Algemene Rekenkamer

BEZORGEN
Voorzitter van de Tweede Kamer
der Staten-Generaal
Prinses Irenestraat 6
2595 BD DEN HAAG

Postbus 20015
2500 EA Den Haag
070 342 43 44
voorlichting@rekenkamer.nl
www.rekenkamer.nl

datum 9 juni 2026

betreft Beantwoording vragen Tweede Kamer over het Verantwoordingsonderzoek 2025 vanuit de vaste commissie Digitale Zaken

Geachte heer Van Campen,

Hierbij bieden wij u onze antwoorden aan op de door de Vaste Kamercommissie van Digitale Zaken gestelde vragen over het Verantwoordingsonderzoek Ministerie van ministerie van Justitie en Veiligheid (Kamerstuk 36945-VI-2), ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Kamerstuk 36945-VII-2) en het ministerie van Economische Zaken ministerie (Kamerstuk 36945-XIII-2), Rapporten bij het Jaarverslag 2025.

Algemene Rekenkamer

Pieter Duisenberg,
president

Mark Smolenaars,
secretaris

ons kenmerk 166432

bijlage(n)

Antwoorden Algemene Rekenkamer bij vragen van de Tweede Kamer over het *Verantwoordingsonderzoek ministerie van Justitie en Veiligheid (36945-VI-2), Rapport bij het Jaarverslag 2025*

Vraag 1
Welke normen hanteert de Algemene Rekenkamer om vast te stellen of een ministerie voldoende maatregelen neemt tegen het risico op uitval door verouderde digitale systemen?

IT-systemen en -processen van de overheid moeten goed werken, goed onderhouden worden en op tijd vernieuwd en vervangen worden. Om verrassingen en uitval van verouderde systemen te voorkomen, moet elke overheidsorganisatie hiervoor een proces hebben. Dit heet in de IT-wereld lifecyclemanagement. Ministers zijn ervoor verantwoordelijk dat dit binnen een ministerie als geheel op orde is. De Algemene Rekenkamer heeft voor IT lifecyclemanagement een apart beoordelingskader. Het is gebaseerd op wet- en regelgeving en internationaal geaccepteerde IT-raamwerken. Met het kader toetst de Algemene Rekenkamer of een minister inzicht heeft in de IT-systemen, plannen voor onderhoud en vernieuwing maakt en uitvoert, de resultaten meet en indien nodig bijstuurt op het IT lifecyclemanagement. Het beoordelingskader is in meer detail beschreven op de website van de Algemene Rekenkamer.
In het Verantwoordingsonderzoek 2025 heeft de Algemene Rekenkamer het beoordelingskader niet gebruikt om vast te stellen of ministers voldoende doen aan alle stappen binnen IT lifecyclemanagement. Wel onderzochten we bij het ministerie van Financiën specifiek de voortgang van de vervanging van verouderde systemen ('IT-legacy') bij de Belastingdienst.

Vraag 2
Ziet u bij het ministerie van Justitie en Veiligheid (JenV) een verhoogd risico op ICT-kwetsbaarheden ten opzichte van andere departementen?

In de Staat van de Rijksverantwoording 2025 maken wij gebruik van indicatoren om de resultaten van geld en beleid in kaart te brengen. Een zorgwekkende trend is dat Nederland op de National Cyber Security Index is gezakt van de 20e naar de 36e plaats. Deze index meet aan de hand van verschillende indicatoren in hoeverre landen paraat zijn om cyberdreigingen en -incidenten te beheersen.
Wij hebben niet onderzocht hoe departementen onderling scoren op ICT-

kwetsbaarheden. Bijgevolg is niet in kaart gebracht welke departementen – mede op basis van hun aard en omvang – een hoger cyberrisico lopen dan andere.

Vraag 3
Heeft u in uw onderzoek inzicht gekregen in de aard en omvang van de ICT-inbreuk bij het OM? Kunt u globaal toelichten over wat de inbreuk heeft betekend voor de bedrijfsvoering van het OM?

De minister heeft aan uw Kamer gerapporteerd over de aard van de ICT-inbreuk bij het OM en de omvang van de schade. Deze openbare informatie hebben wij onder andere gebruikt om inzicht te krijgen in de situatie.
In rapportages aan uw Kamer en in de beantwoording van Kamervragen heeft de minister toegelicht wat de inbreuk heeft betekend voor de bedrijfsvoering van het OM. Dit komt onder meer naar voren in de brief van 21 november 2025, getiteld ‘Antwoorden Kamervragen over de gevolgen van de hack bij het OM op de bedrijfsvoering’.

Vraag 4
Is na het afhandelen van de ICT-inbreuk enig achterstallig werk, zoals het afgeven van voor VOG-relevante informatie, ingehaald?

Hier hebben wij in het kader van ons verantwoordingsonderzoek 2025 geen onderzoek naar gedaan.

Vraag 5
Kunt u nader toelichten welke aanbevelingen u heeft om de drie geconstateerde ICT-gerelateerde onvolkomenheden op te lossen?

In ons rapport bij het jaarverslag 2025 van het ministerie van Justitie en Veiligheid hebben wij twee ICT-gerelateerde onvolkomenheden opgenomen. Dit betreft 'IT-beheer DJI' en 'Accreditaties IT-systemen en opvolging verbeterpunten beveiligingstesten'. De eerder genoemde ICT-inbreuk bij het OM is niet als formele onvolkomenheid geclassificeerd, maar wordt in het rapport specifiek aangehaald om de noodzaak van een grotere digitale weerbaarheid tegen cyberaanvallen te benadrukken.
In de bestuurlijke reactie op ons verantwoordingsonderzoek 2025 licht de minister de maatregelen toe om deze onvolkomenheden te verhelpen. Tijdens het

verantwoordingsonderzoek 2026 zullen wij de effectiviteit van deze maatregelen beoordelen.

Vraag 6
Hoe groot is de achterstand in de accreditatieverlening?

In ons rapport bij het jaarverslag melden wij dat de achterstand in de accreditatieverlening over 2025 onverminderd groot bleef. In juli 2025 was pas 12% van de door het ministerie als hoog risico aangemerkte systemen geaccrediteerd. Gezien de door de minister zelf gepresenteerde voortgang, hebben wij de achterstanden niet verder onderzocht.

Vraag 7
Laat de achterstand in de accreditatieverlening zich alleen uitleggen door een gebrek aan personeel? Welke factoren spelen mogelijk nog een rol?

In ons rapport staat dat de minister een personeelstekort aanwijst als belangrijkste oorzaak van de accreditatieachterstand; wij hebben in ons verantwoordingsonderzoek geen andere mogelijke factoren onderzocht.

Vraag 8
Welke voordelen heeft het decentraal beleggen van de informatiebeveiliging bij 70 JenV-organisaties? Welke risico's kent dit stelsel?

Het decentraal beleggen van informatiebeveiliging biedt onder meer ruimte voor maatwerk en vergroot het eigenaarschap binnen afdelingen. Belangrijke risico's zijn bijvoorbeeld een versnipperd integraal overzicht en een inconsistent kwaliteitsniveau van de beveiliging. In ons verantwoordingsonderzoek hebben wij de kansen en risico's van dit decentrale stelsel overigens niet nader in kaart gebracht.

Vraag 9
Merkt u in de praktijk dat de mate van toezicht tussen organisaties (aanzienlijk) verschilt? Kunt u dit concreet maken?

In ons verantwoordingsonderzoek hebben wij de mate van toezicht door de minister op de afzonderlijke organisaties en de eventuele verschillen daartussen niet onderzocht.

Vraag 10
Welke aanbevelingen heeft u voor de minister en de Kamer om het inzicht in de beveiliging van de IT-systemen van JenV te vergroten?

Wij bevelen aan dat de minister de oorzaken van de geconstateerde onvolkomenheden blijft aanpakken. Het is aan uw Kamer om de minister te bevragen over de voortgang hiervan.

Vraag 11
Weet u of en hoe het iTrechter-systeem wordt gecontroleerd op discriminatoire bias? Als dit gebeurt, heeft u ook deze analyses tot u genomen?

We maken onderscheid tussen directe en indirecte discriminatie. Voor de profielen die we onderzocht hebben, onderbouwt de politie met objectieve informatie welke kenmerken ze gebruiken. Dit mitigeert het risico op directe discriminatie. Voor wat betreft indirecte discriminatie, heeft de politie geen mitigerende maatregelen getroffen.

Vraag 12
Hoe groot acht u het risico voor onrechtmatige inbreuk op privacy door het gebruik van iTrechter?

Op basis van ons onderzoek achten wij het algemene privacyrisico deels beheerst. De politie heeft voor iTrechter geen gegevensbeschermingseffectbeoordeling (GEB) uitgevoerd. Ondanks het ontbreken van een GEB, mitigeert de politie wel actief privacyrisico's door de inzet van profielen te onderbouwen en deze onderbouwingen te laten beoordelen door de officier van justitie. Wel ontbreken er elementen in de werkwijze.

Vraag 13
Hoe heeft de Algemene Rekenkamer in het onderzoeksproces de technische werking van de sensortechnologie (zoals ANPR-camera's) gevalideerd ten opzichte van de juridische kaders voor privacy?

U vraagt hoe de Algemene Rekenkamer de technische werking van de sensortechnologie (zoals ANPR-camera's) heeft gevalideerd ten opzichte van de juridische kaders voor privacy. Daar hebben we geen specifiek onderzoek naar

verricht. Wij hebben in het verantwoordingsonderzoek 2025 alleen de risicobeheersing voor iTrechter zelf onderzocht.

Vraag 14
Bij hoeveel profielen is het gebruiken van persoonsgegevens onvoldoende gemotiveerd door de politie?

Bij ongeveer de helft van de onderzochte profielen is de subsidiariteit en noodzakelijkheid van de gebruikte persoonsgegevens niet expliciet onderbouwd. Wel zijn alle profielen gemotiveerd met een duidelijk doel.

Vraag 15
Heeft de politie uitgelegd waarom zij geen inzage kan geven in de beveiliging van iTrechter? Wat was de redenering?

U vraagt naar reden waarom er door de politie niet altijd inzage in de beveiliging van iTrechter kon worden gegeven. De software en onderliggende IT-componenten die voor de iTrechter worden gebruikt zijn deels verouderd waardoor de implementatie van gangbare IT-beveiligingsprincipes niet altijd aantoonbaar kan worden gemaakt. De politie is hiervan op de hoogte en is voornemens om de iTrechter te vervangen voor een moderne applicatie zie ook alinea lifecycle management pagina 62 van het Verantwoordingsonderzoek 2025 bij het Ministerie van Justitie en Veiligheid (VI).

Antwoorden Algemene Rekenkamer bij vragen van de Tweede Kamer over het *Verantwoordingsonderzoek ministerie van Binnenlandse Zaken en Koninkrijksrelaties* (36945-VII-2), *Rapport bij het Jaarverslag 2025*

Vraag 16
Wanneer zou er sprake zijn van een weerbare digitale werkplek? Aan welke criteria zou voldaan moeten worden? Kunt u dit nader toelichten?

We noemen een digitale werkplek weerbaar als deze onder alle omstandigheden beschikbaar is en alleen toegankelijk is voor de juiste personen. Als er iets misgaat, wordt dat snel opgemerkt en direct hersteld.
Om de beschikbaarheid en het herstelvermogen van een digitale werkplek in het Verantwoordingsonderzoek 2025 te kunnen toetsen hebben we criteria gehanteerd.

Criteria voor beschikbaarheid: risicoanalyse, evaluatie van het beveiligingsontwerp, praktische werking beveiligingsmaatregelen, continue monitoring en opvolging van bevindingen.
Criteria voor herstelvermogen: reactiestructuur, crisismanagementplan, praktijktesten, opleiding en trainingen en evaluatie grote incidenten en crises.
Naast de digitale werkplek van SSC-ICT hebben we ook de digitale werkplek van DICTU onderzocht, dat onder de minister van EZ valt. Op basis van ons onderzoek daarnaar is DICTU voldoende weerbaar en voldoet dus aan beide aspecten.

Vraag 17
Heeft u kennisgenomen van het (ongeredigeerde) onderzoek van de Privacy Company bij SSC-ICT en dit meegewogen in uw analyse (Kamerstuk 29362-399)?

U vraagt naar het onderzoek van de Privacy Company naar significante privacyrisico's en datalekken binnen de nieuwe rijksbrede IT-werkplek DWR 2.0 bij SSC-ICT. Dit onderzoek hebben we in het Verantwoordingsonderzoek 2025 niet meegewogen in onze analyse van de weerbaarheid van de digitale werkplekken van SSC-ICT. De scope van ons onderzoek betrof de huidige digitale werkplek die door SSC-ICT wordt geleverd: DWR Next en niet de digitale werkplek die SSC-ICT momenteel ontwikkelt: DWR 2.0.

Vraag 18
Heeft u ook de mate van digitale autonomie van de digitale werkplekken van SSC-ICT en DICTU onderzocht? Hoe staat het nu met de ambitie om de Digitale Werkplek Rijk 2.0 (DWR2.0) niet afhankelijk te maken van Microsoft?

U vraagt naar de mate van digitale autonomie van de digitale werkplekken van SSC-ICT en DICTU. We hebben in het Verantwoordingsonderzoek 2025 geen specifiek onderzoek verricht naar de digitale autonomie van de digitale werkplekken. We hebben tijdens het Verantwoordingsonderzoek 2025 wel geconstateerd dat SSC-ICT en DICTU in 2025 gezamenlijk het open source platform Nextcloud van een Duitse leverancier onderzochten. Dit initiatief loopt door in 2026 en kan op langere termijn bijdragen aan meer digitale soevereiniteit.

Vraag 19

Wordt digitale onafhankelijkheid ook tot digitale weerbaarheid gerekend? Hoe belangrijk is het afbouwen van digitale afhankelijkheden voor de continuïteit en veiligheid van de overheids-ICT?

U vraagt of digitale onafhankelijkheid ook tot digitale weerbaarheid wordt gerekend. Ook vaagt u het belang van het afbouwen van digitale afhankelijkheid voor de continuïteit en veiligheid van de overheids-ICT.
We hebben tijdens het Verantwoordingsonderzoek 2025 geen specifiek onderzoek verricht naar digitale afhankelijkheden. Wel hebben we in het Verantwoordingsonderzoek 2025 een opmerking gemaakt over het onderzoek naar het open source platform Nextcloud van een Duitse leverancier (zie ons antwoord op vraag 18).
We vinden dat digitale onafhankelijkheid een positief effect kan hebben op de digitale weerbaarheid (i.e., veiligheid en continuïteit). Naast opzettelijke verstoringen (het laten uitvallen van systemen of het manipuleren of onrechtmatig inzien van informatie) is er een risico op verstoring van de beschikbaarheid van systemen als gevolg van een te sterke afhankelijkheid van één leverancier. Geopolitieke omstandigheden versterken dit risico.

Vraag 20
Heeft u inzicht gekregen in het onderzoek naar autonome cloudvoorzieningen, wat wordt uitgevoerd door DICTU en SSC-ICT? Loopt dit op schema?

In het kader van meer autonomie in infrastructuur en werkplekomgeving, hebben DICTU en SSC-ICT in 2025 gezamenlijk het open source platform Nextcloud onderzocht. De centrale vraag van deze proeftuin was “Kan open source als autonoom alternatief bijdragen aan onze huidige softwarevoorzieningen?” Het opzetten en uitproberen van bepaalde functionaliteiten is volgens DICTU en SSC-ICT goed gelukt. Beide organisaties concludeerden dat er ook zaken waren die verder onderzocht moesten worden zoals de inrichting van onderliggende infrastructuur, privacy en security. DICTU en SSC-ICT spraken het voornemen uit om eind 2025 een vervolg te geven aan de proeftuin. We hebben een vervolgplan ontvangen van begin januari 2026. Hierin staan de te nemen stappen voor het vervolg van het Nextcloud-traject van DICTU en SSC-ICT. De planning, voortgang en behaalde resultaten van dit initiatief vielen buiten de scope van het Verantwoordingsonderzoek 2025 en hebben we daarom niet onderzocht.

Vraag 21
Vindt u de keuze voor één of twee werkplekken bij verschillende organisaties binnen het Rijk een politieke keuze? Wat is voor u de reden om hier geen aanbeveling in te doen?

We vinden de keuze voor één of twee werkplekken bij verschillende organisaties binnen het Rijk een politieke keuze en doen daarover dan ook geen aanbevelingen. Bij het thema prijsstelling hebben we de totstandkoming van de tarieven beoordeeld in relatie tot de digitale werkplek die beide organisaties aanbieden. We constateren een groot verschil in tarieven die de ICT-dienstverleners rekenden voor een digitale werkplek in 2025. Een werkplek (account zonder laptop) kostte bij SSC-ICT ongeveer € 1.500 per jaar en bij DICTU ongeveer € 3.000 per jaar. Wij hebben geen verklaring voor dit tariefverschil.

Vraag 22
Welke aanbevelingen heeft u nog meer, op basis van uw onderzoek, om de digitale autonomie van het Rijk te vergroten?

We hebben tijdens het Verantwoordingsonderzoek 2025 geen specifiek onderzoek verricht naar digitale afhankelijkheden. Op basis van ons onderzoek hebben we dan ook geen specifieke aanbevelingen om de digitale autonomie van het Rijk te vergroten. In ons eerdere Cloud-onderzoek, gepubliceerd op 15 januari 2025, hebben we de aanbeveling gedaan om als Rijk realistische EU-alternatieven te overwegen in combinatie met een uitvoerbare exitstrategie. Er kan namelijk een onwenselijk grote afhankelijkheid ontstaan van dominante en monopolistische leveranciers van buiten de Europese Unie/Europese Economische Ruimte.
Wel hebben we in het Verantwoordingsonderzoek 2025 een opmerking gemaakt over het onderzoek naar het open source platform Nextcloud van een Duitse leverancier (zie ons antwoord op vraag 18). We willen meegeven dat het gezamenlijke initiatief Nextcloud op langere termijn bij kan dragen aan meer digitale soevereiniteit.
In ons onderzoeksrapport “Het Rijk in de cloud” doen we verschillende aanbevelingen om de digitale autonomie van het Rijk te vergroten: https://www.rekenkamer.nl/documenten/2025/01/15/het-rijk-in-de-cloud (pp. 52-56).

Vraag 23

Op basis van welke criteria heeft de Algemene Rekenkamer bepaald dat het open source-platform Nextcloud een relevante casus was voor het toetsen van digitale soevereiniteit?

We hebben in het Verantwoordingsonderzoek 2025 geen specifiek onderzoek verricht naar de digitale autonomie van de digitale werkplekken. We hebben tijdens het Verantwoordingsonderzoek 2025 wel geconstateerd dat SSC-ICT en DICTU in 2025 gezamenlijk het open source platform Nextcloud van een Duitse leverancier onderzochten.
We hebben dus niet op basis van criteria bepaald dat het open source-initiatief Nextcloud een relevante casus was voor het toetsen van digitale soevereiniteit.
Vraag 24
Kunt u meer inzicht bieden in de onrechtmatigheden bij aanbestedingen en contracten van Logius, SSC-ICT en RvIG? Lag dit in de lijn van verwachting?

U vraagt of wij meer inzicht kunnen bieden in de onrechtmatigheden bij aanbestedingen en contracten van Logius, SSC-ICT en RvIG.
In het verantwoordingsonderzoek 2025 BZK hebben we gerapporteerd over de onrechtmatigheden bij deze agentschappen.
De € 80,5 miljoen aan onrechtmatigheden bij Logius hebben betrekking op contracten die al een aantal jaren zijn verlopen. Het verlengen van deze contracten is in strijd met de aanbestedingsregels. Het verlengen van deze contracten is nodig voor het in de lucht houden van verschillende voorzieningen zoals de migratie naar een nieuwe ICT infrastructuur (€ 38,6 mln.), DigiD (€ 15,5 mln.), Digipoort en Globe (€ 24,8 mln) zoals vermeld in het jaarverslag BZK.
SSC-ICT heeft voor € 38,5 miljoen bestellingen geplaatst onder overeenkomsten waarvan de maximale contractwaarden zijn overschreden. Daarnaast heeft SSC-ICT voor € 12,5 miljoen een bestelling geplaatst onder een verlopen overeenkomst. SSC-ICT heeft niet in alle gevallen tijdig geconstateerd dat de prestatieverklaring op tijd is vastgesteld (€ 3,3 mln.).
RvIG heeft € 20,5 miljoen aan onrechtmatigheden. € 16,3 miljoen heeft betrekking op het rechtstreeks afsluiten van een overeenkomst met een leverancier voor de levering en het beheer van de berichtendienst binnen de Gemeentelijke Basisadministratie Persoonsgegevens (GBA) en reisdocumenten.
U vraagt of de onrechtmatigheden liggen in de lijn van verwachtingen. Wij hebben hier geen specifiek onderzoek naar verricht.

Vraag 25

Kunt u concreet maken op welke manier Logius, SSC-ICT en RvIG de aanbestedingswetgeving nu niet naleven? Heeft u voorbeelden van projecten waar dit het geval is geweest?

Zie het antwoord op vraag 24.

Vraag 26
Is er sprake van bevoordeling van één of enkele marktpartijen in de aanbestedingen die worden uitgeschreven op het gebied van ICT?

U vraagt of sprake is van bevoordeling van één of enkele marktpartijen in de aanbestedingen die worden uitgeschreven op het gebied van ICT.
We hebben in ons verantwoordingsonderzoek gerapporteerd over de verschillende onrechtmatigheden en de oorzaken hiervan. In een aantal gevallen hebben wij geconstateerd dat gebruik is gemaakt van verlopen contracten (Logius, zie ook beantwoording van vraag 24) en dat een contract rechtstreeks is afgesloten met één leverancier (RvIG, zie ook beantwoording van vraag 24).

Vraag 27
Komen er relatief veel onrechtmatigheden voor bij ICT-organisaties in het Rijk, ten opzichte van andere organisaties? Zo ja, hoe verklaart u dat?

U vraagt of er relatief veel onrechtmatigheden voorkomen bij ICT-organisaties in het Rijk, ten opzichte van andere organisaties. We hebben dit niet onderzocht. Er zijn verschillende oorzaken die leiden tot niet naleven van de aanbestedingswetgeving (zie beantwoording vraag 24) die niet alleen te relateren zijn aan een ICT-organisatie.

Vraag 28
Welke adviezen heeft u om het inzicht in de ICT-uitgaven van het Rijk structureel beter in kaart te brengen, conform de wens van de Kamer? Waar zitten de grootste onvolkomenheden in de jaarverantwoording?

U vraagt welke adviezen wij hebben om het inzicht in de ICT-uitgaven van het Rijk structureel beter in kaart te brengen. Wij hebben hier geen onderzoek naar gedaan. Het kabinet zet met het programma Toekomst Financiële Administratie in op meer

uniformering van financiële data. We verwachten dat dit ook bijdraagt aan een beter inzicht in de IT-uitgaven van de Rijksoverheid.
U vraagt ook waar de grootste onvolkomenheden in de jaarverantwoording zitten. Wij hebben in ons verantwoordingsonderzoek 2025 BZK gerapporteerd over onze financiële oordelen bij het jaarverslag van BZK. Bij de beantwoording van vraag 24 hebben wij inzicht gegeven in de geconstateerde fouten en onzekerheden van de diverse agentschappen (Logius, SSC-ICT en RvIG).
Rijksbreed zijn er in VO 2025 negen onvolkomenheid op IT-gebied gerapporteerd.

Antwoorden Algemene Rekenkamer bij vragen van de Tweede Kamer over het *Verantwoordingsonderzoek ministerie van Economische Zaken* (36945-XIII-2), *Rapport bij het Jaarverslag 2025*

Vraag 29
Kunt u concreet aangeven welke inkoopprocedures en aanbestedingen u heeft gecontroleerd die niet volgens de wet zijn gedaan, met name die zien op ICT?

Het ministerie heeft een groot deel van de onrechtmatigheden zelf geconstateerd en heeft hierover gerapporteerd in haar bedrijfsvoeringsparagraaf. Voor meer informatie over de betreffende kostensoort verwijzen wij naar het ministerie van Economische Zaken zelf.

Vraag 30
Welke risico's ontstaan er door het niet naleven van de aanbestedingswet en -regelgeving? Kunt u duidelijk maken of u risico's heeft geconstateerd voor het vergroten van de strategische afhankelijkheid van één of enkele ICT-leveranciers?

Het voornaamste risico als de aanbestedingswet- en regelgeving niet worden nageleefd, is dat er geen sprake is van concurrentiestelling. Dat betekent dat bedrijven geen gelijke kans hebben om een opdracht van de overheid te krijgen. Een ander risico is dat de overheid te veel betaalt voor de goederen of diensten.

Vraag 31
Op welke wijze kan de Kamer haar controle op het niet naleven van aanbestedingswet en -regelgeving versterken, met name op het gebied van ICT?

Het ministerie van Economische Zaken heeft een onvolkomenheid voor het inkoopbeheer. Hoewel er sprake is van verbetering, zijn er nog te veel inkopen die niet aan de aanbestedingsregels voldoen. Het gaat bijvoorbeeld om onterecht onderhands gegunde opdrachten en om fouten bij de inhuur van personeel. De Kamer kan de controle hierop versterken door deze onvolkomenheid te monitoren. Hiermee wordt inzicht verkregen in de maatregelen die het ministerie neemt om het inkoopbeheer te verbeteren en om onrechtmatigheden te verminderen.