Begroting	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Toelichting op aanbeveling AR	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Staten-Generaal	Beveiliging en beheer financiële systemen	De Tweede Kamer had in 2016 haar financiële systeem nog onvoldoende beveiligd en dit is aangemerkt als een onvolkomenheid. Over 2017 is geconstateerd dat de Tweede Kamer de beveiliging van het financiële systeem had verbeterd, maar beschikte toen nog niet over de benodigde beheerrapportage.	Er is in 2018 geen assurance-rapportage uitgebracht waarin zekerheid wordt gegeven over de beveiliging van het financiële systeem. Hierdoor is het beeld over de beveiliging van het financiële systeem niet compleet. In 2018 heeft de Tweede Kamer verder gewerkt aan de beveiliging van het financiële systeem, maar beschikte nog niet over de benodigde	In het contract met de database-beheerder is vastgelegd dat deze in 2020 een assurance-rapportage over 2019 gaat uitbrengen. Als de assurance-rapportage wordt uitgebracht, wordt voldaan aan de laatste administratieve voorwaarde voor de beveiliging van het financiële systeem.	Met een ISAE 3402 verklaring over het begrotingsjaar 2019 zal de Tweede Kamer de informatiebeveiliging van het financiële systeem laten bevestigen, voor 15 maart 2020.
AZ	Informatiebeveiliging	AZ hecht veel belang aan informatiebeveiliging. Desondanks constateert de Rekenkamer risico's als gevolg van een informele aanpak. Dit wordt als onvolkomenheid gekwalificeerd, omdat AZ onvoldoende voortgang heeft laten zien bij het formaliseren van beleid, bestuur en organisatie, evenals bij het verbeteren van incidentmanagement. AZ erkent het belang van formalisatie en herkent de verbeterpunten, echter de kwalificatie onvolkomenheid vindt AZ te zwaar in het licht van de vooruitgang die het ministerie heeft geboekt in 2018. In 2018 zijn voorwaarden geschapen om de genoemde verbeteringen te kunnen uitvoeren en dit in te bedden in de organisatie.	Verbeteren van de formalisering betreft een meerjarig traject, waarbij de benodigde cultuurverandering niet onderschat mag worden. Dit geldt ook voor het verbeteren van incidentmanagement. In 2018 is één geïntegreerde aanpak voor het managen van incidenten, escalaties en risico's geïntroduceerd die in de volgende jaren vruchten gaat afwerpen. Het is de verwachting dat AZ in 2019 wederom belangrijke stappen zet om de genoemde aandachtspunten te adresseren.	• AZ vernieuwt in 2019 haar Beleidsdocument Informatiebeveiliging. In dit document worden tevens rollen, taken en verantwoordelijkheden van functionarissen die een rol hebben bij informatiebeveiliging beschreven. • In 2018 heeft het CISO Office van AZ al een concept missie- en visiedocument opgesteld. Deze documenten worden waar nodig bijgesteld en geformaliseerd. • Een procesbeschrijving t.b.v. de omgang met incidenten bestaat al bij AZ. Deze procesbeschrijving wordt in 2019 verder gespecificeerd m.b.t. informatiebeveiligingsincidenten.	• Vernieuwen en formaliseren Beleidsdocument Informatiebeveiliging: Q3 2019 • Vastleggen rollen, taken en verantwoordelijkheden: Q3 2019 • Formaliseren missie- en visiedocument: Q4 2019 • Verder specificeren van de bestaande procesbeschrijving m.b.t. informatiebeveiligingsincidenten: Q4 2019
Koninkrijksrelati	Informatiebeveiliging Rijksdienst Caribisch Nederland	Dit is geen ernstige onvolkomenheid meer, maar teruggeschakeld naar een onvolkomenheid. Uit het rapport van de rekenkamer blijkt dat zij waardering heeft voor de stappen die zijn gezet.	De aanbevelingen van de Rekenkamer zijn in lijn met de verbeteringen die al zijn ingezet - o.a. versterking sturing IC maatregelen.	De verbeteringen worden nu in de reguliere organisatie opgepakt, niet als separaat verbeterplan, zoals ook met de Rekenkamer is besproken.	De voorgenomen verbeteringen uit het verbeterplan n.a.v. de onvolkomenheid zijn gerealiseerd. De verbetering van de PDCA-cyclus heeft erin geresulteerd dat risico's eerder worden gesignaleerd en kunnen worden opgepakt.
BZ	Informatiebeveiliging	De twee voornaamste onvolkomenheden die de ADR constateert zijn: achterstand op accreditaties (periodieke controle of systemen nog aan alle beveiligingseisen voldoen) en het niet aantoonbaar in control zijn van de informatiebeveiliging. De Algemene Rekenkamer is tot soortgelijke conclusies gekomen.	De ADR adviseert om de voortgang mbt de accreditaties goed te bewaken en daarnaast om een jaarplan op te stellen, zodat aangetoond kan worden dat BZ als organisatie in control is. De AR vult hierbij ook aan dat, gelet op het belang van een adequate informatiebeveiliging, het treffen van de vereiste maatregelen de prioritaire aandacht van de departementsleiding vereist.	Er is een plan van aanpak opgesteld om de bevindingen van ADR en AR op te lossen. Met name de accreditaties benodigd voordat de EU en NAVO-inspecties plaatsvinden hebben prioriteit. Daarnaast zal een begin gemaakt worden met een compliance framework, om de aantoonbaarheid van het in control zijn te vergroten. Dat is een systeem waarin per belanghebbende de (bestaande) risico analyses, bijbehorende informatiebeveiligingsmaatregelen, de voortgang daarop en het bewijs daarvan wordt vastgelegd.	Het opgestelde plan van aanpak wordt momenteel uitgevoerd. De uitvoering is geborgd door periodieke overleggen en de voortgang wordt vastgesteld binnen het ministerie. De achterstand in accreditaties wordt ingelopen doordat nieuwe accreditaties zijn verleend. Aan resterende accreditaties, die van belang zijn voor de EU- en NAVO-inspecties, wordt gewerkt met de hoogste prioriteit. Tot slot wordt met het plan van aanpak gewerkt aan de verdere groei en verbetering in volwassenheid voor wat betreft informatiebeveiliging.
JenV	Informatiebeveiliging	De aanbeveling over het verbeteren van de centrale sturing op risicomanagement is opgevolgd, maar in 2018 nog niet afgerond. Uit het Verantwoordingsonderzoek van 2018 blijkt ook dat van de vier aandachtsgebieden het risicomanagement nog achterblijft.	AR beveelt aan om de ingeslagen weg op het risicomanagement voort te zetten en af te ronden, zodat de werking kan worden aangetoond.	Beleid risicomanagement Implementatie beleid risicomanagement	Het plan van aanpak informatiebeveiliging is naar de Kamer verstuurd. De ingezette lijn wordt verder geintensiveerd.
BZK	Beveiliging van IT-componenten SSC-ICT	SSC-ICT onderkent te noodzaak om de beveiliging van IT componenten op orde te hebben.	SSC-ICT neemt de aanbevelingen over onderkent dat de beveiliging van IT-componenten op meerdere punten moet worden versterkt, maar stelt tegelijkertijd vast dat de SSC-ICT infrastructuur over meerdere verdedigingslinies beschikt, hetgeen de kans op misbruik aanzienlijk verkleint.	SSC-ICT wil dit jaar het IT-beheer voor een aantal belangrijke, grotere applicaties op orde hebben en zal de consolidatie en standaardisatie van de componenten die voor de dienstverlening van belang zijn om de huidige beveiliging verder te verbeteren en te borgen dat de beveiliging consequent wordt gecontroleerd en verbeterd, is de sturing op security inmiddels versterkt door per dienst een risicohouder aan te wijzen en per divisie een security board in te stellen. Tevens zijn ten behoeve van de monitoring diverse beveiligingsindicatoren per dienst gedefinieerd. Door wekelijks het gehele netwerk in kaart te brengen en te scannen op kwetsbaarheden, en het aantal kwetsbaarheden als beveiligingsindicator aan een risico-eigenaar toe te wijzen ontstaat er extra druk om updates tijdig door te voeren.	De sturing op IB-maatregelen (ook in de techniek) is in 2019 aangepast, waardoor zowel op divisieniveau als directieniveau een beter inzicht ontstaat in de risico's op dienstenniveau. Hoewel dit mechanisme zelf niet zorgt voor een betere beveiliging, zorgt het wel voor effectievere sturing. Alle belangrijke systemen binnen het verzorgingsgebied van SSC-ICT, evenals het netwerk, zijn inmiddels onder monitoring gebracht van het security operating center. Hierdoor is er een wekelijks en direct inzicht in eventuele (nieuwe) kwetsbaarheden en patch levels. Uit een onderzoek door KPMG is gebleken dat de SSC-ICT voor meerdere grote uitdagingen staat. Dit is voor SSC-ICT aanleiding om de beschikbare capaciteit in te zetten op de meest urgente zaken, zoals door de Rekenkamer en ADR zijn bevonden (o.a. GITC bevindingen). Gebruikersbeheer is een van de onderwerpen binnen het GITC-domein.
BZK	Informatiebeveiliging BZK kerndepartement	De onvolkomenheid heeft betrekking op een aantal procedures die niet aanwezig zijn, niet tijdig waren vastgesteld of naar de mening van de Rekenkamer niet goed waren geïmplementeerd.	n.v.t.	Van de vier aanbevelingen die zijn gedaan, zijn er inmiddels drie opgevolgd. De laatste, totstandbrengen van een BZK-breed Incidentproces, volgt later dit jaar. Planning ultimo 2019 gereed.	De vier aanbevelingen zijn opgevolgd. De CIO-BZK heeft het BZK-breed incidentproces vastgesteld. In een periode van zes maanden wordt dit proces beproefd met drie grote uitvoeringsorganisaties: Logius, RvIG en SSC-ICT. Het proces is erop gericht om bestuurlijk en politiek relevante incidenten naar de strategische laag te brengen.
OCW	Informatiebeveiliging DUO (autorisatiebeheer)	Problemen met het beheren van autorisaties: Autorisatiebeheer betreft het juist, tijdig en volledig toekennen, monitoren en intrekken van (toegangs)rechten en bevoegdheden aan gebruikers in een netwerk of systeem. Gebruikers mogen slechts toegang krijgen tot een noodzakelijk geachte set van programma's en data. DUO constateert zelf dat niet altijd wordt voldaan aan de norm die gaat over het beheer van toegangsrechten van gebruikers en, specifieker, het beheer van (speciale) bevoegdheden. Dit probleem speelt al sinds 2016 en verdient meer voortvarendheid.	De AR beveelt de minister van OCW aan om te zorgen dat DUO: • Voortgang maakt met de voorgenomen verbeteringen in het autorisatiebeheer; •Periodiek controleert of de uitgegeven autorisaties op de meest kritische systemen nog juist zijn om zo het risico op datalekken en onbevoegde handelingen te beperken.	Om deze bevinding op te lossen zijn twee acties van belang. De eerste betreft het beheersen van de huidige risico's op autorisatiebeheer risco gebasseerd (nu de structurele oplossing nog niet is ingebed). De tweede actie gaat over de structurele oplossing door het inbedden van de nieuwe tool.	Een geactualiseerde risicobenadering van het autorisatiebeheer wordt geimplementeerd. Dit gaat gezamelijk in een departementaal breed traject.

Begroting	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Toelichting op aanbeveling AR	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Financiën	Informatiebeveiliging kerndepartement	De aanbevelingen die de Algemene Rekenkamer in 2018 heeft gedaan zijn opgevolgd, maar nog niet volledig afgerond. Om die reden wordt de onvolkomenheid gehandhaafd.	Stappen zetten op het aandachtsgebied van het risicomanagement door onder andere een werkend centraal overzicht van verbeterplannen te verkrijgen, daarnaast hierover periodiek te rapporteren aan het seniormanagement en een overzicht van de kritieke systemen inclusief belangrijkste risico's en de laatst uitgevoerde risicoanalyses en penetratietesten op te tellen. Dit is van belang om op centraal niveau een goed overzicht te krijgen waarmee het seniormanagement kan worden geïnformeerd.	Afronden van de maatregelen op gebied van centrale monitoring (kerndepartement en Belastingdienst), risicomanagement en de kwaliteit van het managementsysteem voor informatiebeveiliging.	Verbetermaatregel geimplementeerd, uiterlijk eind 2019.
Defensie	Informatiebeveiliging	In 2017 is een onvolkomenheid geconstateerd op de sturing op informatiebeveiliging en de dossiervorming voor de beveiligingsmaatregelen voor de 14 kritieke systemen.	In 2018 is door de ARK vastgesteld dat voor de onderzochte aandachtsgebieden de BIR in voldoende mate is geïmplementeerd, maar dat de aanbeveling over de accreditering nog niet is afgerond.	De accreditatiedossiers van de 14 kritieke systemen worden gecompleteerd en aangeboden aan de Beveiligingsautoriteit van Defensie ter toetsing en het afgeven van een accreditatie	Bijna alle kritieke systemen zijn geaccrediteerd ultimo 2019.
IenW	Informatiebeveiliging	Bij 3 aandachtsgebieden is de BIR:2012 onvoldoende geïmplementeerd: organisatie van de informatiebeveiliging, incidentenmanagement en risicomanagement.	Zorg dat centraal voldoende inzicht in de kenmerken en risico's van kritieke systemen wordt verkregen zodat dit sturing kan geven aan de prioritering van de (decentrale) verbeterplannen. Geef verder vervolg aan de al ingezette trajecten voor strategie, risicomanagement, incidentmanagement, organisatie-inrichting en het awarenessprogramma.	Het overzicht aan kritieke systemen is uitgebreid en wordt stapsgewijs verder verbeterd, incl. het gebruik als stuurinformatie. Incidentmanagement wordt dit jaar afgerond. Risicomanagement is voor 2019 een speerpunt in het IB-verbeterprogramma.	De organisatie van de informatiebeveiliging, het incidentenmanagement en het risicomanagement zijn verbeterd. De groeiambitie en nadere implementatie volgt in de volgende jaren.
BZK	IT-beheer P-direkt systemen	De door de Algemene Rekenkamer toegekende onvolkomenheid op het IT-beheer van de P-Direkt systemen bestaat uit 'productiebeheer' en 'wijzigingsbeheer' aangevuld met twee punten bij SSC-ICT 'beveiliging van componenten' en 'gebruikersbeheer'. Productiebeheer Productiebeheer is belegd bij een drietal teams die niet op dezelfde wijze werken. In het vooraf overeengekomen en gehanteerde non-GITC-normenkader is daar wel vanuit gegaan. Dit heeft ertoe geleid dat bij controle niet altijd de uitgevoerde procesgang kon worden gereproduceerd door onvoldoende vastlegging van verrichte acties. Wijzigingsbeheer P-Direkt kende al twee methodieken om uitbreidingen en wijzigingen in de systemen te verwerken. Deze twee methodieken zijn voldoende uitontwikkeld in termen van taken/verantwoordelijkheden, functiescheiding en vastlegging. Hier waren in 2017 geen bevindingen op. Begin 2018 is de nieuwe Agile/Scrum methodiek ingevoerd voor het wijzigingsbeheer.	P-Direkt zal met de ADR in 2019 verder afstemmen over de aard en diepgang van de beheersmaatregelen, waarbij P-Direkt meer oog heeft voor de verschillende soorten systemen en uitzonderingen en de wijze waarop de ADR deze vervolgens toetst.	Productiebeheer Diverse verbetermaatregelen, met name gericht op consistente vastlegging van uitgevoerde acties, zijn inmiddels ondernomen. Wijzigingsbeheer De afspraken voor de vastleggingen van de stappen in het wijzigingsbeheerproces voor Agile/scrum wijzigingen moeten worden aangescherpt, zodat achteraf eenvoudig kan worden aangetoond welke werkzaamheden zijn uitgevoerd en wie daar verantwoordelijk voor was. Hierop is al actie ondernomen en de verwachting is dat de reeds in gang gezette verbeteracties worden afgerond in het tweede kwartaal. Beveiliging componenten SSC-ICT heeft de benodigde maatregelen in april 2019 afgerond, zodat de beveiliging van de IT-componenten op orde is. Gebruikersbeheer SSC-ICT heeft ten behoeve van het verbeteren van het gebruikersbeheer in 2018 een autorisatiematrix opgesteld en deze is in april 2019 uitgerold.	In Q2 2019 heeft de ADR als onderdeel van de eerste controle vastgesteld dat P-direkt ten aanzien van de tekortkomingen maatregelen heeft getroffen die in opzet en werking voldoen. Er zijn enkele, niet als zwaarwegend beoordeelde bevindingen. SSC-ICT heeft op technisch niveau de onderliggende systemen verder versterkt.
BZK	Gebruikersbeheer SSC-ICT	SSC-ICT onderkent de noodzaak om gebruikersbeheer in de volle breedte te beheersen.	SSC-ICT neemt de aanbevelingen over.	Ten aanzien van het gebruikersbeheer op de systemen die SSC-ICT in beheer heeft is de huidige aanpak erop gericht om de tekortkomingen vooraleerst op te lossen voor die systemen waar de risico's het grootst zijn. De ervaringen die bij deze specifieke verbetertrajecten zijn en worden opgedaan, worden verwerkt tot een generieke aanpak voor het vervolgtraject. Dit behelst onder andere een overkoepelende procedure voor het beheer van autorisaties en het toepassen van een mechanisme van beveiligingsindicatoren om te sturen op gesignaleerde afwijkingen ten aanzien van het gebruikersbeheer.	De sturing op IB-maatregelen (ook in de techniek) is in 2019 aangepast, waardoor zowel op divisieniveau als directieniveau een beter inzicht ontstaat in de risico's op dienstenniveau. Hoewel dit mechanisme zelf niet zorgt voor een betere beveiliging, zorgt het wel voor effectievere sturing. Alle belangrijke systemen binnen het verzorgingsgebied van SSC-ICT, evenals het netwerk, zijn inmiddels onder monitoring gebracht van het security operating center. Hierdoor is er een wekelijks en direct inzicht in eventuele (nieuwe) kwetsbaarheden en patch levels. Uit een onderzoek door KPMG is gebleken dat de SSC-ICT voor meerdere grote uitdagingen staat. Dit is voor SSC-ICT aanleiding om de beschikbare capaciteit in te zetten op de meest urgente zaken, zoals door de Rekenkamer en ADR zijn bevonden (o.a. GITC bevindingen). Gebruikersbeheer is een van de onderwerpen binnen het GITC-domein.

Begroting	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Toelichting op aanbeveling AR	Maatregel(en) vanuit departement	Stand van zaken maatregelen
BZK	Volledigheid van de opbrengsten RvIG	Onderzoek van de Auditdienst Rijk laat zien dat de RvIG niet voor alle soorten berichten kan aantonen dat de aantallen uit het berichtenverkeer aansluiten op de aantallen in het factureringssysteem. Hierdoor bestaat een onzekerheid over de rechtmatigheid en de betrouwbaarheid en ordelijkheid van de volledigheid van de verantwoorde opbrengsten	RvIG neemt de aanbevelingen over.	In 2018 is gestart met het auditplan 2018-2019 waarin de werking van de systemen en de onderbouwing van de gefactureerde aantallen berichtenverkeer gecontroleerd worden. De resultaten van 2018 tonen aan dat de werking van de geteste systemen correct is. Het tweede deel van de controle zal opgepakt worden in 2019 conform het reeds in 2018 met de ADR afgesproken auditplan. Dit geheel zal leiden tot een aantoonbaar betrouwbare rapportage voor het BRP berichtenverkeer. De aanbeveling met betrekking tot de functionaliteiten bij een mogelijk nieuw systeem voor het berichtenverkeer zullen meegenomen worden binnen de activiteiten in het kader van de Health Check BRP.	De controle op de volledigheid van de BRP opbrengsten is meegenomen bij de Health Check BRP. Het auditplan wordt momenteel uitgevoerd conform planning met betrokkenheid van AR en ADR.
BZK	Rijksbreed IT-beheer	Op de meeste (financiële) IT-systemen binnen de rijksdienst is nog niet voldoende grip. Dit kan volgens de AR in theorie verschillende gevolgen hebben: fraude bij betalingen kan plaatsvinden doordat bankrekeningnummers gewijzigd kunnen worden door onbevoegden, criminelen met kennis van specifieke applicaties kunnen zich als externe laten inhuren en plegen fraude, er kunnen datalekken ontstaan zonder dat die gesignaleerd worden.	• De AR beveelt in navolging van vorig jaar aan om IT-organisaties, die binnen de rijksoverheid verantwoordelijk zijn voor het beheer van kritische financiële informatiesystemen, verantwoording te laten afleggen over het gevoerde IT-beheer op basis van een assurance rapportage (zoals ISAE 3402 of ISAE 3000 assurance rapport). Aan deze aanbeveling wordt vooralsnog verkennend opvolging gegeven. • De AR beveelt aan om één generiek Governance Risk en Compliance (GRC)-kader te ontwikkelen met gestandaardiseerde minimum beheersingsmaatregelen voor de IT-organisaties binnen de rijksoverheid. Aan deze aanbeveling	1. BZK heeft de ADR verzocht een (vraaggestuurd) onderzoek uit te voeren naar verantwoordingen door SSO's. Vraag aan ADR is om in kaart te brengen aan welke eisen SSO's moeten voldoen. 2. In de geest van de aanbeveling om één generiek GRC-kader te ontwikkelen wordt verkend welke bestaande standaarden geschikt zijn om toe te passen binnen de Rijksdienst en hoe deze passen binnen het bestaande kader van de Baseline Informatiebeveiliging Rijksdienst (BIR 2017). 3. Op grond van het Coördinatiebesluit Organisatie, Bedrijfsvoering en Informatiesystemen zal BZK in 2019 een Rijksbreed kader vaststellen voor het profiel van de departementale CIO.	• ADR-onderzoek verantwoordingen SSO's is afgerond; • Verkenning toepassing bestaande standaarden vanuit BIR2017 biedt eerste resultaten eind 2019; • Kader profiel departementale CIO, ultimo 2019 vastgesteld; • Kwaliteitskader voor I-plannen, ultimo 2019 vastgesteld.
OCW	Informatiebeheer	De AR heeft dit jaar de scope van het OCW onderzoek verbreed en op 4 aandachtsgebieden de centrale sturing op de informatiebeveiliging onderzocht. De aandachtsgebieden zijn: bestuur van de informatiebeveiliging, organisatie van de informatiebeveiliging, incidentenmanagement en risicomanagement. • Het ontbreekt aan periodieke rapportages aan het lijnmanagement over beveiligingsaudits en een jaarlijkse bespreking met de departementsleiding over de resultaten op de beveiligings-doelstellingen en informatie-beveilingsmaatregelen. • Het informatiebeveiligingsbeleid is in oktober 2018 opnieuw vastgesteld. Dit beleid moet op veel onderdelen nog worden aangevuld met werkinstructies en is daardoor niet van voldoende diepgang. • De visie op informatiebeveiliging was in 2018 nog beknopt, • Ook ontbreekt het aan een overzicht van de (bedrijfs)kritieke systemen en een vertaling van een informatie-beveiligingsplan naar richtlijnen en maatregelen als onderdeel van een meerjarenplan om formatiebeveiliging gestructureerd te verbeteren.	Wij bevelen de minister van OCW aan: • De basis van de informatiebeveiliging op het kerndepartement op orde te brengen. Denk hierbij aan het verrijken van het informatiebeveiligingsbeleid en het verder uitwerken van de visie op informatiebeveiligingsbeleid. • Een centraal overzicht op te stellen van de (bedrijfs)kritieke systemen met hun relevante informatie, met als doel grip te krijgen op de status van de systemen. • De departementsleiding minimaal eenmaal per jaar te informeren over de te nemen acties om de informatiebeveiliging op centraal niveau op orde te brengen en te houden.	1. Opstellen van een visie op Informatie Beveiliging (IB) in 2019; 2. Inrichten van een governancestructuur IB binnen OCW op strategisch, tactisch en operationeel niveau; 3. inrichten dit jaar van een IB PDCA cyclus d.m.v. een periodieke standaard directierapportage: "Status IB" op dienst- en jaarlijks op departementsniveau op basis van de BIR2017; 4. Vaststellen van een geupdate IB beleid in 2019.	1. visie op Informatie Beveiliging (IB) vastgesteld eind 2019; 2. governancestructuur IB binnen OCW op strategisch, tactisch en operationeel niveau geimplementeerd; 3. standaard directierapportage: "Status IB" ingericht op basis van de BIR2017; 4. Vaststellen van een geupdate IB beleid uiterlijk eind 2019.
Financiën	Legacy problematiek IT Belastingdienst	Tempo vernieuwen verouderde ICT-systemen te laag. Het tempo waarin de verouderde systemen worden gemoderniseerd of vervangen is te laag en de vraag naar IT-capaciteit zal de komende jaren groter zijn dan het aanbod. Om die reden handhaaft de Algemene Rekenkamer de onvolkomenheid.	Het tempo om de verouderde ICT-systemen te vervangen dient omhoog te gaan.	Het programma Modernisering IV-landschap heeft als doelstelling het realiseren van een robuust en wendbaar IV-landschap. Hiermee wordt een belangrijke bijdrage geleverd aan de oplossing van de legacyproblematiek. Daarnaast werkt de Belastingdienst in de vorm van vernieuwingsprojecten aan het stapsgewijs vernieuwen van de werkprocessen en daarbij ondersteunende ICT. Gezien het begrensde aanbod aan ICT-capaciteit wordt steeds een afweging gemaakt aan welke initiatieven voorrang moet worden gegeven. Een extern onderzoek wordt uitgevoerd naar verloop en uitkomsten van het portfolioproces.	In 2022 technische schuld teruggebracht naar 30%. Het onderzoek naar de werking van portfoliomanagement levert de resultaten eind 2019.
Financiën	Bedrijfscontinuïteitsbeheer BD	Te weinig voortgang is geboekt bij het verbeteren van het bedrijfscontinuïteitsbeheer.	Bedrijfscontinuïteitsbeheer neemt meer tijd in beslag dan aanvankelijk gedacht. Het kost meer tijd dan gedacht om kennis en kunde van hiertoe aangewezen medewerkers op peil te brengen.	Invoering van herstelstrategieën en daarop aansluitende herstelplannen en het uitvoeren van business impact analyses.	Intensivering van kennis en kunde, inclusief aanvullende capaciteit, vraagt meer tijd en middelen gezien externe ontwikkelingen.
Defensie	IT-beheer	De onvolkomenheid is reeds een aantal jaren gesignaleerd: 1. de continuiteit van de bestaande IT-infrastructuur 2. realisatie van de nieuwe IT-infrastructuur	De onvolkomenheid op de continuïteit is opgelost de onvolkomenheid op de nieuwe IT kan pas worden opgelost zodra het programma GrIT succesvol is gerealiseerd.	Realiseren programma GrIT	heroverweging GrIT loopt, eind 2019 besluitvorming over mogelijke vervolgscenario's
IenW	Regie beheerder SAP	Het beheer van het SAP-systeem is deels uitbesteed aan een externe partij. De AR heeft in het verantwoordingsonderzoek over de afgelopen jaren geconstateerd dat onvoldoende toezicht is gehouden op deze externe partij.	Geen aanbeveling	IenW heeft o.a. een kwetsbaarhedenscan aangeschaft. Hiermee kan strakker toezicht uitgeoefend worden op de externe beheerder en kan IenW zelf de afweging maken hoe het wenst om te gaan met kwetsbaarheden. IenW heeft hiermee de regie naar zich toe getrokken.	De kwetsbaarheid scan wordt periodiek gedraaid en de uitkomsten blijken waardevol en leiden waar nodig tot maatregelen. Een ISAE verklaring wordt afgegeven.