

36 740 VI Jaarverslag en slotwet Ministerie van Justitie en Veiligheid 2024

36 740 VII Jaarverslag en slotwet Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2024

36 740 XIII Jaarverslag en slotwet Ministerie van Economische Zaken en Klimaat 2024

Nr. 6 Lijst van vragen en antwoorden
Vastgesteld 10 juni 2025

De vaste commissie voor Digitale Zaken heeft een aantal vragen voorgelegd aan de Algemene Rekenkamer over de brief van 21 mei 2025 inzake het rapport Resultaten verantwoordingsonderzoek 2024 bij het Ministerie van Justitie en Veiligheid (Kamerstuk 36 740 VI, nr. 2), over het rapport Resultaten verantwoordingsonderzoek 2024 bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Kamerstuk 36 740 VII, nr. 2) en over het rapport Resultaten verantwoordingsonderzoek 2024 bij het Ministerie van Economische Zaken (Kamerstuk 36 740 XIII, nr. 2).

De Algemene Rekenkamer heeft deze vragen beantwoord bij brief van 10 juni 2025. Vragen en antwoorden zijn hierna afgedrukt.

De voorzitter van de commissie,
Wingelaar

Adjunct-griffier van de commissie,
Muller

Vraag 1

Ziet u in de afgelopen jaren ontwikkelingen in de (kwaliteit van de) verantwoording over ICT-uitgaven aan softwarelicenties, hardware en grote ICT-projecten?

Vragen om kosteninzicht raken aan veel onderwerpen die wij onderzoeken. In diverse rapporten geven wij aan dat het lastig is om inzicht te krijgen in ICT-uitgaven. Dit heeft onder meer te maken met het hanteren van twee boekhoudstelsels binnen de rijksoverheid (kas-verplichtingen en baten-lasten). Bovendien is er nog geen uniforme interdepartementale inrichting van de financiële administratie. We hebben geen onderzoek uitgevoerd naar specifiek de verantwoording over ICT-uitgaven en kunnen daarom geen schets geven over de ontwikkelingen daarin afgelopen jaren. Informatie daarover is te vinden via bijvoorbeeld rijksfinancien.nl [<https://www.rijksfinancien.nl/open-data/Ontvangers%20ICT%20uitgaven>] of het rijksictdashboard [<https://www.rijksictdashboard.nl/>].

Vraag 2

Welke specifieke risico's heeft de Rekenkamer gesignaleerd bij het rijksbrede IT-beheer, met name bij Logius en SSC-ICT?

Onze IT-beheeronderzoeken richten zich met name op de voor de jaarrekening relevante financiële systemen. We bekijken bijvoorbeeld of de cijfers die daarin staan juist zijn, niet zomaar kunnen worden aangepast en alleen kunnen worden gewijzigd door geautoriseerde medewerkers, of wijzigingen in de software beheerst plaatsvinden en hoe de beveiliging van de applicaties is geregeld. We zien al jaren specifieke risico's bij met name (ongeautoriseerde) toegang tot systemen. De Algemene Rekenkamer vraagt al een aantal jaren aan de minister van BZK om duidelijke eisen te stellen aan IT-beheer waar de Rijksoverheid aan moet voldoen. Op dit moment is er nog geen rijksbreed beeld over de kwaliteit van IT-beheer. Wij hebben dus geen volledig zicht op alle ministeries en de organisaties die daaronder liggen, omdat tot dit jaar geen kader was gesteld. Rijksbreed toezicht op naleving van de minimale eisen is nog niet ingevuld door de minister van BZK. Wij hebben het IT-beheer van Logius en SSC-ICT dit jaar niet specifiek onderzocht.

Vraag 3

Heeft u onderzocht of Logius en SSC-ICT voldoende cybersecuritymaatregelen treffen, en zo ja, wat waren de bevindingen?

Ons onderzoek bij Logius en SSC-ICT ging over de manier waarop de minister van BZK stuurt op inhuur van IT-expertise. Dit onderzoek heeft

zich niet gericht op cybersecuritymaatregelen. Ons meest recente onderzoek naar cybersecuritymaatregelen bij SSC-ICT betrof het security operations center (SOC) van SSC-ICT. Dit onderzoek is in 2023 gepubliceerd in het rapport bij het jaarverslag van het ministerie van BZK over 2022. We concludeerden destijds dat het SOC van SSC-ICT een belangrijke bijdrage leverde aan het beheersen van informatiebeveiligingsrisico's voor afnemers van SSC-ICT, maar zagen ook ruimte voor verdere doorontwikkeling en professionalisering. In 2023 publiceerden we ook onderzoek naar DigiD en eHerkenning waarin we IT-beheersingsmaatregelen bij Logius controleerden, waaronder maatregelen rondom informatiebeveiliging. We concludeerden destijds dat bij Logius voldoende maatregelen zijn getroffen om ervoor te zorgen dat DigiD en eHerkenning beschikbaar en veilig zijn.

Vraag 4

Kunt u in meer detail toelichten op welke manier aanbestedingswetgeving niet is nageleefd?

U vraagt naar een toelichting op welke manier aanbestedingswetgeving niet is nageleefd. In het verantwoordingsonderzoek 2025 BZK hebben we gerapporteerd over de onrechtmatigheden bij de agentschappen.

De € 66,6 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 de verschillende voorzieningen zoals de migratie naar een nieuwe ICT-infrastructuur (€ 36 miljoen), DigiD (€ 17,5 miljoen), Digipoort (€ 7,8 miljoen) en Globe (€ 2,9 miljoen).

SSC-ICT heeft voor 16,2 miljoen gebruik gemaakt van verlengingen van contracten die onrechtmatig zijn aanbesteed (onjuiste formulering van verlengingsopties), voor een contract van € 4,4 miljoen is niet de juiste aanbestedingsprocedure gevolgd (de opdracht is uitgebreid en had opnieuw via mini-competitie uitgevraagd moeten worden), ook is voor een bedrag van € 1,3 miljoen sprake van facturering van prijzen en kortingen die afwijken van de contractafspraken.

In het verantwoordingsonderzoek 2024 BZK hebben we onrechtmatigheden gerapporteerd van € 9,3 miljoen bij het RVB en € 4,5 miljoen bij RvIG die grotendeels worden veroorzaakt door inhuren van adviesdiensten op een onrechtmatig verlengde overeenkomst. Dit is de raamovereenkomst interim-management en organisatieadvies (IMOA) waarvoor het ministerie van Infrastructuur en Waterstaat als categoriemanager verantwoordelijk is. Het overige bedrag van € 2 miljoen bij het RVB bestaat uit een aantal overeenkomsten die onrechtmatig zijn aanbesteed waarbij verschillende redenen de oorzaak zijn voor de onrechtmatigheid, zoals:

- 1) het voortzetten van een opdracht die meervoudig aanbesteed had moeten worden;
- 2) een wijziging in de opdracht nadat de aanbesteding heeft plaatsgevonden;
- 3) een opdracht die in eerste instantie als een inbesteding (opdrachtverstrekking aan een onderdeel van de rijksoverheid) is uitgevraagd, echter bleek dit niet realiseerbaar waarna de opdracht is verstrekt aan een leverancier;
- 4) een opdracht die is uitgezet via een versnelde uitvraagprocedure, dit terwijl het raamcontract geen optie heeft tot een versnelde procedure.

Bij RvIG is er een onrechtmatigheid van € 2,5 miljoen als gevolg van het rechtstreeks verstrekken van opdrachten aan leveranciers van reisdocumentenmodules en het daarbij niet volgen van de juiste aanbestedingsprocedures. Ook is voor € 2,2 miljoen gebruik gemaakt van een overbruggingsovereenkomst ICT. Met een overbruggingsovereenkomst zorgt een ministerie ervoor dat na afloop van het oorspronkelijke contract, de inkoop van diensten of leveringen doorgaat terwijl een nieuw contract wordt voorbereid. Het ministerie van Economische Zaken en Klimaat (EZK) is verantwoordelijk voor de overbruggingsovereenkomst van ICT.

Vraag 5

Vergroot het niet naleven van aanbestedingswetgeving mogelijk de (strategische) afhankelijkheid van één of enkele ICT-leveranciers?

We hebben dit niet onderzocht. Er zijn verschillende oorzaken die leiden tot niet naleven van de aanbestedingswetgeving (blijkt ook uit de voorgaande antwoorden) die niets van doen hebben met de afhankelijkheid van één of enkele ICT-leveranciers. Maar ook: de afhankelijkheid van één of enkele ICT-leveranciers is er waarschijnlijk ook als de aanbestedingswetgeving wel wordt nageleefd omdat strategische ICT-keuzes niet voor een beperkt aantal jaar zijn.

Antwoorden Algemene Rekenkamer bij vragen van de Tweede Kamer over Overkoepelende / overige vragen die betrekking hebben op bovenstaande rapporten Resultaten verantwoordingsonderzoek 2024

Vraag 6

Om welke risicomodellen gaat het die zijn onderzocht? Zijn deze risicomodellen opgenomen in het algoritmeregister?

Dit jaar hebben we 3 risicomodellen onderzocht bij Dienst Toeslagen, de Belastingdienst en UWV. Dit waren respectievelijk de algoritmen Persoonlijk begeleiden, Signaalmodel OB Carrouselfraude en de Risicoscan Verwijtbare Werkloosheid. Risicomodellen zijn algoritmes die gebruikt worden om burgers of bedrijven te selecteren die nader

gecontroleerd of geholpen worden. Het algoritme van Dienst Toeslagen is niet opgenomen in het algoritmeregister. Het algoritme van UWV wel. Het algoritme van de Belastingdienst was dit ten tijde van het onderzoek niet, maar momenteel wel.

Vraag 7

Hoe oordeelt u over het gebruik van verouderde ICT-systemen in de strafrechterketen? Wordt modernisering voldoende aangepakt?

We hebben geen specifiek onderzoek uitgevoerd naar verouderde ICT-systemen in de strafrechterketen. In ons verantwoordingsonderzoek 2024 bij het Ministerie van Justitie en Veiligheid geven we wel aan dat de minister de bedrijfsvoering van de strafrechterketen te weinig coördineert. Hieronder valt ook digitalisering. Bovendien noemen de Directie Strafrechterketen en ketenpartners digitalisering één van de prioriteiten om aan te pakken in de strafrechterketen. Hiervoor is in 2024 een meerjarenvizie opgesteld, zie www.strafrechterketen.nl.