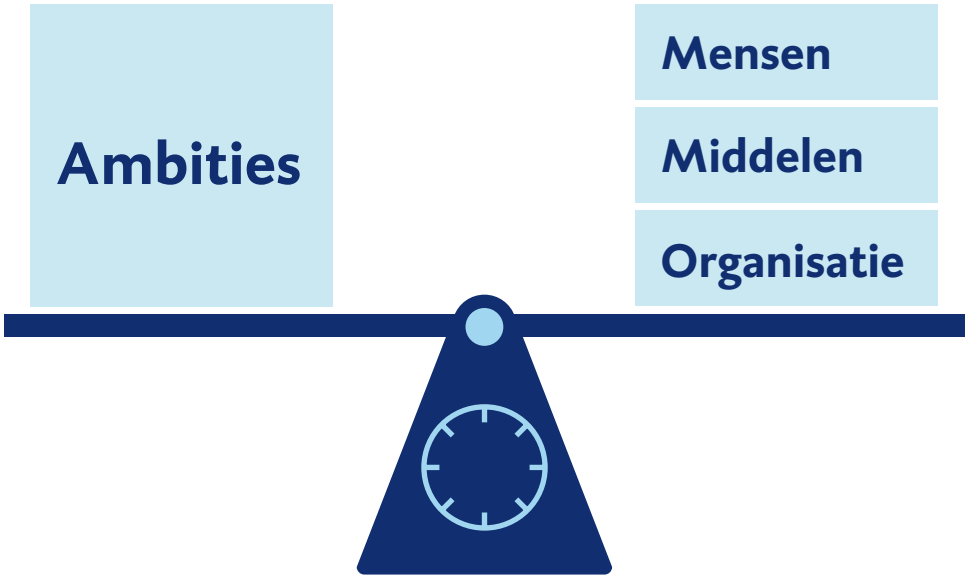
Maart 2020

Grip op digitalisering: rode draden uit tien jaar Rekenkameronderzoek

De Algemene Rekenkamer doet sinds 1991 onderzoek naar digitalisering en de inzet van ICT bij de overheid. Wij hebben onze onderzoeken van de laatste 10 jaar naast elkaar gelegd en opnieuw geanalyseerd. Hieruit blijkt herhaaldelijk dat de gestelde ambities op het gebied van digitalisering niet goed in balans zijn met de mensen, middelen en organisatie.[1] Verouderde ICT-systemen bij de overheid verhinderen bijvoorbeeld dat er nieuwe wetgeving kan worden ingevoerd.



Figuur *Ambities op het gebied van digitalisering moeten in balans zijn met de mensen, middelen en organisatie*

Factsheets voor de Tweede Kamer

De rode draden die we in 3 factsheets hebben opgenomen, zijn kwesties die blijvend aandacht van het parlement vragen. Ze beschrijven knelpunten rondom digitalisering bij de overheid die we in meerdere onderzoeken tegenkwamen en positieve voorbeelden van verbetering. De timing van de publicatie van deze factsheets is niet toevallig. De Algemene Rekenkamer reikt deze factsheets aan ten behoeve van het onderzoek van de Tijdelijke Commissie Digitale Toekomst (TCDT), ingesteld door de Tweede Kamer. We hebben daarbij notitie genomen van hun hoofdvraag: "*Hoe kan de Tweede Kamer de kennispositie versterken op het gebied van digitalisering (informatierecht) en op welke wijze kan de Kamer meer grip krijgen op gewenste en ongewenste ontwikkelingen samenhangend met digitalisering (controlerende en wetgevende taak)?*"

ⓘ Voor meer informatie kunt u terecht bij voorlichting@rekenkamer.nl

Doeltreffende en doelmatige digitalisering: drie belangrijke opgaven

Zowel de private als publieke sector veranderen ingrijpend door digitalisering. De Algemene Rekenkamer heeft als opdracht de doeltreffendheid en doelmatigheid van de publieke sector te controleren. De samenleving heeft baat bij efficiënte en effectieve dienstverlening, een goed functionerende overheid die politieke ambities kan uitvoeren en bij een parlement dat – waar noodzakelijk – bescherming biedt tegen de overheid en tegen negatieve effecten van digitalisering. Vrijwel alle overheidsprocessen en uitvoeringstaken worden in hoge mate digitaal ondersteund. Op basis van onze onderzoeken onderscheiden we 3 belangrijke opgaven om grip te krijgen op digitalisering bij de overheid. Het is van belang dat:
1. de gebruiker centraal staat,
2. de gewenste (digitale) doelstellingen worden gerealiseerd, en
3. het parlement de digitalisering goed kan controleren.[2]

Deze opgaven werken we uit in 3 factsheets en het webdossier.

Voetnoten

1. In de rapporten Lessen uit ICT projecten, deel 1 (2007) en 2 (2008) was een van onze belangrijkste conclusies dat er geen balans was tussen ambities, beschikbare mensen, middelen en tijd bij ICT-projecten. Daarnaast schreven we over de noodzaak de besturing van informatievoorziening en ICT(-projecten) te professionaliseren.
2. De rode draden zijn geïdentificeerd via een systematische inhoudsanalyse van ons onderzoek, een bestuurlijke bespreking met de TCDT en m.b.v. een focusgroep met onderzoekers op het gebied van digitalisering bij de Algemene Rekenkamer.

Opgave 1: centraal zetten van gebruikers

Gebruikers van overheidsdiensten zijn ook consumenten die producten en diensten afnemen van private partijen. Private dienstverlening is mede als gevolg van technologische vooruitgang ongekend snel veranderd en dat uit zich in nieuwe vormen van organisatie en nieuw productaanbod; het uniforme product is vervangen door een persoonsgericht aanbod. Men verwacht als burger een soortgelijke transitie van de overheid. Een digitaliserende overheid dient eerst en vooral op een zorgvuldige manier met data om te gaan, door het borgen van *privacy* en het adequaat beveiligen van informatie.

MENSEN

Burgers, bedrijven en ambtenaren hebben behoefte aan gebruikersvriendelijke systemen

Gebruikersvriendelijk

Wij zien regelmatig dat de gebruikersvriendelijkheid van ICT-voorzieningen van overheidsorganisaties te wensen overlaat.[1] In de digitale systemen rondom CE-markeringen, de berichtenbox voor burgers, bij de politie en bij UWV is onvoldoende rekening gehouden met de wensen en behoeftes van de eindgebruikers.[2] Een positief voorbeeld van een gebruikersvriendelijk overheidsportaal is *publieke dienstverlening op de kaart*, een initiatief van het Kadaster, samen met verschillende ministeries en (uitvoerings)organisaties.[3]

Regie

Zowel burgers, bedrijven als ambtenaren hebben onvoldoende de regie op gegevens die in de systemen van de overheid staan.[4] Open data dragen bij aan een toegankelijke en transparante overheid voor burgers.[5]

MIDDELEN

Een veilige, betrouwbare en gebruikersvriendelijk frontoffice begint 'onder de motorkap'

Verantwoorde omgang met persoonsgegevens

In diverse onderzoeken constateerden we dat privacy onvoldoende is beschermd. Afspraken over de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming worden niet altijd nageleefd waardoor de bescherming en integriteit van persoonlijke gegevens in gevaar komen.[6] Zo stelden we in 2018 "*Enkele ministeries bleken ruim zestien jaar na invoering zelfs nog steeds niet volledig aan de Wet bescherming persoonsgegevens te voldoen.*"[7]

Transparantie over data en navolgbaarheid van afwegingen

De overheid is niet altijd transparant over het gebruik van (persoonlijke) data van burgers en bedrijven bij het nemen van beslissingen: het is niet goed te achterhalen welke data zijn gebruikt en door welke instantie. Hierdoor kunnen mensen in de knel komen, bijvoorbeeld als er fouten staan in de basisregistraties.[8]

Adequate beveiliging
Wij constateerden de afgelopen jaren onvolkomenheden op het gebied van informatiebeveiliging bij diverse ministeries en andere organisaties alsmede bij het Shared Service Center-ICT (SSC-ICT).[9] De gebrekkige informatiebeveiliging kan negatieve gevolgen hebben voor het goed functioneren van de overheid, denk bijvoorbeeld aan waterkeringen die gehackt worden of uitkeringen die niet uitbetaald kunnen worden.[10]

ORGANISATIE

Niet de structuur van de overheid moet leidend zijn, maar het perspectief van de gebruiker

Standaardisatie
De overheid kan digitale dienstverlening efficiënter en effectiever inrichten door te standaardiseren en te sturen op een gemeenschappelijke taal.[11] Standaardisatie en een gemeenschappelijke taal maakt de overheid voor burgers en bedrijven herkenbaar, betrouwbaar en draagt bij aan gebruikersvriendelijkheid. We constateerden dat meer standaardisatie de basisregistraties, de Berichtenbox en ICT bij de politie zou versterken.[12]

Integrale dienstverlening
Het perspectief van de gebruiker vraagt om dienstverlening waarbij overheidsorganisaties goed samenwerken in een keten of een stelsel. Zo zijn burgers en bedrijven gebaat bij één aanspreekpunt met gezag en mandaat dat hen kan helpen wanneer er een probleem in de basisregistraties zit waarbij meerdere overheidsorganisaties betrokken zijn.[13] Het stelsel van basisregistraties is (nog) niet op die manier georganiseerd. Eerder gaven we aandachtspunten mee voor de te ingewikkelde inrichting van het e-ID stelsel voor de digitale authenticatie van burgers en bedrijven. De inrichting van het stelsel was het resultaat van verschillende (ontwikkel)trajecten bij de overheid met eigen governance- en overlegstructuren.[14]

Bronnen

1. Algemene Rekenkamer (2017) *Resultaten verantwoordingsonderzoek 2016 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p. 38
2. Algemene Rekenkamer (2016), *ICT Politie 2016*, p. 39
   Algemene Rekenkamer (2011), *ICT Politie 2010*, p. 31
   Algemene Rekenkamer (2017), *Producten op de Europese markt: CE-markeringen ontrafeld*, p. 57
   Algemene Rekenkamer (2017), *Staat van de rijksverantwoording 2016*, p. 52
   Algemene Rekenkamer (2018), *Resultaten verantwoordingsonderzoek 2017 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, (o.a.)* p. 28
   Algemene Rekenkamer (2014), *Basisregistraties, vanuit het perspectief van de burger,fraudebestrijding en governance*, p. 21
3. Algemene Rekenkamer (2019), *Grip op gegevens: het stelsel van basisregistraties voor burgers en bedrijven*, p. 14
4. Algemene Rekenkamer (2019), *Grip op gegevens: het stelsel van basisregistraties voor burgers en bedrijven*, p.11
   Algemene Rekenkamer (2014), *Basisregistraties, vanuit het perspectief van de burger,fraudebestrijding en governance*, p. 20
5. Algemene Rekenkamer (2016), *Trendrapport open data 2016*, p. 3
   Algemene Rekenkamer (2015), *Trendrapport open data 2015*, p. 7
   Algemene Rekenkamer (2016), *Staat van de rijksverantwoording 2015*, p. 50
6. Algemene Rekenkamer (2018), *Staat van de rijksverantwoording 2017*, p. 45
   Algemene Rekenkamer (2017), *Staat van de rijksverantwoording 2016*, p. 45
   Algemene Rekenkamer (2017), *Rapport bij nationale verklaring 2017*, p. 28
7. Algemene Rekenkamer (2018), *Staat van de rijksverantwoording 2017*, p. 46
8. Algemene Rekenkamer (2019), *Grip op gegevens: het stelsel van basisregistraties voor burgers en bedrijven*, p. 12
   Algemene Rekenkamer (2017), *Staat van de rijksverantwoording 2016*, p. 43
   Algemene Rekenkamer (2014), *Basisregistraties, vanuit het perspectief van de burger, fraudebestrijding en governance*, p. 14
9. Algemene Rekenkamer (2018), *Staat van de rijksverantwoording 2017*, p. 45
   Algemene Rekenkamer (2019), *Resultaten verantwoordingsonderzoek 2018 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p. 21
   Algemene Rekenkamer (2017), *Staat van de rijksverantwoording 2016*, p. 45
   Algemene Rekenkamer (2018), *Rapport bij de nationale verklaring 2017*, p. 28
10. Algemene Rekenkamer (2017), *Staat van de rijksverantwoording 2016*, p. 45
    Algemene Rekenkamer (2018), *Staat van de rijksverantwoording 2017*, p. 44
    Algemene Rekenkamer (2019), *Resultaten verantwoordingsonderzoek 2018 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p. 21
11. Algemene Rekenkamer (2017), *Staat van de rijksverantwoording 2016*, p. 47
12. Algemene Rekenkamer (2019), *Grip op gegevens: het stelsel van basisregistraties voor burgers en bedrijven*, p. 4
    Algemene Rekenkamer (2017), *Staat van de rijksverantwoording 2016*, p. 55
    Algemene Rekenkamer (2017), *Focus op 'kansrijke' aangiften bij de politie*, p. 18
    Algemene Rekenkamer (2010), *Politie ICT 2010*, p. 109
    Algemene Rekenkamer (2019), *Resultaten verantwoordingsonderzoek 2018 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p. 19
13. Algemene Rekenkamer (2019), *Grip op gegevens: het stelsel van basisregistraties voor burgers en bedrijven*, p. 9–10
    Algemene Rekenkamer (2014), *Basisregistraties, vanuit het perspectief van de burger, fraudebestrijding en governance*, p. 6–7
    Algemene Rekenkamer (2018), *Resultaten verantwoordingsonderzoek 2017 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p. 5
14. Algemene Rekenkamer (2016), *Vernieuwing stelsel voor digitale identificatie en authenticatie (eID-stelsel)*, p. 10

Opgave 2: realiseren van (digitale) doelstellingen

In een samenleving die in rap tempo digitaliseert, zijn mensen en organisaties, waaronder de overheid, per definitie verknoopt en verbonden. Iedereen maakt deel uit van verschillende netwerken die de publieke en private sector verbinden, met de afhankelijkheden die daarbij horen. In deze omgeving kunnen resultaten alleen worden geboekt op het moment dat technische verbindingen en samenwerking tussen mensen en organisaties gelijk oplopen. Hiervoor is ICT-kennis onontbeerlijk, evenals andere competenties, zoals contractmanagement en opdrachtgeverschap. De aanwezigheid van deze competenties bij de overheid is belangrijk om samenwerking in goede banen te leiden en een volwaardige partner te kunnen zijn in het netwerk.

MENSEN

Werk aan beschikbaarheid van mensen met ICT-kennis en competenties

Beschikbaarheid deskundig personeel

Beheer, onderhoud en beveiliging van ICT kan alleen gerealiseerd worden door personeel met de juiste kennis en competenties. Er is al jaren een hardnekkig gebrek aan ICT'ers bij het Rijk[1], waardoor er soms 50% inhuur werkt aan digitalisering bij en door de overheid.[2] Ook deskundigheid bij opdrachtgeverschap is een aandachtspunt.[3] Door te investeren in eigen kennis wordt een meer wendbare en weerbare overheid gecreëerd.

CIO en CISO als schakelpunten tussen ICT en business

De *Chief Information Officer* (CIO) en de *Chief Information Security Officer* (CISO) kunnen hun sleutelrol tussen beleid en bedrijfsvoering op het vlak van digitalisering pas goed invullen wanneer zij een sterke positie hebben en de rolverdeling helder is. Dat is niet bij alle ministeries het geval.[4]

Screening

In ons onderzoek naar cybersecurity en informatiebeveiliging bleek dat ambtenaren die werken met vertrouwelijke informatie niet altijd gescreend waren.[5]

MIDDELEN

Een goed onderhouden en functioneel ICT-landschap

Balans tussen onderhoud en vernieuwing: lifecycle management van ICT

Bestaande ICT moet onderhouden worden en er zijn nieuwe applicaties nodig om nieuw beleid of nieuwe wetgeving te ondersteunen. Vaak ligt de nadruk slechts op een van de twee, zoals we in het verleden constateerden bij UWV en bij het Rijk in het algemeen.[6] Lifecycle management vergt inzicht in bestaande ICT en concrete plannen voor beheer, onderhoud én vernieuwing; zoals we in 2018 wel zagen bij de Belastingdienst.[7]

Verwevenheid van digitale systemen
Digitale systemen zijn met elkaar verbonden en kennen onderlinge afhankelijkheden.[8] Niet alleen binnen en tussen ministeries, maar ook tussen ministeries en uitvoeringsinstellingen. Die verwevenheid wordt niet altijd goed in plannen betrokken, zoals bij het e-ID stelsel.[9] De Belastingdienst heeft wel inzicht gecreëerd in de samenhang van de verschillende systemen die het totale IT-landschap vormen.[10]

Gebruik van digitale mogelijkheden om het functioneren van de overheid te verbeteren
Digitalisering biedt mogelijkheden om het functioneren van de overheid te vernieuwen en te verbeteren. Data-analyse en datamining vergroten de effectiviteit en efficiëntie van onder andere handhaving en risicoanalyse, maar worden nog onderbenut. Dit constateerden we in onderzoeken naar btw-verplichtingen bij grensoverschrijdende digitale dienstverlening, naar CE-markeringen en naar btw-aangiften.[11]

ORGANISATIE

Samenwerken is cruciaal, zorg daarbij voor een heldere taakverdeling

Samenwerking tussen ministeries
Burgers en bedrijven verwachten dat overheden samenwerken en in samenhang diensten leveren. Ministers van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Justitie en Veiligheid (JenV), en Economische Zaken en Klimaat (EZK) geven richting aan de digitalisering bij de overheid. Ook decentrale overheden en uitvoeringsorganisaties hebben een rol. Zij doen dit samen, maar elk vanuit hun eigen opdracht en gezichtspunt. Het zoeken naar evenwicht tussen de verschillende gezichtspunten en verantwoordelijkheden heeft meer aandacht nodig zodat alle belangen samen kunnen komen en er draagvlak en eenheid ontstaat.[12]

Bestuurlijke organisatie van verantwoordelijkheden
We vragen regelmatig aandacht voor het eenduidig beleggen van taken en een adequate invulling van verantwoordelijkheden, bijvoorbeeld rondom cybersecurity, informatiebeveiliging, het e-ID stelsel en het stelsel van basisregistraties.[13] We hebben de minister van BZK regelmatig aangespoord om de coördinatierol steviger op te pakken.[14] Dat kan een uitbreiding van bevoegdheden van de minister inhouden, zoals bij informatiebeveiliging, waar resultaten achterblijven.[15]

Aandacht voor uitvoering
Er is te weinig aandacht bij ministeries voor de uitvoering op het vlak van ICT. Zo is er weinig zicht op de IT-beheeractiviteiten van het SSC-ICT.[16] Ook riepen we in verschillende onderzoeken op tot een betere invulling van de rollen van opdrachtgever en opdrachtnemer, zodat de ambities, de prestaties en gemaakte kosten goed naast elkaar worden gelegd.[17]

Samenwerking tussen overheid en marktpartijen
De markt is altijd van de partij. Als leveranciers stoppen met het ondersteunen van een systeem of als een aangegaan contract achteraf niet werkbaar blijkt, kan dat voor problemen bij de overheid zorgen.[18] Die risico's moeten worden beheerst door de overheid.

Bronnen

1. Algemene Rekenkamer (2019), *Staat van de rijksverantwoording 2018*, p. 37
   Algemene Rekenkamer (2019), *Resultaten verantwoordingsonderzoek 2018 Ministerie van Financiën en Nationale Schuld*, p. 25
   Algemene Rekenkamer (2018), *Staat van de rijksverantwoording 2017*, p. 42–43 & p. 45
   Algemene Rekenkamer (2016), *Intensivering toezicht en invordering bij de Belastingdienst*, p. 19
   Algemene Rekenkamer (2016), *Staat van de rijksverantwoording 2015*, p. 28
2. Algemene Rekenkamer (2018), *Staat van de rijksverantwoording 2017*, p. 43
3. Algemene Rekenkamer (2013), *Aanpak van ICT door het Rijk 2012*, p. 34
4. Algemene Rekenkamer (2013), *Aanpak van ICT door het Rijk 2012*, p. 12
   Algemene Rekenkamer (2018), *Resultaten verantwoordingsonderzoek 2017 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p. 32
   Algemene Rekenkamer (2019), *Resultaten verantwoordingsonderzoek 2018 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p. 41
   Algemene Rekenkamer (2011), *Open standaarden en opensourcesoftware bij het rijk*, p. 13
5. Algemene Rekenkamer (2019), *Digitale dijkverzwaring: cybersecurity en vitale waterwerken*, p. 33
   Algemene Rekenkamer (2012), *Informatiebeveiliging en vertrouwensfunctie*, p. 2
6. Algemene Rekenkamer (2017), *UWV, Balanceren tussen ambities en middelen*, p. 64
   Algemene Rekenkamer (2016), *Staat van de rijksverantwoording 2015*, p. 27–28
7. Algemene Rekenkamer (2019), *Resultaten verantwoordingsonderzoek 2018 Ministerie van Financiën en Nationale Schuld*, p. 24, 27
8. Algemene Rekenkamer (2017), *Staat van de rijksverantwoording 2016*, p. 41
   Algemene Rekenkamer (2011), *Open standaarden en opensourcesoftware bij het rijk*, p. 5
9. Algemene Rekenkamer (2016), *Vernieuwing stelsel voor digitale identificatie en authentificatie (eID-stelsel)*, p. 14
10. Algemene Rekenkamer (2017), *Resultaten verantwoordingsonderzoek 2016 Ministerie van Financiën en Nationale Schuld*, p. 28
11. Algemene Rekenkamer (2019), *Datagedreven selectie van aangiften door de Belastingdienst*, p. 22
    AR (2018), *Rapport bij de nationale verklaring 2018*, p. 30
    AR (2018), *BTW op grensoverschrijdende digitale dienstverlening*, p. 8
    AR (2017), *Producten op de Europese markt: CE-markeringen ontrafeld*, p. 54–55
12. Algemene Rekenkamer (2017), *Resultaten verantwoordingsonderzoek 2016 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p. 37–38
13. Algemene Rekenkamer (2019), *Resultaten verantwoordingsonderzoek 2018 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p. 41
    Algemene Rekenkamer (2019), *Digitale dijkverzwaring: cybersecurity en vitale waterwerken*, p. 8, 10
    Algemene Rekenkamer (2016), *Vernieuwing stelsel voor digitale identificatie en authenticatie (eID-stelsel)*, p. 10
14. Algemene Rekenkamer (2019), *Resultaten verantwoordingsonderzoek 2018 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p. 26, 41, 42
    Algemene Rekenkamer (2019), *Grip op gegevens: het stelsel van basisregistraties voor burgers en bedrijven*, p. 4
    Algemene Rekenkamer (2018), *Staat van de rijksverantwoording 2017*, p. 37
    Algemene Rekenkamer (2016), *Vernieuwing stelsel voor digitale identificatie en authenticatie (eID-stelsel)*, p. 10
15. Algemene Rekenkamer (2019), *Toespraak Arno Visser Verantwoordingsdag 2019*
    Algemene Rekenkamer (2019), *Resultaten verantwoordingsonderzoek 2018 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p. 42
    Algemene Rekenkamer (2019), *Staat van de rijksverantwoording 2018*, p. 35–36
    Algemene Rekenkamer (2018), *Staat van de rijksverantwoording 2017*, p. 45
16. Algemene Rekenkamer (2019), *Staat van de rijksverantwoording 2018*, p. 34
17. Algemene Rekenkamer (2017), *UWV, balanceren tussen ambities en middelen*, p. 59–60
    Algemene Rekenkamer (2017), *Staat van de Rijksverantwoording 2016*, p. 53
    Algemene Rekenkamer (2013), *Aanpak van ICT door het Rijk 2012*, p. 14
18. Algemene Rekenkamer (2019), *Resultaten verantwoordingsonderzoek 2018 Ministerie van Financiën en Nationale Schuld*, p. 26
    Algemene Rekenkamer (2019), *Digitale dijkverzwaring: cybersecurity en vitale waterwerken*, p. 8

Opgave 3: goed controleren van digitalisering bij de overheid

Om te kunnen controleren of de overheid de digitale ambities ook waarmaakt, is allereerst de juiste informatie nodig. Informatie over wat digitale systemen kosten, wat ze opbrengen en hoe (goed) ze functioneren. Die informatie is vaak onvolledig en de kwaliteit kan beter. Door een gebrek aan standaarden in deze informatie zijn vergelijkingen tussen overheidsorganisaties en in de tijd bovendien niet te maken. Dat maakt het voor de Tweede Kamer lastig om te controleren en voor de overheid lastig om lessen te trekken en te verbeteren. Het risico daarvan is dat dezelfde fouten steeds opnieuw gemaakt worden.

MIDDELEN

Informatie over de kosten en kwaliteit van ICT

Inzicht in kosten van ICT

De overheid heeft haar ICT-kosten onvoldoende inzichtelijk en mist daardoor de kennis om de juiste investeringsbeslissingen te nemen.[1] Het Rijks ICT-dashboard biedt nog onvoldoende soelaas: het bevat enkel informatie van grote vernieuwingsprojecten.[2] Via het inzichtelijk en bruikbaar maken van open data kan er uitgebreider verantwoording worden afgelegd.[3]

Inzicht in kwaliteit, van ICT en data

Ministeries hebben onvoldoende zicht op de kwaliteit en efficiëntie van hun IT-beheer en stellen daar onvoldoende eisen aan.[4] Recent riepen we ook op tot meer gemeenschappelijk en gestandaardiseerd kwaliteitsmanagement bij de basisregistraties.[5]

ORGANISATIE

Om vergelijkbare en betrouwbare informatie over het presteren van digitale systemen te verkrijgen, zijn afspraken nodig tussen overheidsorganisaties

Afdwingbare afspraken over de vorm van informatie

Informatie over digitale systemen is beperkt uitwissel- en vergelijkbaar door het ontbreken van standaarden.[6] Er zijn afspraken tussen overheidsorganisaties nodig over standaardisatie van informatie over kosten en kwaliteit van ICT. Deze afspraken worden onvoldoende gemaakt of niet gehandhaafd.[7]

Leervermogen wordt gevoed door testen en experimenten

Wij zien dat het leervermogen van de overheid bij de ontwikkeling en beheer van ICT beperkt wordt door risicomijdend gedrag. Door meer in te zetten op kleine, gecoördineerde experimenten kunnen lessen getrokken worden die helpen bij een brede uitrol van ICT.[8] Ook (pen)testen geven waardevolle informatie ten behoeve van verbeteringen van de beveiliging van digitale systemen.[9]

MENSEN

Uiteindelijk moeten parlementariërs in staat zijn digitalisering en de inzet van ICT bij de overheid te controleren

Verdelen van politieke en bestuurlijke aandacht tussen ICT-projecten en bestaande ICT
De totale ICT-uitgaven bij de overheid bedragen (in 2017) 2,7 miljard. Van dit bedrag gaat 'slechts' 25% naar de grote ICT-projecten, terwijl hier wel de meeste politieke en bestuurlijke aandacht naar uitgaat. De overige 75% van de bestedingen gaan naar onderhoud en vernieuwing van bestaande digitale systemen.[10]

Informatiepositie van het parlement
De informatievoorziening door ministeries en uitvoeringsorganisaties aan de Tweede Kamer op het gebied van ICT is onvolledig: informatie gaat veelal over grote vernieuwingsprojecten, terwijl informatie over beheer en onderhoud ontbreekt.[11] Hierdoor wordt het parlement onvoldoende in staat gesteld om beslissingen te nemen op grond van een breed spectrum aan informatie.

Bronnen

1. Algemene Rekenkamer (2019), *Staat van de rijksverantwoording 2018*, p. 33–34
   Algemene Rekenkamer (2017), *Resultaten verantwoordingsonderzoek 2016 Ministerie van Financiën en Nationale Schuld*, p. 30
   Algemene Rekenkamer (2016), *ICT Politie 2016*, p. 25
   Algemene Rekenkamer (2011), *Open standaarden en opensource software bij het rijk*, p. 9
2. Algemene Rekenkamer (2019), *Staat van de rijksverantwoording 2018*, p. 33–34
   Algemene Rekenkamer (2019), *Resultaten verantwoordingsonderzoek 2018 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p.45
3. Algemene Rekenkamer (2016), *Staat van de rijksverantwoording 2015*, p. 51
4. Algemene Rekenkamer (2019), *Staat van de rijksverantwoording 2018*, p. 34
   Algemene Rekenkamer (2018), *Staat van de rijksverantwoording 2017*, p. 45
   Algemene Rekenkamer (2017), *Resultaten verantwoordingsonderzoek 2016 Ministerie van Financiën en Nationale Schuld*, p. 28
   Algemene Rekenkamer (2014), *Staat van de rijksverantwoording 2013*, p. 61
5. Algemene Rekenkamer (2019), *Grip op gegevens: het stelsel van basisregistraties voor burgers en bedrijven*, p. 13
6. Algemene Rekenkamer (2019), *Staat van de rijksverantwoording 2018*, p. 33
   Algemene Rekenkamer (2017), *UWV, balanceren tussen ambities en middelen*, p. 60
7. Algemene Rekenkamer (2019), *Staat van de rijksverantwoording 2018*, p. 33
   Algemene Rekenkamer (2019), *Resultaten verantwoordingsonderzoek 2018 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p. 44
8. Algemene Rekenkamer (2017), *Staat van de rijksverantwoording 2016*, p. 47
   Algemene Rekenkamer (2014), *Basisregistraties, vanuit het perspectief van de burger, fraudebestrijding en governance*, p. 8
9. Algemene Rekenkamer (2019), *Digitale dijkverzwaring: cybersecurity en vitale waterwerken*, p. 11
10. Algemene Rekenkamer (2019), *Resultaten verantwoordingsonderzoek 2018 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p. 46
11. Algemene Rekenkamer (2019), *Resultaten verantwoordingsonderzoek 2018 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*, p. 45–46
    Algemene Rekenkamer (2019), *Staat van de rijksverantwoording 2018*, p. 33–34
    Algemene Rekenkamer (2016), *ICT Politie 2016*, p. 21, 26, 29