Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Aanbeveling rekenkamer	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Eerste Kamer der Staten-Generaal	Informatiebeveiliging	De Eerste Kamer heeft niet alle aanbevelingen uit het verantwoordingsonderzoek 2019 opgevolgd. De risico's op het gebied van informatiebeveiliging worden onvoldoende beheerst.	• Maak een inschatting van de informatiebeveiligingsrisico's voor alle kritieke systemen en verwerk dit zodat een actueel beeld ontstaat van de risico's per IT-systeem. • Zorg ervoor dat de procedures voor het analyseren, categoriseren en escaleren van incidenten zijn opgenomen in het incidentmanagementproces. Rapporteer periodiek. • Werk samen op het gebied van informatiebeveiliging met de Tweede Kamer, de Raad van State, de Algemene Rekenkamer en de Nationale ombudsman.	De aanbevelingen worden overgenomen. De Eerste Kamer wil voldoen aan de Baseline Informatiebeveiliging Overheid (BIO), ook al is zij daar niet toe verplicht. Naast de genomen technische maatregelen moet er meer aandacht komen voor risicomanagement. De samenwerking met andere colleges wordt voortgezet.	Geconstateerd is dat het veel werk is voor een relatief kleine organisatie om aan alle eisen van de BIO te voldoen; meer tijd zal nodig zijn om aan de BIO te gaan voldoen. Een deel van de aanbevelingen is opgevolgd; op basis van een risicoanalyse zijn de belangrijkste maatregelen genomen.
Algemene Rekenkamer	Informatiebeveiliging	De risico's op informatiebeveiliging worden nog onvoldoende beheerst vanuit het aspect van risicomanagement.	Zorg dat het overzicht van de belangrijkste ICT-systemen per systeem de systeemeigenaar, de meest recente risicoanalyse en genomen mitigerende maatregelen vermeldt, alsmede inzicht biedt in de laatst uitgevoerde audit en penetratietest met de reactie daarop.	Het verder verbeteren van het risicomanagement krijgt aandacht. Het overzicht van de belangrijkste ICT-systemen wordt aangevuld. Wederom zal een externe audit uitgevoerd worden. Deze verbeteringen worden, waar mogelijk, in gezamenlijk overleg met de Hoge Colleges opgepakt.	Vooruitgang wordt geboekt bij de maatregelen voor informatiebeveiliging.
Raad van State	Informatiebeveiliging	Risico's worden geconstateerd op alle onderzochte aspecten van informatiebeveiliging.	• Aanbevolen wordt de resterende verbeterpunten voortvarend op te pakken. • Beschrijf in het risicomanagementbeleid alle risicomanagementonderwerpen inhoudelijk zodat inzichtelijk is hoe deze organisatiebreed worden gestandaardiseerd. • Zorg dat het overzicht van de belangrijkste ICT-systemen per systeem de systeemeigenaar, de meest recente risicoanalyse en genomen mitigerende maatregelen vermeldt, alsmede inzicht biedt in de laatst uitgevoerde audit en penetratietest met de reactie daarop.	Op het gebied van gebruikersrechten zijn autorisatiemodellen opgesteld en is het Handboek Autorisatiebeheer vastgesteld. Verdere verbeteringen op het gebied van gebruikersrechten zijn opgepakt. De risicoinschattingen per systeem zijn omgezet naar risicoanalyses per systeem.	Het doel is om de komende jaren de Informatiebeveiliging in overeenstemming te brengen met de Baseline Informatiebeveiliging van de Overheid (de BIO). Belangrijke resultaten zijn geboekt en aan belangrijke verbeteringen wordt gewerkt. De capaciteit rondom informatiebeveiliging is verder geformaliseerd en ingebed in de organisatie.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Aanbeveling rekenkamer	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Nationale Ombudsman	Informatiebeveiliging	De risico's op het gebied van informatie-beveiliging worden nog onvoldoende beheerst.	• Ga verder met inrichting van een incidentmanagementproces in om inzicht te krijgen in de belangrijkste beveiligingsincidenten. • Vervolg vernieuwing proces van risicomanagement om tot de juiste beveiliging van informatie en informatiesystemen te komen. • Zorg dat het overzicht van de belangrijkste ICT-systemen per systeem de systeemeigenaar, de meest recente risicoanalyse en genomen mitigerende maatregelen vermeldt, alsmede inzicht biedt in de laatst uitgevoerde audit en penetratietest met de reactie daarop.	De conclusie over de informatiebeveiliging wordt herkend en de Nationale Ombudsman onderstreept het belang van een goede informatiebeveiliging ook volledig. Ook onderdelen als incidentmanagement en risicomanagement zijn geimplementeerd.	Het overzicht van de ICTsystemen is inmiddels aanwezig en de andere elementen uit de aanbeveling neemt de Nationale ombudsman ter harte.
Binnenlandse Zaken en Koninkrijksrelaties	Informatiebeveiliging, Shared Service Organisatie Caribisch Nederland	De rekenkamer concludeert dat een aanbeveling is opgevolgd en dat de SSO-CN expliciet de focus heeft gelegd op het informatiebeveiligingsbewustzijn van medewerkers bij het thuiswerken als gevolg van de coronacrisis. De rekenkamer constateert risico's op alle onderzochte aspecten van informatiebeveiliging bij de SSO-CN.	• Schenk meer aandacht aan de uitvoering en documentatie van (verbijzonderde) interne controlemaatregelen en onderneem daartoe actie. • Maak goede afspraken met afnemers van SSO-CN over taken en verantwoordelijkheden bij het behalen van de informatie beveiligingsdoelstellingen. • Leg afspraken over taken en verantwoordelijk heden voor het behalen van informatie beveiligingsdoelstellingen helder vast. Dit zorgt ervoor dat de continuïteit van de werkzaamheden voor informatiebeveiliging door de sleutel-functionarissen, zoals de chief information security officer (CISO), wordt geborgd. • Zorg naast de inrichting van het risicomanagement voor informatie-beveiliging ook voor de monitoring op deze risico's. Zorg dat deze voldoende worden beheerst en op verantwoorde wijze kunnen worden geaccepteerd, met als doel om informatie en informatiesystemen voldoende te beveiligen. Met betrekking tot het vanaf 2021 geldende beleidskader van BZK bevelen wij de minister om bij bovenstaande aanbevelingen waar mogelijk een rechtstreekse implementatie van deze	1.Verbetering van de interne securityrapportage aan het management en in aanvulling hierop het sturingsdashboard met specifiek de voortgang van o.a. de ADR en AR punten. 2.Inrichten PDCA waar bij het gebruikte ISMS zowel gebaseerd is op de BIO als dat het de (verbijzonderde) maatregelen van interne controle en de richtlijnen van BZK bevat. 3.Uitvoeren risicoanalyse om te bepalen of en zo ja welke aanvullende (verbijzonderde) maatregelen van interne controle en beveiligingsmaatregelen noodzakelijk zijn. 4.Formaliseren en inrichten van het risicomanagement, daarbij rekening houdend met specifieke bevindingen uit de AR nota. 5.Incident management proces formaliseren, daarbij rekening houdend met specifieke bevindingen uit de AR nota. 6.Vastlegging en besluitvorming over taken en verantwoordelijkheden m.b.t. behalen van informatiebeveiligingsdoelstellingen.	Bij de Rijksdienst Caribisch Nederland is het ontbreken van beschikbare (kennis) capaciteit een belangrijke zorg. Dit wordt thans nog sterker vanwege Covid-19 en reisrestricties. Hierdoor kan het langer duren om de onvolkomenheid op te lossen.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Aanbeveling rekenkamer	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Binnenlandse Zaken en Koninkrijksrelaties	Informatiebeveiliging, BZK kerndepartement	De minister van BZK heeft in 2020 vooruitgang geboekt in het beheersen van de risico's op het gebied van informatiebeveiliging. Van de 4 aanbevelingen uit het verantwoordingsonderzoek 2018 zijn er 3 opgevolgd, 1 is deels opgevolgd. De 2 aanbevelingen uit het verantwoordingsonderzoek 2019 zijn beide deels opgevolgd. Of de risico's bij de informatiebeveiliging hiermee in de praktijk voldoende worden beheerst, moet in 2021 blijken. Gecombineerd met onze overige bevindingen en de werking van het risico- en incidentmanagement voor WebEx en WhatsApp handhaven we de onvolkomenheid en herhalen we de 3 aanbevelingen uit vorige jaren die deels zijn opgevolgd.	* Richt op centraal niveau een incident managementproces in om inzicht te krijgen in de belangrijkste incidenten binnen het ministerie (inclusief die van de dienst-onderdelen) en rapporteer hierover periodiek aan het lijnmanagement. * Geef in de praktijk invulling aan naleving van het opgestelde informatiebeveiligings-beleid. Zorg dat de vastgelegde afspraken over taken en verantwoordelijkheden voor het behalen van informatiebeveiligings-doelstellingen in de praktijk worden nagekomen. * Zorg naast de inrichting van risico-management ook voor de monitoring en aansturing vanuit centraal niveau (vanuit het kerndepartement) richting de decentrale dienstonderdelen, zodat bewaakt wordt dat op decentraal niveau risico's in de informatie-beveiliging voldoende worden beheersten op verantwoorde wijze worden geaccepteerd.	1.Uit de interne rapportages binnen de dienstonderdelen van BZK (de uitvoerings-organisaties) moet de naleving van het beleid en de richtlijnen blijken. De resultaten uit de interne rapportages worden gebruikt voor het opstellen van het BZK-brede IB&P-beeld. 2.Ten aanzien van de kritieke systemen, bij ons genoemd de systemen van een aanmerkelijk te beschermen belang, geven de interne rapportages binnen de dienst-onderdelen zicht op de status en actualiteit van risico analyses. Daar waar risicoanalyses geactualiseerd moeten worden, dient in de rapportage een planning afgegeven te worden.	Met de actualisatie van het beleidskader Privacy- en Informatiebescherming dat per 1 januari 2021 in werking is getreden wordt een P&C-cyclus informatiebeveiliging bij de onderdelen afgedwongen. Ook stelt het de CIO BZK in staat nadrukkelijk op deze cyclus te sturen. De verwachting is dat de onvolkomenheid informatiebeveiliging BZK is opgelost zodra het effect hiervan voldoende zichtbaar is. Over 2021 zien we een duidelijke vooruitgang, zowel in volledigheid van de P&C-cyclus als de kwaliteit van de rapportages. Het inzicht in risico's en risicobeheersing is hierdoor op departementaal niveau sterk verbeterd t.o.v. 2020.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Aanbeveling rekenkamer	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Binnenlandse Zaken en Koninkrijksrelaties	Beveiliging IT-componenten SSC-ICT	In ons verantwoordingsonderzoek over 2019 hebben wij de minister van BZK aanbevolen om de beveiliging van componenten bij SSC-ICT verder te verbeteren volgens het ingezette transitieplan. We zien in 2020 een projectmatige inspanning om de beveiliging van componenten structureel te verbeteren. De inrichting van het lines of defense-model moet waarborgen dat de organisatie zelf controlerend en corrigerend wordt. Het implementeren van de verbetermaatregelen heeft echter nog niet geleid tot betere uitkomsten van de audits in 2020 voor wat betreft de beveiliging van IT-componenten. Wij handhaven daarom de onvolkomenheid.	o Zorg dat SSC-ICT met de te implementeren generieke beveiligingsstandaarden aansluit bij rijksbrede ontwikkelingen en kaders inclusief de periodieke controle op de implementatie. • Betrek de tweede en derde lijn (FEZ en ADR) bij grote IT-wijzigingen en -projecten, waardoor onverwachte terugval van het IT-beheer kan worden voorkomen. • Faseer (de ondersteuning van) systemen uit die niet aan de beveiligingsstandaarden kunnen voldoen.	a. Het hardenen van de infrastructuur is de belangrijkste maatregel om de beveiliging van de componenten structureel te verbeteren. Binnen SSC-ICT wordt in 2021 het hardenen van de IT-infrastructuur én het monitoren van de security baselines gecontinueerd. Daarbij ligt de prioriteit op het hardenen van OS en database. b. Als onderdeel van het hardenen van de infrastructuur worden, waar nodig, ook de AD domain controllers verder gehardened. c. Borging van de periodiek controle op de hardening. De volgende verbetermaatregel wordt daarnaast voortgezet: d. De onvolkomenheid komt voort uit eerdere (2018/2019) ADR-bevindingen inzake de beveiliging van componenten. Door SSC-ICT is in 2020 veel aandacht besteed aan het oplossen van deze backlog aan bevindingen. In de eerste helft van 2021 wordt nog gewerkt aan het oplossen van de laatste bevindingen uit de backlog. Voor de aanvullende aanbevelingen in het VO 2020 treft SSC-ICT daarnaast ook nog de volgende maatregelen: a. Zowel vanuit de 2e lijn als de 3e lijn worden binnen SSC-ICT periodieke controles op	Door SSC-ICT is in 2020 een meerjarig traject gestart dat specifiek deze security tekortkoming adresseert en de risico's reduceert. Dit traject loopt nog door tot en met eind 2022 en voor wat betreft de onvolkomenheid beveiliging IT-componenten vindt een overloop van de maatregelen naar 2022 plaats. Het 'hardenen' van de infrastructuur is een van de belangrijkste uit te voeren maatregelen om de beveiliging van de componenten structureel te verbeteren. Hiertoe zijn beleid en verschillende security baselines opgesteld en goedgekeurd. Voor aantal componenten zijn de goedgekeurde baselines reeds doorgevoerd en nieuwe systemen worden conform deze baselines opgeleverd. Voor de overige IT-componenten wordt het 'hardenen', conform de aangegeven prioritering, verder gecontinueerd. Vanwege de omvang van het serverpark en de noodzakelijke afstemming met de afnemers en technologiepartners vraagt dit traject de nodige zorgvuldigheid in de uitvoering en zal, zoals verwacht, ook in 2022 nog doorlopen. Uiteindelijk wordt het proces rondom 'hardenen' en de controle daarop een continu proces binnen SSC-ICT. Via de Monitoringscommissie van BZK en het

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Aanbeveling rekenkamer	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Binnenlandse Zaken en Koninkrijksrelaties	Gebruikersbeheer SSC-ICT	In het verantwoordingsonderzoek 2019 hebben we de minister van BZK aanbevolen om het gebruikersbeheer bij SSC-ICT verder te verbeteren volgens het ingezette transitieplan. We bevalen aan te streven naar concrete resultaten, waarbij de tekort-komingen vanuit een gestructureerde, eenduidige aanpak over de systemen heen opgelost worden. We zien een projectmatige inspanning om het gebruikersbeheer structureel te verbeteren, maar het implementeren van de verbetermaatregelen heeft nog niet geleid tot betere uitkomsten van de audits in 2020 met betrekking tot gebruikersbeheer. Wij handhaven daarom de onvolkomenheid.	Het is voor 2021 van belang dat de verbetertrajecten worden voortgezet en voorgenomen verbeteringen daadwerkelijk worden gerealiseerd en geïmplementeerd.	De verbetermaatregel valt uiteen in drie delen: a. SSC-ICT richt zich op het intensiveren van identity en access management voor beheeraccounts van risicovolle systemen waaronder de vier ERP-systemen die worden getoetst in het kader van de jaarrekeningcontrole. Rapportage over de voortgang vindt per kwartaal plaats op basis van KPI's. b. Een tweede activiteit betreft het inrichten van het In Control Framework en het intensiveren van de controles door de nieuw ingerichte 2e lijn. Zij controleren maandelijks de GITC aspecten waaronder het gebruikersbeheer voor de vier ERP systemen. De volgende verbetermaatregel wordt daarnaast voortgezet: c. Deze onvolkomenheid komt voort uit eerdere (2018/2019) ADR-bevindingen op het gebied van gebruikersbeheer. Door SSC-ICT is in 2020 veel aandacht besteed aan het oplossen van deze backlog aan bevindingen. In de eerste helft van 2021 wordt nog gewerkt aan het oplossen van de laatste bevindingen uit deze backlog.	Door SSC-ICT is in 2020 een meerjarig traject gestart dat specifiek deze security tekortkoming adresseert en de risico's reduceert. Dit traject loopt nog door tot en met eind 2022. Om het gebruikersbeheer structureel te verbeteren is het noodzakelijk om de bestaande rechten in kaart te brengen en waar nodig op te schonen. Daarnaast wordt de rechtenstructuur wordt verder aan gescherpt op basis van rollen (RBAC) en 'need to use' principe. In 2020 en 2021 is daar voortgang op geboekt en zoals voorzien worden de maatregelen in 2022 verder geïmplementeerd en/of verbeterd. In 2021 zijn veel beheeraccounts en -rechten opgeschoond, is het nieuwe wachtwoordbeleid vertaald naar een policy die stapsgewijs is doorgevoerd en zijn er nieuwe autorisatiematrices voor de belangrijkste systemen/platformen opgesteld. Daarnaast is de eerste functionaliteit van de software rondom het beheer van identiteiten in de ontwikkel en testomgeving opgeleverd en wordt deze momenteel getest. Binnen SSC-ICT zijn flinke stappen gezet met het In Control Framework en de uitvoering van bijbehorende controles. Dit is ook zichtbaar in de resultaten van de huidige ADR-audits waar
Binnenlandse Zaken en Koninkrijksrelaties	IT-beheer P-direkt systemen	P-Direkt en SSC-ICT werken aan verbeteringen om de aanbevelingen uit vorige verantwoordingsonderzoeken op te volgen. Ondanks gerealiseerde verbeteringen in met name het gebruikersbeheer zijn er in 2020 nog tekortkomingen in de deelaspecten beveiliging van componenten en back-up & recovery bij SSC-ICT en wijzigingenbeheer en productiebeheer bij P-Direkt. Wij constateren over 2020 zowel (verwachte) voortgang als (onverwachte) achteruitgang.	o Zorg naast de inrichting van het risico-management voor informatiebeveiliging ook voor de monitoring op deze risico's. Zorg dat deze voldoende worden beheerst en op verantwoorde wijze kunnen worden geaccepteerd, met als doel om informatie en informatiesystemen voldoende te beveiligen.	1. Controle/ beheersing awareness bij medewerkers vergroten 2. P-Direkt breed IB-team opzetten om overzicht te behouden en de samenwerking tussen de afdelingen te intensiveren. 3. Inregelen maandelijkse rapportage interne controles (o.a.) over Gebruikers·, Wijzigingen- en Productiebeheer 4. Aanscherpen beheersmaatregelen in het GITC/non GITC normenkaders 5. Structurele afstemming met de AR: twee vaste momenten om formeel de voortgang te bespreken (aan het eind van derde en vierde kwartaal) 6. Structurele afstemming met de ADR. Operationeel/tactisch maar ook betrokkenheid DT vergroten. Tijdens de audit periode in de operatie 1 keer per maand.	De bij SSC-ICT doorgevoerde verbeteringen t.a.v. de Beveiliging van IT-componenten en het Gebruikersbeheer werken ook door in de IT-dienstverlening aan P-Direkt. T.a.v. back-up & recovery zijn maatregelen getroffen om de aantoonbaarheid van de maatregelen te verbeteren, zodat de opzet, bestaan en werking daarvan ook door de ADR goed vastgesteld kan worden. De interne controles met betrekking tot beveiliging van componenten en gebruikers- en wijzigingsbeheer (operating system en database) zijn onderdeel van het eerdergenoemde In Control Framework en de 1e lijns werkzaamheden. Het oplossen van de backlog aan de bevindingen, waaronder die t.a.v. de beveiliging van componenten, het gebruikersbeheer en back-up & recovery, is afgerond.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Aanbeveling rekenkamer	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Binnenlandse Zaken en Koninkrijksrelaties	IT-beheer, Rijksbreed	Onvoldoende invulling is gegeven aan de eerdere aanbevelingen. Ten aanzien van de inventarisatie en optimalisatie van bestaande kaders zijn eerste stappen gezet. Ten aanzien van (ontbrekende elementen uit) een kader missen wij een concrete aanpak, al dan niet in gezamenlijkheid met de ministeries en SSO's, te ontwikkelen en toe te gaan zien op de implementatie en naleving hiervan.	Aanbevolen wordt: • Kaderstellende rijksbrede rol; de belangrijkste IT-beheerprocessen te identificeren en daarvoor de bestaande kaders aan te vullen met ontbrekende elementen in gezamenlijkheid met de ministeries en SSO's. Een meerjarige, risicogerichte aanpak en het general IT-control-kader van de Auditdienst Rijk kunnen hierbij behulpzaam zijn; • Toezien op de naleving; CIO Rijk monitort de kwaliteit van het IT-beheer op basis van reeds beschikbare assurancerapportages over het IT-beheer en verzoekt IT-beheerorganisaties assurancerapportages toe te voegen aan hun In Control Verklaring. Op basis van deze informatie	Een plan van aanpak is vorm gegeven met maatregelen. Gewerkt wordt aan interdepartementale afstemming waarbij ook bekeken wordt of aanvulling van bestaande kaders nodig is. Structurele verbeteringen zijn in gang gezet met onder meer het Besluit CIO-stelsel Rijksdienst 2021.	Aan de implementatie van het Besluit CIO-stelsel wordt voortvarend gewerkt. Interdepartementaal is IT-beheer in toenemende mate onderwerp van gesprek in de verschillende gremia. Het beschikbaar krijgen van de juiste kennis en kunde in de gevraagde termijn is prioritair zeer lastig.
Buitenlandse Zaken	Informatiebeveiliging	De minister van BZ heeft in 2020 duidelijke vooruitgang geboekt; 3 van de 4 aanbevelingen uit onze eerdere verantwoordingsonderzoeken zijn opgevolgd, 1 is deels opgevolgd. Op de aanbeveling om de achterstand op de (her)accreditaties in te halen is vooruitgang geboekt, maar dit proces is nog niet afgerond. Door de systemen van het ministerie meermaals te voorzien van een tijdelijke accreditatie constateert AR dat het probleem nog niet structureel is opgelost.	AR herhaalt de aanbeveling betreffende het inhalen van de achterstand op de (her)accreditaties en doen daarbij de volgende aanvullende aanbeveling: • Zorg dat de registratie van incidenten geautomatiseerd wordt, zodat het ook niet meer nodig is om het centrale overzicht handmatig op te stellen.	De aanbevelingen worden onderschreven en hebben het ministerie ondersteund bij het opstellen van een uitgewerkt plan van aanpak met duidelijke mijlpalen. De te leveren inspanningen zijn erop gericht om, binnen de ketenafhankelijkheden, de beoogde resultaten zoveel mogelijk eind 2021 te realiseren. Met dat doel wordt tevens in verstevigde sturing en in additionele personele capaciteit voorzien.	a) BZ is van mening dat de PDCA-cyclus voor de accreditaties momenteel goed werkt. De cyclus heeft er ook toe geleidt dat er meerdere accreditaties verleend zijn en aan de invulling van de accreditatievoorwaarden van de te accrediteren systemen aantoonbaar voortgang is geboekt. b) Er is een vooronderzoek uitgevoerd voor de implementatie van een incident management ticketing systeem. c) Het beleid voor toegang tot systemen is aangescherpt in het 'Gesloten tenzij' beleid. De implementatie van dit 'Gesloten tenzij' beleid is in voortgang. d) Er is een meerjarig plan (2021-2023) opgesteld om bewustwording over informatieveiligheid te vergroten. Omgang met gevoelige informatie staat hierin centraal. Middels communicatie, gerichte acties en een trainingsprogramma is er extra aandacht geschonken aan medewerkers op posten.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Aanbeveling rekenkamer	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Buitenlandse Zaken	Toegangsbeveiliging	AR constateert dat de minister van BZ de risico's op het gebied van toegangsbeveiliging onvoldoende beheerst.	Aanbevolen wordt bij deze nieuwe onvolkomenheid: • Verleen uitsluitend toegang tot informatiesystemen na autorisatie door een bevoegde functionaris. Dit kan door, zoals het Ministerie van BZ voornemens is, een 'gesloten, tenzij'-beleid te implementeren. • Draag zorg voor bewustwording onder medewerkers, ook op de posten, bij de omgang met gevoelige gegevens.	De aanbevelingen worden onderschreven en hebben het ministerie ondersteund bij het opstellen van een uitgewerkt plan van aanpak.	* Het beleid voor toegang tot systemen is aangescherpt in het 'Gesloten tenzij' beleid. De implementatie van dit 'Gesloten tenzij' beleid is in voortgang. * Er is een meerjarig plan (2021-2023) opgesteld om bewustwording over informatieveiligheid te vergroten. Omgang met gevoelige informatie staat hierin centraal. Middels communicatie, gerichte acties en een trainingsprogramma is er extra aandacht geschonken aan medewerkers op posten.
Defensie	Autorisatiebeheer	In de materieellogistieke IT-systemen heeft de minister de autorisatiematrices niet vastgesteld op basis van rechten die aan gebruikers worden toegekend. Dit geldt voor bijna alle Defensieonderdelen die rechten hebben verkregen om in deze IT-systemen te werken. Hierdoor is het lastig te beoordelen of zij de rechten die zij uitoefenen terecht hebben verkregen en of dit in de praktijk al dan niet tot te ruime bevoegdheden leidt.	Aanbevolen wordt: • volledige en juiste autorisatiematrices vast te stellen waarin zowel gebruikers als beheerders zijn opgenomen; • beheerrechten in te regelen op basis van actuele en juiste mandaatregisters; • achteraf of continu vast te stellen dat het toekennen, muteren en intrekken van toegangsrechten conform de vastgestelde autorisaties zijn uitgevoerd.	De aanbevelingen van de rekenkamer zijn overgenomen.	• Voor zowel het P als het M domein geldt dat alle autorisatiematrices zijn vastgesteld. P-domein: Opzet, bestaan en werking zijn 'in place'. Vanuit de ADR zijn in 2021 geen onvolkomenheden geconstateerd. Vanzelfsprekend wordt voortdurend de werking in de gaten gehouden en waar nodig verbeterd. M-domein: In oktober 2021 is een geactualiseerde plan van aanpak autorisatiebeheer aangeboden aan het Auditcomité. In het plan is de voortgang van de maatregelen op de bevindingen over 2020 opgenomen en de voorgestelde maatregelen uit de oorzakenanalyse ADR voor het materieel/logistieke domein. Het plan bevat tijdelijke additionele maatregelen om de onvolkomenheid weg te werken voor het materieel logistieke domein en borging van de structurele activiteit te versterken.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Aanbeveling rekenkamer	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Economische Zaken en Klimaat	Autorisatiebeheer	Het autorisatiebeheer van het financiële systeem dat het ministerie gebruikt, Oracle EBS, is onvoldoende op orde. De belangrijke tekortkomingen die zijn geconstateerd, zijn: • Rollen in Oracle EBS zijn niet gekoppeld aan de functie van een medewerker, waardoor niet is gewaarborgd dat aan medewerkers met dezelfde functie ook dezelfde rollen worden toegekend. • Functiescheidingsconflicten en het intrekken van rechten zijn onvoldoende gecontroleerd. Zo zijn rechten na vertrek niet tijdig ingetrokken. • Groepsaccounts zijn nog toegestaan. Voor de accounts worden wachtwoorden gedeeld, en het is niet controleerbaar wie welke handelingen heeft uitgevoerd. • Het is mogelijk autorisaties bij afwezigheid te delegeren, waardoor functie scheidingsconflicten kunnen ontstaan.	De AR beveelt het autorisatiebeheer op orde te brengen door de in de onderzoeken gesignaleerde tekortkomingen in het autorisatiebeheer op te lossen en ervoor te zorgen dat de beheersmaatregelen – ook bij de diensten – aantoonbaar en controleerbaar worden uitgevoerd.	In 2021 worden met betrokken dienstonderdelen afspraken gemaakt om de nog openstaande beheersmaatregelen aantoonbaar en controleerbaar uit te voeren.	1. De opvolging verbeteraanpak is inmiddels in volle gang en de eerste restpunten zijn inmiddels opgelost. Over het opvolgen van de restpunten is intensief contact met de stakeholders, waaronder Auditdienst Rijk, Algemene Rekenkamer en directie FEZ/LNV en EZK. 2. Per dienst zijn, voor de wederzijds vastgestelde conflicten, beheersmaatregelen opgesteld en ingezameld. Veel beheersmaatregelen zijn reeds in werking (en effectief) gedurende 2021 en deze zijn aangevuld met nieuwe maatregelen. De nieuwe set van beheersmaatregelen wordt in 2021 afgestemd met de Auditdienst Rijk en Algemene Rekenkamer. 3. Ten behoeve van vaststellen beheersmaatregelen in geval van conflicten is een rapportage gerealiseerd; op basis hiervan leveren de diensten eind 2021 de geaccordeerde beheersmaatregelen op in geval van conflicten.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Aanbeveling rekenkamer	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Landbouw, Natuur en Voedselkwaliteit	Autorisatiebeheer	Het Ministerie van LNV maakte in 2020 gebruik van Oracle EBS dat bedrijfsprocessen op het kerndepartement automatiseert. Het Ministerie van EZK is eigenaar van dit systeem. Zie verder bij EZK voor een toelichting op de onvolkomenheid.	De AR beveelt aan om als opdrachtgever de oplossing van de tekortkomingen kritisch te volgen en ervoor te zorgen dat LNV en zijn uitvoeringsorganisaties de dienstspecifieke beheersmaatregelen aantoonbaar en controleerbaar uitvoeren.	In 2020 zijn maatregelen getroffen om de tekortkomingen in het autorisatiebeheer op te lossen. In 2021 zal dit samen met EZK voortgezet worden en met de dienstonderdelen afspraken gemaakt worden om de beheersmaatregelen aantoonbaar en controleerbaar uit te voeren.	1. De opvolging verbeteraanpak is inmiddels in volle gang en de eerste restpunten zijn inmiddels opgelost. Over het opvolgen van de restpunten is intensief contact met de stakeholders, waaronder Auditdienst Rijk, Algemene Rekenkamer en directie FEZ/LNV en EZK. 2. Per dienst zijn, voor de wederzijds vastgestelde conflicten, beheersmaatregelen opgesteld en ingezameld. Veel beheersmaatregelen zijn reeds in werking (en effectief) gedurende 2021 en deze zijn aangevuld met nieuwe maatregelen. De nieuwe set van beheersmaatregelen wordt in 2021 afgestemd met de Auditdienst Rijk en Algemene Rekenkamer. 3. Ten behoeve van vaststellen beheersmaatregelen in geval van conflicten is een rapportage gerealiseerd; op basis hiervan leveren de diensten eind 2021 de geaccordeerde beheersmaatregelen op in geval van conflicten.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Aanbeveling rekenkamer	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Financiën	Wijzigingsbeheer IT-systemen (testprocedures)	Uit onderzoek van de AR blijkt dat het testen van wijzigingen in IT-systemen (onderdeel van het wijzigingsbeheer) bij de Belastingdienst nog niet goed is geregeld. Allereerst ontbreekt in de procedure voor wijzigingsbeheer een concrete uitwerking van de wijze van testen. De verantwoordelijkheidsverdeling voor het testen tussen de directie Informatievoorziening (IV) en de opdrachtgevers is niet helder. Ook bleek dat – vanwege tekortschietende documentatie – bij circa 40% van de beoordeelde wijzigingen de inhoud en de resultaten van het testen onduidelijk waren. Er is hierbij geen sprake van voldoende centrale toetsing op de correcte decentrale uitvoering van wijzigingen.	• Zie toe op het centraal opstellen van een adequate procedure (inclusief verantwoordelijkheidsverdeling tussen IV en dienstonderdelen) voor testen in het kader van het wijzigingsbeheer. • Zorg voor centraal toezicht op adequate uitvoering en documentatie van het testen.	De aanbevlingen van de Rekenkamer worden overgenomen. Binnen BD loopt er een programma 'Procesbeschrijvingen en informatievoorziening IV op orde'. De BD heeft in afstemming met de ADR, een onderzoek uitgevoerd naar wijzigingsbeheer. De zgn. 1e deelwaarneming. Het rapport is met de ADR afgestemd. De aanbevelingen uit dit onderzoek geven gerichter aan welke acties IV moet ondernemen om de bevinding/onvolkomenheid op te lossen. In de komende nieuwe versie van het Kader IV-Voortbrenging en Safe Agile Belastingdienst (SABel) referentiemodel zullen, net zoals in de procesbeschrijvingen van het voortbrengings-proces, ook de betreffende noodzakelijke elementen i.r.t. tests worden opgenomen. Tevens vindt er een risicoanalyse plaats met daarin de belangrijkste proces gerelateerde risico's en beheersmaatregelen i.r.t. de voortbrenging. Inmiddels loopt het tweede onderzoek naar wijzigingsbeheer (2e deelwaarneming). Het resultaat hiervan wordt in de tweede helft van december of de eerste helft van januari verwacht.	Verwachting dat in 2021 de opzet kan worden afgerond, maar dat de werking pas in 2022 kan worden aangetoond. Hoewel er veel activiteiten worden ontplooid, kan het zijn dat de opzet niet volledig per eind 2021 wordt beschreven. Mogelijke uitloop in Q1 2022 is voorzien en in de planningen opgenomen.
Infrastructuur en Waterstaat	Informatiebeveiliging	Ambitie van volwassenheidsniveau 3 voor specifieke aandachtsgebieden is nog niet bereikt. Risico's zijn geconstateerd op m.n. inrichting van de organisatie en risicomanagement.	Aanbevolen wordt: • Zorg ervoor dat de verantwoordelijkheden en taken van de CISO als afzonderlijke functie worden onderkend in de organisatie. • Zorg vanuit het kerndepartement voor inrichting, monitoring en sturing op het risicomanagementproces van de decentrale onderdelen.	• De aanbeveling over de verantwoordelijkheden van de CISO is overgenomen binnen de kaders die door de minister van BZK gegeven zijn gesteld met het Besluit op het CIO stelsel. Dit is verwerkt in het O&F rapport van de nieuwe directie CDIB, die is ingericht in Q2 2021. • Vaststellen van risicomanagementbeleid en uitwerking daarvan in kaders is een van de onderwerpen uit het werkprogramma voor informatiebeveiliging van IenW om centraal volwassenheidsniveau 3 te bereiken.	• AR geeft in mondeling terugkoppeling aan dat aanbeveling is opgevolgd door het formaliseren van de taken van de CISO en het aanstellen van de CISO per juli 2021 bij IenW/CDIB. • Het IenW-brede beleid voor risicomanagement is in september 2021 vastgesteld. De uitwerking van het risicomanagement ten behoeve van activiteiten in 2022 wordt in december 2021 in het CISO-overleg IenW besproken. Daarnaast worden er door de CISO periodieke risicogesprekken gevoerd tussen de CISO's om sturing op risico's te versterken.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Aanbeveling rekenkamer	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Infrastructuur en Waterstaat	Lifecycle management	Geconcludeerd wordt dat: • De CIO onvoldoende centraal inzicht in het applicatielandschap en de daar aan verbonden financiële aspecten en risico's heeft. • De CIO onvoldoende centraal inzicht heeft in de levenscyclus van alle applicaties en in welke levensfase zij zich bevinden. • De AR ziet dat er wel initiatieven ter verbetering (o.a. uitbreiding CIO-office) ontplooien.	Aanbevolen wordt: • Uitvoering te geven aan de verdere ontwikkeling van de CIO-functie IenW, inclusief het ontwikkelen van een integraal plan voor beheer en onderhoud van het IT-landschap; • Erop toe te zien dat de IenW-brede kaders over de vastlegging en het onderhoud van applicaties in het IT-landschap inclusief het LCM zijn toegepast; • Ervoor te zorgen dat bovenstaande activiteiten door het centrale CIO-Office in nauwe samenwerking met de CIO's van de dienstonderdelen uitgevoerd worden, en om ervoor te zorgen dat de dienstonderdelen kennis en ervaring over LCM onderling uitwisselen.	De minister van IenW heeft toegezegd: • De concerndirectie informatiebeleid (CDIB) op te richten en uit te breiden; • De positie van de departementale CIO te versterken; • De herinrichting van het CIO-stelsel in lijn met Rijksbrede afspraken; • Een projectleider aan te stellen voor LCM.	• Het Besluit CIO-stelsel Rijksdienst 2021 is in werking getreden. Dit versterkt de positie van de departementale CIO. Dit besluit betekent een verandering van het CIO-stelsel IenW. • Het besluit heeft geleid tot wijziging van het Organisatie- en Mandaat-besluit IenW. • De concerndirectie Informatiebeleid (CDIB) is opgericht en uitgebreid. De uitvoering van de taken van de departementale CIO is bij mandaat belegd bij de directeur CDIB. • De inrichting van het CIO-stelsel is uitgewerkt en wordt vastgesteld in de Bestuursraad, zodat deze zo snel mogelijk in 2022 werkend zal zijn. • Er is een Kernteam en IenW brede werkgroep LCM opgericht. Er is een projectleider aangesteld en een dossierhouder bij CDIB. • Er is een plan van aanpak opgesteld en vastgesteld. • Er is een organisatie brede uitvraag gedaan naar LCM. • Er is een eerste LCM-rapportage opgesteld en hier is een reflectie op uitgevoerd. • Er is een advies opgesteld voor de verdere doorontwikkeling van LCM. Deze wordt in december vastgesteld in de CIO-Raad van IenW.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Aanbeveling rekenkamer	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Onderwijs Cultuur en Wetenschap	Informatiebeveiliging kerndepartement	De Algemene Rekenkamer concludeert in het VO 2020 dat de risico's van informatiebeveiliging nog niet voldoende worden beheerst door de minister van OCW en handhaaft de onvolkomenheid. In het VO 2020 constateert de Algemene Rekenkamer dat de minister van OCW voortuitgang heeft geboekt op het gebied van informatiebeveiliging. De Algemene Rekenkamer constateert dat de aanbeveling om de visie op informatiebeveiliging en het informatiebeveiligingsbeleid uit 2019 te formaliseren is opgevolgd. De aanbevelingen over het jaarplan zijn deels opgevolgd. Voor 2021 ligt er een IB-jaarplan met daarin de concrete activiteiten met bijbehorende kosten en de benodigde capaciteit. De werking moet in 2021 blijken. De aanbeveling over het risico- en incidentmanagement is niet opgevolgd.	De nog openstaande aanbeveling betreft: • Zorg ervoor dat de processen rondom risicomanagement en incidentmanagement helder zijn en dat de rollen, verantwoordelijkheden en taken van medewerkers helder zijn beschreven, zodat iedereen (ook bij de dienstleveranciers) weet wat er moet gebeuren voor wat betreft informatiebeveiliging en daar naar kan handelen.	De verbeteracties voor risicomanagement en incidentmanagement zijn opgenomen in het jaarplan informatiebeveiliging 2021.	In 2021 is ingezet op de uitvoering van het jaarplan informatiebeveiliging. De uitvoering van de verbetermaatregelen rond risico- en incidentmanagement zijn bijna afgerond. Het proces voor risicomanagement is verbeterd, met extra aandacht voor de rolverdeling binnen de organisatie en de integrale sturing op informatiebeveiliging, privacy en veiligheid binnen OCW. Ook is de aansluiting verbeterd tussen het in kaart brengen van risico's op concernniveau en bij de dienstonderdelen. Alle acties en communicatie daarover dragen ook sterk bij aan een verhoogd bewustzijn binnen de hele organisatie. Middels een incident management (IM) plan is ook aandacht besteed aan de opvolging van de aanbevelingen met betrekking tot incident management. Het IM-proces is nieuw ingericht en sinds enkele maanden in uitvoering. Incidenten worden gerapporteerd en komen terecht bij de juiste personen.
Onderwijs Cultuur en Wetenschap	Informatiebeveiliging DUO (autorisatiebeheer)	DUO heeft met betrekking tot autorisatiebeheer belangrijke eerste stappen gezet ter verbetering. Het op orde brengen van het autorisatiebeheer is veelomvattend gezien de omvang van het aantal systemen en de hoeveelheid werk die dit met zich meebrengt. Daarom moet DUO dit onderwerp verscherpte aandacht blijfven geven en verdere voortgang blijven maken op dit onderwerp.	Aanbevolen wordt om het autorisatiebeheer verscherpte aandacht te geven door toe te zien op: • het blijven boeken van de benodigde vooruitgang op het autorisatiebeheer en hierbij de uitgegeven autorisaties periodiek te controleren in lijn met het autorisatiebeleid om zo het risico op onbevoegde handelingen te beperken; • de voortgang van het langetermijnproject 'Role Based Autoriseren'.	Autorisatiebeheer krijgt de volle aandacht door DUO. Er wordt op daadkrachtige wijze uitvoering aan het projectplan gegeven. Het plan kent twee sporen, één voor de korte termijn en één voor de lange termijn. Het lange termijn spoor is de oplossing waar DUO naar toe wil, namelijk 'role based autoriseren'. Dit is behalve een proces en systeem verandering ook cultuur verandering. Mede daardoor heeft dit een langere doorlooptijd. Om de risico's nu al te beheersen is het korte termijn spoor ingericht. Dit richt zich met namen op het periodiek controleren van alle verstrekte autorisaties.	Voor het lange termijn spoor dat doorloopt in 2022 zijn in 2021 zichtbare resultaten behaald en is een deel van de organisatie gemigreerd naar de nieuwe procesgang en bijbehorend systeem om autorisaties te beheersen. De verwachting nu is dat het afronden van de migratie eind 2022 gerealiseerd is. Voor wat betreft de autorisatiematrices is in 2021 een kwaliteitsslag gemaakt. Daarnaast zijn op aanwijzing van de ADR in de risicogerichte benadering van te controleren autorisaties naast vertrouwelijkheid ook de aspecten integriteit en beschikbaarheid meegewogen. Afsluitend blijkt dat ondanks de gezette stappen, er situaties zichtbaar worden waar bij specifieke rollen te ruime autorisaties zijn verstrekt. Elke casus op zich wordt versneld opgepakt en de autorisaties ingeperkt.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Aanbeveling rekenkamer	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Volksgezondheid Welzijn en Sport	Informatiebeveiliging	Op andere onderdelen van informatiebeveiliging zien we voortgang maar zullen de verbeteringen pas in 2021 zichtbaar zijn. Of de risico's rond informatiebeveiliging in de praktijk voldoende worden beheerst, moet in 2021 blijken.	Aanbevolen wordt: • Leg taken en verantwoordelijkheden in de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie helder vast. • Richt op centraal niveau een incidentmanagementproces in, om inzicht te krijgen in de belangrijkste incidenten (inclusief die van de concernonderdelen) en rapporteer hierover periodiek aan het senior management. • Zorg dat de CISO van het concern voldoende inzicht krijgt in de risico's van de decentrale concernonderdelen.	De informatiebeveiliging zal verder versterkt worden in samenwerking met de agentschappen en zbo's die onder het ministerie ressorteren. VWS heeft in januari 2020 een nieuw draaiboek voor incidenten en datalekken vastgesteld om taken en verantwoordelijkheden helder vast te leggen op centraal niveau om het inzicht te vergroten en een incidentmanagementproces in te richten.	• In Q1 2022 zullen de verantwoordelijkheden worden herschreven om meer duidelijkheid te scheppen over de rol verdelingen tussen CISO Concern en CISO kern-departement. • De diversiteit van de organisaties maken nu dat dit een complexe situatie betreft en niet treffend op de problematiek. Wel zijn er uniforme normen in gebruik, uniforme risico afwegingen, maar met andere middelen en procedures simpelweg doordat de sturing per organisatie ook anders is. Die diversietijd moet wel in takt blijven om effectief te kunnen blijven opereren binnen de VWS organisaties. De oplossing zal dus gaan zitten in een onderzoek of de VWS organisaties aan de vereisten voldoen. • De jaarlijkse ICV en volgend jaar IB Beeld zal hier een rol in gaan vervullen om aan te tonen of iedere organisatie structureel hier op volging aan geeft. Dit zal een onderdeel vormen van de ICV verklaring. • De risicokaart zal worden uitgebreid met de organisaties die wel onder concern sturing vallen, maar die vorig jaar niet hebben meegekregen dat zij ook met de risicokaart moeten volgen. Dit heeft te maken met het type organisatie dat zij zijn. Dit zal gelijk worden getrokken.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Aanbeveling rekenkamer	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Volksgezondheid Welzijn en Sport	Lifecycle management	VWS heeft beperkt inzicht in de ICT-applicaties die binnen het ministerie worden gebruikt. Het inzicht beperkt zich tot grote projecten binnen het ICT-landschap en omvat niet het gehele ICT-landschap. Bovendien is het overzicht dat er wel is, niet op een eenduidige en gestructureerde manier op basis van ministeriebrede kaders vormgegeven. Ten tweede is er geen sprake van een ministeriebreed applicatie-lifecyclemanagement (de concernonderdelen mogen dit zelf invullen) en ten derde heeft de CIO geen inzicht in financiële informatie over de specifieke applicaties in het ICT-landschap. Hierdoor kan de CIO niet integraal en planmatig sturen op beheer en onderhoud van het hele ICT-landschap, wat nodig is om risico's voor het Ministerie van VWS te beheersen.	Aanbevolen wordt: • Formaliseer de ministeriebrede kaders voor het onderhouden van een eenduidige en gestandaardiseerde vastlegging van het IT-applicatieportfolio inclusief het lifecyclemanagement. • Zorg dat deze kaders binnen een realistisch tijdpad concernbreed worden geïmplementeerd en toegepast.	Afspraken worden gemaakt over het uniform organiseren van het lifecycle management binnen het getrapte CIO-stelsel van VWS waarin veel is belegd bij decentrale CIO's. Ministeriebrede kaders worden ontwikkeld voor het onderhouden van een eenduidige en gestandaardiseerde vastlegging van het ICT-applicatieportfolio inclusief het lifecycle management. Ook wordt actie ondernomen om te zorgen dat het inzicht in de ICT-applicaties, de levensfase en de risico's versterkt wordt.	• In lijn met de wens van de CIO-raad, is afgesproken het lifecyclemanagement uniform te organiseren binnen het VWS concern met het uitgangspunt alleen noodzakelijk attributen (zie eerder verzonden Excel) in een centraal overzicht te plotten. De concernorganisaties blijven zelf verantwoordelijk voor het uitvoeren van het Lifecyclemanagement. • Daarnaast is een routekaart opgesteld, om het lifecyclemanagement naar een hoger niveau te brengen. Eenduidige en gestandaardiseerde vastlegging van het ICT-applicatieportfolio is conform het proces dat de AR schetst tbv het lifecyclemanagement. De routekaart is besproken in de LCM werkgroep en de CIO-raad en wordt naar verwachting dit jaar nog geformaliseerd. Momenteel is het overzicht (ICT-applicatieportfolio) van bedrijfskritische ICT-applicaties ingevuld door alle concernorganisaties.