.3.2.2	Verwijdering vindt plaats op een veilige manier, bijv. door verbranding of versnippering. Verwijdering van alleen gegevens is ook mogelijk door het wissen van de gegevens voordat de media worden gebruikt voor een andere toepassing in de organisatie (ISO27002 – implementatierichtlijn 8.3.2.a).	nice to have	
		2	8.3.2.3	Voor het wissen van alle data op het medium, wordt de data onherstelbaar verwijderd, bijvoorbeeld door minimaal twee keer te overschrijven met vaste data en één keer met random data. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is.	nice to have	
8.3.3	Media fysiek overdragen: Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	2			x	
		2	8.3.3.1	Er is voor de gehele organisatie beleid voor het fysiek transport van media vastgesteld.	nice to have	
		2	8.3.3.2	Het gebruik van koeriers of transporteurs voor BBN2 of hoger geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.	nice to have	
9. Toegangsbeveiliging						
9.1 Bedrijfseisen voor toegangsbeveiliging						
9.1.1	Beleid voor toegangsbeveiliging: Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	1			x	
9.1.2	Toegang tot netwerken en netwerkdiensten: Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	1			x	
		1	9.1.2.1	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.	nice to have	
		1	9.1.2.2	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.	nice to have	
9.2 Beheer van toegangsrechten						
9.2.1	Registratie en afmelden van gebruikers: Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	1			x	

9.3.1	Geheime authenticatie-informatie gebruiken: Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	1			nice to have	
		2	9.3.1.1	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.	nice to have	
9.4 Toegangsbeveiliging van systeem en toepassing						
9.4.1	Beperking toegang tot informatie: Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	1			x	
		2	9.4.1.1	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	x	
		2	9.4.1.2	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	x	
9.4.2	Beveiligde inlogprocedures: Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	1			x	
		1	9.4.2.1	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	x	
		2	9.4.2.2	Voor het verlenen van toegang tot het netwerk door externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	nice to have	
9.4.3	Systeem voor wachtwoordbeheer: Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	1			x	
		1	9.4.3.1	Als er geen gebruik wordt gemaakt van two factor authentication is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.	x	
		1	9.4.3.2	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.).	x	
		2	9.4.3.3	Het wachtwoordbeleid wordt geautomatiseerd afgedwongen.	x	
		2	9.4.3.4	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.	x	

		2	9.4.3.5	Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.	x	
9.4.4	Speciale systeemhulpmiddelen gebruiken: Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	1			x	
		1	9.4.4.1	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.	x	
		2	9.4.4.2	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	nice to have	
9.4.5	Toegangsbeveiliging op programmabroncode: Toegang tot de programmabroncode behoort te worden beperkt.	1			x	
10. Cryptografie						
10.1 Cryptografische beheersmaatregelen						
10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen: Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	2			x	
		2	10.1.1.1	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) wanneer cryptografie ingezet wordt; (b) wie verantwoordelijk is voor de implementatie; (c) wie verantwoordelijk is voor het sleutelbeheer; (d) welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het forum standaardisatie worden toegepast; (e) de wijze waarop het beschermingsniveau vastgesteld wordt; (f) bij inter-organisatie communicatie wordt het beleid onderling vastgesteld.	nice to have	
		2	10.1.1.2	Cryptografische toepassingen voldoen aan passende standaarden.	nice to have	
10.1.2	Sleutelbeheer: Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.	1			nice to have	
		2	10.1.2.1	Ingeval van PKI-overheid certificaten: hanteer de PKI-Overheid-eisen t.a.v. het sleutelbeheer. In overige situaties: hanteer de standaard ISO-11770 voor het beheer van cryptografische sleutels.	nice to have	
		2	10.1.2.2	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.	nice to have	

11. Fysieke beveiliging						
11.1 Beveiligde gebieden						
11.1.1	Fysieke beveiligingszone: Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	1			x	
		1	11.1.1.1	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.	x	
11.1.2	Fysieke toegangsbeveiliging: Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	1			x	
		2	11.1.2.1	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	nice to have	
11.1.3	Kantoren, ruimten en faciliteiten beveiligen: Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	1			x	
		1	11.1.3.1	Sleutelbeheer is ingericht op basis van een sleutelplan (NkBR 5.4).	x	
11.1.4	Beschermen tegen bedreigingen van buitenaf: Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	1			x	
		1	11.1.4.1	De organisatie heeft geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.	nice to have	
		1	11.1.4.2	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.	x	
11.1.5	Werken in beveiligde gebieden: Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast. Laad- en loslocatie:	2			nice to have	
11.1.6	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	1			nice to have	
11.2 Apparatuur						
11.2.1	Plaatsing en bescherming van apparatuur: Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	1			nice to have	

11.2.2	Nutsvoorzieningen: Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	1			nice to have	
11.2.3	Beveiliging van bekabeling: Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.	1			nice to have	
11.2.4	Onderhoud van apparatuur: Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	1			nice to have	
11.2.5	Verwijdering van bedrijfsmiddelen: Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	1			nice to have	
11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein: Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	1			nice to have	
11.2.7	Veilig verwijderen of hergebruiken van apparatuur: Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	1			nice to have	
11.2.8	Onbeheerde gebruikersapparatuur: Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	1			x	
11.2.9	'Clear desk'- en 'clear screen'-beleid: Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten te worden ingesteld.	1			x	
		2	11.2.9.1	Een onbemensde werkplek is altijd vergrendeld.	x	
		2	11.2.9.2	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.	nice to have	
		2	11.2.9.3	Sessies op remote desktops worden op het remote platform vergrendeld na een vastgestelde periode.	nice to have	
		2	11.2.9.4	Het overnemen van sessies op remote desktops op een ander client apparaat is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd.	nice to have	

		2	11.2.9.5	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van de token de toegangsbeveiligingslock automatisch geactiveerd.	nice to have	
12. Beveiliging bedrijfsvoering						
12.1 Bedieningsprocedures en verantwoordelijkheden						
12.1.1	Gedocumenteerde bedieningsprocedures: Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	1			nice to have	
12.1.2	Wijzigingsbeheer: Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	1			x	
		1	12.1.2.1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: (a) het administreren van wijzigingen; (b) risicoafweging van mogelijke gevolgen van de wijzigingen; (c) goedkeuringsprocedure voor wijzigingen.	x	
12.1.3	Capaciteitsbeheer: Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	1			nice to have	
12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen: Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	1			nice to have	
		2	12.1.4.1	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.	nice to have	
		2	12.1.4.2	Wijzigingen op de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.	nice to have	
12.2 Bescherming tegen malware						
12.2.1	Beheersmaatregelen tegen malware: Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	1			x	
		1	12.2.1.1	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	x	
		1	12.2.1.2	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende linken.	x	

		1	12.2.1.3	Software en bijbehorende herstelsoftware die malware opspoot zijn geïnstalleerd en worden regelmatig geüpdate.	x	
		1	12.2.1.4	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten: (a) alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen; (b) bijlagen en downloads vóór gebruik.	x	
		1	12.2.1.5	De malware scan wordt op verschillende omgevingen uitgevoerd, bijv. op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.	x	
12.3 Back-up						
12.3.1	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemaftbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	1			x	
		1	12.3.1.1	Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld.	x	
		1	12.3.1.2	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	nice to have	
		2	12.3.1.3	In het back-up beleid staan minimaal de volgende eisen: (a) dataverlies bedraagt maximaal 28 uur; (b) hersteltijd in geval van incidenten is maximaal 16 werkuren (2 dagen van 8 uur) in 85% van de gevallen.	nice to have	
		2	12.3.1.4	Het back-up proces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.	nice to have	
		2	12.3.1.5	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de betrouwbaarheid te waarborgen als ze in noodgevallen uitgevoerd moet worden.	nice to have	
12.4 Verslaglegging en monitoren						
12.4.1	Gebeurtenissen registreren: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	1			x	
		1	12.4.1.1	Een logregel bevat minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis.	x	
		1	12.4.1.2	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	x	

12.6.1	Beheer van technische kwetsbaarheden: Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.	1			x	
		1	12.6.1.1	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.	nice to have	
12.6.2	Beperkingen voor het installeren van software: Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	1			x	
		1	12.6.2.1	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).	x	
12.7 Overwegingen betreffende audits van informatiesystemen						
12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen: Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	1			nice to have	
13. Communicatiebeveiliging						
13.1 Beheer van netwerkbeveiliging						
13.1.1	Beheersmaatregelen voor netwerken: Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	1			x	
13.1.2	Beveiliging van netwerkdiensten: Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uithestede diensten.	1			x	
		2	13.1.2.1	Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectie-voorzieningen (zoals beschreven in de richtlijn voor implementatie van detectie-oplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen	nice to have	

		2	13.1.2.2	Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).	nice to have	
		2	13.1.2.3	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied, wordt gebruik gemaakt van encryptie middelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	nice to have	
		2	13.1.2.4	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijv. DDoS attacks, Distributed Denial of Service) te signaleren en hierop te reageren.	nice to have	
13.1.3	Scheiding in netwerken: Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.	1			x	
		2	13.1.3.1	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	nice to have	
13.2 Informatietransport						
13.2.1	Beleid en procedures voor informatietransport: Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	1			x	
13.2.2	Overeenkomsten over informatietransport: Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	1			x	
13.2.3	Elektronische berichten: Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.	1			x	
		1	13.2.3.1	Voor de beveiliging van elektronische berichten gelden de vastgestelde standaarden tegen phishing en af luisteren op pas-toe-of-leg-uit lijst van het forum standaardisatie.	nice to have	
		2	13.2.3.2	Voor veilige berichtenuitwisseling met basisregistraties, wordt conform de pas-toe-leg-uit-lijst, gebruik gemaakt van de actuele versie van Digikoppeling	nice to have	
		2	13.2.3.3	Maak gebruik van PKI-Overheid certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn o.a. digitale documenten binnen de Rijksdienst waar gebruikers rechten aan kunnen ontleen.	nice to have	
		2	13.2.3.4	Om zekerheid te bieden over de integriteit van het elektronische bericht wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard of de of de ETSI TS 102 176-1.	nice to have	

13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst: Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	1			x	
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen						
14.1 Beveiligingseisen voor informatiesystemen						
14.1.1	Analyse en specificatie van informatiebeveiligingseisen: De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	1			nice to have	
		1	14.1.1.1	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de BIO.	nice to have	
14.1.2	Toepassingen op openbare netwerken beveiligen: Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	1			nice to have	
14.1.3	Transacties van toepassingen beschermen: Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routing, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspeelen.	1			nice to have	
14.2 Beveiliging in ontwikkelings- en ondersteunende processen						
14.2.1	Beleid voor beveiligd ontwikkelen: Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.	1			nice to have	
		1	14.2.1.1	De gangbare principes rondom Security by design zijn uitgangspunt voor de ontwikkeling van software en systemen	nice to have	
14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen: Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	1			nice to have	

		1	14.2.2.1	Voor het wijzigingsbeheer gelden de algemeen geaccepteerde beheerframeworks, zoals ITIL, ASL of BiSL.	nice to have	
14.2.3	Technische beoordeling van toepassingen na wijzigingen besturingsplatform: Als besturingsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	2			nice to have	
14.2.4	Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	1			nice to have	
14.2.5	Principes voor engineering van beveiligde systemen: Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	1			nice to have	
		1	14.2.5.1	Zie Rijksmaatregel 14.2.1.1	nice to have	
14.2.6	Beveiligde ontwikkelomgeving: Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	1			nice to have	
		1	14.2.6.1	Uitgangspunt voor systeemontwikkeltrajecten is een expliciete risicoafweging. Deze heeft zowel de ontwikkelomgeving als ook het te ontwikkelen systeem in scope.	nice to have	
14.2.7	Uitbestede softwareontwikkeling: Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	1			nice to have	
		1	14.2.7.1	Een voorwaarde voor uitbestedingstrajecten is een expliciete risicoafweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd.	nice to have	
14.2.8	Testen van systeembeveiliging: Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	1			nice to have	
14.2.9	Systeemacceptatietests: Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	1			nice to have	

		1	14.2.9.1	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	nice to have	
		1	14.2.9.2	Van de resultaten van de testen wordt verslag gemaakt.	nice to have	
14.3 Testgegevens						
14.3.1	Bescherming van testgegevens: Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.	2			nice to have	
15. Leveranciersrelaties						
15.1 Informatiebeveiliging in leveranciersrelaties						
15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties: Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.	1			x	
		1	15.1.1.1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden eisen t.a.v. informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd. Deze eisen zijn gebaseerd op een expliciete risicoafweging.	nice to have	
		2	15.1.1.2	Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekken tot leverancierstoegang tot bedrijfsinformatie vastgesteld.	nice to have	
		2	15.1.1.3	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.	x	
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	1			x	
		1	15.1.2.1	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.	nice to have	
		1	15.1.2.2	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.	nice to have	
		1	15.1.2.3	In situaties waarin contractvoorwaarden worden opgelegd door leveranciers, is voorafgaand aan het tekenen van het contract met een risicoafweging helder gemaakt wat de consequenties hiervan zijn voor de organisatie. Expliciet is gemaakt welke consequenties geaccepteerd worden en welke gemitigeerd moeten zijn bij het aangaan van de overeenkomst.	nice to have	

		1	15.1.2.4	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaard voorwaarden voor inkoop gehanteerd.	nice to have	
		2	15.1.2.5	Voordat een contract wordt afgesloten wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exit-strategie.	nice to have	
		2	15.1.2.6	In inkoopcontracten wordt expliciet de mogelijkheid van een externe audit opgenomen waarmee de betrouwbaarheid van de geleverde dienst kan worden getoetst. Een audit is niet nodig als de contractant d.m.v. certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.	nice to have	
15.1.3	Toeleveringsketen van informatie- en communicatietechnologie: Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	1			x	
		2	15.1.3.1	Leveranciers moeten hun keten van toeleveranciers bekend maken en transparant zijn over de maatregelen die zij genomen hebben om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers.	nice to have	
15.2 Beheer van dienstverlening van leveranciers						
15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers: Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	1			nice to have	
		2	15.2.1.1	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.	nice to have	
15.2.2	Beheer van veranderingen in dienstverlening van leveranciers: Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's	2			nice to have	
16. Beheer van informatiebeveiligingsincidenten						
16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen						
16.1.1	Verantwoordelijkheden en procedures: Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	1			x	

16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	1			x	
		1	16.1.2.1	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.	nice to have	
		1	16.1.2.2	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.	nice to have	
		1	16.1.2.3	Alle medewerkers en contractanten hebben aantoonbaar kennis genomen van de meldingsprocedure van incidenten.	nice to have	
		1	16.1.2.4	Incidenten worden zo snel als mogelijk, maar in ieder geval binnen 24 uur na bekendwording, gemeld bij het meldloket.	nice to have	
		1	16.1.2.5	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.	nice to have	
		1	16.1.2.6	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.	nice to have	
		1	16.1.2.7	Informatie afkomstig uit de responsible disclosure procedure zijn onderdeel van de incidentrapportage.	nice to have	
16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging: Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	1			nice to have	
		1	16.1.3.1	Een responsible disclosure procedure is gepubliceerd en ingericht.	nice to have	
16.1.4	BEOORDELING VAN EN BESLUITVORMING OVER informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	1			nice to have	
		2	16.1.4.1	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT.	nice to have	
16.1.5	Respons op informatiebeveiligingsincidenten: Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	1			x	

17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten: Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	1			nice to have	
18. Naleving						
18.1 Naleving van wettelijke en contractuele eisen						
18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen: Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen behoren voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.	1			x	
18.1.2	Intellectuele-eigendomsrechten: Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele-eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen behoren passende procedures te worden geïmplementeerd.	1			nice to have	
18.1.3	Beschermen van registraties: Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	2			x	
		2	18.1.3.1	De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.	nice to have	
18.1.4	Privacy en bescherming van persoonsgegevens: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	1			x	
		1	18.1.4.1	In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.	x	
		2	18.1.4.2	Organisaties controleren regelmatig de naleving van de privacy regels en informatieverwerking en –procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	x	
18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen: Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	1			nice to have	
		1	18.1.5.1	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de pas-toe-of-leg-uit lijst van het forum standaardisatie.	nice to have	
18.2 Informatiebeveiligingsbeoordelingen						

18.2.1	Onafhankelijke beoordeling van informatiebeveiliging: De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.	1			x	
		2	18.2.1.1	Er is een information security information system (ISMS) waarmee aantoonbaar de gehele plan-do-check-act cyclus op gestructureerde wijze wordt afgedekt.	nice to have	
		2	18.2.1.2	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	nice to have	
18.2.2	Naleving van beveiligingsbeleid en -normen: De directie behoort regelmatig de naleving van de informatieverwerking en - procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	1			x	
		1	18.2.2.1	In de P&C cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording.	nice to have	
18.2.3	Becoordeling van technische naleving: Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	1			x	
		1	18.2.3.1	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijv door (geautomatiseerde) kwetsbaarheidsanalyses of pentesten.	nice to have	