



# Rijksbrede Handreiking IT-sourcing

Versienummer 1.0

Datum 11 oktober 2025

Status Definitieve versie

# Inhoudsopgave

|          |                                                             |           |
|----------|-------------------------------------------------------------|-----------|
| <b>1</b> | <b>Inleiding</b>                                            | <b>3</b>  |
| 1.1      | Aanleiding voor een Rijksbrede handreiking voor IT-sourcing | 3         |
| 1.2      | Wat is IT-sourcing?                                         | 3         |
| 1.3      | Doel van de IT-sourcing handreiking                         | 4         |
| 1.4      | Doelgroep en reikwijdte                                     | 4         |
| 1.5      | Leeswijzer                                                  | 4         |
| <b>2</b> | <b>Positionering IT-sourcing handreiking</b>                | <b>5</b>  |
| 2.1      | Gebruik van de IT-sourcing handreiking                      | 5         |
| 2.2      | Doelen IT-sourcing                                          | 5         |
| <b>3</b> | <b>IT-dienstenmodel</b>                                     | <b>7</b>  |
| 3.1      | IT-dienstenmodel                                            | 7         |
| 3.2      | Definities IT-dienstenmodel Rijksoverheid                   | 8         |
| <b>4</b> | <b>Het IT-sourcing proces</b>                               | <b>9</b>  |
| 4.1      | IT-sourcing levenscyclus Rijksoverheid                      | 9         |
| 4.2      | Fase 1) Behoeftestelling                                    | 10        |
| 4.3      | Fase 2) Strategische sourcing keuze                         | 12        |
| 4.4      | Fase 3) Verwerven en contracteren                           | 14        |
| 4.5      | Fase 4) Implementeren                                       | 15        |
| 4.6      | Fase 5) Monitoren, evalueren en optimaliseren               | 15        |
| 4.7      | Fase 6) Beëindigen                                          | 16        |
| 4.8      | Kennis en regie                                             | 16        |
| <b>5</b> | <b>De IT-sourcing afweging</b>                              | <b>18</b> |
| 5.1      | Sourcing leveringsvormen                                    | 18        |
| 5.2      | Afwegingskader voor IT-sourcing keuze                       | 20        |
| 5.3      | IT-sourcing afwegingskader vragenlijst                      | 21        |
| <b>6</b> | <b>Begrippenlijst</b>                                       | <b>25</b> |
| <b>7</b> | <b>Bijlagen</b>                                             | <b>27</b> |
| A.       | Samenhang met Strategie, Beleid en Wet- en regelgeving.     | 27        |
| B.       | IT-sourcing randvoorwaarden                                 | 28        |
| C.       | IT-sourcing principes                                       | 29        |
| D.       | Bronvermelding                                              | 31        |
| E.       | Afkortingenlijst                                            | 31        |

# 1 Inleiding

## 1.1 Aanleiding voor een Rijksbrede handreiking voor IT-sourcing

In lijn met het bestaande sourcingafwegingskader uit 2012<sup>(1)</sup> leggen Nederlandse overheden de focus op kernactiviteiten en worden veel van de ondersteunende IT-activiteiten uitbesteed aan IT-leveranciers. Enerzijds bieden IT-leveranciers kansen op het gebied van technologische ontwikkelingen, digitale slagkracht en professionele dienstverlening, anderzijds zijn overheden sterker afhankelijk geworden van IT-leveranciers voor IT-diensten die, door de digitalisering van de Nederlandse overheid, van groot strategisch belang zijn<sup>(2)(3)</sup>.

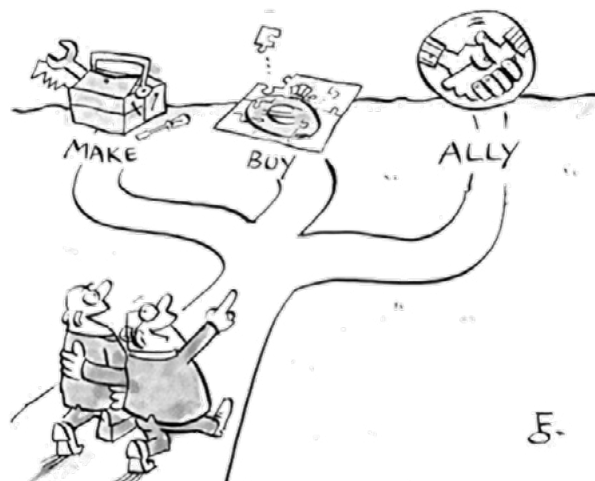
Recente gebeurtenissen leggen de risico's van het huidige IT-sourcingbeleid bloot, zoals (onzichtbare) marktconcentratie, niet-functionerende exit-strategieën en ontbrekende uitwijk-/terugvalopties. Alsmede de risico's van beperkte kennis en kunde binnen organisaties om effectief regie te voeren over een complex landschap van in- en uitbestede IT-diensten, (beleids)wijzigingen en gewenste innovaties. Het complexe speelveld van vele IT-diensten, die op verschillende wijze zijn gesourced, leidt soms onbedoeld tot onder andere lock-in effecten, technische achterstanden, vraagstukken over soevereiniteit en autonomie. Dit resulteert in continuïteits- en concentratierisico's die de digitale weerbaarheid van de Nederlandse overheid beperken<sup>(2)</sup>.

Organisaties hanteren eigen technologische keuzes en kennen verschillende sourcing leveringsvormen voor in essentie vergelijkbare IT-diensten. In lijn met de Nederlandse Digitaliseringsstrategie (NDS), wordt gesteld dat een versnippering van IT-sourcing strategieën *“in de weg zit om onze weerbaarheid te versterken, dienstverlening te verbeteren en versnelling te maken en kwaliteit te borgen. De snelheid in de ontwikkeling van technologie, krapte op de arbeidsmarkt en de geopolitieke ontwikkelingen maken het noodzakelijk om de krachten te bundelen. De EU Digital Decade doelen<sup>(4)</sup>, zoals de digitalisering van overheidsdiensten, hoogwaardige digitale professionals en digitale weerbaarheid en autonomie, versterken deze urgentie”*.

Het huidige Rijksbrede IT-sourcingbeleid, de bijbehorende afwegingskaders en vooral de toepassing daarvan beschermen in de praktijk overheidsorganisaties nog onvoldoende. Deze problematiek, maar ook mogelijke kansen voor de Rijksoverheid en markttrends in IT-sourcing zijn nader toegelicht in de Rijksbrede strategie IT-sourcing<sup>(5)</sup>. Organisaties dragen de verantwoordelijkheid om te acteren op deze problematiek, conform de NDS die stelt dat *“de tijd van vrijblijvendheid voorbij is”*. De ambitie is dat deze handreiking uiteindelijk ook onder de NDS verder doorontwikkeld wordt tot een handreiking voor de gehele overheid.

## 1.2 Wat is IT-sourcing?

IT-sourcing betreft de keuze van een organisatie om IT-producten en IT-diensten zelf te leveren, samen met een andere partij te leveren, of te laten leveren door een andere partij. De keuze voor de gewenste sourcingvorm varieert per sourcingvraagstuk en bepaalt hoe een organisatie haar organisatiedoelen (bijvoorbeeld dienstverlening) en bedrijfsvoering wenst in te vullen.



**Figuur 1** IT-sourcing - de keuze om IT-activiteiten zelf te leveren, samen met een andere partij te leveren of te laten leveren door een andere partij

1 Sourcingafwegingskader binnen het Rijk, 9 mei 2012

2 Van Kwetsbaar naar weerbaar: geleerde lessen uit dreigende acute en langdurige uitval van uitbestede ICT-dienstverlening bij overheidsorganisaties, maart 2025

3 Het Rijk in de cloud: Donkere wolken pakken samen, januari 2025

4 Europa's digitale decennium: Doelstellingen voor 2030, 27 september 2023

5 Rijksbrede Strategie IT-sourcing

## 1.3 Doel van de IT-sourcing handreiking

Deze Rijksbrede IT-sourcing handreiking biedt een eenduidige wijze waarop de afweging gemaakt wordt hoe IT-diensten binnen de Rijksoverheid gesourced worden. Het heeft tot doel om tot een consistente aanpak te komen van IT-sourcing. Het faciliteert het herkennen en beheren van IT-sourcing gerelateerde risico's en stelt de Rijksoverheid in staat om deze risico's effectief te monitoren en te mitigeren, en resterende risico's op bestuurlijk niveau te accepteren.

De handreiking belicht drie elementen van IT-sourcing:

1. De **IT-dienst** ('wat'):

Dit element richt zich op de specifieke IT-diensten die gerealiseerd moeten worden om aan de behoefte te voldoen. Het IT-dienstenmodel biedt een overzicht van het IT-landschap en waarborgt een uniforme terminologie en afbakening van IT-diensten.

2. Het **IT-sourcing proces** ('hoe'):

Dit element focust op de wijze waarop de Rijksoverheid op een eenduidige, gestructureerde en gecontroleerde manier invulling geeft aan het sourcen van IT-diensten. De IT-sourcing levenscyclus van de Rijksoverheid beschrijft dit proces.

3. De **IT-sourcing afweging** ('wie'):

Dit element behandelt de keuze over wie de IT-dienst levert. Het omvat de beslissing over de geschikte sourcing leveringsvorm (zelf doen, samenwerken of uitbesteden) en de geschikte leverende partij. Met het afwegingskader kan een weloverwogen keuze gemaakt worden over de sourcing leveringsvorm.

De handreiking moet organisaties ondersteuning bieden in het uitvoeren van IT-sourcing, alsook handvatten bieden bij het maken van de strategische keuzes hieromtrent. Door uniformiteit in sourcing levert elke organisatie een optimale bijdrage aan de overkoepelende IT-sourcing doelstellingen van de Rijksoverheid.

Het Center of Excellence voor IT-sourcing, zoals uitgelicht in de Rijksbrede Strategie IT-sourcing, heeft als taak om op basis van geleerde lessen en opgedane ervaring deze handreiking te actualiseren en te verrijken, bijvoorbeeld door het aanbieden van templates, procedures en delen van risico's die organisatie-overstijgend zijn.

## 1.4 Doelgroep en reikwijdte

De handreiking IT-sourcing kent verschillende doelgroepen. Het is geschreven voor en vanuit het strategisch perspectief van de bestuurders en lijnmanagers. De verschillende onderdelen variëren in mate van detail en zorgen voor aansluiting bij meer inhoudelijke rollen zoals IT-managers, inkopers en/of IT-sourcing managers.

De reikwijdte van dit document bestrijkt:

- Organisatorisch: de Rijksoverheid zonder zelfstandige bestuursorganen (zbo's).
- Technisch: het volledige IT-landschap van de Rijksoverheid, zie hoofdstuk 3 voor nadere detaillering.

Bovenstaande reikwijdte betreft het eerste plateau. Voor verdere uitbreiding van de Handreiking IT-sourcing naar de twee opvolgende plateau's, waarin plateau 2 de zbo's, Hoge Colleges van Staat en adviescolleges omvat en plateau 3 de gehele overheid, wordt verwezen naar de Rijksbrede strategie IT-sourcing.<sup>(6)</sup>

## 1.5 Leeswijzer

Dit document kent 6 hoofdstukken en 5 bijlagen.

- In hoofdstuk 1 wordt de aanleiding, het doel en de reikwijdte voor dit document nader omschreven (dit hoofdstuk).
- In hoofdstuk 2 wordt de positionering en de (strategische) context van deze handreiking toegelicht.
- In hoofdstuk 3 (**IT-dienst**) wordt het IT-dienstenmodel beschreven dat een overzicht van de geclusterde IT-diensten in zes domeinen.
- In hoofdstuk 4 (**IT-sourcing proces**) wordt de IT-sourcing levenscyclus nader toegelicht, met randvoorwaarden en principes, die beschrijft hoe het IT-sourcing proces dient te worden doorlopen voor elk sourcingsvraagstuk.
- In hoofdstuk 5 (**IT-sourcing afweging**) wordt nader ingegaan op de verschillende sourcing leveringsvormen en bevat een afwegingskader waarmee de geschikte leveringsvorm kan worden vastgesteld.
- In hoofdstuk 6 staat de begrippenlijst waar de meest voorkomende begrippen van deze strategie beschreven staan.
- In de bijlagen van dit document staat nadere onderbouwing, uitwerking van de voorliggende hoofdstukken en de bronvermelding.



# 2 Positionering IT-sourcing handreiking

Dit hoofdstuk beschrijft de wijze waarop deze IT-sourcing handreiking gebruikt dient te worden, alsmede samenhang met bestaande strategische- en beleidskeuzes, en wet- en regelgeving.

## 2.1 Gebruik van de IT-sourcing handreiking

De IT-sourcing handreiking biedt organisaties binnen de Rijksoverheid een gestructureerde richtlijn voor het sourcen van IT-diensten:

- Het bevat een logische structurering van IT-diensten.
- Het bevat de belangrijkste activiteiten, resultaten, randvoorwaarden en principes om in acht te nemen tijdens fasen van het IT-sourcing proces.
- Het bevat essentiële overwegingen die organisaties moeten meenemen in hun keuzeproces rondom IT-sourcing.

Gebruikers van de handreiking zijn verantwoordelijk voor de implementatie ervan in de specifieke situatie van de organisatie en dragen de uiteindelijke verantwoordelijkheid voor de genomen beslissingen.

Het wordt aanbevolen om de verschillende onderdelen (IT-dienstenmodel, het IT-sourcing proces en het IT-sourcing afwegingskader) van de IT-sourcing handreiking te doorlopen, te hanteren of de resultaten ervan te actualiseren op de volgende momenten:

- Bij de identificatie van een nieuwe functionele behoefte
- Bij het aangaan van een nieuwe sourcing overeenkomst
- Bij de verlenging van een bestaande sourcing overeenkomst
- Bij materiële wijzigingen in de aard, duur of voorwaarden van een bestaande sourcing overeenkomst
- Bij ingrijpende gebeurtenissen (o.a. dreigende discontinuïteit van leverancier) en/of ontwikkelingen (o.a. cyberaanvallen) die een bestaande sourcing overeenkomst raken

## 2.2 Doelen IT-sourcing

In de Rijksbrede strategie voor IT-sourcing zijn zes IT-sourcing doelen geformuleerd. Deze IT-sourcing doelen onderlijnen de bredere doelen en strategieën van de Rijksoverheid, zoals weergegeven in bijlage A, en dragen bij aan de duurzame verbetering van IT-sourcing.

De IT-sourcing doelen dienen als leidend te worden gebruikt bij het maken van keuzes en besluiten over sourcing.

### 1. Betrouwbare publieke dienstverlening - betere continuïteit van IT-diensten

We zorgen voor betrouwbare publieke dienstverlening door continuïteit van IT-diensten beter te waarborgen. Dat vraagt om tijdige signalering van kwetsbaarheden, in nauwe samenspraak met ministeries en uitvoeringsorganisaties. Veel cruciale diensten – zoals uitkeringen, vergunningen of veiligheidssystemen – zijn afhankelijk van externe IT-leveranciers. Dat stelt hoge eisen aan contracten, exit-strategieën, monitoring en risicobeheersing. Deze strategie helpt om kritieke afhankelijkheden in beeld te krijgen en daar bewuste keuzes in te maken.

### 2. Meer regie op digitale autonomie, soevereiniteit en veiligheid

Als overheid moeten we in controle blijven over onze digitale infrastructuur. Dat vraagt om kennis van waar onze data staat, hoe ketens verlopen en welke leveranciers sleutels in handen hebben. De strategie versterkt deze autonomie door het stellen van eisen aan interoperabiliteit, transparantie in de keten en heldere uitgangspunten voor sourcingkeuzes. Ingezet wordt op exit-strategieën of andere maatregelen om digitale autonomie en soevereiniteit te kunnen waarborgen.

### **3. Slimmer samenwerken als één overheid**

Veel organisaties lopen tegen vergelijkbare IT-sourcingvraagstukken aan, maar lossen deze afzonderlijk op. Door contracten, kennis en aanpak te bundelen, kunnen we effectiever onderhandelen, risico's beter beheersen en kosten besparen. De strategie zet in op gezamenlijke IT- en inkoopkaders, herbruikbare kennisproducten en betere onderlinge afstemming.

### **4. Meer inzicht in afhankelijkheden en kwetsbaarheden**

Op dit moment ontbreekt een Rijksbreed overzicht van welke leveranciers welke IT leveren. Daardoor zijn concentratierisico's en afhankelijkheden vaak pas zichtbaar als het misgaat. Daarom gaan we aan de voorkant zorgen voor meer inzicht in afhankelijkheden en kwetsbaarheden. Dit vraagt om onder meer om inzicht in afgesloten contracten en monitoring van leveranciers, die bij belangrijke overheidsprocessen betrokken zijn. Het inrichten van strategisch productmanagement op basis van een aantal IT-Domeinen brengt in kaart wie wat levert, voor welke functies, en waar kwetsbaarheden ontstaan. Dit helpt om risico's tijdig te signaleren en beter te beheersen.

### **5. Wendbaarheid en innovatie versnellen**

De markt beweegt snel. Om nieuwe technologieën verantwoord te kunnen inzetten, moeten we flexibel kunnen contracteren, samenwerken en opschalen. Dat vraagt om een betere gezamenlijke regie, aanpasbare contractvormen, betere kennisdeling en een sourcingaanpak die ruimte geeft aan innovatie en samenwerking.

### **6. Beter benutten van bestaande praktijkkennis en best practices**

Binnen het Rijk zijn al veel goede voorbeelden ontstaan van slimme en effectieve sourcingaanpakken. Door deze best practices te verzamelen, zichtbaar te maken en actief te delen, versnellen we gezamenlijke professionalisering. Organisaties kunnen leren van wat elders goed werkt en daarmee hun eigen aanpak versterken.

# 3 IT-dienstenmodel

Dit hoofdstuk introduceert het IT-dienstenmodel. Het geeft daarmee invulling aan de ‘Wat’-vraag van IT-sourcing en geeft een gemeenschappelijk definitie (in de vorm van domeinen en sub-domeinen) van het Rijksbrede IT-landschap.

## 3.1 IT-dienstenmodel

Het IT-dienstenmodel biedt gebruikers een manier om IT-diensten (en onderliggende IT-producten) binnen het IT-landschap van de organisatie te categoriseren. Het stelt een organisatie in staat om IT-diensten te verkavelen en ondersteunt bij het op consistente en herkenbare wijze doorlopen van het sourcing proces met resulterende sourcingkeuzes (per domein of sub-domein).

Het IT-dienstenmodel is opgesteld aan de hand van bestaande (architectuur-) modellen binnen de Rijksoverheid (denk aan het RORA capabiliteitsmodel, huidige sourcing strategie

et cetera) en is afgestemd met vertegenwoordigers uit verschillende perspectieven.

Het model is een schematische weergave waarbij de omvang van de domeinen en sub-domeinen los staan van de werkelijke omvang of het belang van een domein binnen de organisatie.

Voor verschillende sub-domeinen met een gelijke kleur geldt dat deze een zodanige afhankelijkheid hebben dat een sourcing afweging mogelijk in samenhang gemaakt moet worden. De definities van de sub-domeinen zijn nader beschreven in de onderstaande sub-sectie.

### Domein A. Strategie, Beleid & Regie

|                        |
|------------------------|
| 1. Strategie en Beleid |
| 2. Regie               |

### Domein B. Domeinoverstijgende diensten

|                            |                       |
|----------------------------|-----------------------|
| 3. Gebruikersondersteuning | 4. Beveiliging        |
| 5. Toegangsbeheer          | 6. Gegevensmanagement |

### Domein C. Operationele Technologie

|                             |
|-----------------------------|
| 7. Operationele Technologie |
|-----------------------------|

### Domein D. Bedrijfstechnologie

|                          |                                       |                                   |
|--------------------------|---------------------------------------|-----------------------------------|
| 8. Functioneel beheer    |                                       |                                   |
| 9. Producten (licenties) |                                       |                                   |
| 11. Cloud SaaS           | 10. Applicatieontwikkeling en -beheer |                                   |
|                          | 12. Cloud PaaS/IaaS                   | 13. IT-platform en infrastructuur |

### Domein E. Kantoorautomatisering

|                                      |                                 |
|--------------------------------------|---------------------------------|
| 14. Werkomgeving                     |                                 |
| 15. IT-platform en infrastructuur KA | 16. Multifunctionals en netwerk |

### Domein F. Connectiviteit

|                    |
|--------------------|
| 17. Connectiviteit |
|--------------------|

Figuur 2 IT-dienstenmodel Rijksoverheid

## 3.2 Definities IT-dienstenmodel Rijksoverheid

| #  | Sub-domein                                           | Definitie                                                                                                                                                                                                                                                                                                                                     |
|----|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Strategie & beleid                                   | Betreft activiteiten zoals strategieontwikkeling, -advies en (IT), besluit- en beleidsvorming om het beheer en de realisatie van wet en regelgeving, beleid, informatieplannen, dienstenportfolio's, etc.. te waarborgen.                                                                                                                     |
| 2  | Regie                                                | Betreft de gehele set aan samenhangende activiteiten om integraal IT-diensten en ketens binnen een IT-landschap te realiseren, beheren en in stand te houden (e.g. architectuur, portfolio management, SIAM, contract- en leveranciersmanagement)                                                                                             |
| 3  | Gebruikers-ondersteuning                             | Betreft het eerste aanspreekpunt voor eindgebruikers, met directe ondersteuning gebaseerd op organisatie-specifieke kennis en IT-complexiteit.                                                                                                                                                                                                |
| 4  | Beveiliging                                          | Betreft het beheren van de securityprotocollen en procedure, en diensten zoals SIEM en SOC, allen gericht op het waarborgen en versterken van de digitale weerbaarheid van de overheid.                                                                                                                                                       |
| 5  | Toegangsbeheer                                       | Betreft het realiseren en beheren van de identiteits- en toegangsprotocollen en -procedures binnen de overheid, essentieel voor het waarborgen van de veiligheid van gebruikers en systemen, en de data-integriteit.                                                                                                                          |
| 6  | Gegevensmanagement                                   | Betreft het realiseren en beheren van de protocollen en procedures om te waarborgen dat publieke en gerubriceerde gegevens op een veilige en effectieve wijze binnen en buiten de overheid beschikbaar worden gesteld.                                                                                                                        |
| 7  | Operationele technologie (OT)                        | Betreft het leveren en instandhouding van hardware- en softwareoplossingen die essentieel zijn voor de primaire bedrijfsprocessen (binnen de industriële omgevingen) van organisaties.                                                                                                                                                        |
| 8  | Functioneel beheer                                   | Betreft het onderhoud en beheer van de IT-functionaliteit van programmatuur, gebaseerd op de functionele en technische eisen en wensen van eindgebruikers.                                                                                                                                                                                    |
| 9  | Producten (licenties)                                | Betreft standaard programmatuur die gebruikt wordt ten behoeve van primaire bedrijfsprocessen en de bedrijfsvoering.                                                                                                                                                                                                                          |
| 10 | Applicatieontwikkeling en -beheer                    | Betreft het ontwerpen, bouwen, testen, implementeren, beheren, onderhouden en doorontwikkelen van programmatuur ten behoeve van primaire bedrijfsprocessen en de bedrijfsvoering.                                                                                                                                                             |
| 11 | Cloud SaaS                                           | Betreft in hoge mate gestandaardiseerde software die door een leverancier As a Service vanuit de Cloud (online) wordt aangeboden ten behoeve van primaire bedrijfsprocessen en de bedrijfsvoering.                                                                                                                                            |
| 12 | Cloud PaaS/IaaS                                      | Betreft een leveringsmodel waarmee kant-en-klare IT-infrastructuur en ontwikkelingsplatform wordt aangeboden vanuit de Cloud.                                                                                                                                                                                                                 |
| 13 | IT-platform en infrastructuur                        | Betreft het leveren en instandhouding van een platform omgeving inclusief databases, middleware en operating systemen ten behoeve van het ontwikkelen, onderhouden en draaien van programmatuur.                                                                                                                                              |
| 14 | Werkomgeving                                         | Betreft – waar van toepassing – het leveren en instandhouding van de werkplekapplicaties en collaboratieve diensten (zoals Microsoft Office en SharePoint) en andere essentiële werkplekdiensten zoals Unified Communications en Virus Management.                                                                                            |
| 15 | IT-platform en infrastructuur Kantoor-automatisering | Betreft het leveren en instandhouding van de infrastructuur- en platformomgeving die nodig is voor de ontwikkeling, het beheer, het onderhoud en de exploitatie van werkomgeving applicaties. Het omvat ook de databases, middleware en besturingssystemen, gebaseerd op zowel traditionele als container technologieën die dit ondersteunen. |
| 16 | Multifunctionals en netwerk                          | Betreft het leveren en instandhouding van de communicatie-infrastructuur binnen kantooromgevingen, inclusief print-, scan- en faxapparatuur, vaste en mobiele telefoniediensten, en WLAN-beheer zoals WiFi-routers en switches.                                                                                                               |
| 17 | Connectiviteit                                       | Betreft het leveren en instandhouding van de connectiviteit tussen (fysieke) locaties en de verbinding met het internet inclusief de benodigde beveiligingselementen.                                                                                                                                                                         |

Tabel 1 Definities van de IT-diensten in het IT-dienstenmodel Rijksoverheid



# 4 Het IT-sourcing proces

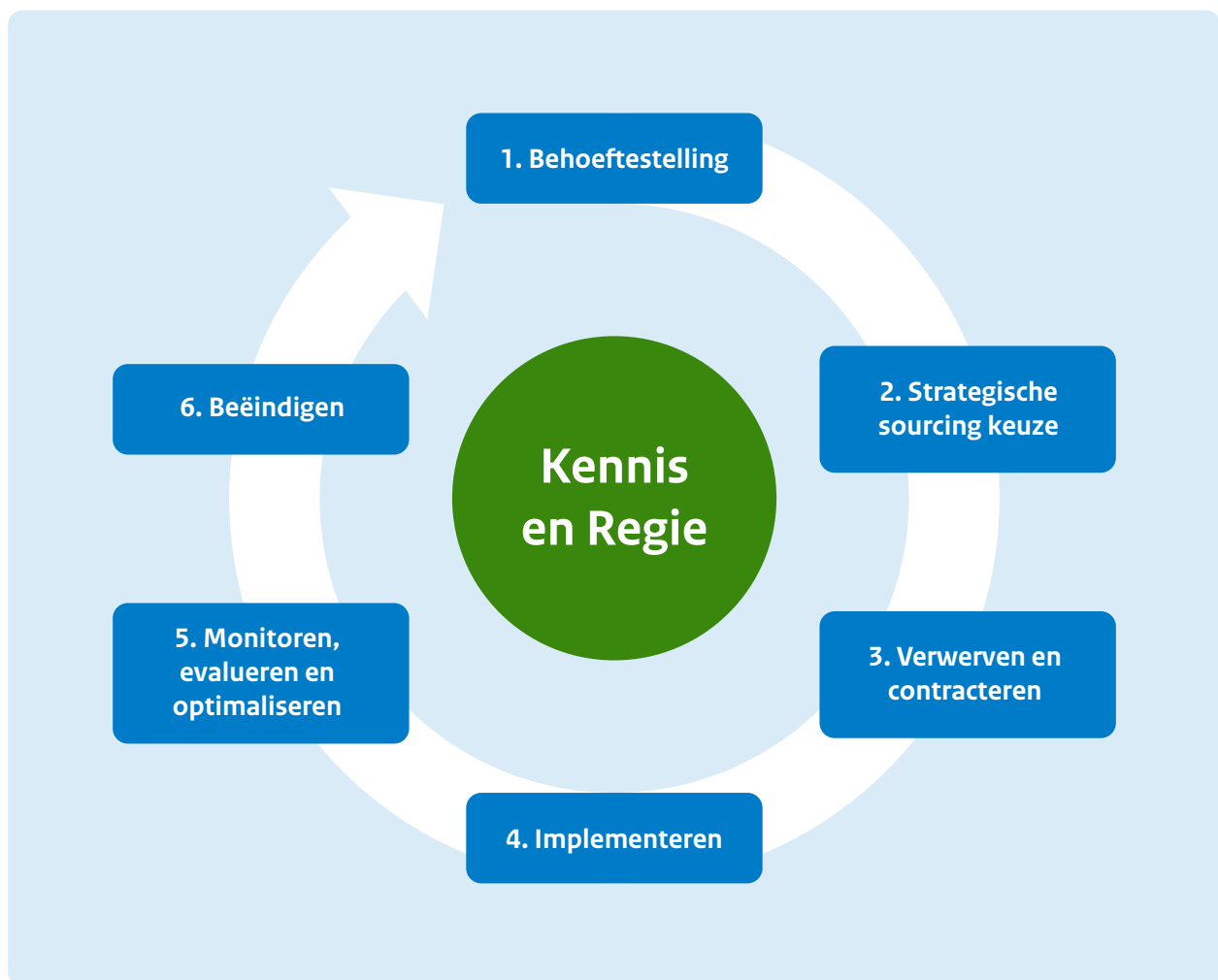
Dit hoofdstuk beschrijft de IT-sourcing levenscyclus van de Rijksoverheid. Het biedt een leidraad voor de invulling van het sourcing proces en beschrijft de aanbevolen manier voor de uitvoering van sourcing van IT-diensten binnen de Rijksoverheid.

## 4.1 IT-sourcing levenscyclus Rijksoverheid

De levenscyclus vormt de basis voor het proces van IT-sourcing binnen de Rijksoverheid. De fasen in de levenscyclus bevatten de benodigde activiteiten en resultaten voor sourcingtrajecten in de specifieke context van de

Rijksoverheid. De levenscyclus is gebaseerd op de Digital Operational Resilience Act (DORA)<sup>(7)</sup> en EBA-richtlijnen<sup>(8)</sup>, welke reeds in gebruik zijn genomen binnen de Europese financiële sector.

Elk sourcingtraject doorloopt de volledige cyclus, ongeacht of het interne levering, een samenwerking of uitbesteding betreft. De cyclus begint met het vaststellen van behoeften en loopt door tot de beëindiging van de sourcing relatie, zie figuur 3. De activiteiten binnen de fasen zijn soortgelijk voor alle sourcing leveringsvormen. Afhankelijk van de gekozen leveringsvorm kan het aanbestedingsrecht van toepassing zijn; in dat geval dienen de daarvoor geldende procedures gevolgd te worden.



**Figuur 3** IT-sourcing levenscyclus Rijksoverheid

7 Digital Operational Resilient Act (DORA), december 2022

8 EBA Guidelines of outsourcing arrangements, maart 2019

De levenscyclus vergroot het handelingsperspectief van de organisatie en bevordert het verkrijgen van grip op IT-sourcing. Dit gebeurt door actieve risicobeheersing, uniformiteit in het sourcing proces en het creëren van overzicht in alle fasen van de levenscyclus.

De verschillende fasen hebben onderstaande specifieke doelen:

1. **Behoeftestelling.** Het doel van deze fase is het definiëren van de functionele behoefte en de daaraan gerelateerde IT-diensten. Dit biedt een gestructureerde en duidelijke basis voor het verdere sourcing proces.
2. **Strategische sourcing keuze.** Het doel van deze fase is het bepalen van de meest geschikte sourcing leveringsvorm voor het verwerven van de benodigde IT-diensten. Deze keuze moet strategisch zijn afgestemd op zowel de organisatorische behoeften als de Rijksbrede en organisatie strategieën voor IT-sourcing.
3. **Verwerven en contracteren.** Het doel van deze fase is het selecteren van de juiste dienstverlening en het formaliseren van de overeenkomsten conform de benodigde procedures. Deze fase moet zorgen voor een effectieve en juridisch solide overeenkomst die de basis legt voor een succesvolle implementatie, uitvoering en wanneer nodig toekomstige beëindiging.
4. **Implementeren.** Het doel van deze fase is de daadwerkelijke implementatie van de IT-dienst. De IT-dienst dient te worden geïntegreerd in het IT-landschap en leverancierslandschap van de organisatie en de Rijksoverheid, met minimale beperkingen voor de bestaande IT-dienstverlening.
5. **Monitoren, evalueren en optimaliseren.** Het doel van deze fase is het waarborgen en verbeteren van de prestaties, veiligheid en kosteneffectiviteit van de geïmplementeerde IT-dienst. Hierbij is het noodzakelijk om continu de prestaties te monitoren en evaluaties uit te voeren om te garanderen dat de IT-dienst blijvend voldoet aan wet- en regelgeving en aan de vastgestelde kwaliteitsstandaarden.
6. **Beëindigen.** Het doel van deze fase is het correct beëindigen van de overeenkomst en/of gemaakte afspraken<sup>9</sup>. Dit kan zijn vanwege de afloop van contracttermijnen of tussentijdse beëindiging. De (re) transitie dient zo soepel mogelijk te verlopen, met de focus op het minimaliseren van risico's en beperkte onderbreking van de IT-dienst.

7. **Kennis en Regie.** De aanwezigheid van kennis, zowel op het gebied van sourcing als functionele kennis van IT-diensten, ondersteunt de activiteiten in alle fasen. Effectieve regievoering over zowel interne als externe dienstverleners waarborgt de continuïteit en kwaliteit van dienstverlening, en zorgt ervoor dat er efficiënt kan worden ingespeeld op veranderende behoeften en technologische ontwikkelingen. Organisaties worden hierin ondersteunt door Rijksbrede (sourcing)kennis en regievoering.

Binnen normale omstandigheden wordt aanbevolen de fasen in figuur 3 procesmatig te doorlopen. Echter, onvoorziene omstandigheden kunnen zorgen voor een alternatieve volgorde van de sourcing levenscyclus. Bijvoorbeeld, in het geval van faillissement van een leverancier tijdens fase 4 (Implementatie), wordt de organisatie gedwongen direct over te gaan tot fase 6 (Beëindigen).

In de volgende paragrafen is per fase een omschrijving, de activiteiten, de resultaten en de belangrijkste principes en randvoorwaarden beschreven. Een volledige lijst van principes en randvoorwaarden staan in respectievelijk bijlage B en C.

## 4.2 Fase 1) Behoeftestelling

De fase van behoeftestelling richt zich op het definiëren van de functionele behoefte en benodigde IT-dienst die als basis dient voor opvolgende fasen. Een correct vastgestelde behoefte is noodzakelijk om de juiste IT-dienst te kunnen selecteren.

### Activiteiten:

1. **Definiëren van de functionele behoefte:** Definieer de behoefte en indien van toepassing het onderliggende probleem in samenspraak met de behoeftesteller. De functionele behoefte moet de 'wat' vraag beantwoorden van (eind)gebruikers en niet ingaan op wijze waarop dit moet worden geleverd. Maak gebruik van een multidisciplinair team met voldoende expertise van alle aspecten (functioneel, technisch, et cetera.). Het advies is hierbij gebruik te maken van het beleidskompas en de business doelstellingen van de organisatie.

9 Er wordt gesproken over afspraken indien er sprake is van zelf doen. Ook in deze situatie dienen afspraken voor gemaakt te worden maar hebben niet dezelfde contractuele aard.

2. **Vaststellen van bundelingsmogelijkheden:** Onderzoek of andere afdelingen binnen de eigen organisatie, of andere organisaties van de Rijksoverheid, vergelijkbare behoeften hebben. Dit maakt het mogelijk om gezamenlijk op te treden. Zie ook figuur 4, dat een overzicht biedt van de verschillende niveaus waarop behoeften gebundeld kunnen worden. Gebruik hiervoor de volgende middelen:
  - a. De Rijksbrede product en diensten catalogus
  - b. De categorieplannen van inkoop
  - c. Het contractenregister en Rijksinkoop register
  - d. Lijst met generieke voorzieningen
3. **Specificeren van de benodigde IT-dienst:** Specificeer de benodigde IT-dienst op basis van de vastgestelde (business) behoeften en, indien van toepassing, de stappen uit het beleidskompas. Stel vervolgens een gedetailleerde dienstenomschrijving op met de eisen en wensen. Vul daarnaast de Business Impact Analysis (BIA), de Privacy Impact Assessment (PIA) en de Informatiebeveiligingsscan (IB-scan) in om een volledig overzicht van de IT-vereisten en risico's te verkrijgen.
4. **Stel een sourcingstrategie op:** Bepaal aan de hand van de uitkomsten van voorgaande activiteiten de sourcingstrategie voor de IT-dienst. Geef aan hoe de dienst moeten worden gesourced door te beschrijven hoe de vervolgfasen van de IT-sourcing levenscyclus eruitzien.

#### Resultaten

- Dienstomschrijving, incl. eisen en wensen
- Uitgevoerde Business Impact Analyse (BIA)
- Uitgevoerde Privacy Impact Analyse (PIA)
- Uitgevoerde Informatiebeveiligingsscan (IB-scan)
- Sourcingstrategie IT-dienst

#### Belangrijke randvoorwaarden

- Een BIA en PIA maken structureel deel uit van de voorafgaande risicoanalyse in het kader van de behoeftebepaling.
- Regievoering wordt uitgevoerd door de Rijksoverheid, waarbij de bevoegdheid voor strategische en autonome besluiten volledig gewaarborgd is binnen de Rijksoverheid.

#### Belangrijkste principes

- Waar mogelijk worden behoeften (vragen) gebundeld zodat op uniforme wijze IT-dienstverlening kan worden afgenomen.
- Bij verkaveling wordt rekening gehouden met de samenhang met overige IT-dienstverlening en ketens.
- De IT-sourcing strategie wordt geïntegreerd in de bredere bedrijfsvoering en IT-sourcing strategieën van Rijksonderdelen.

### Rijksbreed

De behoefte voor de IT-dienst kan gebundeld worden binnen de Rijksoverheid.

### Departementaal

De behoefte voor de IT-dienst kan worden gedeeld met organisaties binnen het departement.

### Organisatie

De behoefte van de IT-dienst is specifiek voor de organisatie en wordt individueel ingevuld.

**Figuur 4** Niveaus binnen de Rijksoverheid voor het bundelen van behoeften.

## 4.3 Fase 2) Strategische sourcing keuze

In de fase van strategische sourcing keuze wordt bepaald welke sourcing leveringsvorm het beste aansluit bij het verkrijgen van de benodigde IT-dienst. Deze keuze stemt overeen met de organisatorische behoeften en IT-sourcing strategieën van de organisatie en de Rijksoverheid. Het wordt aanbevolen om voor deze besluitvorming de noodzakelijke technische en functionele expertise te raadplegen. Daarnaast wordt op basis van het risicoprofiel een beheersregime bepaald voor de vervolgfases van de levenscyclus.

### Activiteiten:

1. **Bepalen van het kritieke of strategische belang van de IT-dienst:**  
Controleer of de IT-dienst als kritiek of strategisch wordt gekenmerkt binnen de organisatie. Indien deze classificatie niet beschikbaar is dient dit aan de hand van het belang voor de “Vitale processen Rijksoverheid” vastgesteld te worden<sup>(10)</sup>.
2. **Bepalen van de sourcing leveringsvorm:**  
Bepaal aan de hand van het IT-sourcing afwegingskader in hoofdstuk 5 de meest geschikte sourcing leveringsvorm. Belangrijk hierbij is of een IT-dienst zelf wordt uitgevoerd, in samenwerking wordt gerealiseerd of uitbesteed wordt. De keuze om een IT-dienst intern of extern te beleggen heeft invloed op de vervolgfases in de sourcing levenscyclus.
3. **Actualiseren van risicoprofiel IT-dienst:**  
Actualiseer de Business Impact Analysis (BIA) en Privacy Impact Assessment (PIA) op basis van de inzichten uit stap 1 en 2 van deze fase.
4. **Opstellen continuïteitsplan en terugvaloptie:**  
Ontwikkel een continuïteitsplan (Business Continuity Plan – BCM) dat zorgt voor de continuïteit van de IT-dienst, gebaseerd op de BIA en PIA, de vitaliteit en de sourcing leveringsvorm.

### 5. Vaststellen regime sourcing levenscyclus:

Beoordeel op basis van de uitkomsten van de Business Impact Analysis (BIA), het Basisbeveiligingsniveau (BBN), de Informatiebeveiligingsscan, de geschatte waarde (in euro) en eventueel de Privacy Impact Assessment (PIA) of de IT-dienst onder een streng (verscherpt) of minder streng (regulier) regime valt<sup>(11)</sup>. Het vastgestelde regime bepaalt vervolgens welke activiteiten en resultaten geadviseerd worden in de verschillende fasen van de levenscyclus voor de sourcing van de betreffende IT-dienst.

#### Resultaten

- Project initiatie document
- Project start architectuur
- Verwervingsstrategie
- Stakeholdermanagement en communicatieplan (verscherpt regime)

#### Belangrijkste randvoorwaarden

- Rijksbrede ketenverantwoordelijkheid wordt altijd meegenomen bij IT-sourcing beslissingen.
- De Rijksoverheid beschikt over middelen en vaardigheden om de sourcing van IT-diensten gecontroleerd en effectief uit te voeren.
- Sourcing voldoet aan geldende richtlijnen en kaders en draagt bij aan Rijksbrede strategieën, zoals de I-strategie Rijk en NDS.

#### Belangrijkste principes

- Afhankelijkheidsrelaties worden meegenomen in sourcing keuzes, zodanig dat concentratierisico's worden voorkomen en/of worden gemitigeerd door maatregelen.
- Sourcing wordt zoveel mogelijk modulair toegepast, wat betekent dat kavel individueel van sourcing leveringsvorm kunnen wijzigen zonder significante technologische, functionele of contractuele impact.
- Belangrijke afwegingen in de sourcing keuze zijn de marktbeschikbaarheid, kosten, stabiliteit, meetbaarheid en inwisselbaarheid van leveranciers.

<sup>10</sup> De vitaliteitsclassificatie wordt ontwikkeld in Q2 2025, een referentie wordt opgenomen wanneer beschikbaar.

<sup>11</sup> De uitkomsten van BIA, BBN, IB-scan, PIA en de grenswaarde voor de geschatte waarde die leiden tot een verscherpt regime dienen nader te worden bepaald.

| Regulier regime                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Verscherpt regime                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>Een regulier regime is van toepassing op IT-diensten met een gemiddeld of laag risicoprofiel. Waarbij, indien van toepassing, ook de contractuele afspraken uit de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO)<sup>(12)</sup> dienen te worden opgenomen.</li> <li>Het regime voorziet in standaard beheer- en controleprocessen die adequaat zijn om de dienstverlening efficiënt te sourcen, te realiseren en te exploiteren binnen de geaccepteerde risico's en mitigerende maatregelen.</li> <li>Procedures onder dit regime zijn gestandaardiseerd en de controlemechanismen zijn relatief eenvoudig, gericht op het realiseren van een stabiele dienstverlening zonder uitgebreide aanpassingen voor specifieke of complexe risico's.</li> </ul> | <ul style="list-style-type: none"> <li>Een verscherpt regime is van toepassing op IT-diensten die van strategisch en kritiek belang zijn voor de organisatie en/of de Rijksoverheid of die significant hogere risico's dragen.</li> <li>Dit regime vereist intensievere management- en controleprocessen, inclusief uitvoerige Due Diligence en regelmatige evaluaties.</li> <li>Het regime vereist verdergaande contractuele afspraken om de beheersbaarheid, kwaliteit, continuïteit en overdraagbaarheid van de IT-dienst te waarborgen.</li> <li>Het regime omvat grondige risicobeheersingsmaatregelen om de betrouwbaarheid, veiligheid en continuïteit te waarborgen.</li> </ul> |

**Tabel 2** Beheersingsregimes in de IT-sourcing levenscyclus van de Rijksoverheid

Afhankelijk van het regime moeten onderstaande resultaten worden opgeleverd per fase. Onderstaande tabel geeft een overzicht van de resultaten.

| Fase                                            | Regulier regime                                                                                                                                                                                                                                                                                                                                                           | Verscherpt regime<br>(Aanvullend op het reguliere regime)                                                                                                                                                                                                                                |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1. Behoeftestelling</b>                      | <ul style="list-style-type: none"> <li>Dienstenomschrijving</li> <li>BIA</li> <li>PIA</li> <li>IB-scan</li> <li>Sourcingstrategie</li> </ul>                                                                                                                                                                                                                              | Geen aanvullende resultaten <sup>(13)</sup>                                                                                                                                                                                                                                              |
| <b>2. Strategische sourcing keuze</b>           | <ul style="list-style-type: none"> <li>Project initiatie document</li> <li>Project start architectuur</li> <li>Verwervingsstrategie</li> </ul>                                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>Stakeholdermanagement en communicatieplan</li> </ul>                                                                                                                                                                                              |
| <b>3. Verwerven en contracteren</b>             | <ul style="list-style-type: none"> <li>Due Diligence</li> <li>Risicobeheersplan</li> <li>Inkoopplan (indien van toepassing)</li> <li>Aanbestedingsdossier en PvE</li> <li>Overeenkomst met bepalingen rondom aansprakelijkheid, intellectueel eigendom, eigenaarschap, voortijdige beëindiging (op basis van ARBIT)</li> <li>Registratie in sourcing overzicht</li> </ul> | <ul style="list-style-type: none"> <li>Uitvoerige Due Diligence</li> <li>Uitvoerig Risicobeheersplan</li> <li>Uitvoerige overeenkomst (met aanvullende bepalingen rondom aansprakelijkheid, eigenaarschap, overdraagbaarheid, stuurmechanismen, risicobeheersing, et cetera.)</li> </ul> |
| <b>4. Implementeren</b>                         | <ul style="list-style-type: none"> <li>Continuïteits- en exit-plannen</li> <li>Architecture en ontwerpdocumentatie</li> </ul>                                                                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>Leverancier en contractmanagement plan</li> </ul>                                                                                                                                                                                                 |
| <b>5. Monitoren, evalueren en optimaliseren</b> | <ul style="list-style-type: none"> <li>Certificering en assurance verklaringen (naar aanleiding van periodieke audits)</li> <li>Vastlegging in document managementsysteem</li> </ul>                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>Proactieve Risicobeheersing middels monitoring op continuïteitsrisico's</li> </ul>                                                                                                                                                                |
| <b>6. Beëindigen</b>                            |                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                          |
| <b>Kennis en Regie</b>                          | <ul style="list-style-type: none"> <li>Sourcing overzicht</li> </ul>                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                          |

**Tabel 3** Resultaten per regime

12 De Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO) zijn voorschriften voor het beoordelen en waarborgen van de nationale veiligheid bij inkoopopdrachten door de overheid.

13 Regimes zijn in fase 1 nog niet van toepassing, waardoor de resultaten niet afhankelijk zijn van het specifieke regime.

## 4.4 Fase 3) Verwerven en contracteren

Het doel van de fase Verwerven en contracteren is het selecteren van de juiste dienstverlener(s) en indien nodig het formaliseren van de overeenkomsten. Deze fase moet zorgen voor een effectieve en juridisch solide overeenkomst die de basis legt voor een succesvolle implementatie en samenwerking.

### Activiteiten:

1. **Opstellen verwervingsstrategie:** Beschrijf de wijze waarop de IT-dienst wordt verworven, inclusief aspecten zoals de reikwijdte van de verwerving, de benodigde capaciteit en kosten, en de impact op de bedrijfsvoering. Hierbij dient rekening gehouden te worden met onder andere de Algemene Beveiligingseisen Rijksoverheidsopdrachten (ABRO), de NDS, en de Aanbestedingswet. Dit omvat ook het maken van een onderscheid tussen interne en externe sourcing leveringsvormen, evenals andere relevante overwegingen:
  - a. Interne sourcing leveringsvormen: de wijze waarop de leverende partij wordt getoetst.
  - b. Externe sourcing leveringsvormen: de vaststelling van de contractwaarde en een aanbestedingsprocedure (met onder meer minimumeisen, uitsluitingsgronden, geschiktheidseisen en gunningscriteria). Afhankelijk van de contractwaarde wordt een toets uitgevoerd op risico mitigatie.
2. **Finaliseren eisen en wensen:** Finaliseer met een multidisciplinair team (Business, inkoop, Juridische Zaken, IT, et cetera.) de eisen en wensen.
3. **Selecteren en contracteren:** Voer de selectie uit volgens de benodigde procedure. Afspraken in het geval van interne sourcing leveringsvormen worden vastgelegd in een dienstverleningsovereenkomst (DVO) of soortgelijke afspraken. In het geval van een externe sourcing leveringsvorm wordt een formele procedure gevolgd, conform de Aanbestedingswet en ARBIT, en worden de afspraken vastgelegd in een contract. De overeenkomst omvat minimaal de volgende elementen:
  - a. Dienstbeschrijving: Een gedetailleerde omschrijving van de IT-diensten die worden geleverd.
  - b. Prestatie-indicatoren: Duidelijk vastgestelde maatstaven om de kwaliteit en prestaties van de geleverde diensten te evalueren.
  - c. Rapportage en informatievoorziening: Protocollen voor het regelmatig rapporteren en vastleggen van relevante informatie.

- d. Due diligence: Procedures voor regelmatige controle en evaluatie van de dienstverlening, verzekering van naleving van beleid en standaarden.
- e. Beheer en (door)ontwikkeling van de dienst: Procedures en afspraken voor het beheer en de (door)ontwikkeling van de IT-diensten om aan veranderende behoeften en technologieën te voldoen.
- f. Overdraagbaarheidsmaatregelen: Beleid voor het borgen van de overdraagbaarheid van de IT-diensten gedurende en na de contractperiode.
- g. Escalatie- en interventiemechanismen: Protocollen voor het ingrijpen in situaties waar een serviceprovider een te hoge concentratie risico's zou creëren.
- h. Contractbeëindiging: Voorwaarden onder welke de overeenkomst kan worden herzien of beëindigd.

### Resultaten

- Due Diligence
- Risicobeheersplan
- Inkoopplan (indien van toepassing)
- Aanbestedingsdossier en PvE
- Overeenkomst (op basis van ARBIT), incl. afspraken uit de ABRO indien van toepassing
- Registratie in sourcing overzicht
- Uitvoering Due Diligence (verscherpt regime)
- Uitvoering Risicobeheersplan (verscherpt regime)
- Uitvoering overeenkomst (verscherpt regime)

### Belangrijkste randvoorwaarden

- Samenwerking vindt plaats met financieel gezonde partners die beschikken over vereiste accreditaties, zoals gesteld in de BIO en wettelijke kaders.
- De organisatie waarborgt kennisbehoud binnen de eigen organisatie bij verwervingen.

### Belangrijkste principes

- Rijksfaciliteiten worden altijd overwogen bij het verwerven van dienstverlening.
- Risico's van leveranciersconcentratie en de financiële situatie van leveranciers worden meegenomen in het verwervingsproces.
- Bij complexe IT-dienstverlening van externe leveranciers wordt een marktconsultatie uitgevoerd.
- Bij externe complexe IT-dienstverlening wordt een aanbestedingsprocedure waarin er mogelijkheid is tot dialoog met marktpartijen uitgevoerd.



## 4.5 Fase 4) Implementeren

Het doel van de fase Implementeren is de daadwerkelijke implementatie van de IT-dienst. De IT-dienst dient te worden geïntegreerd in het IT-landschap van de organisatie en de Rijksoverheid, met minimale beperkingen voor de bestaande IT-dienstverlening.

### Activiteiten:

1. **Operationaliseren van gemaakte afspraken:** Concretiseer de gemaakte afspraken in een implementatieplan.
2. **Voorbereiden interne organisatie:** Communiceer de aankomende verandering en alloceer mensen voor de implementatie.
3. **Uitvoeren (eventuele) transitie en implementatie:** Voer de transitie uit, van de latende partij naar de nieuwe partij (indien van toepassing). Implementeer de dienst conform de eisen en wensen en de contractafspraken. Zorg hierbij voor een uitgebreide architecturen en ontwerpdocumentatie en de benodigde continuïteits- en exit-plannen.
4. **Accepteren van IT-dienst:** Accordeer de opgeleverde IT-dienst door de daarvoor gemandateerde functionaris.

### Resultaten

- Geformaliseerde continuïteits- en exit-plannen
- Architecturen en ontwerpdocumentatie
- Leverancier en contractmanagement plan (verscherpt regime)

### Belangrijkste randvoorwaarden

- Beschikbaarheid en continuïteit worden te allen tijde gegarandeerd bij de implementatie.

### Belangrijkste principes

- Interoperabiliteit en flexibiliteit in technologie wordt aangewend om lock-in met externe partijen te minimaliseren.
- Bij implementatiekeuzes wordt rekening gehouden met de overdraagbaarheid van de IT-dienst, onder andere door standaardisatie.
- Bij een eventuele overdracht tussen leverende partijen dient rekening worden gehouden met de huidige en toekomstige (her)transitierisico's en -kosten.

## 4.6 Fase 5) Monitoren, evalueren en optimaliseren

Het doel van de fase Monitoren, evalueren en optimaliseren is waarborgen en verbeteren van de prestaties, de veiligheid en de kosteneffectiviteit van de geïmplementeerde IT-dienst. Het doel is om continu de prestaties in de gaten te houden en evaluaties uit te voeren, om te garanderen dat de IT-dienst blijvend voldoet aan wet- en regelgeving, de vastgestelde kwaliteitsstandaarden en indien van toepassing de ABRO en ARBIT eisen.

### Activiteiten:

1. **Monitoren van prestatie-rapportages:** Monitor de kwaliteit door het toetsen van prestatie-rapportages op basis van harde en zachte indicatoren.
2. **Valideren van assurance en compliance rapportages:** Valideer jaarlijks de afgesproken assurance en compliance rapportages, inclusief de bijbehorende Verklaring van Toepasselijkheid.
3. **Uitvoeren evaluaties:** Evalueer periodiek de IT-dienst conform de contractafspraken.
4. **Actualiseren van (overdraagbaarheids)documentatie:** Actualiseer van relevante documentatie zoals exit-plan, risicoanalyses, huidige situatie documenten, zodat overdragen mogelijk blijft.
5. **Testen en actualiseren van continuïteitsplannen, uitwijktesten en terugvalopties:** het (jaarlijks) testen en actualiseren van continuïteitsplannen en terugvalopties, inclusief een rapport van bevindingen en het opvolgen van deze bevindingen.
6. **Opstellen verbetervoorstellen en/of wijzigingen:** Stel op basis van activiteit 1 t/m 3, of externe ontwikkelingen, verbetervoorstellen en/of wijzigingen in de (contract) afspraken op.

### Resultaten

- Certificering en assurance verklaringen (naar aanleiding van periodieke audits)
- Geactualiseerd dossier in het Document managementsysteem
- Proactieve Risicobeheersing middels monitoring op continuïteitsrisico's (verscherpt regime)

#### Belangrijkste randvoorwaarden

- Financiële status en digitale soevereiniteit ten opzichte van gecontracteerde leveranciers wordt periodiek gecontroleerd en geëvalueerd.
- De opslag en verwerking van Rijksoverheid data door externe leveranciers wordt gemonitord en periodiek geëvalueerd.

#### Belangrijkste principes

- De Rijksoverheid dient te allen tijde de kwaliteit van de dienstverlening door interne en externe leveranciers te kunnen monitoren op basis van harde (KPI's en SLA's) en zachte (relatie en klanttevredenheid) indicatoren.
- Bij onvoorziene en/of aanzienlijke veranderingen bij de dienstverlener, wordt een passende herbeoordeling van de risico's uitgevoerd.
- Duurzaamheid en kansen voor het verduurzamen van IT-dienstverlening worden regelmatig geëvalueerd.

## 4.7 Fase 6) Beëindigen

Het doel van de fase Beëindigen is het correct beëindigen van de overeenkomst en/of gemaakte afspraken<sup>(14)</sup>. Dit kan zijn vanwege de afloop van contracttermijnen of tussentijdse beëindiging. De (re)transitie dient zo soepel mogelijk te verlopen, met de focus op het minimaliseren van risico's en onderbreking van de IT-dienst.

#### Activiteiten:

1. **Uitvoeren exit-plan:** Actualiseer het overeengekomen exit-plan en voer – in gezamenlijkheid of onder aansturing van de verantwoordelijke partijen – het plan uit.
2. **Accepteren beëindiging:** Accordeer/accepteer de beëindiging van de IT-diensten/producten na succesvol uitvoering van het exit-plan. In het geval de dienstverlening wordt overgedragen, borg gedurende deze overdracht en na de overdracht “dubbele dijkbewaking”, zowel om succesvolle en volledige overdracht te realiseren maar ook om beschikking te houden over kennis en kunde van de IT-diensten en/of producten na decharge van de latende partij, om issues effectief te verhelpen.

#### 3. Overdragen van documentatie, informatie en kennis:

Borg dat alle relevante kennis (documentatie en gegevens betreffende de dienstverlening) van de latende partij wordt overgedragen en effectief wordt opgeslagen in het dossier in het document managementsysteem van de organisatie. Borg dat back-up van data en systemen die worden uitgefaseerd, effectief worden opgeslagen.

#### 4. Verwijderen van persoonsgegevens:

Borg dat persoonsgegevens niet langer bewaard worden dan noodzakelijk, door deze tijdig te verwijderen (rekening houdend met de betreffende wettelijke bewaartermijnen)

#### Resultaten

- Beëindigen van de dienstverlening door de leverancier conform Exit/overdrachtsplan
- Vastleggen van de relevante kennis in het dossier in het DMS

#### Belangrijkste randvoorwaarden

- Bij overnames van gecontracteerde leveranciers dient opnieuw een geschiktheidstest en risicoanalyse uitgevoerd te worden.
- Exit-plannen worden periodiek getest, bevindingen worden meegenomen in een bijgewerkte versie van het exit-plan.

#### Belangrijkste principes

- Bij het beëindigen van de IT-dienstverlening dient het vooropgestelde exit-plan gevolgd te worden.

## 4.8 Kennis en regie

De activiteiten in alle fasen van de IT-sourcing levenscyclus kennen het belang van kennis en regievoering. De aanwezigheid van kennis ondersteunt de activiteiten, zowel kennis op het gebied van sourcing, alsook functionele kennis van IT-diensten. Effectieve regievoering over zowel interne als externe dienstverleners waarborgt de continuïteit en kwaliteit van IT-diensten, en zorgt ervoor dat er efficiënt kan worden ingespeeld op veranderende behoeften en technologische ontwikkelingen. Organisaties worden hierin ondersteund door Rijksbrede (sourcing)kennis en regievoering vanuit het nog op te richten Center of Excellence IT-sourcing en bijbehorende community.

14 Er wordt gesproken over afspraken indien er sprake is van zelf doen. Ook in deze situatie dienen afspraken voor gemaakt te worden maar hebben niet dezelfde contractuele aard.

#### Activiteiten:

1. **Coördineren en afstemmen:** Coördineer sourcing door overleg te faciliteren en centrale principes te borgen binnen de organisatie, waardoor strategische doelen en operationele behoeften tussen opdrachtgever en opdrachtnemer meer effectief worden afgestemd.
2. **Leverancier en contractmanagement:** Richt leverancier- en contractmanagement processen in om effectief de leverende partij aan te sturen, en te beschikken over de kennis en kunde om te monitoren zodat overeengekomen afspraken effectief door alle betrokken worden nagevolgd.
3. **Kennismanagement:** Bevorder continu leren door een kennisbank met sourcing informatie en best practices te onderhouden en deze te delen met andere organisaties binnen de Rijksoverheid. Organiseer of participeer in kennissessies (ronde tafels) over actuele IT-sourcing thema's. Borg dat medewerkers een trainingscurriculum kunnen volgen om de (inhoudelijk) IT-en IT-sourcing kennis te vergroten.
4. **Adviseren over sourcing vraagstukken:** Verhoog de kwaliteit van sourcingbeslissingen door Rijksbrede strategieën te vertalen naar een concrete sourcingstrategie voor de organisatie en proactief risico's te signaleren gedurende de sourcing levenscyclus.

#### Resultaten

- Organisatie specifiek sourcing overzicht: een inventaris van alle sourcing relaties binnen de organisatie, zodat de feitelijke situatie inzichtelijk is en concentratie- en continuïteitsrisico's inzichtelijk gemaakt kunnen worden. Informatie zoals de naam van de leverancier, onderaannemers, landen waar IT-diensten worden aangeboden en de uitvoering van meest recente risicoanalyses worden binnen het overzicht opgeslagen<sup>(15)</sup>.

#### Belangrijkste randvoorwaarden

- Vragen en/of behoeften van gebruikers worden vastgelegd ten behoeve van de ontwikkeling voor nieuwe of betere kennisproducten.
- De organisatie van kennis dient waar mogelijk aan te sluiten op bestaande initiatieven binnen de Rijksoverheid en deze te versterken.

#### Belangrijkste principes

- Bij het opstellen van kennisproducten wordt zoveel mogelijk gebruik gemaakt van bestaand materiaal binnen de Rijksoverheid.
- Bestaande kennis binnen de Rijksoverheid wordt hergebruikt ten behoeve van kennis en regie.

#### Risicobeheersing

Een van de diensten van belang voor kennis en regie is de monitoringsfunctie. Deze ondersteunende functie is een instrument om de continuïteits- en concentratierisico's van (kritieke en strategische) IT-diensten effectief te beheren binnen de Rijksoverheid. Het is van belang dat deze functie wordt ingericht binnen de organisatie met aansluiting op het Rijksbrede Center of Excellence (CoE), om actief bij te dragen aan de monitoring van leveranciers binnen de Rijksoverheid en inzichten van het CoE optimaal te benutten binnen de organisatie. Het CoE adviseert tevens het CIO beraad en de ICIA, waardoor Rijksbreed informatie wordt gedeeld.

Het verzamelen en delen van informatie over de prestaties van verschillende IT-leveranciers stelt de Rijksoverheid en de organisatie in staat om snel te reageren op problemen en passende maatregelen te nemen indien nodig.

Het opzetten van deze monitoringsmechanismen en -processen vereist investeringen in opleiding en capaciteitsopbouw voor medewerkers, zodat zij over de vereiste kennis en vaardigheden beschikken om effectieve monitoring uit te voeren. Het opstellen van crisismanagementplannen en -procedures is van belang om een snelle en adequate respons te garanderen op geïdentificeerde problemen.

15 Er zijn bestaande deelverzamelingen waar het sourcing overzicht op kan aansluiten.

# 5 De IT-sourcing afweging

Dit hoofdstuk gaat in op de sourcing leveringsvormen en biedt een afwegingskader voor het maken van sourcing keuzes. Het geeft daarmee inzicht in de sourcing vormen en geeft invulling aan de vragen die geadresseerd moeten worden in IT-sourcing afwegingen.

## 5.1 Sourcing leveringsvormen

Om de gewenste IT-sourcing situatie op een efficiënte en effectieve manier in te vullen, is vastgesteld welke sourcing leveringsvormen van toepassing zijn in de context van de Rijksoverheid. De sourcing leveringsvormen beschrijven wie en de wijze waarop een IT-dienst/product geleverd kan worden.

In algemene zin zijn er drie categorieën waar de sourcing leveringsvormen binnen vallen:

- Zelf doen: de IT-dienst wordt uitgevoerd binnen en onder de verantwoordelijkheid van een Rijksonderdeel.
- Samenwerken: de IT-dienst wordt uitgevoerd door een samenwerking van organisaties binnen de Rijksoverheid of met de markt.
- Uitbesteden: de IT-dienst wordt uitgevoerd door een externe (markt)partij.

Binnen deze drie categorieën zijn nadere sourcing leveringsvormen te onderscheiden. Deze zijn in onderstaand figuur weergegeven.



Figuur 5 Overzicht sourcing leveringsvormen per categorie

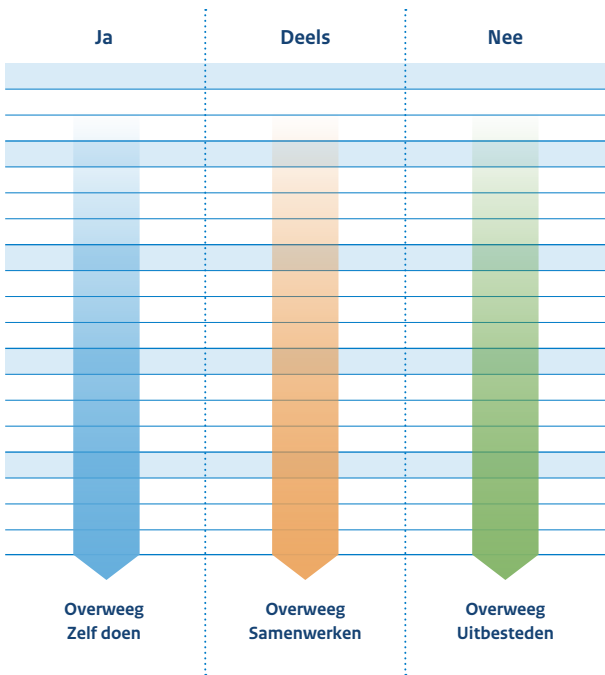
De sourcing leveringsvormen zijn in de onderstaande tabel nader gedefinieerd.

| # | Sourcing leveringsvorm                               | Definitie                                                                                                                                                                                                                                                                             |
|---|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Rijksonderdeel                                       | De dienstverlening wordt door een organisatie binnen de Rijksoverheid zelfstandig uitgevoerd, waarbij indien nodig producten en/of diensten worden ingekocht.                                                                                                                         |
| 2 | Rijksdienstverlener (inbesteding)                    | Diensten worden door een dienstverlener binnen de Rijksoverheid uitgevoerd, waar mogelijk op basis van resultaatverplichtingen.                                                                                                                                                       |
| 3 | Inhuur                                               | Het intern beleggen van de werkzaamheden voor specifieke activiteiten door inhuur van externe resources met kennis in een specifiek domein en op basis van inspanningsverplichting.                                                                                                   |
| 4 | Co-sourcing                                          | Een samenwerkingsverband voornamelijk op basis van inspanningsverplichtingen tussen de Rijksoverheid en interne of externe leverancier(s) waarbij partijen zich confirmeren aan het behalen van overeengekomen resultaten.                                                            |
| 5 | Gezamenlijke onderneming                             | Een samenwerkingsverband tussen de Rijksoverheid en een interne (bijvoorbeeld agentschap) of externe leverancier waarin beide partijen kapitaal en kennis en kunde inbrengen, om gezamenlijk een nieuwe separate entiteit te vormen voor de levering van de gewenste dienstverlening. |
| 6 | Managed services/<br>Resultaatverplichtende opdracht | De levering van integrale IT-diensten door een leverancier, op basis van een resultaatsverplichting conform overeengekomen dienstencatalogus, Service Level Agreements (SLA's), Kritieke Prestatie Indicatoren (KPI's) en prijsmodellen.                                              |
| 7 | Cloud/ As-a-service                                  | Online-dienstverlening met een hoge mate van standaardisatie die geleverd wordt over een decentraal netwerk (veelal het internet) op basis van een licentiemodel. Clouddiensten zijn bekende sourcing leveringsvormen die als "As-a-Service" wordt afgenomen.                         |
| 8 | Uitbesteding van taken of producten                  | Het extern beleggen van de werkzaamheden voor specifieke activiteiten door het beleggen van een cluster van taken bij een externe partij op basis van resultaatverplichting.                                                                                                          |

**Tabel 4** definities sourcing leveringsvormen

## 5.2 Afwegingskader voor IT-sourcing keuze

Het afwegingskader biedt organisaties binnen de Rijksoverheid een gestructureerde aanpak en praktische ondersteuning bij het nemen van verantwoorde IT-sourcing beslissingen. De verantwoordelijkheid voor het nemen van de beslissingen blijft bij de gebruiker. Het doel van de handreiking is om gebruikers te helpen bij het stellen van de juiste kernvragen die een rol spelen bij de afweging tussen zelf doen, samenwerken of uitbesteden. Het afwegingskader bestaat uit veertien vragen op basis van de IT-sourcing doelstellingen, randvoorwaarden en principes uit de Rijksbrede Strategie voor IT-sourcing (zie volgende paragraaf) en dienen per vraag te resulteren in een antwoord: “Ja”, “Deels” of “Nee”.



**Figuur 6** Afweging van de leveringsvorm

De vragen zijn zodanig opgesteld dat de antwoorden richting geven aan de sourcing categorie die overwogen dient te worden (bijvoorbeeld zelf doen, samenwerken, uitbesteden). Nadat de gewenste categorie is bepaald dient de best passende sourcing leveringsvorm te worden geselecteerd uit de sourcing leveringsvormen als beschreven in de voorgaande paragraaf.

Er zijn bewust geen wegingen per vraag opgenomen. Deze weging dient de gebruiker zelf te bepalen, rekening houdend met de context, nuances en zwaartepunten van het vraagstuk waar de afweging voor wordt gemaakt.

De gebruiker van het afwegingskader wordt gevraagd om:

- De antwoorden op de vragen in detail te motiveren;
- De rationale op te stellen en/of mitigerende maatregelen te treffen op antwoorden van vragen die niet passend zijn bij de voorkeurlieferingsvorm;
- De conclusie van de geschikte sourcing leveringsvorm op basis van de vragen en het eventueel eigen afwegingskader samen te voegen en te motiveren.

Toepassing van het IT-sourcing afwegingskader verloopt in 6 stappen:

1. Formeer een multidisciplinair team van medewerkers voor het doorlopen van het afwegingskader. Denk hierbij aan business, IT, inkoop, juridische zaken, architectuur en HR.
2. Beantwoord (gezamenlijk) de vragen voor de te verwerven IT-dienst.
3. Vul waar nodig deze aan met het afwegingskader van de eigen organisatie (indien aanwezig).
4. Bespreek gezamenlijk de uitkomsten. Betrek waar nodig ook andere stakeholders. Bij deze stap dienen zowel de uitkomsten als de motivatie ervan besproken te worden. Op basis van nieuwe inzichten kunnen de uitkomsten worden aangescherpt.
5. Maak gezamenlijk de afweging voor de sourcing leveringsvorm en (rest)risico's + mitigerende maatregelen.
6. Laat de uitkomsten, sourcingkeuze en (rest)risico's + mitigerende maatregelen, goedkeuren op bestuurlijk niveau.

## 5.3 IT-sourcing afwegingskader vragenlijst

De vragen in het onderstaand overzicht zijn gebaseerd op de eerder benoemde IT-sourcing doelen, randvoorwaarden en principes en zijn gestructureerd naar de eerste 5 IT-sourcing doelen.

### 1. Vormt de IT-dienst een kritiek of strategisch element voor de Rijksoverheid?

*Nadere toelichting:* Indien een IT-dienst van kritiek<sup>(16)</sup> belang is, dan relateert de IT-dienst aan vitale processen, in industrieën die door de Rijksoverheid als vitaal zijn geclassificeerd. Omdat deze taken gevoelig zijn voor het opereren van de kerntaken, lenen ze zich meer om zelf te organiseren.

Voorbeelden van antwoorden:

- Ja, de IT-dienst is kritiek voor het uitvoeren van de kerntaken door de Rijksoverheid.
- Deels, dit is geen optie voor deze vraag.
- Nee, de IT-dienst is niet kritiek voor het uitvoeren van de kerntaken door de Rijksoverheid.

### 2. Vormt de IT-dienst een element dat onderscheidend en van strategische waarde is voor de organisatie?

*Nadere toelichting:* het classificeren van de IT-dienst als onderscheidend onderdeel voor het Rijksonderdeel is van belang om de importantie voor de bedrijfsvoering inzichtelijk te maken. IT-diensten die relateren aan de bedrijfsstrategie en Enterprise Architectuur horen hierbij. IT-diensten die relateren aan processen die het verschil maken voor de burger, patiënt, student, ondernemer of ambtenaar zijn hier van belang.

|                                                                                                                                    | Ja                    | Deels                | Nee                  |
|------------------------------------------------------------------------------------------------------------------------------------|-----------------------|----------------------|----------------------|
| <b>Doel 1. Betrouwbare publieke dienstverlening - betere continuïteit van IT-diensten</b>                                          |                       |                      |                      |
| 1. Vormt de IT-dienst een kritiek of strategisch element voor de Rijksoverheid?                                                    |                       |                      |                      |
| 2. Vormt de IT-dienst een element dat onderscheidend en van strategische waarde is voor de organisatie?                            |                       |                      |                      |
| <b>Doel 2. Meer regie op digitale autonomie, soevereiniteit en veiligheid</b>                                                      |                       |                      |                      |
| 3. Bevat de IT-dienst gevoelige, hoog gerubriceerde en/of staatsgeheime data?                                                      |                       |                      |                      |
| 4. Verhoogt het uitbesteden van de IT-dienst de risico's voor de digitale weerbaarheid?                                            |                       |                      |                      |
| 5. Komt het vermogen om autonoom te kunnen beslissen en handelen over essentiële digitale aspecten bij de IT-dienst in het geding? |                       |                      |                      |
| <b>Doel 3. Slimmer samenwerken als één overheid</b>                                                                                |                       |                      |                      |
| 6. Is de benodigde technologie voor de IT-dienst uniek en specifiek voor de organisatie?                                           |                       |                      |                      |
| 7. Is de IT-dienst effectief beschikbaar binnen de producten- en dienstencatalogus van het Rijk?                                   |                       |                      |                      |
| 8. Is het mogelijk om de IT-dienst met andere Rijksorganisaties af te nemen?                                                       |                       |                      |                      |
| 9. Is de IT-dienst alleen beschikbaar tegen hoge kosten, onacceptabele voorwaarden, of helemaal niet beschikbaar op de markt?      |                       |                      |                      |
| <b>Doel 4. Meer inzicht in afhankelijkheden en kwetsbaarheden</b>                                                                  |                       |                      |                      |
| 10. Is de IT-dienst gekenmerkt door instabiliteit en gebrek aan meetbare prestatie-indicatoren?                                    |                       |                      |                      |
| 11. Zijn er beperkingen in de overdraagbaarheid van de IT-dienst naar andere leveranciers of interne partijen?                     |                       |                      |                      |
| 12. Heeft de organisatie de noodzakelijke functionele en/of technische vaardigheden in huis om de IT-dienst effectief te leveren?  |                       |                      |                      |
| <b>Doel 5. Wendbaarheid en innovatie versnellen</b>                                                                                |                       |                      |                      |
| 13. Is de IT-dienst niet effectief (als standaard IT-dienst) beschikbaar op de markt?                                              |                       |                      |                      |
| 14. Zijn benodigde innovaties voor de IT-dienst beschikbaar binnen het Rijk?                                                       |                       |                      |                      |
|                                                                                                                                    | Overweeg zelf te doen | Overweeg samenwerken | Overweeg uitbesteden |

16 De ambitie is om op lange termijn een eenduidige definitie te hebben van kritieke IT-diensten en vitale processen binnen het Rijk.



Voorbeelden van antwoorden:

- Ja, de IT-dienst is direct impactvol voor de primaire processen. Denk een aan systeem voor het bepalen van de hoogte van uitkeringen.
- Deels, de IT-dienst is gerelateerd aan primaire processen, maar betreft niet een doorslaggevend aspect. Denk aan het beheer van een stabiel systeem gerelateerd aan het bepalen van de hoogte van de uitkeringen.
- Nee, de IT-dienst relateert aan secundaire processen van de organisatie. Denk aan een planning-tool.

### 3. Bevat de IT-dienst gevoelige, hoog gerubriceerde en/of staatsgeheime data?

Nadere toelichting: Wanneer binnen de IT-dienst gegevens worden verwerkt die als gerubriceerd kunnen worden beschouwd, ontstaan er extra veiligheidsrisico's bij samenwerking of uitbesteding van deze IT-dienst, in vergelijking met het zelf uitvoeren ervan. Daarom gaat de voorkeur uit naar het zelf uitvoeren van deze taken. Maak bij het beantwoorden van deze vraag ook gebruik van de uitkomsten van de BIA en PIA.

Voorbeelden van antwoorden:

- Ja, de IT-dienst verwerkt staatsgeheime data.
- Deels, is niet van toepassing op deze vraag.
- Nee, de IT-dienst verwerkt uitsluitend geanonimiseerde data.

### 4. Verhoogt het uitbesteden van de IT-dienst de risico's voor de digitale weerbaarheid?

Nadere toelichting: In het licht van cyberveiligheid en digitale weerbaarheid voor de organisatie dient overwogen te worden of het uit handen geven van de IT-dienst leidt tot verhoogde risico's voor de organisatie.

Voorbeelden van antwoorden:

- Ja, de IT-dienst is belangrijk voor de bedrijfsvoering, wegvallen van de dienst zal leiden tot verstoringen van processen voor de organisatie.
- Deels, uitbesteden van de IT-dienst leidt tot een kleine verhoging van risico's, maar dit is bekend en beheersbaar.
- Nee, de IT-dienst is niet belangrijk voor de organisatie en beïnvloed daarmee niet de digitale weerbaarheid van de organisatie.

### 5. Komt het vermogen om autonoom te kunnen beslissen en handelen over essentiële digitale aspecten bij de IT-dienst in het geding?

Nadere toelichting: Het uitvoeren of niet uitvoeren van de IT-dienst door de leverancier kan aanzienlijke impact hebben op IT en/of de bedrijfsvoering van de organisatie. Indien dit impact heeft op cruciale onderdelen van de organisatie, kan het de autonomie van de organisatie verzwakken.

Voorbeelden van antwoorden:

- Ja, de bedrijfsvoering van de organisatie is afhankelijk van de uitkomsten uit de IT-dienst.
- Deels, de autonomie van bepaalde aspecten komen in het geding door de IT-dienst, maar niet van essentiële of belangrijke aspecten.
- Nee, de IT-dienst beïnvloed geen andere aspecten binnen de organisatie.

### 6. Is de benodigde technologie voor de IT-dienst uniek en specifiek voor de organisatie?

Nadere toelichting: De IT-dienst kan hele specifieke toepassingen hebben voor de organisatie, die niet generiek te leveren valt of die niet door de markt geleverd kan worden.

Voorbeelden van antwoorden:

- Ja, de bedrijfsvoering van de organisatie is afhankelijk van de uitkomsten uit de IT-dienst.
- Deels, de autonomie van bepaalde aspecten komen in het geding door de IT-dienst, maar niet val essentiële of belangrijke aspecten.
- Nee, de IT-dienst beïnvloed geen andere aspecten binnen de organisatie.

### 7. Is de IT-dienst effectief beschikbaar binnen de producten- en dienstencatalogus van het Rijk?

Nadere toelichting: Indien de dienst binnen de Rijksoverheid al wordt aangeboden en het technisch mogelijk is om hierop aan te sluiten, kan deze bundeling van vraag naar de IT-dienst helpen schaalvoordelen te benutten en tijd en kosten te besparen tijdens het verwervingsproces.

Voorbeelden van antwoorden:

- Ja, de IT-dienst is beschikbaar in de PDC van het Rijk en hier kan op aangesloten worden.
- Deels, een vergelijkbare IT-dienst staat in het PDC en hier kan op aangesloten worden.

- Nee, de IT-dienst maakt nog geen deel uit van de bestaande catalogi of kan vanwege juridische beperkingen (bijvoorbeeld een oorspronkelijk niet-deelnemende organisatie kan in beginsel niet aansluiten op een reeds aanbestede raamovereenkomst) niet worden geïntegreerd.

#### 8. Is het mogelijk om de IT-dienst met andere Rijksorganisaties af te nemen?

*Nadere toelichting:* Indien de behoefte groter is binnen het Rijk, kan het lonen om de IT-dienst zelf uit te voeren.

*Voorbeelden van antwoorden:*

- Ja, de behoefte naar de IT-dienst ligt breder in binnen het Rijk en kan gezamenlijk afgenomen worden.
- Deels, er zijn mogelijkheden voor samenwerking, maar slechts op bepaalde functionaliteiten van de IT-dienst.
- Nee, de dienst is te specifiek of onmogelijk om samen te werken met andere onderdelen.

#### 9. Is de IT-dienst alleen beschikbaar tegen hoge kosten, onacceptabele voorwaarden, of helemaal niet beschikbaar op de markt?

*Nadere toelichting:* Indien de IT-dienst niet onder normale of acceptabele omstandigheden geleverd kan worden, wordt het te overwegen om de IT-dienst zelf aan te bieden.

*Voorbeelden van antwoorden:*

- Ja, de IT-dienst is niet beschikbaar op de markt en kan alleen door partijen ontwikkeld worden voor onacceptabel hoge kosten.
- Deels, de IT-dienst is beschikbaar, maar de voorwaarden zijn ongunstig voor de organisatie.
- Nee, de IT-dienst is beschikbaar en tegen acceptabele omstandigheden.

#### 10. Is de IT-dienst gekenmerkt door instabiliteit en gebrek aan meetbare prestatie-indicatoren?

*Nadere toelichting:* Als niet geborgd kan worden dat de IT-dienst beschikbaar blijft of meetbaar is, is het risico te hoog om dit in de markt te zetten.

*Voorbeelden van antwoorden:*

- Ja, de IT-dienst is instabiel en lastig te meten met KPI's.
- Deels, de IT-dienst kan stabiel geleverd worden, maar is lastig te meten met KPI's.
- Nee, de IT-dienst is zowel stabiel als meetbaar met KPI's.

#### 11. Zijn er beperkingen in de overdraagbaarheid van de IT-dienst naar andere leveranciers of interne partijen?

*Nadere toelichting:* Indien de IT-dienst beperkt overdraagbaar is en zo geleverd wordt dat er kans op lock-in effecten kan ontstaan, is de voorkeur om de IT-dienst zelf te ontwikkelen, om latere complicaties te voorkomen.

*Voorbeelden van antwoorden:*

- Ja, de IT-dienst wordt heel specifiek geleverd en is niet overdraagbaar naar andere partijen.
- Deels, de IT-dienst is overdraagbaar, maar dit gaat gepaard met redelijke kosten en tijd.
- Nee, de IT-dienst is goed overdraagbaar en is niet leverancier afhankelijk.

#### 12. Heeft de organisatie de noodzakelijke functionele en/of technische vaardigheden in huis om de IT-dienst effectief te leveren?

*Nadere toelichting:* Om de IT-dienst te kunnen faciliteren moet de organisatie over de juiste middelen, kennis en vaardigheden beschikken of in staat zijn die op korte termijn te verkrijgen. Digitaal vakmanschap speelt hierbij een rol.

*Voorbeelden van antwoorden:*

- Ja, de organisatie heeft alle benodigde middelen, kennis en vaardigheden in huis om de IT-dienst te kunnen leveren.
- Deels, sommige, maar niet alle, vereiste vaardigheden zijn intern beschikbaar voor de IT-dienst.
- Nee, de organisatie mist de kritieke vaardigheden om de IT-dienst te kunnen leveren.

#### 13. Is de IT-dienst niet effectief (als standaard IT-dienst) beschikbaar op de markt?

*Nadere toelichting:* Als de IT-dienst effectief en als standaarddienst geleverd kan worden vanuit de markt, biedt het mogelijk (schaal)voordelen om de IT-dienst te verwerven via derde partijen. Doordat de dienst als standaarddienstverlening beschikbaar is.

*Voorbeelden van antwoorden:*

- Ja, de IT-dienst is specifiek en niet als standaarddienst beschikbaar op de markt.
- Deels, de IT-dienst is gedeeltelijk als standaarddienst beschikbaar, maar heeft specifieke aanpassingen nodig.
- Nee, de IT-dienst is breed en gemakkelijk beschikbaar als standaarddienstverlening.

#### 14. Zijn benodigde innovaties voor de IT-dienst beschikbaar binnen het Rijk?

*Nadere toelichting:* Als de gewenste innovaties binnen het Rijk aanwezig zijn, dan biedt dat mogelijkheden om met de IT-dienst daarop aan te sluiten. Indien dit niet beschikbaar is, kan het waardevol zijn om de markt te betrekken.

*Voorbeelden van antwoorden:*

- Ja, de benodigde innovatie voor de IT-dienst is al beschikbaar binnen het Rijk.
- Deels, een deel van de benodigde innovatie is beschikbaar, maar moet worden aangevuld vanuit de markt.
- Nee, de benodigde innovaties is niet beschikbaar binnen het Rijk en moet op een andere wijze verworven worden.

# 6 Begrippenlijst

Hieronder staat een selectie van de belangrijkste begrippen uit dit document.

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Business Impact Analyse (BIA)</b> | BIA betreft een methode om de mogelijke bedrijfsimpact te bepalen die een organisatie kan ervaren door een incident, die de functionaliteit van of de informatie in een applicatie in gevaar brengt.                                                                                                                                                                                                                                                                                               |
| <b>Center of Excellence</b>          | In het document wordt een Center of Excellence (CoE) beschreven als een centrale organisatie-eenheid die wordt ingericht om kennis en expertise over IT-sourcing binnen de Rijksoverheid te bundelen en te delen.                                                                                                                                                                                                                                                                                  |
| <b>Concentratie-risico's</b>         | Risico's die ontstaan wanneer de IT-diensten, waar de Rijksoverheid gebruik van maakt, afhankelijk zijn van een klein aantal leveranciers. Dit kan leiden tot kwetsbaarheden en navenante risico's voor continuïteit.                                                                                                                                                                                                                                                                              |
| <b>Digitale autonomie</b>            | Het vermogen van de overheid om zelfstandig haar digitale systemen, data en infrastructuur te beheren en te beveiligen, zonder buitensporige afhankelijkheid van externe partijen.                                                                                                                                                                                                                                                                                                                 |
| <b>Digitale soevereiniteit</b>       | Het vermogen van de overheid om volledige controle en zeggenschap te behouden over haar digitale infrastructuur, data en IT-diensten. Dit houdt in dat strategische beslissingen, toegang tot systemen en gegevensbeheer onafhankelijk van marktpartijen of buitenlandse partijen kunnen worden genomen.                                                                                                                                                                                           |
| <b>Digitale weerbaarheid</b>         | Borgen dat (basis)informatie onder alle omstandigheden beschikbaar, tijdig, correct en volledig is en alleen toegankelijk is voor de juiste personen. Als er iets misgaat, wordt dat snel opgemerkt en direct hersteld.                                                                                                                                                                                                                                                                            |
| <b>DORA</b>                          | De Digital Operational Resilience Act (DORA) Verordening stelt een uitgebreid kader vast voor digitale operationele veerkracht voor financiële entiteiten in de EU.                                                                                                                                                                                                                                                                                                                                |
| <b>EBA Outsourcing Guidelines</b>    | De EBA Outsourcing Guidelines, uitgegeven door de European Banking Authority (EBA), zijn richtlijnen die financiële instellingen helpen bij het beheren van uitbestedingsrisico's en het naleven van regelgeving met betrekking tot uitbesteding.                                                                                                                                                                                                                                                  |
| <b>IB-Scan</b>                       | De IB-scan, of de Informatiebeveiligingsscan, wordt gedefinieerd als een evaluatieproces waarbij systematisch de informatiebeveiligingsmaatregelen van een organisatie worden geanalyseerd en beoordeeld. Deze scan is gericht op het identificeren van kwetsbaarheden en risico's in de beveiliging van informatie en informatiesystemen, met als doel het verstrekken van aanbevelingen ter verbetering van de beveiligingspraktijken binnen de organisatie om beveiligingsrisico's te verlagen. |
| <b>Sourcing leveringsvorm</b>        | De verschillende manieren waarop IT-diensten kunnen worden geleverd aan de Rijksoverheid. Er worden acht specifieke sourcing leveringsvormen onderscheiden binnen drie hoofdcategorieën                                                                                                                                                                                                                                                                                                            |
| <b>Privacy Impact Analyse (PIA)</b>  | Een PIA is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen. Zodat de organisatie maatregelen kan nemen om deze risico's te verkleinen                                                                                                                                                                                                                                                                                                                  |

**Taskforce CID**

Taskforce Continuïteit ICT-dienstverlening focust zich op het ontwikkelen, implementeren en monitoren van strategieën en plannen die ervoor zorgen dat kritieke bedrijfsfuncties onder alle omstandigheden kunnen blijven functioneren, zelfs in geval van noodsituaties of crises.

**Kritieke en strategische IT-diensten**

Kritieke en strategische IT-diensten worden gedefinieerd als de essentiële informatietechnologiediensten die noodzakelijk zijn voor het uitvoeren van de vitale processen en daarmee operationele continuïteit van een organisatie. Deze diensten zijn cruciaal voor het behouden van de bedrijfsvoering en strategische doelen van de organisatie. Ze omvatten systemen die belangrijk zijn voor de veiligheid, economie en de infrastructuur van de organisatie, en een uitval ervan zou significante impact hebben op de stabiliteit en functioneren van de organisatie.

# 7 Bijlagen

## A. Samenhang met Strategie, Beleid en Wet- en regelgeving.

### *Samenhang met bestaande strategische- en beleidskeuzes*

De IT-sourcing handreiking moet beschouwd worden binnen een samenhangend geheel aan bestaande strategische- en beleidskeuzes. De handreiking dient bij te dragen aan de strategische en beleidsdoelen van de Rijksoverheid. De volgende vijf documenten zijn als leidend beschouwd in het vormgeven van de handreiking IT-sourcing.

- De Nederlandse Digitaliseringsstrategie (NDS)
- De I-strategie Rijk 2021-2025<sup>17</sup>
- Sturing en Organisatie Rijksinkoopstelsel
- Inkopen met Impact
- Het rapport Van kwetsbaar naar Weerbaar

Deze vijf document worden derhalve gebruikt als belangrijke richting, tezamen met sourcing marktontwikkelingen en de huidige speerpunten uit het IT-sourcing beleid uit 2012. Meer informatie over deze richtinggevende documenten en de relatie met de Rijksbrede strategie IT-sourcing is weergegeven in tabel 5.

| #  | Beleid, standaarden, kaders, kamerbrieven, programma's         |
|----|----------------------------------------------------------------|
| A  | Algemene Beveiligingseisen voor de Rijksoverheid (ABRO)        |
| B  | Architectuur Digitale Overheid 2030                            |
| C  | Architectuurkaders NORA/RORA                                   |
| D  | Baseline Informatiebeveiliging Rijksoverheid (BIO)             |
| E  | Besluit voorschift Informatiebeveiliging Rijksoverheid (VIRBI) |
| F  | Critical Entities Resilience (CER 20)                          |
| G  | (Concept) Cloudstrategie Rijk 2025                             |
| H  | De Nationale Technologiestrategie                              |
| I  | (Agenda) Digitale Open Strategische Autonomie (DOSA)           |
| J  | Donkere Wolken Pakken Samen                                    |
| K  | Evaluatie CISO Rijk en ADR                                     |
| L  | Evaluatie AR                                                   |
| M  | Forum standaardisatie                                          |
| N  | Gateway naar het inkoopstelsel                                 |
| O  | Generieke Digitale Infrastructuur (GDI)                        |
| P  | Het Rijksinkoopstelsel                                         |
| Q  | Inkopen met Impact                                             |
| R  | Interbestuurlijke datastrategie (IBDS)                         |
| S  | I-strategie Rijk 2021-2025                                     |
| T  | IT Identity en Access management (IAM)                         |
| U  | Kaderboek Organisatie en Bedrijfsvoering Rijk                  |
| V  | Meerjarenprogramma Infrastructuur Digitale Overheid (MIDO)     |
| W  | Migreren overheids IT                                          |
| X  | Nederlandse Digitaliseringsstrategie (NDS)                     |
| Y  | Nederlandse Overheid Referentie Architectuur (NORA)            |
| Z  | Network and Information Security directive (NIS2)              |
| AA | Normenkader Datacenters Rijksoverheid                          |
| BB | Overheidsbrede Beveiligingsassessments Risico's (OBAR)         |
| CC | Rijkscloudbeleid 2022                                          |
| DD | RijksOverheid Referentie Architectuur (RORA)                   |
| EE | Staat van de Digitale Infrastructuur                           |
| FF | Strategisch inkoopplan SLM                                     |
| GG | Sturing en organisatie Rijksinkoopstelsel                      |
| HH | Van kwetsbaar naar weerbaar                                    |
| II | Wolken aan de Horizon                                          |

**Tabel 5** Overzicht van relevante strategische- en beleidskeuzes voor IT-sourcing

17 Op dit moment wordt de I-strategie Rijk 2021-2025 vernieuwd. Op het moment dat de uitkomsten hiervan bekend zijn zal de strategische context herijkt geactualiseerd worden.

### Samenhang met wet- en regelgeving

De handreiking IT-sourcing dient logischerwijs zich te confirmeren aan wet- en regelgeving. In tabel 6 is de relevante wet- en regelgeving beschreven waar in het opstellen van dit document rekening mee gehouden.

| # | Wet- en regelgeving                                        |
|---|------------------------------------------------------------|
| A | Aanbestedingswet 2012 (Europese aanbestedingsrichtlijnen)  |
| B | Aanbestedingswet op defensie- en veiligheidsgebied (ADV)   |
| C | AI Act                                                     |
| D | Algemene verordening gegevensbescherming (AVG)             |
| E | Algemene Wet Bestuursrecht (AWB)                           |
| F | Beveiliging netwerk- en informatiesystemen (WBNI)          |
| G | Coördinatiebesluit en besluit CIO-stelsel Rijksdienst      |
| H | Corporate Sustainability Due Diligence Directive (CSDDD)   |
| I | Corporate Sustainability Reporting Directive (CSRD)        |
| K | Energy Efficiency Directive                                |
| L | Government Procurement Agreement (GPA)                     |
| M | Klimaatwet                                                 |
| N | Nationale veiligheid                                       |
| O | Wet markt en Overheid (WM&O)                               |
| P | Wet Digitale Overheid (WDO)                                |
| Q | Wet Digitale Toegankelijkheid (WDT)                        |
| R | Wet Modern Elektronische bestuurlijk Verkeer (WMEBV)       |
| S | Wet veiligheidstoets op investeringen, fusies en overnames |
| T | Wet weerbaarheid kritieke entiteiten (Wwke)                |

**Tabel 6** Overzicht relevante wet- en regelgeving voor IT-sourcing

## B. IT-sourcing randvoorwaarden

| #        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1</b> | <b>Behoeftestelling</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 1.1      | Regievoering wordt uitgevoerd door de Rijksoverheid, waarbij de bevoegdheid voor strategische en autonome besluiten volledig gewaarborgd is binnen de Rijksoverheid.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 1.2      | Alle behoeften worden geclassificeerd op het belang voor de organisatie, waarbij ten minste rekening wordt gehouden met de gebruikte informatie en de impact op de bedrijfsvoering. Over deze classificatie wordt gerapporteerd om centraal inzicht te verkrijgen.                                                                                                                                                                                                                                                                                                                                  |
| 1.3      | Een BIA en PIA maken structureel deel uit van de voorafgaande risicoanalyse in het kader van de behoeftebepaling.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 1.4      | Veiligheidsaspecten voortkomend uit de AVG, BIO en BBN zijn structureel meegenomen in de behoeftestelling.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>2</b> | <b>Strategische sourcing keuze</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 2.1      | Bij elke IT-sourcing keuze wordt geborgd dat de basis infrastructuur op orde blijft.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 2.2      | De aansluiting op IT-diensten door het gebruik van standaarden en interoperabiliteit wordt geborgd in de sourcing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 2.3      | Sourcing voldoet aan geldende richtlijnen en kaders en draagt bij aan Rijksbrede strategieën, zoals de I-strategie Rijk en NDS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 2.4      | De Rijksoverheid beschikt over middelen en vaardigheden om de sourcing van IT-diensten gecontroleerd en effectief uit te voeren.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 2.5      | Rijksbrede ketenverantwoordelijkheid wordt altijd meegenomen bij IT-sourcing beslissingen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>3</b> | <b>Verwerven en contracteren</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 3.1      | Sourcing is altijd in overeenstemming met de wet Markt en Overheid en andere geldende wet- en regelgeving.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 3.2      | De organisatie waarborgt kennisbehoud binnen de eigen organisatie bij verwervingen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 3.3      | Samenwerking vindt plaats met financieel gezonde partners die beschikken over vereiste accreditaties zoals gesteld in de BIO en wettelijke kaders.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 3.4      | Uitbesteding van IT-diensten aan externe partijen gebeurt alleen indien: <ul style="list-style-type: none"> <li>• Er hiervoor een positieve (kwalitatieve en kwantitatieve) business case bestaat waarin het financiële aspect, de invloed op digitale soevereiniteit en de toepasbaarheid van de dienstverlening overwogen is (i.e. de uitbesteding zinvol is);</li> <li>• Er een formeel exit-plan, uitwijkmogelijkheden en risicoanalyses ontwikkeld zijn, en;</li> <li>• De Rijksoverheid beschikt over de benodigde competenties om regie te voeren over de uitbestede IT-diensten.</li> </ul> |

| #        |                                                                                                                                          |
|----------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>4</b> | <b>Implementeren</b>                                                                                                                     |
| 4.1      | Beschikbaarheid en continuïteit worden te allen tijde gegarandeerd bij de implementatie.                                                 |
| <b>5</b> | <b>Monitoren, evalueren en optimaliseren</b>                                                                                             |
| 5.1      | Financiële status en digitale soevereiniteit ten opzichte van gecontracteerde leveranciers wordt periodiek gecontroleerd en geëvalueerd. |
| 5.2      | De opslag en verwerking van Rijksoverheid data door externe leveranciers wordt gemonitord en periodiek geëvalueerd.                      |
| <b>6</b> | <b>Beëindigen</b>                                                                                                                        |
| 6.1      | Bij beëindiging wordt de continuïteit van de dienstverlening geborgd en worden verstoringen voorkomen.                                   |
| 6.2      | Bij overnames van gecontracteerde leveranciers dient opnieuw een geschiktheidstest en risicoanalyse uitgevoerd te worden.                |
| 6.3      | Exit-plannen worden periodiek getest, bevindingen worden meegenomen in een bijgewerkte versie van het exit-plan.                         |
| 6.4      | Levenscyclus management van IT-dienstverlening wordt na beëindiging geëvalueerd en gecontinueerd.                                        |

**Tabel 7** Overzicht IT-sourcing randvoorwaarden

## C. IT-sourcing principes

| #        |                                                                                                                                                                                                         |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1</b> | <b>Behoeftestelling</b>                                                                                                                                                                                 |
| 1.1      | Elke behoefte wordt onderbouwd met een business case.                                                                                                                                                   |
| 1.2      | Behoeften van de Rijksoverheid worden getoetst op relevantie met nieuwe en innovatieve IT-oplossingen                                                                                                   |
| 1.3      | Bij IT-sourcing worden normen en maatregelen geanalyseerd om te bepalen welke te beschermen belangen betrokken zijn. Zo wordt bepaald of het ABRO- en Cloudbeleid relevant zijn voor de sourcing vraag. |
| 1.4      | Waar mogelijk worden behoeften (vragen) gebundeld zodat op uniforme wijze IT-dienstverlening kan worden afgenomen.                                                                                      |
| 1.5      | Bij verkaveling wordt rekening gehouden met de samenhang met overige IT-dienstverlening en ketens.                                                                                                      |
| 1.6      | Bij IT-sourcing wordt geëvalueerd of de IT-middelen een relatie hebben met de vitale processen van het Rijksonderdeel en wat de impact van beschikbaarheid is op deze processen.                        |
| 1.7      | De IT-sourcing strategie wordt geïntegreerd in de bredere bedrijfsvoering en IT-sourcing strategieën van Rijksonderdelen.                                                                               |
| 1.8      | Er wordt rekening gehouden met het modulaair en deelbaar houden van de IT-omgeving om onafhankelijkheid van de markt te borgen.                                                                         |
| <b>2</b> | <b>Strategische sourcing keuze</b>                                                                                                                                                                      |
| 2.1      | Het verwerven van vitale dienstverlening kan alleen onder voorwaarden worden uitbesteed.                                                                                                                |
| 2.2      | Resultaatverantwoordelijkheid voor vitale diensten blijft binnen de Rijksoverheid.                                                                                                                      |
| 2.3      | Als de IT-dienst direct verbonden is met een vitale rol voor de Rijksoverheid, heeft de kwaliteit van de te leveren dienst een hogere prioriteit dan de prijs.                                          |
| 2.4      | De gekozen sourcing leveringsvorm sluit aan op de regie organisatie van de Rijksoverheid.                                                                                                               |
| 2.5      | De IT-sourcing strategie dient diverse werkwijzen, zoals SAFe, te faciliteren.                                                                                                                          |
| 2.6      | De mate van overdraagbaarheid van diensten wordt meegenomen in de keuze voor een sourcing leveringsvorm.                                                                                                |
| 2.7      | Afhankelijkheidsrelaties worden meegenomen in sourcing keuzes, zodanig dat concentratierisico's worden voorkomen en/of worden gemitigeerd door maatregelen – zie ook principe 3.2 en 3.3.               |



| #        |                                                                                                                                                                                                                                        |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.8      | Indien er standaarddiensten beschikbaar zijn die voldoen aan de gestelde behoefte, wordt daarvan gebruik gemaakt in plaats van maatwerk.                                                                                               |
| 2.9      | Sourcing wordt zoveel mogelijk modulair toegepast, wat betekent dat kavel individueel van sourcing leveringsvorm kunnen wijzigen zonder significante technologische, functionele of contractuele impact.                               |
| 2.10     | De uitkomsten van een analyse voor het in kaart brengen van conflicterende belangen wordt meegenomen in de sourcing keuze.                                                                                                             |
| 2.11     | Duurzaamheid en mogelijkheden tot verduurzaming van IT-dienstverlening worden meegenomen in sourcing keuzes.                                                                                                                           |
| 2.12     | Ruimte voor innovatie en doorontwikkeling wordt meegewogen in de sourcing keuze.                                                                                                                                                       |
| 2.13     | Streef naar een multi-leverancier en multi-technologie aanpak ten aanzien van sourcing. Dit principe bevordert de spreiding van afhankelijkheidsrelaties en vermindert risico's door diversificatie van leveranciers en technologieën. |
| <b>3</b> | <b>Verwerven en contracteren</b>                                                                                                                                                                                                       |
| 3.1      | Rijksfaciliteiten worden altijd overwogen bij het verwerven van dienstverlening.                                                                                                                                                       |
| 3.2      | Bij het selecteren van leveranciers waarvoor een door SLM Rijk opgestelde raamovereenkomst bestaat, wordt gebruikgemaakt van dat raamwerk.                                                                                             |
| 3.3      | Risico's van leveranciersconcentratie en de financiële situatie van leveranciers worden meegenomen in het verwervingsproces.                                                                                                           |
| 3.4      | Risico's en maatregelen voor (vroegtijdige) beëindiging en (re)transitie van de dienst worden opgenomen in het verwervingsproces.                                                                                                      |
| 3.5      | Bij vitale diensten of diensten waar bijzondere gegevens verwerkt worden, worden aanvullende contractuele voorwaarden opgenomen rondom onderaannemers, informatiebeveiliging en audit rechten.                                         |
| 3.6      | Bij complexe IT-dienstverlening van externe leveranciers wordt een marktconsultatie uitgevoerd.                                                                                                                                        |
| 3.7      | Bij externe complexe IT-dienstverlening wordt een aanbestedingsprocedure waarin er mogelijkheid is tot dialoog met marktpartijen uitgevoerd.                                                                                           |

| #        |                                                                                                                                                                                                                                       |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>4</b> | <b>Implementeren</b>                                                                                                                                                                                                                  |
| 4.1      | Interoperabiliteit en flexibiliteit in technologie wordt aangewend om lock-in met externe partijen te minimaliseren.                                                                                                                  |
| 4.2      | Bij implementatiekeuzes wordt rekening gehouden met de overdraagbaarheid van de IT-dienst.                                                                                                                                            |
| 4.3      | Bij een eventuele overdracht tussen leverende partijen dient rekening worden gehouden met de huidige en toekomstige (her)transitierisico's en -kosten.                                                                                |
| <b>5</b> | <b>Monitoren, evalueren en optimaliseren</b>                                                                                                                                                                                          |
| 5.1      | De Rijksoverheid dient te allen tijde de kwaliteit en prijs van de dienstverlening door interne en externe leveranciers te kunnen monitoren op basis van harde (KPI's en SLA's) en zachte (relatie en klanttevredenheid) indicatoren. |
| 5.2      | De Rijksoverheid houdt rekening met huidige en toekomstige (re)transitierisico's en -kosten en neemt waar nodig maatregelen om deze laag te houden, waarbij de continuïteit gewaarborgd blijft.                                       |
| 5.3      | Bij onvoorziene en aanzienlijke veranderingen bij de dienstverlener, wordt een passende herbeoordeling van de geleverde dienst en bijbehorend risico's uitgevoerd.                                                                    |
| 5.4      | De Rijksoverheid en partners dragen zorg voor de medewerkers (intern en extern), door begeleiding en een veilige werkomgeving te bieden.                                                                                              |
| 5.5      | Duurzaamheid en kansen voor het verduurzamen van IT-dienstverlening worden regelmatig geëvalueerd.                                                                                                                                    |
| <b>6</b> | <b>Beëindigen</b>                                                                                                                                                                                                                     |
| 6.1      | Bij het beëindigen van de IT-dienstverlening dient het vooropgestelde exit-plan gevolgd te worden.                                                                                                                                    |

**Tabel 8** Overzicht IT-sourcing principes

## D. Bronvermelding

In onderstaand overzicht staan de bronnen die zijn gebruikt in dit document.

| #  | Bron                                                                                                                                                           |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Rijksbrede strategie IT-sourcing, versie 0.7, april 2025                                                                                                       |
| 2  | Discussienotitie Microsoft-365 i.r.t. Open Source en AVG                                                                                                       |
| 3  | Digital Operational Resilient Act (DORA)                                                                                                                       |
| 4  | EBA Guidelines of outsourcing arrangements                                                                                                                     |
| 5  | Europa's digitale decennium: Doelstellingen voor 2030, 27 september 2023                                                                                       |
| 6  | Het Rijk in de cloud: Donkere wolken pakken samen, jan 2025                                                                                                    |
| 7  | Inkopen met Impact, 28 oktober 2019                                                                                                                            |
| 8  | I-strategie Rijk 2021-2025, 11 januari 2022                                                                                                                    |
| 9  | Nederlandse digitaliseringsstrategie, 2025                                                                                                                     |
| 10 | Rijkscloudbeleid door ADR en CISO Rijk, 2022                                                                                                                   |
| 11 | Rijksinkoopstelsel Strategie en organisatie                                                                                                                    |
| 12 | Sourcingsafwegingskader binnen het Rijk, 9 mei 2012                                                                                                            |
| 13 | Van Kwetsbaar naar weerbaar: geleerde lessen uit dreigende acute en langdurige uitval van uitbestede ICT-dienstverlening bij overheidsorganisaties, maart 2025 |

Tabel 9 Bronnen

## E. Afkortingenlijst

In onderstaand overzicht staan de afkortingen die zijn gebruikt in dit document.

|      |                                                              |
|------|--------------------------------------------------------------|
| ADR  | Auditdienst Rijk                                             |
| AVG  | Algemene Verordening Gegevensbescherming                     |
| BBN  | Basisbeveiligingsniveau                                      |
| BIA  | Business Impact Analysis                                     |
| BIO  | Baseline Informatiebeveiliging Overheid                      |
| CISO | Chief Information Security Officer                           |
| CoE  | Center of Excellence                                         |
| DORA | Digital Operational Resilience Act                           |
| EBA  | European Banking Authority                                   |
| ICBR | Interdepartementale Commissie Bedrijfsvoering<br>Rijksdienst |
| ICT  | Informatie- en Communicatietechnologie                       |
| ICIA | Interdepartementale Commissie Inkopen en<br>Aanbesteden      |
| KPI  | Key Performance Indicator                                    |
| NDS  | Nederlandse Digitaliseringsstrategie                         |
| PIA  | Privacy Impact Assessment                                    |
| SLA  | Service Level Agreement                                      |
| SLM  | Service Level Management                                     |

**Deze publicatie is een uitgave van:**

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Oktober 2025