Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Toelichting op aanbeveling AR	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Raad van State	Informatiebeveiliging	Risico's op gebied van informatiebeveiliging worden geconstateerd bij de Raad van State. Vooral het autorisatiebeheer, het leveranciersmanagement, de beschikbare capaciteit en de risicoanalyses moeten verbeterd worden.	Aanbevolen wordt: • Zorg in de eigen organisatie en formatie voor structureel voldoende gekwalificeerde capaciteit inclusief vervanging. • Richt het autorisatiebeheer zodanig in dat er functieprofielen zijn en er per functieprofiel rechten worden toegekend. • Maak goede afspraken met IT-leveranciers om te voldoen aan de beveiligingseisen die volgens de BIO van toepassing zijn. • Stel per systeem een risicoanalyse op zodat de juiste maatregelen worden genomen om de informatie in de systemen op het juiste niveau te beveiligen. • Stel een overzicht op waarin alle soorten informatie van de Raad van State zijn geclassificeerd.	Naar aanleiding van de bevindingen ten aanzien van de informatiebeveiliging zal de Raad van State een plan van aanpak opstellen, waarin de aanbevelingen zullen worden uitgewerkt in concrete maatregelen en actiepunten.	De Raad van State heeft inmiddels een plan van aanpak vastgesteld, waarin de aanbevelingen zijn uitgewerkt in concrete maatregelen en actiepunten. De uitvoering van het plan van aanpak is voortvarend ter hand genomen. Het doel is om de komende jaren de Informatiebeveiliging in overeenstemming te brengen met de Baseline Informatiebeveiliging van de Overheid (de BIO).
Nationale Ombudsman	Informatiebeveiliging	Op alle 4 de aandachtsgebieden van informatiebeveiliging worden risico's geconstateerd bij de Nationale Ombudsman.	Aanbevolen wordt: • Richt een incidentmanagementproces in om inzicht te krijgen in de belangrijkste beveiligingsincidenten en rapporteer hierover periodiek aan het lijnmanagement. • Herzie en vernieuw het proces van risicomanagement en neem daarin op de risicobereidheid, risicoacceptatie en risicomitigatie om tot de juiste beveiliging van informatie en informatiesystemen te komen. • Leg afspraken over taken en verantwoordelijkheden van medewerkers helder vast ten aanzien van het behalen van informatiebeveiligingsdoelstellingen.	Om de informatiebeveiliging te verbeteren zijn er diverse maatregelen doorgevoerd die in 2020 zijn ingegaan. Zo heeft de Nationale Ombudsman een informatiebeleid ontwikkeld, is eigenaarschap ingekleurd en zijn de verantwoordelijkheden belegd. Ook wordt er een ICT-plan opgesteld dat helpt om de juiste keuzes te maken m.b.t. planning en noodzaak. De Nationale Ombudsman heeft in 2019 een Europese aanbesteding uitgevoerd en een partij geselecteerd die hierbij gaat helpen. Ondertussen is een onderzoek uitgevoerd en is bekend wat de Nationale Ombudsman moet doen om te voldoen aan de Baseline Informatiebeveiliging Overheid.	Om de informatiebeveiliging te verbeteren zijn er diverse maatregelen doorgevoerd die in 2020 zijn ingegaan. De Nationale Ombudsman gaat hier gestructureerd mee aan de slag. De capaciteit is inmiddels opgehoogd en verwacht wordt dat dit aan de verbetering gaat bijdragen. De belangrijkste aanbeveling is de verbetering van de processen en ook hier verwacht de Nationale Ombudsman in 2020 een aanzienlijke verbetering. De planning is dat alle adviezen van de ARK eind 2020 grotendeels of helemaal zijn geïmplementeerd.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Toelichting op aanbeveling AR	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Buitenlandse Zaken	Informatiebeveiliging	De aanbevelingen uit het VO 2018 zijn nog niet afgerond. In 2019 bestaan op de 4 aandachtsgebieden van informatiebeveiliging (IB) nog steeds risico's, met name op het gebied van accreditaties. Het ministerie voldoet voor het derde jaar op rij niet aan de binnen de rijksoverheid geldende regelgeving voor IB. De rekenkamer kwalificeert de IB bij BZ als een ernstige onvolkomenheid.	• De aanbeveling uit het VO 2018 om de achterstand op de accreditaties in te halen wordt onderstreept; in aanvulling op die aanbevelingen uit het VO 2018 wordt ook aanbevolen: • Zorg dat de documentatie, zoals de visie op IB op het juiste niveau wordt geformaliseerd om aansturing op, en steun voor IB in overeenstemming met organisatie-eisen en relevante wet- en regelgeving te krijgen. • Zorg voor een overkoepelend jaarplan voor IB met de vertaling naar projecten met daarin opgenomen budget, bemensing en benodigdheden. • Beschrijf het risicomanagementproces met de belangrijkste elementen zoals beheersing, acceptatie en eigenaarschap van risico's .	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 2020 te realiseren. Met dat doel wordt tevens in verstevigde sturing en in additionele personele capaciteit voorzien. Het doel is de voor een adequate informatiebeveiliging vereiste documentatie en processen beschreven en geformaliseerd te hebben. Het huis moet orde. Voor accreditaties wordt er conform planning in voorzien dat er in 2020 voor 3 systemen een FATO wordt behaald en dat de accreditaties van de EU en NATO systemen volledig zijn afgerond. Daarnaast zal voor het resterende deel van 2020 en voor 2021 een overkoepelend jaarplan voor de informatiebeveiliging worden opgesteld.	• In opdracht van PSG is de projectorganisatie ingericht en opgeschaald. Ook zijn betrokken externe stakeholders die noodzakelijk zijn voor de voortgang zoals SSC-ICT, NBV en de ADR direct betrokken en is commitment gekregen op het plan van aanpak. • De afgelopen maanden zijn op de aandachtsgebieden governance, organisatie, incidentmanagement, risicomanagement resultaten geboekt conform het plan van aanpak. • Ook op het vlak van accreditaties zijn resultaten geboekt. In de planning en uitvoering van de activiteiten voor de accreditaties is de afhankelijkheid van derde partijen in combinatie met de Corona-crisis merkbaar. De voorziene en georganiseerde escalatieladders worden waar nodig ingezet. BZ onderhoudt hierbij actief contacten met de ADR en AR.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Toelichting op aanbeveling AR	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Binnenlandse Zaken en Koninkrijksrelaties	Informatiebeveiliging, Rijksdienst Caribisch Nederland	RCN/SSO-CN heeft in 2019 vervolgstappen gezet om de informatiebeveiliging te verbeteren. Geconstateerd wordt dat er in 2019 op 3 van de 4 aandachtsgebieden risico's bestaan.	Aanvullend op het VO2018 wordt aanbevolen: • Leg afspraken over taken en verantwoordelijkheden voor het behalen van informatiebeveiligingsdoelstellingen helder vast. Dit zorgt ervoor dat de continuïteit van de werkzaamheden voor informatiebeveiliging door de sleutelfunctionarissen, zoals de Chief Information Security Officer (CISO), worden geborgd. • Zorg naast de inrichting van het risicomanagement voor informatiebeveiliging ook voor de monitoring op deze risico's, zodat deze voldoende worden beheerst en op verantwoorde wijze kunnen worden geaccepteerd, met als doel om informatie en informatiesystemen voldoende te beveiligen.	Verdere verbeteringen zijn ondergebracht in projecten en de reguliere PDCA-cyclus. Het vervolgplan is vertaald naar verbeteringen die projectmatig opgepakt worden.	In 2019 zijn de urgente risico's weggenomen. Verdere verbeteringen zijn ondergebracht in projecten en reguliere werkzaamheden. De specifieke Caribische context blijft onvermijdelijk beperkingen stellen. Dit uit zich onder meer in problemen bij het werven en vasthouden van gekwalificeerd personeel. Binnen SSO-CN is een gebruikerstafel actief waar met dienstafnemers gesproken wordt over gemeenschappelijke eisen en wensen. Specifiek voor informatiebeveiliging is in 2019 begonnen om te inventariseren welke behoeften er zijn binnen RCN. In 2020 wordt dit verder gecontinueerd. SSO-CN herkent zich daarmee niet in het beeld dat het zijn positie als schakel in de informatiebeveiliging keten niet onderkent. In 2020 zal door het nader analyseren van risico's en het inrichten van een controlestructuur verder invulling gegeven worden aan het inzichtelijk maken van risico's. Daarnaast bevindt SSO-CN zich in de afrondende fase om afspraken te maken met SSC-ICT over het inrichten van de noodzakelijke monitoring en control (Security Operations Center (SOC)). In samenspraak tussen beleidsadviseurs, SSO-ICT Dienstverlening en de CISO zal nader invulling gegeven worden hoe de taken en verantwoordelijkheden benoemd en verdeeld moeten worden.
Binnenlandse Zaken en Koninkrijksrelaties	Informatiebeveiliging, BZK kerndepartement	Geconstateerd wordt dat in 2019 stappen zijn gezet om de aanbevelingen uit het VO 2018 op te volgen, maar dat over 2019 nog steeds risico's bestaan op 3 van de 4 aandachtsgebieden van IB: governance, risico- en incidentmanagement.	Aanvullend op het VO 2018 worden de volgende aanbevelingen gedaan: • Geef in de praktijk invulling aan naleving van het opgestelde informatiebeveiligingsbeleid. • Zorg naast de inrichting van risicomanagement ook voor de monitoring en aansturing vanuit centraal niveau (vanuit het kerndepartement) richting de decentrale dienstonderdelen.	Allereerst wordt het CIO-stelsel binnen BZK versterkt door tussen CIO-BZK en de CIO's van de onderdelen van BZK, formele werkafspraken te maken. Gezien de diversiteit van de taakgebieden en het applicatielandschap bij de uitvoeringsorganisaties, wordt niet ingezet op verdere centralisatie. De CISO's spelen bij de advisering over, en het toezicht op naleving van de werkafspraken een belangrijke rol, zowel bij het kerndepartement als bij de onderdelen van BZK.	Het CIO-stelsel is binnen BZK versterkt door tussen CIO BZK en de CIO's van de onderdelen van BZK formele werkafspraken te maken. Daarnaast is de tweede lijn adviesrol versterkt en wordt er sterker gestuurd op naleving beleidskaders IB en privacy. Periodiek (elke vier maanden) wordt de voortgang van de werkafspraken besproken. Voor het onderwerp IB & Privacy zijn de werkafspraken gebaseerd op het vastgestelde beleidskader. De gesprekken zullen voor het onderwerp IB & Privacy worden voorbereid door de CISO-BZK en de CISO van het onderdeel. Hierbij zien we dat bij sommige onderdelen de interne sturing versterkt moet worden.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Toelichting op aanbeveling AR	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Binnenlandse Zaken en Koninkrijksrelaties	Beveiliging IT-componenten SSC-ICT	Het IT-beheer bij SSC-ICT is nog niet op orde. Dit geldt met name voor de beveiliging van componenten en het gebruikersbeheer. In 2019 heeft SSC-ICT voortgang gerealiseerd in relatie tot de aanbevelingen uit het VO 2018, maar voor een deel van de systemen voldoet de beveiliging van componenten nog niet aan de daaraan gestelde eisen.	Aanbevolen wordt: • de beveiliging van componenten bij SSC-ICT verder te verbeteren volgens het transitieplan vanuit de per 1 januari 2020 opgezette tijdelijke werkorganisatie; • te streven naar concrete resultaten, waarbij de tekortkomingen vanuit een gestructureerde eenduidige aanpak over de systemen heen opgelost worden.	Door SSC-ICT wordt ingezet op een breed transitietraject, waarbij de beveiliging van componenten en het gebruikersbeheer integraal worden meegenomen.	Door SSC-ICT wordt ingezet op een breed transitietraject, waarbij de beveiliging van componenten en het gebruikersbeheer prominent worden meegenomen. SSC-ICT beseft zich uiteraard dat er nog veel werk moet worden verzet en richt zich in 2020 en verder op het oplossen van de tekortkomingen en het uitvoeren van structurele verbeteringen. In driemaandelijkse werkpakketten worden bevindingen opgelost naast het nieuwe beheerplatform dat fundamenteler voor een oplossing gaat zorgen.
Binnenlandse Zaken en Koninkrijksrelaties	Gebruikersbeheer SSC-ICT	Geconstateerd is dat, net als bij de beveiliging van IT-componenten, ook hier werk is verzet, maar er in 2019 toch nog tekortkomingen zijn, zoals ontbrekende autorisatiematrices en de aanwezigheid van beheeraccounts met te ruime rechten.	Aanbevolen wordt: • het gebruikersbeheer bij SSC-ICT te optimaliseren volgens het transitieplan vanuit de per 1 januari 2020 opgezette tijdelijke werkorganisatie. • streef daarbij naar concrete resultaten, waarbij de tekortkomingen vanuit een gestructureerde, eenduidige aanpak over de systemen heen opgelost worden.	Door SSC-ICT wordt ingezet op een breed transitietraject, waarbij de beveiliging van componenten en het gebruikersbeheer integraal worden meegenomen.	Door SSC-ICT wordt ingezet op een breed transitietraject, waarbij de beveiliging van componenten en het gebruikersbeheer prominent worden meegenomen. SSC-ICT beseft zich uiteraard dat er nog veel werk moet worden verzet en richt zich in 2020 en verder op het oplossen van de tekortkomingen en het uitvoeren van structurele verbeteringen. In driemaandelijkse werkpakketten worden bevindingen opgelost naast het nieuwe beheerplatform dat fundamenteler voor een oplossing gaat zorgen.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Toelichting op aanbeveling AR	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Binnenlandse Zaken en Koninkrijksrelaties	IT-beheer P-direkt systemen	Bij de twee P-Direkt-systemen zijn nog risico's voor wat betreft de vertrouwelijkheid en de betrouwbaarheid van gegevens van 130.000 ambtenaren. Ook bestaan er risico's voor wat betreft de juistheid van de salarisbetalingen. Overigens zijn dit nadrukkelijk risico's; over 2019 hebben wij geen gevallen aangetroffen van daadwerkelijke incidenten.	SSC-ICT zal de beveiliging van de IT-infrastructuur waarop P-Direkt draait verder moeten verbeteren. Dit geldt met name voor het controleren op en het monitoren van kwetsbaarheden. Tevens zal SSC-ICT het gebruikersbeheer op orde moeten brengen. Dit geldt met name voor de naleving van procedures voor de toegangsrechten voor gebruikers. P-Direkt zal het productiebeheer bij PDS-DH moeten verbeteren. Bij het gebruikersbeheer en het wijzigingenbeheer zal P-Direkt met name de correcte naleving van procedures moeten waarborgen.	De ingezette verbeteracties op het gehele productiebeheer hebben er in 2019 reeds toe geleid dat het aantal bevindingen hierop sterk is afgenomen. Er worden al maatregelen getroffen om het PDS-DH op orde te brengen. In het maandelijks tactisch overleg met SSC-ICT bewaakt P-Direkt de voortgang op de verbeterpunten van de P-Direkt systemen.	De procedures die betrekking hebben op de beheerprocessen productiebeheer, wijzigingsbeheer en gebruikersbeheer zijn aangescherpt en er zijn verbetermaatregelen ingevoerd. Per 1 januari 2020 zijn het Individueel Keuzebudget (IKB) en de Wet Normalisering Rechtspositie Ambtenaren (WNRA) geïmplementeerd. In de eerste maanden van 2020 hebben deze veranderingen veel effect gehad op de dienstverlening van P-Direkt, waarbij de prioriteit is gelegd op de correcte uitbetaling van de salarissen. Hierdoor worden er naar verwachting opnieuw bevindingen voor de beheerprocessen vastgesteld voor specifiek deze maanden. Als extra maatregel wordt naast versterkte interne controle ingezet op het begin dit jaar gestarte cultuurveranderingstraject bij P-Direkt. De voortgang wordt op Directie niveau en in de managementgesprekken met de eigenaar gevolgd. We verwachten overigens dat de ADR in het kader van de wettelijke taak ook over dit jaar opnieuw zal concluderen dat de salarisverwerking correct is verlopen. De voortgang op de verbeterpunten van de P-Direkt systemen worden in het maandelijks tactisch overleg met SSC-ICT bewaakt.
Binnenlandse Zaken en Koninkrijksrelaties	IT-beheer, Rijksbreed	De resultaten van ingezette acties uit 2019 moeten nog zichtbaar worden in 2020 en later. Ook dient de minister van BZK aandacht te schenken aan de aanvullende elementen uit een GRC-kader, zoals de inbedding van het IT-beheer in een bredere strategie, om het gehele IT-beheer bij de rijksdienst structureel op orde te krijgen.	Aanbevolen wordt: • in navolging van vorig jaar 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). • één generiek Governance Risk en Compliance (GRC)-kader te ontwikkelen met gestandaardiseerde minimum beheersingsmaatregelen voor de IT-organisaties binnen de rijksoverheid.	De minister zal opvolging doen dat departementen een opdrachtgevende rol opnemen in relatie tot de behoefte/noodzaak tot uniformiteit en standaardisatie bij de SSO's om zo een goede basis voor IT-beheer te realiseren. Aanvullend zal de minister onderzoeken in hoeverre de aanvullende elementen uit het GRC-kader in deze fase van ontwikkeling het IT-beheer naar een hoger plan kunnen brengen en in hoeverre deze elementen reeds in lopende initiatieven geadresseerd worden.	Op korte en middellange termijn wordt ingezet op onderzoek naar de mate van implementatie van kaders en volgen van de status en de daaruit volgende benodigde actie. Het verduidelijken van het bestaan en de samenhang van relevante kaders krijgt hierbij aandacht. Ook wordt onderzocht hoe om wordt gegaan met aanvullende GRC elementen in afstemming met AR. Het creëren van bewustzijn en betrokkenheid bij klantorganisaties / opdrachtgevers / eigenaren m.b.t. hun rol bij verantwoording en risico inschatting wordt gestimuleerd. Evaluatie en optimalisatie van verantwoordingsprocessen o.b.v. ADR onderzoek en analyse CIO Rijk zijn daarbij te hanteren instrumenten.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Toelichting op aanbeveling AR	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Onderwijs Cultuur en Wetenschap	Informatiebeveiliging kerndepartement	De minister van OCW heeft in 2019 de aanbevelingen uit het verantwoordingsonderzoek 2018 nog niet afgerond of niet opgevolgd. Op alle vier de aandachtsgebieden blijven risico's bestaan.	De eerdere aanbevelingen worden aangevuld met de volgende: • Zorg voor voldoende aandacht voor de informatiebeveiliging bij het senior management door de visie op informatiebeveiliging en het informatiebeveiligingsbeleid daar te bespreken en door hen te laten formaliseren. • Stel een jaarplan op waarin een doorvertaling wordt gemaakt naar projecten waarin budget, bemensing en benodigdheden voor informatiebeveiliging zijn opgenomen. • Zorg ervoor dat de processen rondom risicomanagement en incidentmanagement helder zijn en dat de rollen, verantwoordelijkheden en taken van medewerkers helder zijn beschreven.	De verbeteracties op Informatiebeveiliging worden o.l.v. een door de SG ingestelde projectgroep opgepakt. De projectgroep pakt alle aanbevelingen op en kijkt daarbij nog eens extra naar de organisatie en sturing van informatiebeveiliging, privacy en veiligheid binnen OCW.	Er is en wordt veel gedaan om informatiebeveiliging (IB) met het senior management te bespreken. Recent is de periodieke rapportage IB-beeld besproken met het MT-OCW. De IB-visie is reeds door het MT-OCW vastgesteld en de herijking en vaststelling van het IB-beleid volgt later dit jaar. De ingestelde projectgroep ligt op schema om dit jaar ook nog de procedures voor risico- en incidentmanagement af te ronden. De vorming van een expert-team, ten slotte gaat er voor zorgen dat risico's ook op decentraal niveau in kaart gebracht gaan worden. Alle acties en communicatie daarover samen dragen ook sterk bij aan een verhoogde awareness binnen de hele organisatie.
Onderwijs Cultuur en Wetenschap	Informatiebeveiliging DUO (autorisatiebeheer)	DUO heeft in 2019 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 in 2020 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.	De periodieke controles worden uitgevoerd en uitkomsten (lees intrekken van autorisaties) verwerkt. De processen voor het beheren van autorisaties van medewerkers zijn aangescherpt en van bijna elk systeem is beschreven welke autorisaties er zijn. Het korte termijn spoor loopt derhalve op schema. Het lange termijn spoor heeft dit jaar nog niet de voortgang die verwacht was. Oorzaken hiervoor zijn het moeizame en langdurige traject voor het aantrekken van een implementatiepartner en productieverlies door corona.
Defensie	IT-beheer	Mocht de staatssecretaris besluiten het programma Grensverleggende IT (GrIT) toch door te zetten of in een aangepaste vorm door te zetten, dan zal zij om het programma GrIT goed te kunnen aansturen de totale kosten, planning en personele capaciteit ervan opnieuw in beeld moeten brengen. Sinds 2017 is gewezen op het belang van deze informatie.	Aanbevolen wordt om een businesscase met een meerjarige kosten-batenanalyse van het programma GrIT op te stellen, inclusief de totale kosten, de planning en de benodigde personele capaciteit.	De aanbevelingen van de rekenkamer worden overgenomen.	Verloopt volgens planning. De business case is nagenoeg gereed.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Toelichting op aanbeveling AR	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Defensie	Autorisatiebeheer	In 2019 zijn er opnieuw onvolkomenheden geconstateerd voor het 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 worden overgenomen.	• Voor zowel het P als het M domein geldt dat alle autorisatiematrices zijn vastgesteld. • Beheerrechten inregelen op basis van actuele en juiste mandaatregisters: loopt op schema. Het gaat hier om het formaliseren van matrices voor de beheerorganisatie. • achteraf of continu vast te stellen dat het toekennen, muteren en intrekken van toegangsrechten conform de vastgestelde autorisaties zijn uitgevoerd: Actualisatie van de matrices is per kwartaal vereist. De tweede ronde controles wordt begin oktober afgerond. Als gevolg van beperkte capaciteit blijven functiescheidingsconflicten vooralsnog een feit.
Infrastructuur en Waterstaat	Informatiebeveiliging	Risico's zijn geconstateerd op 3 van de 4 aandachtsgebieden van informatiebeveiliging: inrichting van de organisatie, risicomanagement en incidentmanagement.	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 wordt overgenomen binnen de kaders die door de minister van BZK gegeven zullen worden met het Besluit op het CIO stelsel. Dit zal verwerkt worden in het O&F rapport van de nieuwe directie CDIV, dat momenteel wordt opgesteld.	Risicomanagement is een van de onderwerpen uit het werkprogramma voor informatiebeveiliging van IenW om centraal volwassenheidsniveau 3 te bereiken. Hier binnen zal voor eind 2020 een kader voor risicomanagement zijn gerealiseerd.
Infrastructuur en Waterstaat	Lifecycle management	Geconcludeerd wordt dat de CIO onvoldoende inzicht heeft in het hele ICT-landschap van het ministerie. Het inzicht beperkt zich tot grote ICT-projecten en programma's; er zijn geen kaders of processen voor applicatieportfoliomanagement op basis waarvan de CIO dit inzicht kan krijgen. Hierdoor kan de CIO niet planmatig sturen op beheer en onderhoud van het hele ICT-landschap waarmee risico's voor het Ministerie van IenW worden beheerst en waarmee kritieke ICT-applicaties gedurende hun hele levensduur operationeel en functioneel worden gehouden. Een dergelijk plan is nodig om te kunnen sturen op de totstandkoming van robuuste en wendbare ICT.	Aanbevolen wordt: • het huidige decentrale CIO-stelsel te herzien en opnieuw in te richten; meer capaciteit beschikbaar te stellen bij het centrale CIO-office. • IenW-brede kaders te ontwikkelen over de vastlegging en het onderhoud van de applicaties in het ICT-landschap inclusief het lifecycle management; • een integraal plan voor beheer en onderhoud van het hele ICT-landschap te maken; • de activiteiten door het centrale CIO-office in nauwe samenwerking met de CIO's van de onderdelen uit te voeren om de kennis en ervaring van de onderdelen als Rijkswaterstaat te hergebruiken.	IenW zal in de komende tijd actie gaan nemen om een plancyclus voor ICT-onderhoud, heldere kaders en een koppeling met de begroting waar te maken. Ook zal de minister gaan inzeten om meer centraal inzicht en grip te krijgen op de belangrijkste ICT risico's voor de continuïteit van de primaire processen.	IenW is stappen aan het zetten naar een concernbrede sturing op i. In nauwe samenwerking met de CIO's van de diensten wordt gekeken hoe i meer en beter in de departementale besluitvorming kan worden betrokken. Ook bij de verbetering van het concernbrede inzicht in projecten en applicaties worden stappen gezet. Daarbij wordt gebruik gemaakt van wat de diensten aan inzicht en instrumenten hebben. Een goede sturing op beheer en onderhoud van het ICT-landschap begint immers op het niveau van de dienst. Tevens is een nieuwe concerndirectie IV in opbouw die werkt aan een IenW brede ICT-portfolio, met het doel om inzicht en overzicht te creëren. Ook wordt nagedacht over een vernieuwing van het CIO-stelsel binnen IenW en dat waar nodig te verbeteren. Dit traject is mede afhankelijk van het Besluit CIO-stelsel dat BZK aan het voorbereiden is en dat moet leiden tot een versterking van de positie van de (departementale) CIO's.

Organisatie	Categorie onvolkomenheid	Toelichting op onvolkomenheid	Toelichting op aanbeveling AR	Maatregel(en) vanuit departement	Stand van zaken maatregelen
Volksgezondheid Welzijn en Sport	Informatiebeveiliging	In 2019 is geconstateerd dat er onvoldoende opvolging is gegeven aan de aanbeveling uit 2018 over incidentmanagement en over 2019 dat er zelfs een achteruitgang is in het incidentmanagement. Daarnaast zijn ook risico's geconstateerd op de andere 3 aandachtsgebieden van informatiebeveiliging: bestuur (governance), organisatie-inrichting en risicomanagement.	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 het jaarplan 2020 zijn relevante maatregelen opgenomen, die worden momenteel uitgevoerd. Deze activiteiten worden volgens planning uitgevoerd.
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: • de aanbevelingen uit de notitie van het CIO-office uit mei 2019 uit te werken, acties te concretiseren en uit te voeren; met name op het versterken van inzicht in de ICT-applicaties, de levensfase en de risico's. • ministeriebrede kaders te ontwikkelen voor het onderhouden van een eenduidige en gestandaardiseerde vastlegging van het ICT-applicatieportfolio inclusief het lifecycle management.	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.	Er wordt gewerkt aan een plan van aanpak waarin de afspraken en de uitwerking van het applicatie life cycle management verder worden vormgegeven.