Algemene Bestuursdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Van kwetsbaar naar weerbaar

Geleerde lessen uit dreigende acute en langdurige uitval van uitbestede ICT-dienstverlening bij overheidsorganisaties

25 februari 2025
Definitief versie 1.0

ABDTOPconsult
Dichtbij en onafhankelijk

Colofon
ABDTOPConsult

Muzenstraat 97
2511 WB DEN HAAG
www.abdtopconsult.nl

Aart van der Vlist

ABDTOPConsult
Dichtbij en onafhankelijk

De consultants van ABDTOPConsult zijn lid van de topmanagementgroep (TMG) van de Algemene Bestuursdienst en worden benoemd door de ministerraad. Ze zijn rijksbreed en interbestuurlijk inzetbaar voor interim-opdrachten, projecten en onafhankelijke advisering bij complexe en (politiek) gevoelige zaken.

Managementsamenvatting

"Er worden geen uitkeringen meer uitbetaald aan miljoenen Nederlanders en de rechtsgang is tot stilstand gekomen. Indicatiestellingen in de zorg lopen vast en er zijn operationele problemen bij veel overheidsorganisaties." Begin 2024 bestond een reële kans dat een grote ICT-leverancier van de overheid ongecontroleerd failliet zou gaan. In dat geval zouden cruciale overheidsprocessen abrupt en langdurig uitvallen, met een maatschappij-ontwrichtend effect tot gevolg. Die kans lijkt klein, maar áls het onverhoopt gebeurt, dan is de vraag hoe digitaal weerbaar overheidsorganisaties zijn. Dit risico is afgelopen jaren in diverse rapporten benoemd[1,2,3]. Dit onderzoek toont desondanks aan dat de Nederlandse overheden nog onvoldoende weerbaar zijn.

Kernboodschap voor de politiek en bewindspersonen
Burgers moeten kunnen rekenen op een betrouwbare overheid[4]. Het is de verantwoordelijkheid van de politiek, bewindspersonen en de ambtelijke top om overheden weerbaar te maken tegen langdurige uitval van ICT-diensten. Maak daarom een politieke afweging om de digitale weerbaarheid van overheidsorganisaties op orde te krijgen in de juiste verhouding ten opzichte van het realiseren van nieuw beleid. Maak substantieel budget beschikbaar om rijksfaciliteiten te bouwen die de overheid minder kwetsbaar maken voor ICT-risico's met betrekking tot leveranciers, geopolitieke ontwikkelingen en cyber.

Kernboodschap voor bestuurders, opdrachtgevers en eigenaren
Uw primair proces is niet bestand tegen abrupte en langdurige uitval van (uitbestede) ICT-diensten. Voer daarom direct een risicoanalyse uit naar de digitale weerbaarheid van uw organisatie tegen abrupte en langdurige uitval van ICT-diensten. Neem daar vergelijkbare risico's in mee, zoals cyberaanvallen en gevolgen van geopolitieke conflicten. Veranker en prioriteer afspraken over het vergroten van de weerbaarheid, mitigeren van continuïteitsrisico's en het opruimen van technische achterstand in de planning en control cyclus en de informatieplannen. Borg mitigerende maatregelen in de meerjarenplanning, laat de opvolging onafhankelijk toetsen, laat de werking van de maatregelen periodiek testen en doe jaarlijks bewuste rest-risico acceptatie.

Kernboodschap voor beleids-DGs en beleidsmakers
Digitale weerbaarheid moet een prioriteit worden in beleidsvorming en uitvoering, zelfs boven andere beleidspunten ('uitruil'). Bestaand beleid, monitoring en toezicht is onvoldoende gericht op de risico's van acute en langdurige uitval van ICT-dienstverleners. Versterk de Cyber BeveiligingsWet (NIS-2) met verdergaande wetgeving uit de financiële sector (i.e. Digital Operational Resilience Act). Prioriteer in de beleidsbepaling het vergroten van de weerbaarheid van bestaande ICT-dienstverlening boven de realisatie van nieuwe functies in een kwetsbaar ICT landschap. Richt een onafhankelijk, rijksbreed competence center in en waarborg toezicht en controle op kritische ICT-inkoop en -dienstverlening naar digitale weerbaarheid.

[1] Nationaal Coördinator Terrorismebestrijding en Veiligheid (2024). *Cybersecuritybeeld Nederland 2024*.
[2] Wetenschappelijke Raad voor het Regeringsbeleid (2019). *Voorbereiden op digitale ontwrichting*.
[3] Algemene Rekenkamer (2025). *Het Rijk in de cloud. Donkere wolken pakken samen.*
[4] SCP. Burgerperspectieven 2024 en Commissie van Dam (januari 2025). *Minder beloven, meer doen*.

Inhoud

1 Inleiding

De Nederlandse overheid is sterk gedigitaliseerd

Nederland behoort tot de top vijf van meest gedigitaliseerde landen in Europa[5]. ICT speelt een cruciale rol in het primaire proces van (uitvoerings)organisaties, zoals DUO, SVB, UWV, CJIB en de Belastingdienst. Ook overheidsorganisaties met veel fysieke middelen en processen zoals Rijkswaterstaat, RIVM, Defensie en de Nationale Politie zijn sterk gedigitaliseerd.

Doordat Nederlandse overheden de focus op kernactiviteiten leggen, zijn veel ICT-activiteiten uitbesteed aan ICT-leveranciers. Enerzijds bieden ICT-leveranciers kansen op het gebied van technologische ontwikkelingen, digitale slagkracht en professionele dienstverlening, anderzijds zijn overheden ook meer afhankelijk geworden van ICT-leveranciers. Zowel binnen als buiten de overheid is daardoor veel kennis en ervaring aanwezig op het gebied van het reguliere gebruik van ICT-diensten en het aanbesteden van ICT-diensten, waaronder het beheren en overbrengen van ICT naar leveranciers.

De risico's van acute uitval van ICT-dienstverlening nemen toe

In de afgelopen jaren zijn grote incidenten voorgevallen met ICT-dienstverlening, zoals de uitval bij de TU Eindhoven (2025), het NAFIN-netwerk[6] (2024), Crowdstrike (2024), Citrix (2020) en DigiNotar (2011). Vaak worden deze incidenten met veel krachtsinspanning binnen dagen of weken opgelost, met nog veel reparatiewerk daarna. De vraag nu is hoe weerbaar overheden zijn als grote ICT-incidenten niet binnen weken of maanden kunnen worden opgelost.

De oorzaken van deze incidenten zijn uiteenlopend; de overeenkomst is dat de ICT in het primaire proces van de overheidsorganisaties acuut en voor langere tijd niet beschikbaar is. De DNB benoemt dit in de financiële sector recent in haar rapport 'weerbaar zijn in een gure wereld'[7]. Terugvallen op fysieke processen is geen optie meer, de Nederlandse overheid is 'analoog onbekwaam' geworden.

Het ging bijna goed mis

Begin 2024 had de sterk verslechterde financiële situatie van een grote ICT-leverancier tot een landelijke crisissituatie kunnen uitgroeien. In geval van ongecontroleerd faillissement van deze dienstverlener had dit, ook door concentratierisico's bij deze leverancier, tot acute, langdurige en mogelijk onherstelbare uitval van kritieke ICT-dienstverlening van veel bedrijven en

[5] Zie Rathenau Instituut. *De digitale overheid in kaart?,* de DESI index score (EC) en de EGDI score (VN).
[6] Netherlands Armed Forces Integrated Network (NAFIN), een glasvezelnetwerk van het ministerie van Defensie.
[7] De Nederlandsche Bank (2024). *Weerbaar in een gure wereld: Geopolitieke risico's en financiële instellingen.*

overheidsorganisaties kunnen leiden. Met verstoring van dienstverlening aan burgers en bedrijven en daardoor mogelijk maatschappelijke ontwrichting als gevolg.
Dit zou daarna nog jarenlange effecten kunnen hebben op de digitalisering van bedrijven en overheden, denk aan herinvesteringen, nieuwe aanbestedingen en het weer moeten opbouwen van infrastructuren, applicaties en gegevens-verzamelingen bij de eigen organisatie of andere ICT-leveranciers.

Het concentratierisico neemt toe

Het Cybersecuritybeeld Nederland 2024[8] benadrukt de dreiging van grootschalige uitval en noemt hierbij expliciet het risico van een 'digitale monocultuur', "waarin vele organisaties afhankelijk zijn van een klein aantal aanbieders". Denk aan de vele bedrijven en overheden die hun ICT onderbrengen bij Amerikaanse 'hyperscalers' zoals Microsoft, Amazon en Google. Statelijke actoren en criminele organisaties richten hun pijlen steeds vaker op ICT-leveranciers, want eenmaal binnen hebben ze mogelijk toegang tot vele organisaties die hun ICT daar ondergebracht hebben[9].

Dit onderzoek gaat over geleerde lessen

Dit rapport is geen onderzoek naar een ICT-leverancier. De toenmalige situatie was slechts de aanleiding voor dit onderzoek. Dit onderzoek richt zich op de lessen die in algemene zin hiervan kunnen worden geleerd. Hiertoe beschrijft dit rapport aanbevelingen naar aanleiding van bevindingen die volgen uit het onderzoek naar deze crisissituatie. Met interviews en deskresearch zijn de lessen opgehaald en geanalyseerd. Zie de bijlagen voor risicoclassificatie van de bevindingen, de lijst van geïnterviewden en de geraadpleegde literatuur.

ABDTOPConsult heeft deze evaluatie uitgevoerd in opdracht van Binnenlandse Zaken, de directeur-generaal Digitalisering en Overheidsorganisatie, en werd daarbij ondersteund door een kernteam van specialisten uit de taskforce CID (Continuïteit ICT-dienstverlening). De bevindingen, conclusies en aanbevelingen zijn breed getoetst in meerdere reviewsessies met geïnterviewden en deskundigen binnen en buiten de overheid.

Reikwijdte van dit onderzoek

Dit onderzoek richt zich op de vraag in welke mate rijksbreed én op het niveau van individuele overheidsorganisaties maatregelen zijn getroffen om de impact van een acute uitval van ICT-dienstverlening te minimaliseren. Acute uitval wordt in dit onderzoek gedefinieerd als het onmiddelijk niet-beschikbaar zijn van ICT-dienstverlening van een derde partij, met het aannemelijke risico dat deze voor langere tijd niet hersteld kan worden ("maanden" of langer). Hierdoor kunnen

[8] CSBN 2024, wordt jaarlijks uitgebracht door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).
[9] Bijvoorbeeld FD 25/1/'25. *Russische cybercriminelen konden data Centric stelen door softwarelek*.

vitale overheidsprocessen uitvallen waarbij ad-hocmaatregelen (zoals handmatig bijspringen of extra financiële middelen) niet volstaan om de dienstverlening te herstellen. Hierbij is ook gekeken naar recente literatuur en geleerde lessen uit vergelijkbare situaties waarbij ICT acuut niet meer beschikbaar is, zoals:

- *Cyberdreiging*: een ransomwareaanval of wiper-attack[10] op de organisatie óf op een ICT-dienstverlener die meerdere organisaties bedient.
- *Geopolitieke ontwikkelingen*: sancties als gevolg van geopolitieke ontwikkelingen die de ICT-dienstverlening gedwongen beperken.
- *Overdracht eigenaarschap ICT-leveranciers*: overnamen, afsplitsingen en fusies door een partij die niet voldoet aan wettelijke vereisten of sancties.

Daarmee raakt dit rapport aan een aantal bredere onderwerpen op het gebied van nationale veiligheid en digitale onafhankelijkheid[11]. Dit rapport kan daar ook input voor zijn en past ook in actie 1D van de Nederlandse Digitaliseringsstrategie "De overheid versterkt haar digitale weerbaarheid en digitale autonomie".[12]

Opbouw van het rapport

Het rapport bestaat uit twee delen. Hoofdstuk 2 richt zich op de bevindingen volgend uit deskresearch en interviews. Hoofdstuk 3 richt zich op conclusies en aanbevelingen. Per hoofdstuk worden zaken besproken op een rijksbreed niveau en op het niveau van individuele overheidsorganisaties.

Op het niveau van volgende inhoudelijke leerpunten zijn bevindingen en aanbevelingen beschreven:

Rijksbreed:

- Beleid
- Kennis
- Toetsing
- Monitoring
- Faciliteiten

Overheidsorganisaties:

- Informatieplanning
- Kennis
- Risicobeheersing
- Aanbesteding
- Testen

[10] Een cyberaanval waarbij malware wordt geïnstalleerd die data, systemen en back-ups (permanent) verwijdert.
[11] Zie bijvoorbeeld *De Veiligheidsstrategie voor het Koninkrijk der Nederlanden*, NCTV 2023. En Kamerbrief Initiatiefnota *Wolken aan de horizon*, Kamerstuk 17-01-2025.
[12] Verzamelbrief Digitalisering, 18 december 2024, BZK DGDOO referentie 2024-0000935451.

2 Bevindingen

2.1 Rijksbreed

De bestuurlijke organisatie van Nederland bestaat uit drie bestuurslagen: Het Rijk, de provincies en de gemeenten. Het Rijk bestaat uit ministeries, uitvoerende diensten, inspecties, Hoge Colleges van Staat en de adviescolleges. In dit rapport wordt onderscheid gemaakt naar leerpunten op het niveau van individuele overheidsorganisaties en op rijksniveau. Eerst wordt ingegaan op de leerpunten en bevindingen op rijksniveau. Daarna wordt ingegaan op het niveau van de individuele overheidsorganisatie.

Nederland is ten opzichte van veel andere landen sterk gedigitaliseerd. Overheden met gedigitaliseerde processen zijn dan ook bijna te vergelijken met een ICT-bedrijf, denk aan de DUO, het CJIB, de Belastingdienst, het UWV en de SVB. Vanuit het CIO-stelsel en inkoopstelsel worden rijksbrede (ICT)-kaders en richtlijnen meegegeven die de mogelijkheid bieden tot meer controle op ICT-dienstverleners[13]. Daarnaast zijn op rijksniveau vele vormen van crisismanagement ingericht voor crises van nationale veiligheid; denk aan de Nationale Crisisstructuur en cyber crisis management van het NCSC. Structuren die, in geval van acute uitval, direct ingezet kunnen worden om de consequenties te adresseren en af te handelen.

Uit deze leerpuntenstudie blijkt echter dat bestaande structuren, kennis en maatregelen onvoldoende gehanteerd worden voor het mitigeren van het risico op en de impact van acute en langdurige uitval van ICT. In de audittermen 'opzet, bestaan en werking' is er veel beschikbaar qua opzet, maar ontbreekt het vaak aan de implementatie daarvan en toetsing daarop (bestaan en werking).

Beleid

Er zijn veel beleidsdocumenten en kaders beschikbaar voor ICT-uitbestedingen. Denk aan het rijksbrede sourcingsbeleid[14], cloudbeleid en afwegingskaders van Rijks-CIO, Rijks-CISO, BVA, NCSC, IFHR, enzovoort. Echter, in vergelijking met bijvoorbeeld de eerder genoemde DORA-wetgeving in de financiële sector, zijn deze kaders nog onvoldoende specifiek over de risico's met betrekking tot grootschalige, acute en langdurige uitval van ICT-dienstverleners. Een goede stap vooruit is de komende implementatie van NIS-2 in de Cyber BeveiligingsWet (CBW), gepland voor implementatie nog in 2025.

Naast het beschikbaar hebben en toepassen van dergelijk beleid en zulke wetgeving bestaan er geen ICT-kaders binnen de overheid voor de beheersing

[13] Bijvoorbeeld: *Baseline Informatiebeveiliging Overheid (BIO)*, *de Toolbox Veilig inkopen* en de *Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT-2022)*.
[14] *Sourcingsafwegingskader binnen het Rijk* (2012).

van concentratierisico's. Denk hierbij aan dat meerdere overheden hun ICT uitbesteed kunnen hebben aan dezelfde leverancier (wereldwijd, Nederland). Dit speelt bij meerdere ICT-uitbestedingen in Nederland bij één ICT-dienstenleverancier maar ook bij het onderbrengen van ICT-verwerking in cloudoplossingen van grote Amerikaanse 'hyperscalers' zoals Microsoft, Amazon en Google[15].
De ICT-markt is daarbij niet stabiel. Grote innovaties volgen elkaar snel op (zoals internet of things, operational IT, blockchain, AI, quantum computing), de cyberdreigingen nemen toe, geopolitieke ontwikkelingen en verhoudingen veranderen en er is in sommige gevallen sprake van faillissementrisico's door financiële instabiliteit. Dit leidt tot een stijgend ICT-risicoprofiel voor sterk gedigitaliseerde organisaties.

Begin 2024 is in opdracht van CIO en CPO Rijk een analyse uitgevoerd naar de contracten van overheidsorganisaties die mogelijk geraakt zouden worden als de betreffende ICT-leverancier in continuïteitsproblemen zou komen. Hieruit volgde unaniem het beeld dat continuïteitsrisico's voor acute en langdurige uitval contractueel niet effectief afgedekt waren. Daarbij werden de contracten onvoldoende effectief beheerd en gemonitord. Enkele voorbeelden:

- In een belangrijk overheidscontract was niet duidelijk geregeld wie de eigenaar is van de software (intellectual property rights).
- Bij een overheidsorganisatie die de computers in een eigen datacentrum had staan, waren de toegangsrechten niet geregeld in de situatie dat de leverancier zou wegvallen.
- Bij diverse contracten was niet duidelijk waarvandaan de dienstverlening door welke afdeling van de leverancier geleverd werd (wereldwijd inzicht in de leveringsketens).
- Bij een grote overheidsorganisatie was de uitbestede ICT-oplossing onderdeel van een eigen leveranciersoplossing ('proprietary'), waardoor het overbrengen naar een andere partij vrijwel onmogelijk zou zijn.
- In geen van de onderzochte contracten waren 'step-in-rechten' geregeld waarmee in geval van een calamiteit de dienstverlening door de eigen organisatie of een derde ICT-dienstverlener overgenomen zouden kunnen worden.
- Bij de geïnterviewde overheidsorganisaties is afgelopen maanden geprobeerd op basis van bestaande terugvalopties te testen of dat zou werken. Geen van die testen is succesvol gebleken (escrow, uitwijkmogelijkheden, fail-over testing, etcetera).
- Het was vooraf niet bekend welke overheden bij deze specifieke ICT-leverancier hun ICT hadden ondergebracht (concentratierisico).

Deze voorbeelden zijn niet uniek en ook van toepassing op contracten met andere ICT-leveranciers, blijkt uit meerdere voorbeelden van geïnterviewden.

Bevinding A: *Het huidige rijksbrede ICT-sourcingsbeleid, de bijbehorende afwegingskaders en vooral de toepassing daarvan beschermen in de praktijk*

[15] Zie ook rapport van de Algemene Rekenkamer. *Het Rijk in de cloud. Donkere wolken pakken samen.* 15/1/2025.

overheidsorganisaties onvoldoende tegen de continuïteits- en concentratierisico's bij acute en langdurige uitval van ICT-dienstverlening.

Er bestaat op dit moment geen eenduidige, leidende definitie van wat als belangrijke (met andere woorden begrippen als kritisch, vitaal, materieel publieke cloud, te beschermen belangen) ICT-dienst moet worden beschouwd (denk aan definities van het NIPV, de BIO, NIS-2/CBW, BZK en het VIRBI). Dit geeft individuele overheidsorganisaties de ruimte om eigen invulling te geven aan wat wordt gezien als een belangrijke ICT-dienst. Vanuit een breder overheidsperspectief is dit ongemakkelijk en waarschijnlijk ook ongewenst.

***Bevinding B**: Er bestaan geen eenduidige overheidsbrede definities of afwegingskaders van wat kritieke, cruciale of vitale ICT-dienstverlening is, waardoor onduidelijk is welke kaders wel of niet van toepassing zijn.*

Kennis

De kennis over continuïteitsrisico's bij acute uitval van ICT-leveranciers en over concentratierisico's zijn beperkt en gefragmenteerd aanwezig bij de Nederlandse overheid. Er is kennis over het regulier uitbesteden van ICT-diensten binnen bijvoorbeeld CPO en CIO Rijk (BZK DGDOO). Er bestaat beleid op dat gebied. Veel kennis bestaat bij overheden die veel aanbestedingen doen (denk bijvoorbeeld aan Rijkswaterstaat).
Bij incidenten wordt expertise bij elkaar gebracht van meerdere partijen zoals van NCTV/NCSC, CPO/CIO Rijk, SLM en specialistische externe bedrijven. Afhankelijk van het type incident wordt technische expertise, juridische expertise, contractkennis, privacykennis (enzovoort) bij elkaar gebracht om het acute incident op te lossen. Uit interviews met diverse Europese landen ontstaat hetzelfde beeld: bij incidenten wordt kennis en ervaring ad hoc bij elkaar gebracht en zijn er geen landelijke hoogwaardige expertisecentra op dit gebied. Ook wordt slechts incidenteel en gefragmenteerd kennis uitgewisseld tussen de Nederlandse en Europese individuele kennishouders op dit gebied.

De borging van opgedane kennis van een groot ICT-incident wordt sporadisch gedaan en niet geborgd bij een rijksbreed expertisecentrum. Deze kennis en ervaringen zouden juist input moeten zijn voor het opstellen van toekomstig beleid en kaders, en met name kunnen dienen ter ondersteuning van overheden bij complexe ICT-uitbestedingen en bij incidenten.

***Bevinding C:** Kennis en expertise met betrekking tot acute continuïteits- en concentratierisico's zijn centraal bij de overheid beperkt aanwezig. Er is ook onvoldoende kennisdeling op nationaal en internationaal niveau.*

Toetsing

Het aantal ICT-diensten en ICT-producten dat van ICT-leveranciers wordt afgenomen, groeit stevig door. Het biedt overheden veel kansen op het gebied van de doorontwikkeling van ICT-diensten, (digitale) slagkracht en professionele dienstverlening. Echter, het vergroot de afhankelijkheid van ICT-leveranciers en maakt het ICT-management ingewikkelder door aanvullende overdrachtsmomenten en contractuele beperkingen, terwijl datzelfde ICT-

management verder onder druk komt te staan door aanvullende nieuwe technologieën zoals AI, OT, IoT, Cloud, 'Low-Code', enzovoort[16].

Aanbesteden is normaliter de eerste en verplichte stap voor overheidsorganisaties om ICT-diensten van ICT-leveranciers af te nemen. ICT-aanbestedingen zijn vaak complexe, kennisintensieve en langdurige trajecten. De meeste individuele overheden doen niet regelmatig grote, complexe aanbestedingen. Ze missen daardoor de benodigde routine en kennis. Dit compenseren zij meestal door het inhuren van externe expertise.
Bij de strategische voorbereiding van een ICT-aanbesteding maken overheidsorganisaties cruciale keuzes die betrekking hebben op beheersmaatregelen om (acute) continuïteits- en concentratierisico's en risicovolle afhankelijkheden bij de uitbesteding te minimaliseren en te mitigeren. Overheidsorganisaties kunnen veelal, al dan niet binnen de kaders van het eigen departement en de aanbestedingswetgeving, een eigen koers varen, ook in het geval van meer risicovolle aanbestedingstrajecten.

Er bestaat toezicht op privacy (DPIA[17] tot toetsing door de Autoriteit Persoonsgegevens) en op grote ICT-projecten (boven vijf miljoen euro) door het Adviescollege ICT-toetsing (AcICT). Er wordt kwaliteitstoetsing ontwikkeld voor toetsing op staatsveiligheidsaspecten (ABRO[18]). Er bestaat toetsing op business-continuïteitsrisico's (vanuit BVA en CISO). Maar er is op dit moment geen (overheidsbrede) kwaliteitstoetsing op de beheersing van concentratierisico's bij uitbestede ICT-dienstverlening en op de beheersing van risico's bij acute langdurige uitval van een ICT-dienstverlener.

Bevinding D: *Er is onvoldoende onafhankelijke toetsing bij individuele overheden op de beheersing van risico's bij acute cq. langdurige uitval en concentratierisico's van uitbestede kritieke/vitale ICT-dienstverlening.*

Monitoring

Rijksbreed wordt de vitaliteit en marktontwikkelingen van ICT-leveranciers niet actief gemonitord, afgezien van het strategisch leveranciersmanagement voor enkele zeer grote ICT-leveranciers (zoals Microsoft, Oracle, IBM en SAP) en rijksbreed ICT-categoriemanagement voor contracten en leveranciers. Er bestaat geen centraal overzicht van ICT-leveranciers en uitbestede ICT-diensten en contracten. Er bestaat voor individuele overheden geen meldplicht en registratie van (nieuwe) contracten met ICT-leveranciers.

Dit leidt tot een gebrek aan centraal overzicht van de spreiding van ICT-diensten en ICT-leveranciers en de achterliggende (internationale) ICT-leverketens. Dit gebrek maakt dat continuïteit- en concentratierisico's rijksbreed niet effectief beheerst kunnen worden. Als bijvoorbeeld een ICT-leverancier zich opsplitst (casus IBM – Kyndryl in 2021), wordt niet op overheidsniveau geacteerd op de impact daarvan.

[16] Artificiële Intelligentie, Operational Technology, Internet of Things.
[17] Data Protection Impact Assessment, zie bijvoorbeeld www.autoriteitpersoonsgegevens.nl.
[18] Algemene Beveiligingseisen Rijksoverheid Opdrachten, Kamerbrief 2024-0000311206, 23 augustus 2024.

***Bevinding E**: Rijksbreed wordt niet gemonitord welke contracten (voor kritieke/vitale ICT-diensten) met welke leveranciers zijn overeengekomen. Slechts een beperkt aantal ICT-leveranciers worden gemonitord door strategisch leveranciersmanagement en rijksbreed ICT-categoriemanagement. Continuïteits- en concentratierisico's worden niet (centraal) gemonitord, waardoor hier ook niet op kan worden gestuurd.*

Faciliteiten

Om de digitale weerbaarheid te verhogen, zijn er diverse ontwikkelingen op sectorniveau vanuit Europese wetgeving, maar daarnaast zijn een aantal Europese buurlanden op eigen initiatief stappen aan het zetten om hun digitale afhankelijkheid van ICT-dienstverleners te verkleinen. Zij ontwikkelen digitale alternatieven voor bepaalde applicaties en cloudomgevingen om de afhankelijkheden te minimaliseren. In geval van acute en langdurige uitval zouden deze alternatieven kunnen helpen.

Binnen de Nederlandse overheid zijn bij de bestaande overheids-ICT-serviceproviders op dit moment nauwelijks serieuze alternatieven beschikbaar om op terug te vallen bij acute en langdurige uitval van grote ICT-operaties. Dan moet – in volgorde van complexiteit – gedacht worden aan het beschikbaar hebben van datacentrumvloeren, computers/netwerken, dataopslagfaciliteiten tot en met operationele omgevingen en beheerders voor specifieke toepassingen. Een veelgenoemd voorbeeld van een centrale-overheiduitwijkfaciliteit is de 'data ambassade' van Estland in Luxemburg[19]. Daarbij geven veel van de in dit onderzoek geïnterviewde partijen aan dat – met de kennis van vandaag - te veel kennis lijkt te zijn uitbesteed en dat de eigen aansturende regieorganisatie professionalisering behoeft.

***Bevinding F**: Organisaties in het Rijk kunnen in noodsituaties wel terugvallen op de afspraken ten aanzien van crisisbeheersing (onder leiding van NCTV), maar niet tot nauwelijks op gezamenlijke noodvoorzieningen.*

Op rijksniveau zijn vele vormen van crisismanagement ingericht voor crises van nationale veiligheid. Denk aan de Nationale Crisisstructuur (NCTV) en cyber crisis management (NCSC). Echter, deze mechanismen worden niet geactiveerd bij een mogelijke crisis als een ongecontroleerd faillissement van een grote ICT-leverancier dreigt. Hiervoor is het afgelopen jaar veel geïmproviseerd, er wordt voor dergelijke situaties nu aanvullende crisisplanning ontwikkeld.
Op het niveau van de CIO Rijk en CPO Rijk zijn niet de mensen en middelen beschikbaar, en daardoor ontbreekt het aan slagkracht om preventief of reactief te anticiperen op een mogelijke crisissituatie.

***Bevinding G**: Er bestaat geen rijksbrede organisatie en/of governance om snel te anticiperen op een 'bijna-crisissituatie'.*

[19] Zie: e-estonia.com/solutions/e-governance/data-embassy

2.2 Overheidsorganisaties

In deze paragraaf wordt ingegaan op de bevindingen op het niveau van individuele overheidsorganisaties.

Veel overheden hebben de afgelopen jaren de strategie gevolgd van "Focus op kerntaken, uitbesteden van de rest". Daardoor is ICT-dienstverlening bij veel overheden vergaand uitbesteed geraakt. Door sterke digitalisering is de eigen en uitbestede ICT-dienstverlening onderdeel geworden van die kerntaken en de primaire processen voor dienstverlening aan burgers, bedrijven en de maatschappij. Dit legt een steeds grotere nadruk op het belang om effectief ICT- en leveranciersrisico's te beheersen.

Bij verschillende overheidsorganisaties zijn maatregelen getroffen om de gevolgen van acute uitval te mitigeren, bijvoorbeeld:

- Bij uitbesteding zijn de computers in een eigen datacenter gehouden, waardoor (fysieke) toegang tot computers en data behouden blijft bij acute uitval van de ICT-dienstverlener die deze computers beheert.
- De mogelijkheid om terug te vallen op onderleveranciers voor de continuering van de ICT-dienstverlening.
- De ontwikkeling van een noodscenario, waarbij, in geval van crisis, de data overgaat naar een overheidsdienstverlener (bijvoorbeeld SSC-ICT).
- Overbrengen van de ICT-diensten van een shared (leverancierspecifiek) platform naar een eigen afzonderlijke en separeerbare omgeving, om die omgeving makkelijker over of terug te kunnen nemen bij een calamiteit.
- Droogoefeningen (table-tops) en testen om op basis van bestaande contracten, escrow en bedrijfscontinuïteitsplannen uit te wijken.

Deze maatregelen zijn goed, maar zijn in de meeste gevallen bij geïnterviewde partijen onvoldoende gebleken om het risico van acute en langdurige uitval van een ICT-dienstverlener afdoende te mitigeren.

Informatieplanning

Veel overheidsorganisaties hebben ICT-applicaties en -systemen van vele jaren oud. Soms is dit verouderde technologie, systemen die bijna geen onderhoud meer krijgen, systemen waarvan de documentatie niet op orde is en ICT die moeizaam gekoppeld is aan nieuwere technologieën. Hiervoor worden vaak de begrippen legacy en technische schuld gebruikt. Vaak zijn grote investeringen nodig om deze verouderde ICT te moderniseren en sneuvelen deze 'moderniseringsprojecten' ten opzichte van andere prioriteiten zoals functionele vernieuwingen en verplichte compliancy- en informatiebeveiligingstrajecten. De strategie en prioritering voor ICT-investeringen worden meestal vastgelegd in een informatieplan.

Over het algemeen kan gesteld worden dat verouderde ICT (en bijbehorende data) moeilijker overdraagbaar is van de ene naar de andere leverancier en is het dus belangrijk dat overheidsorganisaties hun ICT goed onderhouden en waar mogelijk 'verplaatsbaar' maken ('portabiliteit van ICT'). Dit kan op meerdere manieren; denk aan het gebruik van open standaarden, opensourcesoftware en

het gebruik van mainstream technologie. Omdat de 'omloopsnelheid' van technologie hoog is, vraagt het continu bijblijven van technologie en voorkomen van legacygroei ieder jaar een substantieel investeringsbudget. Als er weinig gestandaardiseerd is, gebruik wordt gemaakt van leverancierspecifieke oplossingen ('proprietary') en de technische schuld hoog is, is het niet makkelijk weg te gaan bij een ICT-dienstenleverancier, vaak wordt hier ook het begrip 'vendor lock-in' gebruikt.

***Bevinding H**: Veel overheidsorganisaties hebben een ICT-landschap waar sprake is van technische achterstand, een beperkte mate van standaardisatie en 'proprietary' software (leverancierspecifieke ICT-oplossingen). Dat leidt tot beperkte wendbaarheid, in het bijzonder in het geval van acute en langdurige uitval van een ICT-leverancier. In dat geval is herstel van de ICT-dienstverlening vaak een langdurig traject, terwijl het ook lastiger is om maatregelen te treffen voor het mitigeren van de risico's van directe uitval. Het structureel wegwerken van technische schuld moet daarom een belangrijke prioriteit zijn in informatieplannen van overheidsorganisaties.*

Kennis

Het aanbesteden van complexe ICT-dienstverlening vraagt om een multidisciplinaire aanpak. Alle aspecten en invalshoeken uit de organisatie moeten samenkomen in de specificaties en het bestek voor de aanbesteding. Variërend van functionele en niet-functionele vereisten, organisatorisch, financiële en juridische voorwaarden, etc. Er is naast inkoop en juridische expertise ook detailkennis nodig van de bedrijfsvoering, de onderliggende ICT-dienstverlening, de architectuur, en informatiebeveiliging, de financiën en het contract- en leveranciersmanagement. Bij verscheidene overheidsorganisaties ontbreekt het aan een integrale aanpak die over alle te betrekken bedrijfsfuncties heen strekt. Hierdoor ontstaat een gat tussen beschikbare kennis/kaders en wat daarvan daadwerkelijk terechtkomt in een contract met een ICT-dienstverlener.

Hierbij speelt ook dat contracteren en onderhandelen voor leveranciers dagelijks werk is en voor een individuele overheidsorganisatie vaak een eenmalige exercitie. Dat komt ook naar voren in het belang van een leverancier om een leverancierseigen ('proprietary') oplossing te verkopen versus het belang van een overheidsorganisatie om een meer marktstandaardoplossing te kopen (om bijvoorbeeld eenvoudiger te kunnen migreren naar een andere leverancier in tijden van nood). Om diezelfde reden lijkt de markt tamelijk passief om marktoplossingen te bieden die overheden en bedrijven meer weerbaarheid bieden.

***Bevinding I**: Alhoewel op overheidsniveau en binnen individuele overheidsorganisaties vaak wel de kaders en kennis aanwezig zijn om de meeste risico's contractueel goed af te hechten in een ICT-aanbesteding, komt – door een gebrek aan een degelijke multidisciplinaire werkwijze en gebrek aan ervaring binnen een overheidsorganisaties – dit niet in afdoende mate terecht in het uiteindelijk getekende contract.*

Bij veel overheidsorganisaties blijkt relatief veel te zijn uitbesteed. Dat komt voort uit het managementdenken van afgelopen decennia om op secundaire bedrijfsvoering ontzorgd te willen zijn, om de volledige focus te kunnen behouden op het primaire proces. Denk aan facilitaire zaken, huisvesting, technische diensten, catering, beveiliging, salarisverwerking, maar ook ICT-diensten.

De regieorganisatie die de meeste overheidsorganisaties hebben ingericht om de ICT-diensten en ICT-leveranciers aan te sturen, worden door vele geïnterviewden benoemd als onvoldoende professioneel. Veel kennis (alsmede de verantwoordelijkheid voor kennisbehoud) voor wat betreft de ICT-dienstverlening is overgedragen aan marktpartijen. Het zelf beschikken over kennis van de eigen ICT-dienstverlening is door de verdere digitalisering van de overheid van groter strategisch belang geworden. Met het inzicht van vandaag vinden veel geïnterviewden dat meer kennis in de eigen organisatie moet blijven om de uitbestede ICT bij hun leverancier goed aan te kunnen sturen (ICT-modernisering, risicomanagement, cyber-risico's, etcetera).

***Bevinding J**: Overheidsorganisaties vinden de eigen regievoering over en aansturing van belangrijke ICT-leveranciers onvoldoende door een gebrek aan kennis en kunde om ICT-leveranciers effectief aan te sturen. Kennis en kunde die door de verdere digitalisering van de overheid van groter strategisch belang is geworden.*

Risicobeheersing

Omdat ICT onderdeel is geworden van de primaire processen van gedigitaliseerde overheden zijn het besturen en risicomanagement van ICT niet meer te beperken tot de ICT-afdeling. Inhoudelijke ICT-kennis, ICT-risicobeheer en operationele ICT-aansturing zijn vervlochten met het aansturen van bedrijfsprocessen. Dat vraagt kennis en ervaring over ICT bij bedrijfsmanagers en bestuurders. Vanuit meerdere perspectieven is dit afgelopen jaren geconstateerd en wordt er aandacht aan gegeven, tot aan de ABD directeuren- en TMG-trainingen. Uit de interviews blijkt echter dat ICT-kennis en strategisch ICT-risicomanagement onvoldoende prioriteit heeft op de bestuurstafels. Zoals hygiëne op een operatiekamer geen discussie meer heeft in een ziekenhuis, zouden ook ICT-aspecten op alle managementniveaus een regulier onderdeel moeten zijn van de cultuur, kennis, risicomanagement en awareness van iedere digitaal opererende overheidsorganisatie.

***Bevinding K**: De verantwoordelijkheid, kennis en awareness over ICT, beheer en risico's in de gedigitaliseerde overheidsorganisaties zijn nog onvoldoende op alle managementniveaus. Dit onderwerp krijgt daardoor makkelijk te weinig prioriteit, tenzij er een incident is en dan is het te laat. Het ontbreekt aan voldoende digital savvy bestuur en management[20].*

ICT-uitbesteding

De beleidsdepartementen hebben de uitbesteding van ICT overgelaten aan uitvoeringsorganisaties. Bestuurders van de uitvoeringsorganisaties hebben ICT-uitbestedingen overgelaten aan het ICT-management van de organisatie. En die hebben dat laten uitvoeren door project-, inkoop- en sourcingsmanagers. Bij zo goed als alle geïnterviewden werd aangegeven dat voorafgaand geen strategische risicoanalyse op bestuurlijk niveau is uitgevoerd.

[20] MIT CISR (2020). *Companies With a Digitally Savvy Top Management Team Perform Better*.

Ook werd daarbij aangegeven dat er in de reguliere planning- en controlcyclus wel jaarlijks naar risico's is gekeken, maar dat daarin nooit het risico van acute uitval van uitbestede ICT-dienstverlening van een grote ICT-dienstverlener prominent naar voren is gekomen. Geïllustreerd door een citaat uit een interview: "dat hielden we eigenlijk niet voor mogelijk".

***Bevinding L**: ICT-uitbestedingen van cruciale ICT-diensten worden op een te laag operationeel niveau uitgevoerd. Het strategisch risicomanagement bij uitbesteding van cruciale ICT-dienstverlening is onvoldoende en heeft tot nu toe te weinig rekening gehouden met scenario's van acute en langdurige uitval van ICT-dienstverlening.*

Individuele overheidsorganisaties houden bij de aanbesteding en selectie van de ICT-leveranciers weinig tot geen rekening met het voorkomen van concentratierisico's. Dat staat ook op gespannen voet met het vrij verkeer van goederen en diensten van de aanbestedingswet ('gelijke behandeling' en 'non-discriminatie'). Hierdoor kunnen belangrijke delen van de overheids-ICT-dienstverlening bij een kleine groep ICT-leveranciers terechtkomen.
Hierdoor ontstaat een concentratierisico, wat leidt bij acute en langdurige uitval van een ICT-leverancier tot grote gevolgen bij meerdere overheden.
Dit risico wordt ook gezien door de DNB in hun eerder genoemde rapport over de digitale weerbaarheid van de financiële sector (De Nederlandsche Bank, 'Weerbaar in een gure wereld', 2024) en in het Cyber Security Beeld Nederland 2024 ('digitale monocultuur').
Alhoewel het vraagstuk van concentratierisico's ook een overheidsbreed vraagstuk is, ontslaat het individuele overheidsorganisaties niet van de verantwoordelijkheid om een visie te ontwikkelen en de regie te nemen ("alle eieren in één mandje").

***Bevinding M**: Overheidsorganisaties besteden niet tot nauwelijks aandacht aan concentratierisico's bij aanbestedingen van ICT-dienstverlening. Europese wetgeving (aanbestedingswet) beperkt de ruimte hiervoor. Kaders om concentratierisico's te beperken, ontbreken. De consequenties van concentratierisico's worden op bestuurlijk niveau onvoldoende afgewogen.*

De meeste betrokken overheidsorganisaties hebben te beperkt inzicht in hun ICT-landschap (applicaties, infrastructuren, gebruikte software, kennishouders, contracten, locaties, koppelingen, certificaten, autorisaties), de (internationale) leverancierssketen(s) en de bijbehorende risicoprofielen. Bestaande overzichten van het ICT-landschap van de organisaties worden vaak als ontoereikend en/of gedateerd beschouwd[21]. Een dergelijk overzicht is desondanks cruciaal om risico's en afhankelijkheden inzichtelijk te maken en effectieve beheermaatregelen te treffen, maar ook om tot actie over te gaan bij acute en langdurige uitval.

Daarbij wordt uitbestede dienstverlening binnen een ICT-dienstenleverancier vaak opgeknipt in meerdere onderdelen die uitgevoerd worden door verschillende afdelingen, via onderleveranciercontracten en intercompany-verrekeningen. Bijvoorbeeld: een datacenter ligt in het ene land en de beheerfuncties worden vanuit een ander land uitgevoerd. Hierdoor ontstaan binnen één ICT-leverancier

[21] Vaak wordt hier verwezen naar de 'Configuration Management DataBase', de registratie waarin alle hardware en software wordt bijgehouden.

leveringsketens van ICT-componenten en ICT-diensten die geïntegreerd aangeboden worden aan de opdrachtgever. Bij de meeste overheidsorganisaties ontbreekt dit inzicht. Overheidsorganisaties hebben veel moeite om dat netwerk van onderaannemers en bedrijfsonderdelen van de hoofdaannemer over verschillende leveringsketens heen in kaart te krijgen. Het leidt tot een gebrek aan inzicht in potentiële leveringsrisico's bij de ICT-leveranciers en een gebrek aan inzicht en kennis om de ICT-dienstverlening te kunnen ontvlechten en effectief over te dragen bij een leveranciersovergang (ook bij een reguliere overgang).

***Bevinding N**: Er bestaat onvoldoende zicht op het eigen ICT-landschap, de gehele leverancierskete en onderliggende afhankelijkheden bij de ICT-leverancier. De risico's, in het geval van acute uitval, zijn voor de opdrachtgever (klantorganisatie) daarom niet inzichtelijk.*

Testen

Overheidsorganisatie hebben vaak niet of nauwelijks de contractuele afspraken (bijvoorbeeld gebruiksrechten van software, eigenaarschap van hardware, uitwijkmogelijkheden, step-in-rechten, autorisaties, escrow, exitplannen) ingeregeld om zich te beschermen tegen acute uitval. Wel zijn er vaak exitplannen overeengekomen, maar worden deze alleen op papier getest (tabletops) en gaan uit van voldoende tijd (bijvoorbeeld na conflict, heraanbesteding of migratie) om de exit vorm te geven. Er wordt onvoldoende rekening gehouden met de consequenties van een exit in geval van faillissement van de ICT-leverancier. Uitwijkmogelijkheden en escrow worden sporadisch getest, de uitkomsten van uitwijktesten tonen veelal aan dat getroffen maatregelen onvoldoende zijn om de continuïteit van de ICT-dienstverlening bij acute uitval te waarborgen.

***Bevinding O**: De meeste overheidsorganisatie hebben (contractueel) te weinig terugvalopties ingericht om een crisissituatie en/of acute uitval van hun ICT-diensten op te vangen. Bestaande continuïteitsbeheersmaatregelen (bijvoorbeeld uitwijkmogelijkheden, step-in-rechten, autorisaties, escrow, exitplannen) zijn beperkt geregeld, worden onvoldoende getest of zijn niet voldoende snel te realiseren.*

De meeste overheidsorganisaties voeren jaarlijkse (basis)audits uit naar de kwaliteit van de geleverde ICT-dienstverlening (bijvoorbeeld een ISAE 3402-verklaring in het kader van de jaarrekeningcontrole). Geen van de geïnterviewde organisaties kijken periodiek naar de (continuïteits)risico's van de eigen ICT-leveranciers.
Daarbij wordt in de interviews aangegeven dat overheidsorganisaties nog onvoldoende geleerd lijken te hebben van vergelijkbare incidenten met grootschalige uitval van ICT uit het verleden (bijvoorbeeld CrowdStrike, Citrix, DigiNotar). Bijna alle geïnterviewde overheidsorganisaties geven aan dat ze zich overvallen voelen en te laat in actie zijn gekomen bij het mogelijke faillissement van de betreffende ICT-leverancier begin 2024.

***Bevinding P**: Overheidsorganisaties monitoren op operationeel niveau de risico's van uitbestede ICT-dienstverlening, maar beschouwen en wegen onvoldoende de (strategische) risico's van hun ICT-leveranciers en ICT-dienstverlening. Aanvullend blijkt dat overeengekomen beheersmaatregelen en toezicht zich vooral richten op de kwaliteit en continuïteit van de ICT-dienstverlening en niet van de betreffende ICT-leverancier.*

3 Aanbevelingen

3.1 Conclusies

De bevindingen laten zien dat de Nederlandse sterk gedigitaliseerde overheidsorganisaties kwetsbaar zijn bij acute en langdurige uitval van externe ICT-dienstverleners. De kennis en maatregelen die nu genomen zijn, houden onvoldoende rekening met meer extreme crisissituaties zoals het direct en langdurig wegvallen van cruciale ICT-dienstverlening door uitval van een ICT-leverancier of een cyberaanval. Uit dit onderzoek blijkt dat overheidsorganisaties in die situaties een te beperkt handelingsperspectief kennen. Noodvoorzieningen ontbreken en door technische achterstand, ontbrekende of onduidelijke contractuele afspraken en onvoldoende specialistische kennis hebben overheidsorganisaties beperkt tot geen handelingsperspectief om snel uit een dergelijke crisissituatie te komen.

Afgelopen jaar zijn door de ontstane situatie diverse inventarisaties, crisisoefeningen en uitwijktesten gedaan met wisselend resultaat. Hieruit blijkt dat het proactieve risicomanagement ten aanzien van acute en langdurige uitval van ICT-dienstverleners niet op orde is. Organisaties beschikken onvoldoende over een integraal overzicht van en inzicht in de ICT-leveranciers, ICT-dienstverlening, ICT-componenten en ICT-middelen betrokken in de ICT-leveringsketens (hardware, software, licenties, contracten, leveringsketens bij leveranciers, netwerkverbindingen, certificaten, autorisaties, etc.). Hierdoor is het nu nauwelijks mogelijk om de ICT-risico's van de (primaire) bedrijfsprocessen in kaart te brengen en daarvoor proactief beheersmaatregelen te treffen. Het (strategische) risicomanagement vergt daarom directe aandacht van bestuurders. Dit wordt echter in de praktijk gedelegeerd naar het ICT-management van de uitvoeringsorganisaties. Oplopende geopolitieke spanningen en eerder genoemde alarmerende rapporten van de WRR, het Rathenau Instituut, de Cybersecurity Raad, De Nederlandsche Bank, de Algemene Rekenkamer en NCTV/NCSC onderstrepen de urgentie.

Wat opvalt is dat het binnen de overheid niet ontbreekt aan kennis, wetgeving, good practices en richtlijnen/kaders in vergelijking met het reguliere ICT-uitbesteden. Maar het ontbreekt aan het op een juiste wijze toepassen hiervan. Als ICT-risicomanagement en de daaruit voortvloeiende mitigerende maatregelen serieus genomen zouden worden, hadden ook risico's van acute langdurige uitval al reeds onderkend en beheerst kunnen worden. De kaders en wetgeving zoals BIO, Wwke/CER[22] en NIS-2 (CBW) geven hiervoor een passend instrumentarium. Waar het aan ontbreekt, is awareness, begrip, kennis en prioritering van deze onderwerpen op de bestuurstafel, bij het management van de bedrijfsonderdelen en van ICT. Er moet meer prioriteit worden gegeven aan het weerbaarder maken

[22] Wet weerbaarheid kritieke entiteiten. Naar verwachting worden deze in samenhang met NIS-2/CBW derde kwartaal 2025 van kracht in Nederland.

van bestaande ICT, zodat makkelijker uitgeweken kan worden in geval van nood (bijvoorbeeld door het overdragen naar een nieuwe aanbieder). Weerbaarheid kan geborgd worden in contractuele afspraken alsmede in het ontwerp van het ICT-systeem. Dit vereist een pas op de plaats in de informatieplanning voor het nóg meer ontwikkelen van nieuwe ICT-diensten (met nieuwe technologie of naar aanleiding van nieuw beleid).

Er kan geleerd worden van de financiële sector die met de adoptie van DORA financiële instellingen verplicht om maatregelen te treffen tegen acute uitval van ICT-dienstverlening, wat een stap verder gaat dan CBW/NIS-2 en Wwke/CER. DORA stelt specifieke maatregelen voor bij de acute uitval van ICT-leveranciers, eist inzicht in (internationale) ICT-leveringsketens bij die leveranciers en stelt maatregelen voor bij concentratierisico's, waarop actief toezicht gehouden wordt door DNB en AFM. DORA is gekoppeld aan de legitimiteit van de instelling (denk aan de banklicentie) en stelt bestuurders aansprakelijk.

3.2 Aanbevelingen

De rijksbrede overheid en individuele overheidsorganisaties hebben duidelijk een been bij te trekken als het gaat om het versterken van (ICT-)risicomanagement op het gebied van inkoopprocessen, bijbehorende bestaande kaders en daaruit voortvloeiende mitigerende maatregelen om bestand te zijn tegen de groeiende dreiging van acute en langdurige uitval van hun ICT-diensten en ICT-dienstenleveranciers.

De belangrijkste aanbevelingen zijn hieronder beschreven op twee niveaus: op overheidsbreed/bestuurlijk beleidsniveau (centrale taken en regie), en op het niveau van de uitvoering (individuele overheidsorganisaties).

Dit rapport beperkt zich tot de belangrijkste aanbevelingen, met als opmerking dat in het algemeen wordt aanbevolen om voort te bouwen op bestaande mechanismen en bestaande processen en structuren te versterken. Per aanbeveling is de afweging gemaakt of deze ongeveer in een jaar uitvoerbaar is en of de maatregel maximaal inpasbaar is in bestaande mechanismen of organisaties. Zie de bijlage voor een voorstel implementatiekalender.

Aanbevelingen op overheidsbreed/bestuurlijk beleidsniveau

1. **Beleid**. Vernieuw het sourcingsbeleid uit 2012 en werk dit uit naar concrete richtlijnen voor acute en langdurige uitval van ICT-dienstverlening en –dienstverleners. Werk concrete rijkskaders uit voor (ICT-)risicomanagement, rekening houdend met zowel continuïteits- als concentratierisico's. Schep duidelijkheid in de definities van vitale/kritieke/primaire dienstverlening van de verschillende overlappende kaders (denk aan de BIO en NIS-2/CBW) en welke risico's en maatregelen bij welke begrippen passen. Maak daarmee duidelijk voor de overheden wat de normen zijn, met passende communicatie over deze normen (binnen CIO- en CPO-stelsel).

2. **Kennis**. Bouw voldoende kennis en kunde op over kaders, richtlijnen, monitoring en toezicht bij centrale regelgevende overheden, met name bij CIO Rijk, CPO Rijk en CISO Rijk van BZK DGDOO, BVA's, Strategisch Leveranciers Management (SLM) en bij het NCSC. Bouw actieve kennisuitwisseling op met gerelateerde kenniscentra in de overheid, semioverheid, met de markt Europees/internationaal. Investeer in een competence center, dat naast kennisopbouw en -deling, ook bijdraagt aan het voorbereiden en uitvoeren van decentrale aanbestedingen. Maak een leercyclus van alle incidenten die gemeld worden door de individuele overheden. En bouw met deze groep mensen en bestaande domeinen (bijvoorbeeld BVA, CISO, CPO, CIO en CTO) een ecosysteem, met noodzakelijke kennis en kunde, om (preventief) te kunnen anticiperen op crisissituaties.

3. **Toetsing**. Ontwikkel positieve stimulansen om de risicobeheersing van acute en langdurige ICT-uitval meer effectief in te regelen.

   Veranker binnen bestaande toetsende organen de proactieve toetsing op de borging van het risicomanagement op acute en langdurige ICT-uitval van (zowel in- als uitbestede) hooggevoelige ICT. Bijvoorbeeld door dit te organiseren als aanvullende onderzoekstaak bij Adviescollege ICT Toetsing en in het CIO-oordeel voor grote ICT-projecten. Veranker digitale weerbaarheid in jaarlijkse opdrachtbrieven aan uitvoeringsorganisaties en vraag de Algemene Rekenkamer dit in hun jaarlijkse verantwoordingsonderzoek te toetsen op voortgang.

   Toets overheidsorganisaties op de werking van toegepaste kaders, risicomanagement en de effectiviteit van mitigerende maatregelen voor digitale weerbaarheid van de bedrijfsprocessen.

4. **Monitoring**. Versterk bestaande (strategisch) leveranciersmanagement-processen. Richt een centrale monitoringorganisatie in voor het proactief volgen van marktontwikkelingen van ICT-diensten en ICT-leveranciers om proactief te kunnen handelen bij dreigende acute en langdurige uitval van ICT-diensten en -leveranciers. Ontwikkel hiervoor de informatiepositie die nodig is om dit rijksbreed te kunnen doen (bijvoorbeeld registratie van risicoregisters). Breng deze taken onder bij een uitvoerende centrale overheidsorganisatie.

5. **Faciliteiten**. Ontwikkel overheidsbrede terugvalfaciliteiten voor noodsituaties, te beginnen met dataopslagmogelijkheden. Gezien de kosten die hiermee gemoeid zijn, kan overwogen worden dit in Europees verband te onderzoeken. Versterk met deze faciliteiten de positie van de bestaande overheids-ICT-serviceorganisaties. Maak het mogelijk dat alle overheden gebruik kunnen maken van deze terugvalfaciliteiten. Werk de technische en financiële businesscase uit voor deze terugvalfaciliteiten. Onderzoek tegelijkertijd in samenwerking met ICT-leveranciers en ICT-brancheorganisaties de mogelijkheden om binnen de ICT-markt passende (terugval)maatregelen te treffen (zowel technische als organisatorische uitwijkfaciliteiten) bij een acute uitval van een concurrent. Denk aan uitbesteding aan een consortium met onderlinge uitwijkmogelijkheid 'by design'.

Aanbevelingen op het niveau van de uitvoering

6. **Informatieplanning.** Prioriteer in de informatie- en portfolioplanning de modernisering van het ICT-landschap en het 'resilience by design' maken van het ICT-landschap om te voorkomen dat verouderde ICT ('legacy') leidt tot een lock-in. Maak hier financiële middelen voor beschikbaar, die ingezet kunnen worden voor capaciteit en kennis om modernisering van het landschap aan te pakken.

   Investeer bij modernisering en nieuwbouw van ICT-systemen in zogenaamde 'portabiliteit', waardoor ICT-systemen, applicaties, infrastructuren en data overdraagbaar zijn. Denk hierbij bijvoorbeeld aan het gebruik van standaarden, het beperken van maatwerk, interoperabiliteit van systemen, het loskoppelen van data van systemen, en het gebruik van opensourceproducten.

   Verhoog de weerbaarheid van ICT-dienstverlening in het ontwerp en de architectuur van het ICT-landschap. De mogelijkheden hiervoor zijn divers. Denk aan het veiligstellen van back-ups via SAAS-/cloudoplossingen, separeerbare ('ringfenced') omgevingen tot dubbele omgevingen bij meerdere leveranciers. Maak dit onderdeel van de reguliere architectuur en prioritering in de informatieplanning. Ontwikkel in de organisatie en bij het ICT-management, net als bij 'privacy en security by design', een cultuur van 'ICT resilience by design'. Borg de realisatie van 'resilience by design' ook in de contractuele afspraken met ICT-leveranciers, bijvoorbeeld door het verplicht stellen van een afgeschermde eigen omgeving voor kritieke dienstverlening.

7. **Kennis.** Investeer in 'digital savvy' bestuur en management. Bouw kennis en ervaring op zodat ICT-risicomanagement en de te nemen mitigerende maatregelen de juiste prioriteit krijgen. Zorg dat op alle managementniveaus de juiste inschatting gemaakt kan worden ten aanzien van de impact van ICT-risico's op de bedrijfsvoering, inclusief nieuwe risico's op het gebied van cyberdreigingen, operational IT (OT), internet of things (IoT), quantum computing en acute langdurige uitval van ICT-diensten(-verleners).

   Investeer in het versterken van de ICT-regievaardigheden van de eigen ICT-organisatie; denk aan het beschikken over voldoende technische kennis en ervaring op het gebied van architectuur, kwaliteitsmanagement, risicomanagement, servicemanagement, portfoliomanagement, service-integratie, contract-, leveranciers- en sourcingsmanagement. Werk hierbij samen met andere overheden, met name bij hooggevoelige en tijdelijke trajecten als complexe ICT-aanbestedingen met een hoog risico. Meld incidenten aan centrale overheden zodat daar de gehele overheid ervan kan leren.

8. **Risicobeheersing**. Richt (ICT-)risicomanagement in en professionaliseer het als regulier instrument in de beleidscyclus, in de planning & control-cyclus, en in de driehoeksafspraken (eigenaar – opdrachtgever – uitvoeringsorganisatie). Richt het risicomanagement zodanig in dat het proces

het eindverantwoordelijke bestuur faciliteert om haar verantwoordelijkheid ten aanzien van ICT-risico's te kunnen nemen. Stel op rijksbreed niveau de kaders vast waar individuele overheidsorganisaties aan moeten voldoen op gebied van (ICT-)risicomanagement en toets of hieraan wordt voldaan.

9. **ICT-uitbesteding.** Classificeer aanbestedingstrajecten van (kritieke) bedrijfsprocessen risicogebaseerd, reeds bij de start van het traject. Neem extra maatregelen bij hoogrisicotrajecten (inclusief cloud, SAAS, etc.). Zorg dat bij hoogrisicotrajecten het bestuur actief betrokken is, zorg dat de expertise van de eigen organisatie waar nodig aangevuld wordt en laat het aanbestedingstraject en onderliggende dossier toetsing ondergaan, ook op weerbaarheid, door een onafhankelijke partij (bijvoorbeeld via de bestaande CIO-toets, AcICT toets, ADR of een review door externe partij).

   Maak bij (hoogrisico-)trajecten een analyse van hoe de uit te bestede ICT-dienstverlening tot concentratierisico's kan leiden (rijksbreed) en pas de eigen sourcingsstrategie en het aanbestedingstraject daarop aan. Verbeter de contractuele overeenkomst met aanbieders, bijvoorbeeld door het verplichten tot transparantie over de opbouw van de ICT-dienstverlening, het opstellen en testen van exitplannen (inclusief uitwijkmogelijkheid en back-up), toegang verlenen tot alle actuele gegevens van de ICT-diensten, inzicht verlenen in de (financiële) ontwikkeling van de ICT-leverancier, mogelijkheid tot opzeggen van de overeenkomst en afnemen van ICT-diensten bij onderaannemers bij een (dreigend) faillissement en het inregelen van step-in-rechten. Borg dat dergelijke bepalingen als standaard worden opgenomen in de rijksbrede contractuele standaarden en raamwerken (bijvoorbeeld ARBIT en ARVODI). Ga met ICT-aanbieders in gesprek en betrek hen actief in het doorvoeren van verbeteringen ten aanzien van concentratie- en continuïteitsrisico's.

10. **Testen.** Borg dat uitwijk- en exitplannen per ICT-dienst zijn uitgewerkt, actueel worden gehouden en worden getest. Zorg bij het beheer van ICT dat alle objecten bekend zijn (hardware, software, licenties, contracten, leveringsketens bij leveranciers, netwerkverbindingen, certificaten, autorisaties, etc.), om in staat te zijn uit te wijken wanneer dat nodig is. Overweeg om hiervoor geautomatiseerde hulpmiddelen in te zetten omdat de omvang en complexiteit van ICT-landschappen bij de overheid te groot zijn voor handmatige volledige en juiste ICT-administraties. Gezien de complexiteit om uit te wijken met de volledige dienstverlening, wordt aanbevolen om in de uitwijk- en exitplannen risicogebaseerd vast te stellen welke minimale faciliteiten, systemen en organisaties nodig zijn (m.a.w. 'minimum viable organisation') om in tijden van nood de continuïteit van de (belangrijkste) primaire processen te waarborgen.

    Plan periodieke echte 'real life'-uitwijktesten en crisisoefeningen in voor verschillende scenario's, maar ook voor acute en langdurige uitval van ICT-dienstverlening en ICT-dienstverleners. Dit kan door oefeningen maar ook door het regulier wisselen van omgevingen (denk aan het ene kwartaal de verwerking in de primaire omgeving, het andere kwartaal in de uitwijkomgeving).

Slotoverweging

Zoals de DNB constateert voor de financiële sector, moet de gedigitaliseerde overheid van Nederland steviger inzetten om zich weerbaar te maken voor een 'gure' omgeving. Wat goed gedaan is tot vandaag is niet goed genoeg meer voor morgen.

Geopolitieke, markt-, leveranciers- en cyberrisico's kunnen tot onverwachte verstoring in het ICT-landschap leiden en daarmee tot abrupte, langdurige verstoring van de digitale dienstverlening aan maatschappij, burgers en bedrijven. Een verhoogde digitale weerbaarheid draagt bij aan de maatschappelijke weerbaarheid. Dit maakt het een maatschappelijke opgave voor álle overheden.

De kennis om dit te doen is aanwezig, de uitdaging zit in prioriteit, investeringsbeslissingen, kennisdeling en -opbouw en sturing op het weerbaar maken van de eigen overheidsorganisatie, maar ook het inregelen van centrale voorzieningen om dit te faciliteren. Uit de verrichte studie blijkt dat bij een aantal omringende landen en Nederlandse overheidsorganisaties er inmiddels geen crisissituatie en urgentie meer wordt ervaren. Geïnterviewden geven aan: "we zijn weer back to normal". Begrijpelijk, omdat het toenmalige directe risico is afgewend door herfinanciering van de ICT-leverancier die de aanleiding was voor dit onderzoek. Anderzijds onacceptabel omdat het risico op vergelijkbare incidenten met deze of andere ICT-leveranciers niet is verdwenen.

Burgers en bedrijven moeten kunnen rekenen op de leverbetrouwbaarheid van de overheid, die zich goed heeft voorbereid op risico's van een sterk gedigitaliseerde samenleving. De appreciatie van de bevindingen uit dit rapport en de urgentie om de aanbevelingen op te pakken is een keuze voor het Rijk (CIO's, DG DOO, ICBR, SG's, bewindspersonen) en ook welk 'risk appetite' acceptabel is (mate van hoeveel risico je bereid bent te nemen). Dit is een afweging die gemaakt moet worden vanuit meerdere perspectieven; denk aan taakstellingen tot het realiseren van doelen van kabinetsbeleid, kosten, doorlooptijd, doorontwikkeling ICT, technologische ontwikkelingen, innovatie, schaarste in capaciteit, enzovoort.

Desalniettemin zijn de bevindingen uit dit rapport van dien aard dat wordt aanbevolen de voorgestelde aanbevelingen de noodzakelijke prioriteit te geven en aan te pakken in een programma-aanpak. In de bijlage is een voorbeeld routekaart uitgewerkt waarin de aanbevelingen in de tijd zijn geprioriteerd.

Bijlagen

Bijlage A: Aanbevelingen gekoppeld aan de bevindingen

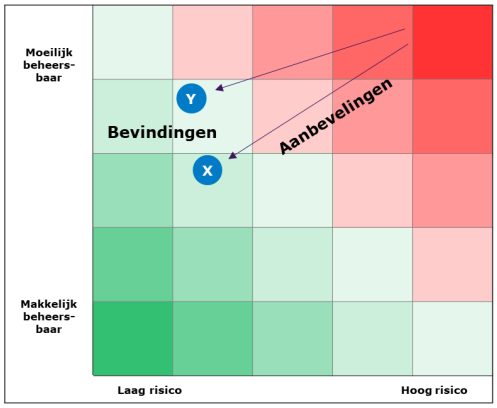
#	Bevinding	Aanbeveling
Rijksbreed		
A	Het huidige rijksbrede ICT-sourcingsbeleid, de bijbehorende afwegingskaders en vooral de toepassing daarvan beschermen in de praktijk overheidsorganisaties onvoldoende tegen de continuïteits- en concentratierisico's bij acute en langdurige uitval van ICT-dienstverlening.	1 – Beleid; 3 – Toetsing
B	Er bestaan geen eenduidige overheidsbrede definities of afwegingskaders van wat kritieke, cruciale of vitale ICT-dienstverlening is, waardoor onduidelijk is welke kaders wel of niet van toepassing zijn.	1 – Beleid
C	Kennis en expertise met betrekking tot acute continuïteits- en concentratierisico's zijn centraal bij de overheid beperkt aanwezig. Er is ook onvoldoende kennisdeling op nationaal en internationaal niveau.	2 – Kennis
D	Er is onvoldoende onafhankelijke toetsing bij individuele overheden op de beheersing van risico's bij acute cq. langdurige uitval en concentratierisico's van uitbestede kritieke/vitale ICT-dienstverlening.	3 – Toetsing
E	Rijksbreed wordt niet gemonitord welke contracten (voor kritieke/vitale ICT-diensten) met welke leveranciers zijn overeengekomen. Slechts een beperkt aantal ICT-leveranciers worden gemonitord door strategisch leveranciersmanagement en rijksbreed ICT-categoriemanagement. Continuïteits- en concentratierisico's worden niet (centraal) gemonitord, waardoor hier ook niet op kan worden gestuurd.	4 – Monitoring
F	Organisaties in het Rijk kunnen in noodsituaties wel terugvallen op de afspraken ten aanzien van crisisbeheersing (onder leiding van NCTV), maar niet tot nauwelijks op gezamenlijke noodvoorzieningen.	5 – Faciliteiten
G	Er bestaat geen rijksbrede organisatie en/of governance om snel te anticiperen op een 'bijna-crisissituatie'.	2 – Kennis

Overheidsorganisaties		
H	Veel overheidsorganisaties hebben een ICT-landschap waar sprake is van technische achterstand, een beperkte mate van standaardisatie en 'proprietary' software (leverancierspecifieke ICT-oplossingen). Dat leidt tot beperkte wendbaarheid, in het bijzonder in het geval van acute en langdurige uitval van een ICT-leverancier. In dat geval is herstel van de ICT-dienstverlening vaak een langdurig traject, terwijl het ook lastiger is om maatregelen te treffen voor het mitigeren van de risico's van directe uitval. Het structureel wegwerken van technische schuld moet daarom een belangrijke prioriteit zijn in informatieplannen van overheidsorganisaties.	6 – Informatie-planning
I	Alhoewel op overheidsniveau en binnen individuele overheidsorganisaties vaak wel de kaders en kennis aanwezig zijn om de meeste risico's contractueel goed af te hechten in een ICT-aanbesteding, komt – door een gebrek aan een degelijke multidisciplinaire werkwijze en gebrek aan ervaring binnen een overheidsorganisaties – dit niet in afdoende mate terecht in het uiteindelijk getekende contract.	7 – Kennis; 9 – ICT-uitbesteding
J	Overheidsorganisaties vinden de eigen regievoering over en aansturing van belangrijke ICT-leveranciers onvoldoende door een gebrek aan kennis en kunde om ICT-leveranciers effectief aan te sturen. Kennis en kunde die door de verdere digitalisering van de overheid van groter strategisch belang is geworden.	7 – Kennis
K	De verantwoordelijkheid, kennis en awareness over ICT, beheer en risico's in de gedigitaliseerde overheidsorganisaties zijn nog onvoldoende op alle managementniveaus. Dit onderwerp krijgt daardoor makkelijk te weinig prioriteit, tenzij er een incident is en dan is het te laat. Het ontbreekt aan voldoende digital savvy bestuur en management.	7 – Kennis; 8 – Risico-beheersing; 9 – ICT-uitbesteding
L	ICT-uitbestedingen van cruciale ICT-diensten worden op een te laag operationeel niveau uitgevoerd. Het strategisch risicomanagement bij uitbesteding van cruciale ICT-dienstverlening is onvoldoende en heeft tot nu toe te weinig rekening gehouden met scenario's van acute en langdurige uitval van ICT-dienstverlening.	8 – Risico-beheersing; 9 – ICT-uitbesteding
M	Overheidsorganisaties besteden niet tot nauwelijks aandacht aan concentratierisico's bij aanbestedingen van ICT-dienstverlening. Europese wetgeving (aanbestedingswet) beperkt de ruimte hiervoor.	9 – ICT-uitbesteding

	Kaders om concentratierisico's te beperken, ontbreken. De consequenties van concentratierisico's worden op bestuurlijk niveau onvoldoende afgewogen.	
N	Er bestaat onvoldoende zicht op het eigen ICT-landschap, de gehele leverancierssketen en onderliggende afhankelijkheden bij de ICT-leverancier. De risico's, in het geval van acute uitval, zijn voor de opdrachtgever (klantorganisatie) daarom niet inzichtelijk.	7 – Kennis; 10 – Testen
O	De meeste overheidsorganisatie hebben (contractueel) te weinig terugvalopties ingericht om een crisissituatie en/of acute uitval van hun ICT-diensten op te vangen. Bestaande continuïteitsbeheersmaatregelen (bijvoorbeeld uitwijkmogelijkheden, step-in-rechten, autorisaties, escrow, exitplannen) zijn beperkt geregeld, worden onvoldoende getest of zijn niet voldoende snel te realiseren.	9 – ICT-uitbesteding; 10 – Testen
P	Overheidsorganisaties monitoren op operationeel niveau de risico's van uitbestede ICT-dienstverlening, maar beschouwen en wegen onvoldoende de (strategische) risico's van hun ICT-leveranciers en ICT-dienstverlening. Aanvullend blijkt dat overeengekomen beheersmaatregelen en toezicht zich vooral richten op de kwaliteit en continuïteit van de ICT-dienstverlening en niet van de betreffende ICT-leverancier.	7 – Kennis; 8 – Risico-beheersing

Bijlage B: Risicoclassificatie

De bevindingen ten aanzien van acute uitval van uitbestede ICT-dienstverlening in dit rapport zijn geclassificeerd op twee assen. Verticaal is de moeilijkheidsgraad en inspanning die nodig is om de bevinding opgelost te krijgen. Horizontaal wordt de impact van het risico afgebeeld (laag tot hoog risico). Er is een inschatting gemaakt van de huidige positionering van de bevindingen én het effect daarop van de aanbevelingen. In de risicomatrices is dit met pijlen gevisualiseerd.



Figuur 1 Risicoclassificatiematrix voor bevindingen

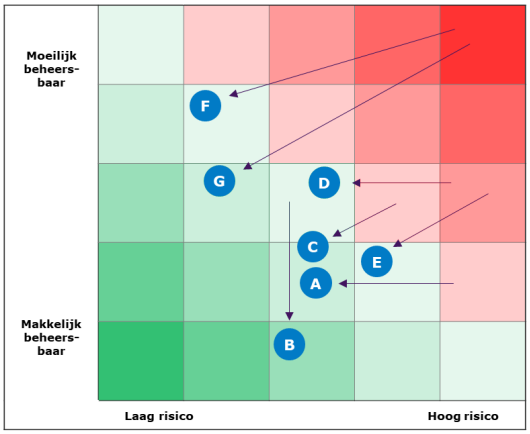
In dit rapport worden voor het plaatsen van bevindingen/risico's op deze assen de volgende definities aangehouden:

Moeilijk beheersbaar:	Om het risico van deze bevinding te mitigeren, is een serieuze inspanning nodig, een projectorganisatie, een directe rapportagelijn naar het bestuur, investeringen van meer dan één miljoen euro en meer dan een half jaar doorlooptijd nodig.
Makkelijk beheersbaar:	Deze bevinding kan waarschijnlijk meegenomen worden in de normale operatie en vraagt nauwelijks extra inspanning. De bevinding kan in enkele weken en hooguit een paar maanden worden weggewerkt.
Laag risico:	Het primaire proces van de organisatie kan doorgang blijven vinden. Misschien met extra tijdelijke inspanning of met inzet van uitwijkfaciliteiten, maar de impact op burger en maatschappij blijft minimaal.
Hoog risico:	Cruciale dienstverlening van de organisatie valt weg, vele burgers, de overheid en bedrijven worden voor langere tijd geraakt op het niveau 'ontwrichtend'.

De aanbevelingen in het derde hoofdstuk zijn bedoeld om hooggeclassificeerde risico's ("rood") met mitigerende maatregelen terug te brengen tot acceptabel niveau ("groen"). Het verantwoordelijke management van een organisatie heeft hierbij altijd zelf de afweging te maken hoe de risico's worden ingeschat, welke mitigerende maatregelen getroffen worden en welke (rest)risico's worden geaccepteerd. Dit is onderdeel van regulier risicomanagement.

A.1 Risicoprofiel overheid, Rijksbreed

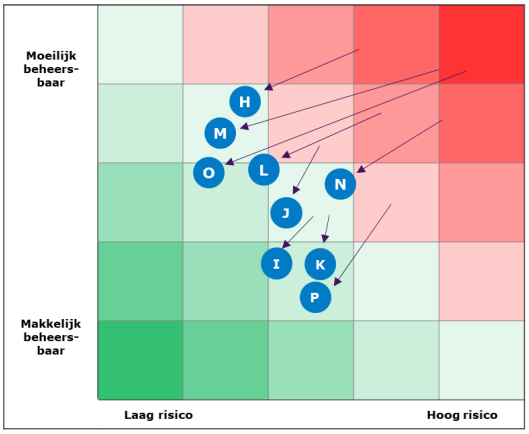
De bevindingen op overheidsniveau zijn geprioriteerd in een risicomatrix op basis van de mate van beheersbaarheid en het risicoprofiel. Er zijn een flink aantal risico's die op overheidsniveau serieus aandacht vragen om te worden opgelost, met name als het gaat om de daadwerkelijke implementatie ("werking"), centraal overzicht en gemeenschappelijke terugvalvoorzieningen.



Figuur 2: Risicoprofiel bevindingen rijksbreed

A.2 Risicoprofiel individuele overheidsorganisaties

De bevindingen voor individuele overheidsorganisaties zijn geprioriteerd in een risicomatrix op basis van de mate van beheersbaarheid en het risicoprofiel. Bij de meeste overheidsorganisaties is niet eerder geanticipeerd op het acuut wegvallen van een (ICT-)dienstverlen***er***, de aandacht gaat in de praktijk uit naar kwaliteit en risico's rond ICT-dienstverlening. Om daar een slag in te maken, zijn er een aantal serieuze bevindingen geconstateerd die overheidsorganisaties moeten willen oppakken om ook bestand te zijn tegen acute en mogelijk langdurige uitval van hun ICT-dienstverleners.



Figuur 3 Risicoprofiel bevindingen overheidsorganisaties

Bijlage C: Voorstel routekaart aanbevelingen

Korte termijn (2025):

- *Aanbevelingen 2*: Investeer en versterk in een competence center voor digitale weerbaarheid van de overheid en investeer in 'digital savvy' bestuur en management (ook op politiek niveau).
- *Aanbeveling 5:* Onderzoek de realisatie van een businesscase voor centrale uitwijkfaciliteiten.
- *Aanbeveling 10:* Bereid 'real life'-uitwijktesten voor en voer ze uit, evenals crisisoefeningen voor hooggevoelige ICT-diensten, deel geleerde lessen.
- *Aanbevelingen 1:* Herijk het rijksbrede sourcingsbeleid, kaders rondom het ICT-risicomanagement en respectievelijke definities.

Middellange termijn (2026):

- *Aanbevelingen 9:* Richt ICT-risicomanagement in, en veranker dit in de P&C-cyclus, etc.
- *Aanbeveling 8:* Start met het op orde maken van een centrale en decentrale registratie van ICT-diensten en producten, en respectievelijk risicomanagement.
- *Aanbeveling 2 en 6:* Blijf continu investeren in kennismanagement, het versterken van digital savvy bestuur en management (ook op politiek niveau), alsmede het versterken van de technische kennis en regievaardigheden van de eigen ICT-organisaties.
- *Aanbeveling 3 en 4:* Richt een rijksbrede toezicht op en monitoring van ICT-risico's in.
- *Aanbeveling 7:* Prioriteer de modernisering van het ICT-landschap in de informatie- en portfolioplanning, prioriteer het inhalen van technische achterstand en het vervangen van legacy in de informatieplanning, prioriteer 'security by design' en 'resilience by design', start initiatieven om de ICT-regiecapaciteit van de eigen (ICT-)organisatie te versterken, etc.
- *Aanbeveling 5:* Bereid de realisatie van centrale uitwijkfaciliteiten voor.
- *Aanbeveling 10:* Houd uitwijkplannen actueel. Voer periodieke 'real life'-uitwijktesten en crisisoefeningen uit, en monitor erop dat aandachtspunten en risico's volgend uit deze testen zo snel als mogelijk worden gemitigeerd.

Lange termijn (2027 en verder):

- *Aanbevelingen 1, 2, 3, 4, 6, 7, 8, 9, 10, 11:* Investeer blijvend in de opbouw en het behoud van kennis en (regie)vaardigheden om de continuïteitsrisico's effectief te beheersen. Voer monitoring en toezicht consequent uit door ICT-diensten, producten en leverancier en bijbehorende risico's te registreren (centraal), de werking van het (ICT)-risicomanagement blijvend te toetsen, het risicolandschap voor (vitale) ICT-dienstverlening proactief te monitoren, hoogrisicoaanbestedingstrajecten vóór publicaties te toetsen, crisisoefeningen en uitwijktesten uit te voeren, etc.
- *Aanbeveling 5:* Realiseer de centrale uitwijkfaciliteiten.

Bijlage D: Geïnterviewden

#	Organisatie
1	Interprovinciaal Overleg (IPO), BIJ12
2	Adviescollege ICT-toetsing (AcICT)
3	Vereniging van Nederlandse Gemeenten (VNG)
4	Universiteit Utrecht
5	Universiteit Tilburg
6	Ministerie van Sociale Zaken en Werkgelegenheid (SZW)
7	Ministerie van Volksgezondheid, Welzijn en Sport (VWS)
8	Ministerie van Infrastructuur en Waterstaat (IenW)
9	Centrum Indicatiestelling Zorg (CIZ)
10	Ministerie van Binnenlandse Zaken, Directoraat-generaal Digitalisering en Overheidsorganisatie (BZK DGDOO)
11	Ministerie van Buitenlandse Zaken (BZ)
12	Belgische overheid
13	Sociale Verzekeringsbank (SVB)
14	Landsadvocaat
15	ICT dienstverleners
16	Ministerie van Defensie
17	Ministerie van Financiën
19	Rijkswaterstaat (RWS)
20	Duitse overheid
21	Rijks inkoop samenwerking(RIS)
22	Ministerie van Justitie en Veiligheid (J&V)
23	Ministerie van Economische Zaken (EZ)
24	Openbaar Ministerie (OM)
25	Belastingdienst
26	Universiteit Twente
27	Universiteit Manchester
28	Nationaal Cyber Security Centrum (NCSC)

Bijlage E: Brondocumenten

- Al-Azad, S., Mohiuddin, M. & Su, Z. (2022). *The Client and Service Provider Relationship in IT Oursourcing Project Success: The Moderating Effects of Organizational Attitudes on Knowledge Sharing and Partnership Quality.*
- Algemene Rekenkamer (2025). *Het Rijk in de cloud. Donkere wolken pakken samen*. Geraadpleegd van: Het Rijk in de cloud | Rapport | Algemene Rekenkamer
- Aubert, B.A., Patry, M. & Rivard, S. (2001). *Managing IT Oursourcing Risk: Lessons Learned.*
- Beljaarts, D. & Szabó, Z. (2025, 17 januari). Initiatiefnota *Wolken aan de horizon* [Kamerbrief]. Geraadpleegd van: Kamerbrief Initiatiefnota Wolken aan de horizon | Kamerstuk | Rijksoverheid.nl
- Berenschot (z.d.). *Mogelijkheden om de afhankelijkheid van ICT-leveranciers te verminderen.*
- Beulen, E. & Ribbers, P.M.A. (2002). *Managing Complex IT Outsourcing-Partnerships.*
- *Companies with a Digitally Savvy Top Management Perform Better*. (2020). MIT CISR. Geraadpleegd van : Companies With a Digitally Savvy Top Management Team Perform Better | MIT CISR
- Cyber Security Raad (2024*). CSR Advies: 'Verkleinen van de Cyberweerbaarheidskloof'.* Geraadpleegd van: CSR Advies 'Verkleinen van de Cyberweerbaarheidskloof' | Advies | Cyber Security Raad
- Data Embassy – e-Estonia. Data Embassy - e-Estonia
- De Nederlandsche Bank (2024). *Weerbaar in een gure wereld: Geopolitieke risico's en financiële instellingen.*
- EU. *Cyber Resilience Act.*
- EU. *The Digital Operational Resilience Act (DORA) – Regulation (EU) 2022/2554.*
- Grant, O. (2024). *Supplier Relationship Management in the Age of Digital Transformation: Insights from E-commerce Businesses.*
- Haq, M.Y.M., Anand, S., Ahista, A. & Nieuwenhuis, L.J.M. (2024). *Cloud Outsourcing Risk Management for Cloud Consumers: A Systematic Literature Review.*
- Hsu, C. et al. (2021). *The Role of Vendor Legitimacy in IT Outsourcing Performance: Theory and Evidence.*
- IAOP. *Outsourcing Professional Body of Knowledge – version 10.* Hoofdstukken 1, 6, 8-10.
- Jia, F., Orzes, G., Sartor, M. & Nassimbeni, G. (2015). *Global sourcing strategy and structure: towards a conceptual framework.*
- Kaiser, J. & Buxmann, P. (2012). *Organizational design of IT supplier relationship management: a multiple case study of five client companies.*
- KPMG (2024). *Presentatie: Strategic Sourcing* [PowerPoint].
- Lioliou, E., Zimmermann, A., Willcocks, L. & Goa, L. (2014). *Formal and relational governance in IT outsourcing: Substitution, complementarity and the role of the psychological contract.*
- Ministerie van Algemene Zaken. *Algemene Rijksvoorwaarden bij IT-overeenkomsten 2022 (ARBIT-2022).* Geraadpleegd van: wetten.nl - Regeling - Besluit vaststelling Algemene Rijksvoorwaarden bij IT-overeenkomsten 2022 (ARBIT-2022) - BWBR0047124
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. *Baseline Informatiebeveilig Overheid.* Geraadpleegd van: Baseline Informatiebeveiliging Overheid Cybersecurity - Digitale Overheid
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. *Sourcingsafwegingskader binnen het Rijk.* Geraadpleegd van: Sourcingsafwegingskader binnen het Rijk
- Ministerie van Justitie en Veiligheid. *Wetsvoorstel Cyberbeveilingswet (NIS2-richtlijn).* Geraadpleegd van: Cyberbeveiligingswet | Overheid.nl | Wetgevingskalender

- Ministerie van Justitie en Veiligheid. *Wetsvoorstel Wet weerbaarheid kritieke entiteiten.* Geraadpleegd van: Wet weerbaarheid kritieke entiteiten | Overheid.nl | Wetgevingskalender
- Nationaal Coördinator Terrorismebestrijding en Veiligheid (2023). *Veiligheidsstrategie voor het Koninkrijk der Nederlanden.* Geraadpleegd van: Veiligheidsstrategie voor het Koninkrijk der Nederlanden | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid
- Nationaal Coördinator Terrorismebestrijding en Veiligheid (2024). *Cybersecuritybeeld Nederland 2024.* Geraadpleegd van: Cybersecuritybeeld Nederland 2024 | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid
- Nationaal Coördinator Terrorismebestrijding en Veiligheid (2024). *Toolbox veilig inkopen.* Geraadpleegd van: Toolbox veilig inkopen (2024) | Economische veiligheid | Nationaal Coördinator Terrorismebestrijding en Veiligheid
- Onderzoeksraad voor Veiligheid (2012). *Het DigiNotarincident – Waarom digitale veiligheid de bestuurstafel te weinig bereikt.* Het DigiNotarincident - Onderzoeksraad voor Veiligheid
- Pels Rijcken (2024). *Verkenning juridische inbedding ABRO.*
- Plugge, A., Bouwman, H & Molina-Castillo, F.J. (2013). *Outsourcing capabilities, organisational structure and performance quality monitoring: toward a fit model.*
- Oshri, I., Kotlarsky, J., & Willcocks, L. (2023). *The Handbook of Global Outsourcing and Offshoring.*
- Rathenau Instituut (2020). *Digitale dreigingen voor de democratie – Over nieuwe technologie en desinformatie.* Geraadpleegd van: Digitale dreigingen voor de democratie | Rathenau Instituut
- Rathenau Instituut (2023). *De digitale overheid in kaart?* Geraadpleegd van: De digitale overheid in kaart? | Rathenau Instituut
- Sociaal en Cultureel Planbureau (2024). Burgerperspectieven 2024 Bericht 1. Geraadpleegd van: Burgerperspectieven 2024 Bericht 1 | Publicatie | Sociaal en Cultureel Planbureau
- Szabó, Z. (2024, 22 november). Overzicht geplande en voorgenomen cloudmigraties van overheids-ICT naar het buitenland [Kamerbrief]. Geraadpleegd van: Kamerbrief over geplande en voorgenomen cloudmigraties van overheids-ICT naar het buitenland | Kamerstuk | Rijksoverheid.nl
- Szabó, Z. (2024, 18 december). Verzamelbrief digitalisering december 2024 [Kamerbrief]. Geraadpleegd van: Kamerbrief diverse onderwerpen digitalisering december 2024 | Kamerstuk | Rijksoverheid.nl
- Van Dam, C., Dortmans, C. & Sibma, S. (2025). *Minder beloven, meer doen – Een eerlijk en uitvoerbaar plan om toeslagenouders verder te helpen*. Geraadpleegd van: Minder beloven meer doen | Kamerstuk | Rijksoverheid.nl
- *Russische cybercriminelen konden data Centric stelen door softwarelek. (2001, 24 januari)*. FD.nl. https://fd.nl/bedrijfsleven/1543474/russische-cybercriminelen-konden-data-centric-stelen-door-softwarelek
- Uitermark, J.J.M. & Brekelmans, R. (2024, 23 augustus). Motie voortgangsrapportage en versnelling ABRO-programma (Algemene Beveiligingseisen Rijksoverheid Opdrachten) [Kamerbrief]. Geraadpleegd van: Kamerbrief over ABRO-programma | Kamerstuk | Rijksoverheid.nl
- Vereniging Sourcing Nederland (2024). *Handboek Sourcing: De belangrijkste inzichten van experts* (1ste editie). Van Duuren Media.
- Wetenschappelijke Raad voor het Regeringsbeleid (2019). *Voorbereiden op digitale ontwrichting"*. Geraadpleegd van: Voorbereiden op digitale ontwrichting | Rapport | WRR