DANW
Digital Architects NetWork

Een Enterprise Architectuur aanpak voor Digitale Soevereiniteit

Een whitepaper van het Digital Architects NetWork

Oktober 2026

© Copyright 2026, Digital Architects NetWork

Deze publicatie is, tenzij anders vermeld, beschikbaar onder de licentie Creative Commons Naamsvermelding 4.0 Internationaal (CC BY 4.0).

Hergebruik, verspreiding en bewerking zijn toegestaan, mits de volgende bronvermelding wordt opgenomen: *Digital Architects NetWork, Een enterprise-architectuuraanpak voor digitale soevereiniteit, versie 1, 2026.*

Bij bewerkingen moet worden aangegeven dat het oorspronkelijke werk is gewijzigd. Het gebruik van de naam of het logo van DANW mag niet de indruk wekken dat DANW de bewerking of de gebruiker daarvan onderschrijft.

Digital Architects NetWork, Een Enterprise Architectuur aanpak voor Digitale Soevereiniteit

Versie 1.0 Oktober 2026

Gepubliceerd door Digital Architects NetWork, oktober 2026

Opmerkingen met betrekking tot het materiaal in dit document kunnen worden ingediend bij:

Digital Architects NetWork
Transistorstraat 71-M
1322 CK Almere

of per e-mail aan:
info@danw.nl

DANW
Digital Architects NetWork

Inhoudsopgave

1 Management samenvatting 1

2 Aanleiding en context 2

3 Begrippenkader en afbakening 4

4 Wat maakt digitale soevereiniteit een architectuurvraagstuk 5

4.1 Ontwerpkeuzes kunnen essentieel zijn voor soevereiniteit 5

4.2 Aanpassingen vereisen van meet af aan draagvlak 5

4.3 Keuzes moeten bewust en consistent gemaakt worden 5

4.4 Hoe krijg je inzicht? 6

4.5 Hoe ondersteun je besluitvorming? 6

4.6 Vertaling naar de praktijk 6

5 Governance- en architectuurprincipes 8

5.1 Maak kritieke afhankelijkheden expliciet 8

5.2 Hanteer proportionaliteit op basis van kritische belangen 8

5.3 Ontwerp voor interoperabiliteit en openheid 9

5.4 Beperk lock-in door modulariteit en vervangbaarheid 9

5.5 Borg regie op data, sleutels en toegang 9

5.6 Ontwerp voor continuïteit, herstelbaarheid en vervangbaarheid 10

5.7 Veranker besluitvorming in expliciete risicokaders 10

5.8 Borg transparantie en toetsbaarheid in governance 11

5.9 Soevereiniteit ‘by-design’ 11

6 Het managen van soevereiniteitsrisico’s 12

6.1 Inleiding 12

6.2 Overzicht 13

6.3 Context Establishment 14

6.4 Risk Assessment – Risk Identification 14

6.5 Risk Assessment – Analysis and Evaluation 15

6.6 Risk Treatment 15

6.7 Risk Acceptance 16

6.8 Doorlopende fasen: Communication and Consulting, Monitoring and Review 16

7 Hulpmiddelen voor de architect 18

7.1 Dreigingenbibliotheek 18

7.2 Model voor risicotolerantie 18
7.3 Context Model 18
7.4 Bedrijfsimpact Canvas 18
7.5 Stakeholder power grid 19
7.6 Dreigingsactoren 19
7.7 Architectuur heatmap 19
7.8 Risicomatrix 20
7.9 Self-assessment ('radar') 20
7.10 Potentiële maatregelen 20
8 Governance, rollen en verantwoordelijkheden 22
9 Conclusies en aanbevelingen 23
10 Gebruikte bronnen en inspiratiebronnen 24
11 Begrippenlijst 25
12 Bijbehorende hulpmiddelen 28

Figuren

Figuur 1 - TOGAF risiciobeheersing volgens ISO 27005 13
Figuur 2 - Stakeholder Power Grid 19
Figuur 3 - Risico evaluatie matrix 20

De bijdragen aan dit document van de volgende personen en/of werkgroepen worden dankbaar erkend:

- Ronald Coenen
- André van Dalen
- Lydia Duijvestijn
- Joost Melsen
- Raymond Slot
- Ingrid Stap
- Hugo Valk

DANW
Digital Architects NetWork

1 Management samenvatting

Digitale soevereiniteit is voor veel organisaties uitgegroeid tot een strategisch vraagstuk. Waar voorheen het economische voordeel dominant was in technologiekeuzes, ontstaat steeds meer behoefte aan grip op afhankelijkheden van leveranciers, cloudplatformen, geopolitieke invloeden en digitale ketens. Voor digitaalkundige architecten betekent dit dat architectuurkeuzes mede moeten worden beschouwd vanuit het digitale soevereiniteitsbelang, en dat het behouden of versterken van keuzevrijheid daarbinnen (digitale autonomie) een doel wordt.

Deze whitepaper positioneert digitale soevereiniteit als een integraal architectuurvraagstuk. Het onderwerp raakt niet alleen data en infrastructuur, maar ook businessprocessen, governance, sourcing, security, compliance en de bestuurlijke besluitvorming over risico's. De kernboodschap van deze whitepaper is dat digitale soevereiniteit een essentieel te beschouwen aspect is van de digitale architectuur. De mate waarin dit doorwerkt in concrete keuzen of beperkingen kan verschillen per organisatie of per organisatie-element. Niet elke waardestroom, capability of voorziening vraagt om dezelfde mate van autonomie.

Om organisaties hierbij te ondersteunen, introduceert deze whitepaper praktische hulpmiddelen en een risicogebaseerde aanpak voor contextanalyse, het stellen van doelen, het creëren van draagvlak, en de concretisering naar identificatie, beoordeling en behandeling van risico's. Via de daarbij in te zetten hulpmiddelen is er een relatie te leggen naar het reguliere architectuurproces. Het geheel dient een cyclisch proces te zijn, omdat omstandigheden, risico-afwegingen en oplossingen zich continu ontwikkelen. Deze whitepaper is daarmee een eerste stap naar een meer architectuurgedreven benadering van digitale soevereiniteit. De aanpak biedt een praktisch vertrekpunt dat in organisaties verder kan worden ingebed, getoetst en doorontwikkeld.

De whitepaper sluit af met aanbevelingen voor digitaalkundige architecten en organisaties die digitale soevereiniteit belangrijk vinden. Door digitale soevereiniteit niet te benaderen als los thema, maar als een structureel onderdeel van enterprise-architectuur, risicosturing en governance, kan gericht worden gestuurd op verbeteringen. Daardoor worden cruciale afhankelijkheden in kritieke processen, data, technologie en ketenrelaties transparant en bestuurbaar, en zijn ze op gestructureerde wijze te adresseren.

2 Aanleiding en context

Organisaties opereren in een digitale werkelijkheid met steeds sterkere afhankelijkheden van internationaal opererende leveranciers, wereldwijd gebruikte infrastructuur- en platformdiensten, en AI-platforms en toepassingen die daarop voortbouwen. Cloudmigraties, toenemende cyberdreigingen, en geopolitieke ontwikkelingen maken organisaties kwetsbaar voor risico's ten aanzien van die afhankelijkheden. Tegelijkertijd worden organisaties geconfronteerd met strengere eisen rond security, continuïteit, compliance en uitlegbaarheid van digitale keuzes. In dat speelveld groeit de noodzaak om zelf regie te behouden over data, processen, technologie en ketenafhankelijkheden.

Voor publieke organisaties speelt daarbij bovendien dat digitale keuzes vaak direct raken aan publieke waarden zoals rechtszekerheid, continuïteit van dienstverlening, bestuurlijke controle en maatschappelijke weerbaarheid. Voor private organisaties geldt dat afhankelijkheden van leveranciers, data-ecosystemen en platformdiensten directe invloed hebben op concurrentievermogen, risicoprofiel en strategische wendbaarheid. Digitale soevereiniteit raakt daarmee zowel de publieke als private sector, zij het vanuit een andere bestuurlijke en operationele context.

Binnen het Digital Architects NetWork Nederland (DANW) merken we dat architecten in de praktijk worden geconfronteerd met uiteenlopende vragen rondom digitale soevereiniteit. Een greep:

- Wat is digitale soevereiniteit? Wat zijn de risico's voor onze organisatie?
- Voor welke waardestromen en ketens is digitale soevereiniteit een zorgpunt? Is deze scope gelijk aan wat we vanuit continuïteits- en beveiligingsperspectief hebben geïdentificeerd?
- Welke mate van autonomie is vereist? Wanneer is afhankelijkheid acceptabel? Wanneer moet een organisatie aanvullende waarborgen inbouwen?
- Hoe ga je om met de toenemende afhankelijkheid van platformdiensten, vendor lock in of het besef dat “het vijf jaar duurt voordat je weg kunt zijn bij een cloud provider”?
- Hoe maken we dit alles inzichtelijk en hanteerbaar? Hoe weten we zeker dat we er op een goede manier mee bezig zijn? Wat is de relatie van soevereiniteitsdiscussies met bredere risicobenaderingen en volwassenheidsmodellen?
- Welke ontwerpkeuzes dragen bij aan autonomie zonder innovatie onnodig te remmen?

Deze vragen laten zien dat digitale soevereiniteit een thema is dat een digitaalkundige architect dient te beheersen zoals andere thema's: het raakt aan dagelijkse ontwerpkeuzes, strategische afhankelijkheden en het vinden van de juiste balans voor elk toepassingsgebied.

Voor organisaties is niet langer de vraag of ze grip moeten houden op de digitale ondersteuning van de bedrijfskritische ketens en waardestromen, maar vooral hóe zij hun zeggenschap en keuzevrijheid daarin kunnen borgen. Zij zullen daarbij aandacht moeten hebben voor jurisdictie, overeenkomsten met externe partijen, eigenaarschap, autonomie over identiteiten, data en technologie, en daarnaast onder andere over beheerverantwoordelijkheden en te hanteren standaarden. Deze whitepaper is geschreven vanuit de overtuiging dat architecten een sleutelrol hebben in het zichtbaar maken, wegen en beheersen van deze vraagstukken.

De voorgestelde risicogebaseerde werkwijze waarborgt een goede balans tussen kosten en baten en laat een consistent en organisatiebreed toepasbaar denkkader ontstaan. Na het opstellen van de aanpak en het onderliggende model hebben enkele leden van het Digital Architects NetWork (DANW) deze in verschillende praktijkcontexten getoetst. De bevindingen, inzichten en

verbeterpunten die hieruit voortkwamen, zijn verwerkt en worden in deze paper gedeeld om collega-architecten te ondersteunen met direct toepasbare praktijkervaring.

3 Begrippenkader en afbakening

Van oudsher gaat autonomie over het kunnen nemen van besluiten, en soevereiniteit over het juridische en bestuurlijke gezag om dat te doen.

Digitale autonomie gaat dan over het vermogen om keuzes te maken in het digitale domein. Dit betekent zeggenschap over de inrichting van de eigen digitale infrastructuren en controle over hoe de eigen data verwerkt (mag) worden, waar data ligt opgeslagen en wie daar toegang toe heeft tegen welke kosten.

Digitale soevereiniteit gaat (op staatsniveau) over het juridische en bestuurlijke gezag over de essentiële digitale aspecten in economie, maatschappij en democratie. Voor een organisatie gaat het specifiek over juridische en bestuurlijke controle over digitale infrastructuren, data en systemen.

In de context van deze whitepaper wordt de volgende definitie gehanteerd:

Digitale soevereiniteit is het vermogen van een organisatie om juridische, bestuurlijke en operationele regie te behouden over haar digitale middelen, data, processen en afhankelijkheden, zodanig dat zij haar strategische, maatschappelijke en operationele doelstellingen kan blijven realiseren binnen aanvaardbare grenzen van risico en afhankelijkheid.

Het gaat daarmee niet om het realiseren van volledige onafhankelijkheid, maar om aantoonbare beheersing van kritieke afhankelijkheden en om het vermogen om verantwoorde keuzes te maken.

In deze whitepaper gebruiken we de term *regie* als overkoepelend begrip voor het kunnen sturen, voorwaarden stellen, afdwingen en bijsturen. De term *zeggenschap* verwijst vooral naar het juridische of bestuurlijke recht om te beslissen. Als we het hebben over *controle* dan verwijst dit naar de feitelijke technische of operationele mogelijkheid om die keuzes ook uit te voeren en te beheersen. In 12.1 Begrippenlijst op pagina 52 is een lijst van begrippen met omschrijving opgenomen die betrekking hebben op de inhoud van dit document.

Deelgebieden zoals data-soevereiniteit, cloud-soevereiniteit en technologische autonomie kunnen bijdragen aan digitale soevereiniteit, maar vallen daar niet één-op-één mee samen. Data-soevereiniteit richt zich primair op zeggenschap over data, inclusief opslag, verwerking, toegang en gebruik. Cloud-soevereiniteit richt zich op de vraag onder welke voorwaarden cloudvoorzieningen kunnen worden ingezet zonder ongewenste juridische, operationele of geopolitieke afhankelijkheden. Technologische soevereiniteit betreft de bredere mate waarin een organisatie of samenleving zelfstandig kan beschikken over essentiële digitale capaciteiten. Digitale soevereiniteit vraagt om de bestuurlijke en architecturale afweging van deze deelaspecten in samenhang.

In deze whitepaper beschouwen wij digitale soevereiniteit als een architectuur- en besturingsvraagstuk, dat doorlopende aandacht vereist. Daarbij ligt de focus op de analyse van context, afhankelijkheden, risico's en ontwerpkeuzes.

Dit document is echter geen juridisch normenkader en biedt evenmin een volledig compliance-raamwerk. Wet- en regelgeving, normen en sectorale kaders worden gezien als relevante randvoorwaarden en input voor besluitvorming, maar vormen niet het primaire onderwerp van deze publicatie.

4 Wat maakt digitale soevereiniteit een architectuurvraagstuk

4.1 Ontwerpkeuzes kunnen essentieel zijn voor soevereiniteit

Het handelingsperspectief van een organisatie voor de toekomst wordt in hoge mate mede bepaald door essentiële architectuurkeuzes uit het verleden, omdat deze keuzen in de praktijk zelden makkelijk te wijzigen zijn: waar data staat, wie toegang heeft, wie sleutels beheert, hoe systemen gekoppeld zijn, van welke leveranciers, platformen en diensten gebruik wordt gemaakt.

De keuze voor een cloudplatform, het gebruik van een leveranciersgebonden AI-dienst, de inrichting van identity- en keymanagement, de manier waarop data worden gedeeld in ketens, of de mate waarin processen afhankelijk zijn van één leverancier: het zijn allemaal architectuurbesluiten met directe invloed op autonomie en beheersbaarheid.

De toekomstvastheid van ontwerpkeuzes is een standaard kwaliteitscriterium voor digitaalkundige architecten. In digitale soevereiniteitsvraagstukken moet de architect in sterkere mate rekening houden met afhankelijkheden van juridische, contractuele en geografische aard, of daaruit voortvloeiende risico's op bijvoorbeeld operationeel vlak. Algemene kwaliteitseigenschappen nastreven zoals wendbaarheid, vervangbaarheid en beheerbaarheid kunnen daarbij helpen.

4.2 Aanpassingen vereisen van meet af aan draagvlak

Digitale soevereiniteit zal in de regel worden gezien als een aspect dat niet direct bijdraagt aan de primaire bedrijfsdoelen, vergelijkbaar met bijvoorbeeld informatiebeveiliging, privacy en bedrijfscontinuïteit. Dat kan het dus lastig maken om het onderwerp "op de agenda te krijgen en houden."

Anderzijds kunnen de eraan verbonden risico's op bestuurlijk niveau niet worden genegeerd. Het is dus van belang om een goede afstemming te hebben met de leiding van de organisatie over de risico's, risicotolerantie en de te realiseren doelen.

Juist de digitaalkundige architect kan de leiding van de organisatie helpen een positie in te nemen, door de risico's per beschouwingsgebied en op alle architectuurlagen inzichtelijk te maken. Daarmee kan de organisatie zich concreet uitspreken welke mate van afhankelijkheid zij, gegeven haar publieke, maatschappelijke of bedrijfsmatige belangen, nog aanvaardbaar vindt en wanneer aanvullende maatregelen, herontwerp of bestuurlijke escalatie nodig zijn.

4.3 Keuzes moeten bewust en consistent gemaakt worden

Omdat volledige onafhankelijkheid van derde partijen niet bestaat, blijven keuzes over digitale soevereiniteit altijd een risico-afweging in zich houden. Daarom dienen voorgenomen architectuurkeuzes gepaard te gaan met een risicoanalyse op digitale soevereiniteit. De op bestuurlijk niveau uitgesproken risicobereidheid ten aanzien van afhankelijkheden kan daarbij fungeren als toetssteen.

Dat geldt bijvoorbeeld voor afhankelijkheid van niet-EU-jurisdicties, vendor lock-in, toegang van derde partijen tot data of beheerfuncties, het gebruik van leverancier specifieke platformdiensten of de mate waarin sleutelbeheer en identiteiten buiten de eigen regie komen te liggen. Door dit expliciet te maken, wordt digitale soevereiniteit van een abstract streven tot een navolgbaar besluitvormingskader.

4.4 Hoe krijg je inzicht?

Digitale soevereiniteit raakt in potentie alle lagen en elementen van de digitale architectuur. Bestaande architectuurmodellen en -inzichten van de digitale architect kunnen dienen als startpunt voor risicoanalyses en gewenste aanpassingen, vanuit verschillende perspectieven:

- Op bedrijfsarchitectuurniveau gaat het om hoe bedrijfscontinuïteit en grip op afhankelijkheden van externe partijen is georganiseerd voor bedrijfskritische processen en concrete dienstverleners/leveranciers;
- Op informatieniveau gaat het om het op orde zijn van informatiebeveiliging, privacy en juridische zeggenschap over informatie voor de diverse objecten, hun classificatie, en de implementatie van opslag, verwerking en uitwisseling;
- Op applicatieniveau gaat het om koppelbaarheid, interoperabiliteit, onderhoudbaarheid, beheerbaarheid en - niet in de laatste plaats – vervangbaarheid;
- Op het vlak van toegang en beveiliging gaat het om identiteiten, sleutelbeheer, privileged access en de rol van externe beheerders of leveranciers;
- Op technologisch en operationeel niveau raakt het vraagstukken als continuïteit, herstelbaarheid, vervangbaarheid, interoperabiliteit, robuustheid en de beheersing van concentratie- en ketenrisico's.

De modellen en analyses kunnen inzicht geven voor afzonderlijke keuzes, of voor afwegingen over het totaal.

4.5 Hoe ondersteun je besluitvorming?

In de initiële gesprekken over soevereiniteit voelen organisaties wel dat afhankelijkheden van leveranciers, cloudplatformen, jurisdicties of ketenpartners ertoe doen, maar kunnen ze vaak niet scherp aangeven welke afhankelijkheden nog acceptabel zijn en waar de grens ligt.

Zoals eerder aangegeven, zien we twee onderwerpen die bijdragen aan consistente weging en besluitvorming, oftewel het "bestuurbaar" maken van digitale soevereiniteit als vraagstuk. De eerste is het hebben van een zo concreet geformuleerde risicobereidheid die bestuurlijk is vastgesteld, en die kan helpen als toetssteen voor concrete ontwerpkeuzes. De tweede is een risicoanalyse (per beschouwingsgebied, of per onderwerp van een voorgenomen besluit).

Samen maken ze concreet, of een architectuurkeuze nog past binnen de gewenste mate van soevereiniteit, dan wel dat ze de afhankelijkheid zodanig vergroot dat ze niet langer acceptabel is of aanvullende waarborgen vereist.

4.6 Vertaling naar de praktijk

Een risicogebaseerde aanpak draagt niet alleen bij aan het nemen van inhoudelijke architectuurbesluiten, maar ook aan consistente besluitvorming door de leiding van de organisatie. Wanneer vooraf duidelijk is welke risico's en afhankelijkheden acceptabel zijn, kunnen projecten en besluitvormers sneller en uniformer handelen. Uitzonderingen worden beter uitlegbaar, investeringen in mitigaties kunnen gerichter worden geprioriteerd en compliance-eisen kunnen eerder in het ontwerp worden meegenomen.

De hierboven beschreven aandachtspunten zijn geen kant-en-klare aanpak. Architecten zullen ze moeten inpassen in de werkwijzen die ze binnen hun eigen organisatie hanteren.

Het aansluiten bij (of inrichten van) gestandaardiseerde processen kan helpen om te zorgen dat zorgvuldige besluitvorming door alle betrokkenen plaatsvindt.

Ter ondersteuning van architecten die in hun organisaties omgaan met vraagstukken rondom digitale soevereiniteit, beschrijft deze whitepaper hierna generieke principes, de procesmatige risicobeheersing, en modellen die houvast bieden bij besluitvorming.

De rol van de digitaalkundige architect is daarmee niet om volledige digitale onafhankelijkheid te ontwerpen, maar om de feitelijke afhankelijkheden, risico's en keuzeruimte zichtbaar te maken en te vertalen naar proportionele architectuurkeuzes.

5 Governance- en architectuurprincipes

Voor architecten kunnen principes een middel zijn om het gesprek over digitale soevereiniteit concreet te maken. Zij helpen om abstracte ambities te vertalen naar ontwerpkeuzes en om bestuurlijke discussies te verbinden met de technische en organisatorische realiteit.

De principes in dit hoofdstuk zijn bedoeld als richtinggevend kader voor architecten en besluitvormers. Ze zijn zo opgesteld, dat ze iedere organisatie ruimte laten voor proportionele concretisering naar architectuurkeuzes, passend bij de context van de eigen organisatie, de mate waarin waardestromen bedrijfskritisch zijn, de dataclassificatie, de afhankelijkheden in de keten en de risicotolerantie.

De kans is groot, dat de principes voor digitaalkundige architecten herkenbaar zijn. Vreemd is dat niet, want als algemene uitgangspunten voor goed ontwerp gelden ze ook voor aspecten zoals continuïteit, informatiebeveiliging en privacy.

5.1 Maak kritieke afhankelijkheden expliciet

Een eerste en fundamenteel principe is dat kritieke afhankelijkheden zichtbaar moeten worden gemaakt. Veel organisaties zijn in de loop der jaren afhankelijk geworden van leveranciers, platforms, diensten, technologieën en regio's zonder dat deze afhankelijkheden expliciet zijn benoemd of bestuurd. Juist daardoor worden risico's vaak pas zichtbaar wanneer er zich een incident, prijsverhoging, contractueel geschil, geopolitieke verandering of technische blokkade voordoet.

Voor digitale soevereiniteit is het daarom noodzakelijk om systematisch in kaart te brengen van welke externe partijen en voorzieningen een organisatie afhankelijk is, hoe diep die afhankelijkheid reikt en welke gevolgen het heeft wanneer deze wegvalt of verandert. Het gaat daarbij niet alleen om primaire IT-diensten, maar ook om onderliggende bouwstenen zoals werkplekdiensten, platformdiensten, logisch toegangsbeheer, cryptografie, beheertools, dataopslag, externe (beheer-)diensten, netwerkvoorzieningen, rekenkracht, fysieke apparatuur.

Architectuur moet deze afhankelijkheden niet alleen registreren, maar ook duiden. Een afhankelijkheid is pas bestuurbaar wanneer duidelijk is welke risico's eraan verbonden zijn en of deze acceptabel, te mitigeren of onwenselijk zijn. Dit principe vormt daarmee het vertrekpunt voor alle verdere afwegingen in digitale soevereiniteit.

5.2 Hanteer proportionaliteit op basis van kritische belangen

Niet elke voorziening hoeft maximaal soeverein te worden ingericht. Een generieke kantoorfunctie stelt andere eisen dan een bedrijfskritische waardestroom, een vitale overheidsdienst of een proces waarin gevoelige gegevens, publieke waarden of hoge continuïteitseisen een rol spelen. Daarom dient digitale soevereiniteit altijd proportioneel benaderd te worden.

Dit betekent dat organisaties hun eisen aan autonomie, controle en beheersbaarheid in de praktijk zullen differentiëren op basis van de kritische belangen. Hoe groter de impact van verstoring, ongewenste toegang, dataverlies of lock-in, des te zwaarder de eisen die aan de architectuur moeten worden gesteld. De kritische belangen kunnen daarbij voortkomen uit operationele impact, maatschappelijke gevolgen, wettelijke verplichtingen, financiële schade, reputatierisico, afhankelijkheid van ketenpartners of effecten op bestuurlijke controle.

Voor architecten betekent dit principe dat ontwerpkeuzes niet los mogen worden beoordeeld, maar altijd in relatie tot de aard van het proces, de data en de afhankelijkheden die ermee samenhangen. Proportionaliteit voorkomt enerzijds overspecificatie en onnodige kosten, en anderzijds onderschatting van risico's in kritieke omgevingen.

5.3 Ontwerp voor interoperabiliteit en openheid

Digitale soevereiniteit wordt versterkt wanneer systemen, diensten en gegevensuitwisselingen gebaseerd zijn op open, overdraagbare en breed toepasbare afspraken. Interoperabiliteit is daarom een kernprincipe. Organisaties die hun architectuur op alle lagen baseren op gestandaardiseerde interfaces, open gegevensmodellen en helder gedefinieerde koppelvlakken, behouden meer wendbaarheid dan organisaties die sterk leunen op leveranciersgebonden integraties of gesloten platformvoorzieningen.

Dit principe betekent niet dat alleen open source of uitsluitend open standaarden zijn toegestaan. Wel betekent het dat architecten bewust moeten afwegen in hoeverre keuzes leiden tot technische of functionele lock-in. Wanneer een oplossing alleen goed functioneert binnen één leverancier specifiek ecosysteem, neemt de afhankelijkheid toe en wordt eventuele vervanging lastiger. Interoperabiliteit verlaagt die drempel en vergroot de ruimte om in de toekomst te migreren, te combineren of te vervangen.

Voor digitale soevereiniteit is openheid vooral van belang bij dataopslag, logische toegangsbeveiliging, toegankelijkheid van de data zelf, en portabiliteit van functionaliteit. Het ontwerp moet daarom voorkomen dat kernprocessen onnodig worden verankerd in gesloten mechanismen waarvoor geen reëel alternatief beschikbaar is.

5.4 Beperk lock-in door modulariteit en vervangbaarheid

Een toekomstbestendige architectuur is modulair van opzet. Dat betekent dat functies, data, integraties en technische voorzieningen zoveel mogelijk zodanig worden ingericht dat zij afzonderlijk kunnen worden aangepast of vervangen zonder disproportionele impact op de rest van het landschap. Modulariteit is daarmee een praktisch antwoord op ongewenste vendor lock-in.

Voor digitale soevereiniteit is vervangbaarheid een aspect dat extra aandacht vraagt. Een organisatie hoeft niet iedere component op korte termijn te kunnen uitwisselen, maar moet wel weten welke onderdelen feitelijk niet vervangbaar zijn en waarom. Waar een leverancier of platform een unieke en diep verweven positie heeft in een bedrijfskritische waardestroom, moet dit expliciet worden afgewogen en bestuurlijk worden gedragen.

Architecten kunnen dit principe concreet maken door te ontwerpen met duidelijke scheidingen tussen businesslogica, data, integratie, identity, beheer en infrastructuur. Ook helpt het om zoveel mogelijk te sturen op contractuele en technische vervangbaarheid, exporteerbaarheid van data, overdraagbaarheid van configuraties en beperking van afhankelijkheid van unieke platformservices wanneer daar geen proportionele rechtvaardiging voor bestaat.

5.5 Borg regie op data, sleutels en toegang

Digitale soevereiniteit raakt direct aan de vraag wie feitelijk controle heeft over data en over de middelen waarmee toegang tot die data wordt verkregen. Daarom is een belangrijk ontwerpprincipe dat organisaties expliciet sturen op eigenaarschap, classificatie, locatie, toegang en bescherming van data, inclusief de inrichting van sleutelbeheer en identiteitsvoorzieningen.

Het gaat hierbij niet alleen om opslaglocatie of juridische datalocatie, maar ook om de bredere keten van verwerking, beheer, supporttoegang, replicatie, logging, back-up en herstel. Ook moet duidelijk

zijn onder welke voorwaarden derden toegang kunnen krijgen tot gegevens of beheerfunctionaliteiten. Zeker bij cloud- en platformdiensten is dit een cruciaal aandachtspunt, omdat de feitelijke controle over identity, sleutelbeheer en privileged access mede bepaalt in hoeverre een organisatie daadwerkelijk autonoom opereert.

Voor architecten betekent dit dat regie op data niet mag worden gereduceerd tot een privacy- of complianceonderwerp. Het is een ontwerpvraagstuk dat raakt aan de kern van digitale autonomie. Waar de organisatie de feitelijke controle over data, sleutels of toegang verliest, bestaat het risico dat ze alle zeggenschap over de eigen data kwijtraakt, ook als de functionele dienstverlening intact blijft.

5.6 Ontwerp voor continuïteit, herstelbaarheid en vervangbaarheid

Digitale soevereiniteit wordt pas werkelijk relevant wanneer omstandigheden veranderen. Een leverancier kan diensten wijzigen of beëindigen, toegang kan worden beperkt, geopolitieke verhoudingen kunnen verschuiven, of een organisatie kan genoodzaakt zijn een andere koers te kiezen. Daarom moet architectuur niet alleen gericht zijn op normaal gebruik, maar juist ook op verstoring, herstel en vervangbaarheid.

Dit principe vraagt dat organisaties al in het ontwerp nadenken over scenario's waarin diensten niet of slechts beperkt beschikbaar zijn, communicatieketens verstoord raken of data en functionaliteit elders moeten worden ondergebracht. Het gaat dan om vragen als: wat gebeurt er bij langdurige uitval, welke processen moeten blijven functioneren, welke gegevens moeten beschikbaar blijven, hoe snel moet kunnen worden hersteld, en hoe realistisch is het om een voorziening daadwerkelijk te verlaten?

Vervangbaarheid mag daarbij niet uitsluitend contractueel worden benaderd. Een contractuele clausule om een afgenomen dienst te kunnen migreren naar een andere leverancier zonder technische uitvoerbaarheid biedt schijnzekerheid. Architectuur moet daarom ook zicht geven op de mate van exporteerbaarheid van data, afhankelijkheid van specifieke configuraties, benodigde migratiestappen, overdraagbaarheid van kennis en de operationele impact van een overstap. Continuïteit, herstelbaarheid en vervangbaarheid zijn in dat opzicht geen sluitstuk, maar fundamentele ontwerpeisen aan elke digitale oplossing.

5.7 Veranker besluitvorming in expliciete risicokaders

Digitale soevereiniteit vraagt om keuzes die zelden zwart-wit zijn. Er is vaak sprake van een afweging tussen gebruiksgemak, kosten, snelheid, continuïteit en autonomie. Om te voorkomen dat dergelijke keuzes willekeurig of incident-gedreven worden gemaakt, moeten zij worden ingebed in expliciete risicokaders.

Een belangrijk ontwerpprincipe is daarom dat architectuurbesluiten over afhankelijkheden en autonomie toetsbaar moeten zijn aan vooraf bepaalde kaders, zoals een model voor risicotolerantie. Daarmee wordt zichtbaar welke mate van afhankelijkheid nog acceptabel is, welke mitigerende maatregelen verplicht zijn en wanneer escalatie of bestuurlijke besluitvorming nodig is.

Voor architecten heeft dit twee voordelen:

1. Er ontstaat meer consistentie in besluitvorming tussen projecten, domeinen en waardestromen.
2. Uitzonderingen worden beter uitlegbaar. Niet elke keuze voor een buitenlandse cloudvoorziening die leidt tot een afhankelijkheid hoeft onwenselijk te zijn, maar dergelijke keuzes moeten wel bewust, navolgbaar en aantoonbaar binnen de afgesproken kaders passen.

5.8 Borg transparantie en toetsbaarheid in governance

Een architectuur die digitale soevereiniteit ondersteunt, vraagt om governance die inzicht geeft in gemaakte keuzes, resterende risico's en de werking van mitigerende maatregelen. Transparantie is daarmee niet alleen een bestuurlijk beginsel, maar ook een ontwerpprincipe. Wanneer een organisatie niet kan uitleggen hoe afhankelijkheden zijn georganiseerd, welke datastromen bestaan, welke toegangspaden actief zijn en welke restrisico's zijn geaccepteerd, ontbreekt de basis voor effectieve sturing.

Dit principe vraagt om een architectuur waarin relevante informatie over leveranciers, integraties, datastromen, toegangsmodellen, classificaties en maatregelen vindbaar en actualiseerbaar is. Ook moeten de uitkomsten van beoordelingen periodiek kunnen worden herzien, omdat technologische en geopolitieke omstandigheden veranderen. Wat vandaag proportioneel en acceptabel is, kan morgen een te groot risico vormen.

Toetsbaarheid betekent dat architectuurkeuzes niet alleen op ontwerpmomenten worden besproken, maar ook in beheer en governance een plaats krijgen. Digitale soevereiniteit moet zichtbaar zijn in architectuurreviews, in risicobeoordelingen, in sourcingbesluiten en in de verantwoording aan bestuur en toezicht.

5.9 Soevereiniteit 'by-design'

Experimentele trajecten, pilots en proof-of-concepts (PoC's) zijn waardevol om nieuwe technologie te verkennen, maar kunnen ook nieuwe afhankelijkheden introduceren. Daarom moeten soevereiniteitsprincipes al vanaf experiment en ontwerp worden meegewogen.

Tegelijk kunnen experimentele trajecten ook worden gebruikt om alternatieve technologieën of diensten, complexiteitsreductie en vervangingsscenario's vroegtijdig te toetsen. Door deze eerst als innovaties, PoC's of pilots neer te zetten, kan de haalbaarheid in een vroeg stadium worden getoetst.

Juist in situaties waar vervanging van een bestaande dienst of oplossing een meerjarig en duur traject dreigt te worden, kan het interessant zijn te verkennen welke complexiteitsreductie en tastbare resultaten te behalen zijn via experimentele, innovatieve initiatieven. Zo krijgen betrokkenen de mogelijkheid te leren hoe soevereiniteit succesvol is op te nemen in de architectuur en ontwerpen.

6 Het managen van soevereiniteitsrisico’s

6.1 Inleiding

Dit hoofdstuk geeft organisaties een aanzet voor een systematische aanpak om met digitale soevereiniteitsvraagstukken om te gaan. De aanpak bestaat uit een aantal concrete processtappen, met concrete hulpmiddelen als input en deliverables als output. De focus ligt in de aanpak op de analyse- en besluitvormingsfase. Digitale soevereiniteit vraagt daarbij niet om een eenmalige beoordeling, maar een cyclisch proces waarin context, dreigingen, risicotolerantie, maatregelen en restrisico’s periodiek worden herijkt.

In tegenstelling tot het ontwikkelen van een volledig eigen model, is heel sterk gekeken naar bestaande methoden om op voort te bouwen. Er is daarbij bewust aangesloten op het standaard raamwerk voor risicobeheersing ISO/IEC 27005:2022 en op TOGAF voor architectuur. SABSA is gebruikt als inspiratiebron voor het expliciet verbinden van businessdoelen, risico’s en architectuurkeuzes. Het is niet als formeel procesmodel overgenomen, maar sluit aan bij de stelling dat architectuur traceerbaar moet bijdragen aan businessdoelstellingen en risicobeheersing. Dit alles geeft digitaalkundig architecten de gelegenheid tot inbedding en aanpassing van het beschrevene in de werkwijze van hun eigen organisatie.[1]

Het raakvlak tussen een risicobeheersingsmethode en digitale architectuur bestaat er uit dat risico-informatie gevolgen kan hebben voor ontwerpkeuzes. Riskmanagement levert inzicht in risico's, restrisico's en risicobereidheid: digitale architectuur vertaalt deze naar principes, ontwerpcriteria en governance mechanismen. Dit vergt uiteraard afstemming en samenwerking met stakeholders over prioriteiten, haalbaarheid, en restrisico’s.

Dit hoofdstuk kiest bewust voor een enterprise-architectuur invalshoek, om ook de situatie te omvatten dat belangen en impact op het (hoogste) bestuurlijke niveau geadresseerd moeten worden. Digitale soevereiniteit is immers te zien als een architectuuraspect, dat op alle architectuurlagen beschouwd moet worden. Volgens TOGAF moet dat al worden geadresseerd in de fase “Architecture Vision,” door daarin de concrete dreigingen, te beschermen belangen (use cases), risicotolerantie en de business doelen voor digitale soevereiniteit expliciet te maken.[2]

Een tweede belangrijk aandachtsgebied bestaat uit de samengestelde fase voor het bepalen van de doelarchitectuur (die in dit document de Business Architecture, Information, Data, Technology Architecture fasen omvat). Daarin gaat het om het verder concretiseren van risico’s en de vertaling naar te nemen maatregelen in de architectuur.

Uiteraard zijn implementatie-evaluatie, continue analyse van dreigingen en risico’s, en bijstelling van doelen en acties relevant:

[1] Er is gekozen voor TOGAF, maar in principe is ieder raamwerk toepasbaar dat digitale architectuur in alle lagen en dimensies van de organisatie adresseert.

[2] TOGAF benoemt digitale soevereiniteit niet expliciet als kwaliteitsattribuut, architectuurprincipe, domein, of governance laag. Dat betekent dat organisaties zelf moeten bepalen hoe ze digitale

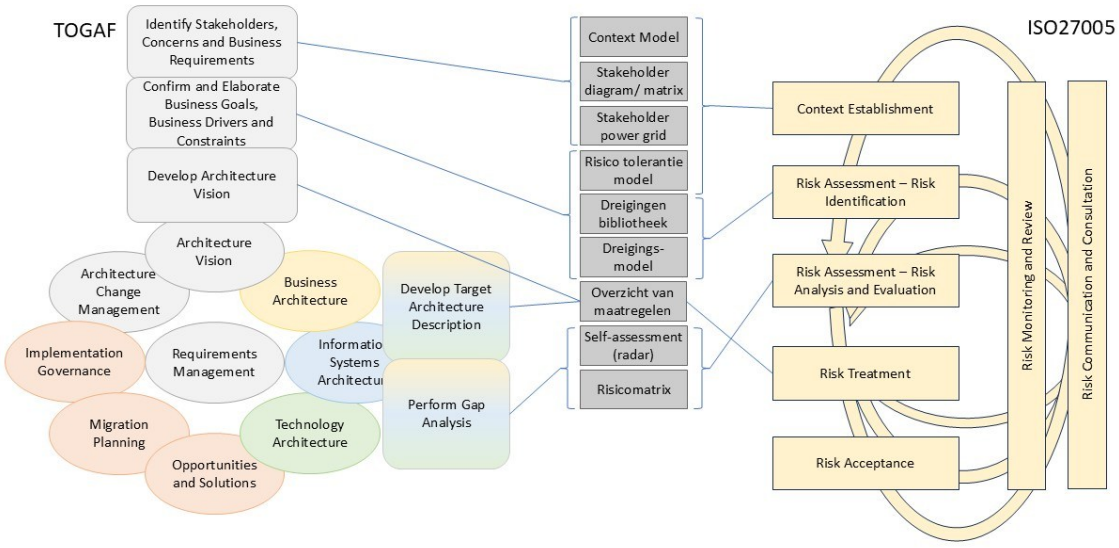
Digitale soevereiniteit vereist een cyclische aanpak voor risicoanalyse, het bepalen en realiseren van doelen, en implementatie-evaluatie.

Dit sluit aan bij zowel ISO 27005 als TOGAF: TOGAF ADM heeft een voor architecten bekend, cyclisch karakter, en ISO 27005 ondersteunt binnen hetzelfde raamwerk zowel kortere cycli (zoals iteratieve risicoclassificatie en uitwerking van maatregelen) als langere cycli (van hernieuwde vaststelling van een bedrijfscontext tot en met formele acceptatie).

6.2 Overzicht

De onderstaande figuur geeft links de TOGAF Architecture Development Method en rechts de hoofdstappen van risicobeheersing conform ISO 27005. Bij de TOGAF ADM cyclus zijn de concrete architectuurtaken benoemd die ook relevant zijn voor risicobeheersing. In de risicobeheersingscyclus kunnen producten worden gebruikt die uit de architectuurcyclus kunnen volgen, of die in samenwerking worden opgesteld. Deze producten zijn hier ingetekend met de mogelijke, expliciete verbinding tussen beide cycli.

Het volgende hoofdstuk en de bijlagen bij deze whitepaper bevatten omschrijvingen en sjablonen voor deze producten.



Figuur 1 - TOGAF risiciobeheersing volgens ISO 27005

ISO 27005 is een raamwerk dat zich richt op risicobeheersing binnen het domein informatiebeveiliging. Net als TOGAF laat het ruimte voor nadere methodische invulling. Het proces en de daarin gebruikte producten zijn daarmee prima algemener toe te passen, inclusief voor het oplossen van digitale soevereiniteitsvraagstukken.

De paragrafen hierna beschrijven de doelen en typische taken per fase van de risicobeheersingscyclus conform ISO 27005. Elke fase bevat ook een lijstje van de architectuurproducten die een hulpmiddel kunnen zijn in de fase. De hulpmiddelen zelf zijn toegelicht in het volgende hoofdstuk.

De in de volgende paragrafen beschreven fasen vormen de kern van een risicobeheersingscyclus in ISO 27005. Deze zijn:

- Context Establishment
- Risk Assessment – Risk Identification
- Risk Assessment – Analysis and Evaluation
- Risk Treatment
- Risk Acceptance

De verwijzingen naar zowel TOGAF als ISO 27005 zijn om reden van herkenbaarheid in het Engels opgenomen.

6.3 Context Establishment

In deze fase worden de voorwaarden ingevuld om de rest van de risicobeheersing goed te laten verlopen, zoals:

- Bepaal missie, waarden, doelen en prioriteiten
- Bepaal te beschermen belangen en niet-acceptabele uitkomsten
- Bepaal kritische bedrijfsdomeinen
- Bepaal verplichtingen en voorwaarden (juridisch, compliance, …)
- Bepaal de risicobeheersingsopdracht
- Identificeer beslissers
- Bepaal risicotolerantie
- Bepaal governance
- Identificeer risicoeigenaren voor systemen, diensten en andere assets

In relatie tot digitale soevereiniteit betekent dit, dat de stakeholders en te vermijden bedreigingen voor dit onderwerp expliciet moeten worden bepaald. Ook dient de scope en het doel van mogelijke initiatieven op voorhand afgestemd te zijn, zodat er in latere fasen draagvlak voor inzet van bedrijfsmiddelen is. Het is bij een uitbreiding van de beschouwing van risicotypen immers niet vanzelfsprekend, dat bestaande stakeholders een uitbreiding van hun verantwoordelijkheden zullen accepteren.

Hulpmiddelen:

- Model voor risicotolerantie – input voor de in deze fase te bepalen risicotolerantie
- Context Model – output van deze fase
- Stakeholder Diagram/Matrix - output van deze fase
- Stakeholder Power Grid – output van deze fase

6.4 Risk Assessment – Risk Identification

Dit is de eerste analysefase om te komen tot concrete risicobehandeling. Deze fase wordt uitgevoerd voor de scope die in de voorliggende fase is gedefinieerd, op grond van de hiervoor aangewezen (interne) assets, dan wel de gekozen (externe) bedreigingen. Hierin horen taken zoals:

- Begrijp de dreigingen uit de omgeving
- Identificeer externe actoren en beperkingen/afhankelijkheden daarvan
- Begrijp de scope en aard van risico’s
- Begrijp hoe risico’s evolueren
- Bepaal relaties naar andere typen risico’s

- Bepaal benodigde soorten beheersmaatregelen (controls)

De eerste twee items zijn hier expliciet genoemd, omdat digitale soevereiniteit een ‘outside in’ blik vereist.

Een goed risicobegrip is voor digitale soevereiniteit zeer relevant. Enerzijds omdat afhankelijkheden overal kunnen zitten in procesketens of in technology stacks. Potentiële maatregelen kunnen dus behoorlijk fundamenteel van aard zijn. Anderzijds omdat het aanpassen van eerdere, fundamentele keuzen nieuwe risico’s kan introduceren. Ook die moeten worden beschouwd.

Hulpmiddelen:

- Dreigingenbibliotheek– input voor de in deze fase te bepalen risico's
- Dreigingsmodel – input voor de in deze fase te bepalen risico's

6.5 Risk Assessment – Analysis and Evaluation

ISO 27005 kent na risicoidentificatie twee fasen die we hier samennemen: analysis en evaluation. In de analysefase worden per risico kans en mogelijke gevolgen bepaald. In de evaluatiefase wordt daaraan met stakeholders een classificatie verbonden, en bepaald welke risico’s opvolging krijgen. Typische taken zijn:

- Identificeer en classificeer risico’s
- Bepaal restrisico’s
- Definieer aanbevelingen

Nadat in de volgende fase beheersingsmaatregelen zijn bepaald, wordt deze fase herhaald ter beoordeling van de restrisico’s, net zolang tot het geheel aan maatregelen leidt tot acceptabele risiconiveaus.

Hulpmiddelen:

- Self-assessment (radar) - output van deze fase, een manier voor visualisatie van restrisico's
- Risicomatrix – output van deze fase voor risicoclassificatie

6.6 Risk Treatment

In deze fase worden de risicobeheersingsmaatregelen bepaald en geïmplementeerd. Typische taken binnen deze fase zijn:

- Definieer beheersmaatregelen en toetsing ervan (controls assurance)
- Implementeer beheersmaatregelen
- Implementeer toetsing van beheersmaatregelen
- Beoordeel de beheersmaatregelen baseline en werk bij
- Beoordeel de beheersmaatregelen toetsing baseline en werk bij
- Review aanwezige beheersmaatregelen
- De beheersmaatregelen dienen niet alleen het primair onderkende risico te adresseren, ook hun effectiviteit moet (idealiter) kunnen worden bepaald door toetsing ervan (controls assurance).

Hulpmiddel:

- Overzicht van maatregelen – input voor de in deze fase te bepalen risicobeheersingsmaatregelen

6.7 Risk Acceptance

Risk acceptance is de formele fase waarin wordt vastgesteld of de overblijvende risico's, na analyse en eventuele risicobehandeling, acceptabel zijn binnen de eerder vastgestelde risicotolerantie. Voor digitale soevereiniteit is dit een cruciaal besluitmoment, omdat het vaak gaat om afhankelijkheden die niet volledig kunnen worden weggenomen. Een organisatie kan bijvoorbeeld bewust blijven werken met een dominante cloudleverancier, een buitenlandse platformdienst, een leveranciersspecifieke technologie of een ketenafhankelijkheid, mits duidelijk is welke risico's daarmee samenhangen en waarom deze binnen de gekozen context acceptabel zijn.

Risicoacceptatie betekent niet dat een risico wordt genegeerd. Het betekent dat expliciet wordt vastgesteld:

- welk restrisico overblijft
- wie daarvoor verantwoordelijk is
- onder welke voorwaarden dit risico wordt geaccepteerd
- wanneer het opnieuw moet worden beoordeeld

Hiermee wordt voorkomen dat digitale-soevereiniteitsrisico's impliciet ontstaan of in projecten blijven hangen als onopgeloste aandachtspunten.

Voor digitaalkundige architecten is deze fase vooral van belang omdat zij de verbinding leggen tussen risicoanalyse, architectuurkeuzes en bestuurlijke besluitvorming. De architect maakt inzichtelijk welke afhankelijkheden en restrisico's voortkomen uit de gekozen architectuur, welke alternatieven of maatregelen beschikbaar zijn, en wat de consequenties zijn van accepteren, mitigeren, vermijden of delen van risico's.

Risk acceptance vormt als fase daarmee niet alleen het einde van een iteratie, maar ook het startpunt voor monitoring en herijking. Wanneer omstandigheden veranderen — bijvoorbeeld door gewijzigde wetgeving, geopolitieke ontwikkelingen, leveranciersbeleid, prijsstelling, technische afhankelijkheden of incidenten — kan een eerder geaccepteerd risico opnieuw buiten de risicotolerantie vallen. In dat geval moet de cyclus opnieuw worden doorlopen.

De formele acceptatie zelf ligt echter bij de daarvoor aangewezen risico-eigenaar, business eigenaar, directie of bestuurlijke opdrachtgever.

6.8 Doorlopende fasen: Communication and Consulting, Monitoring and Review

De hiervoor beschreven fasen vormen de kern van de risicobeheersingscyclus. Daarnaast kent ISO 27005 twee doorlopende activiteiten die voor digitale soevereiniteit van bijzonder belang zijn:

- *Communication and consulting*: gericht op de stakeholders voor continue betrokkenheid en besluitvorming en nodig omdat digitale soevereiniteit zelden uitsluitend binnen het mandaat van de architectuurfunctie valt.
- *Monitoring and review*: een bewakingsfunctie op alles wat in de overige fasen gebeurt zoals de effectiviteit van aanwezige beheersmaatregelen, het initiëren van onafhankelijke reviews/audits en op nieuwe ontwikkelingen die aanleiding geven tot een nieuwe risicobeheersingscyclus. Het is nodig omdat digitale-soevereiniteitsrisico's in de tijd veranderen. Afhankelijkheden kunnen toenemen door uitbreiding van platformdiensten, wijziging van leveranciersvoorwaarden of -strategie , geopolitieke verhoudingen kunnen verschuiven, wet- en regelgeving kan veranderen en nieuwe technologieën kunnen bestaande architectuurkeuzes onder druk zetten. Wat op het moment van besluitvorming

acceptabel is, kan daardoor later alsnog buiten de vastgestelde risicotolerantie vallen. Het moet daarmee onderdeel worden van reguliere architectuurreviews, risicomanagement, sourcingevaluaties, portfoliosturing en strategische herijking. Het richt zich daarom niet alleen op de vraag of afgesproken maatregelen zijn geïmplementeerd, maar ook op de vraag of zij nog voldoende effectief zijn.

Deze activiteiten zijn geen losse afsluitende stappen, maar lopen door het hele proces heen.

Zonder expliciete communicatie en consultatie bestaat het risico dat digitale soevereiniteit een technische analyse blijft, terwijl de feitelijke keuzes over risicotolerantie, prioriteiten, investeringen en acceptatie van restrisico's bestuurlijk moeten worden gemaakt. Het onderwerp moet daarmee onderdeel worden van reguliere architectuurreviews, risicomanagement, sourcingevaluaties, portfoliosturing en strategische herijking.

Typische taken in deze doorlopende fasen zijn:

- Het organiseren van afstemming met diverse relevante stakeholders.
- Opvolging van wijzigingen in leveranciers, contracten, technologie, jurisdicties, wetgeving en ketenrelaties.
- Periodiek toetsing of genomen beheersmaatregelen nog effectief zij en restrisico's nog binnen de vastgestelde risicotolerantie vallen.
- Vastlegging van besluiten, uitzonderingen en geaccepteerde restrisico's,

7 Hulpmiddelen voor de architect

7.1 Dreigingenbibliotheek

Een overzicht van potentiële dreigingen is opgenomen in bijlage 1 (werkblad praktische instrumenten), op het tabblad Dreigingen.

7.2 Model voor risicotolerantie

Een model voor het bepalen van de eigen risicohouding (risicotolerantie) voor digitale soevereiniteit is opgenomen in bijlage 1 (werkblad praktische instrumenten), op het tabblad Risicotolerantie.

7.3 Context Model

Een Context Model is een hulpmiddel waarmee op bestuurlijk niveau bewustzijn kan worden gecreëerd voor factoren in de buitenwereld die van belang kunnen zijn voor de organisatie. Door de relevante externe invloeden in de markt, politiek, wet- en regelgeving, vanuit de maatschappij, en op technologisch vlak gestructureerd te positioneren, ontstaat een helder beeld van hoe een organisatieonderdeel is van een groter ecosysteem. Digitaalkundige architecten kunnen dit gebruiken, om in één overzicht de omgeving, afhankelijkheden en beïnvloedende factoren rondom een systeem, dienst of domein in kaart te brengen. Het canvas helpt om de bredere context van een oplossing te begrijpen, voordat er keuzes worden gemaakt op het gebied van architectuur, technologie of soevereiniteit.

In het gebruik vormt het Context Model een hulpmiddel voor zowel analyse als communicatie: het creëert gedeeld begrip binnen teams en stakeholders, ondersteunt besluitvorming en legt een transparante basis voor vervolgstappen in het architectuurproces.

Het model maakt expliciet welke partijen invloed uitoefenen, welke afhankelijkheden en interacties bestaan en welke regels, verplichtingen en beperkingen van toepassing zijn. Hierdoor kunnen architecten vroegtijdig bepalen waar soevereiniteitsrisico's ontstaan, zoals geopolitieke afhankelijkheden, datalokaties, leveranciersrelaties of ketenrisico's. Het helpt bovendien om rollen en belangen scherp neer te zetten, zodat maatregelen voor digitale soevereiniteit in de juiste context worden ontworpen.

Een sjabloon voor een Context Model Canvas en een ingevuld voorbeeld zijn opgenomen in bijlage 2 (slides praktische instrumenten).

NB: op internet zijn meer sjablonen te vinden, ook onder de benamingen Context Map Canvas en Context Canvas.

7.4 Bedrijfsimpact Canvas

Een bedrijfsimpact canvas biedt een gestructureerde manier om digitale soevereiniteitsvraagstukken te analyseren door twee cruciale dimensies te combineren: de mate van afhankelijkheid van externe partijen en de potentiële risico impact. Door deze dimensies tegen elkaar uit te zetten, ontstaat een matrix waarin duidelijk wordt in welke waardestromen/kernprocessen bedrijfskritische afhankelijkheden bestaan.

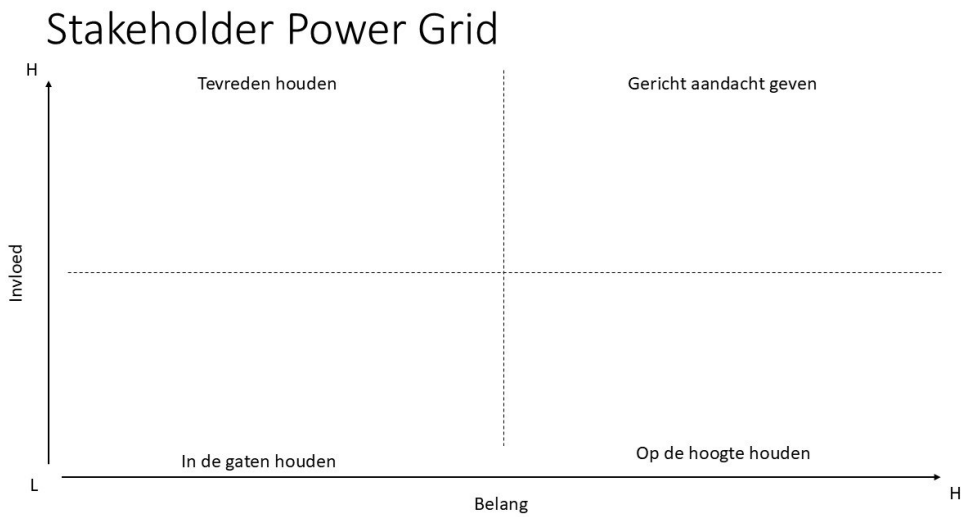
Een sjabloon voor een Bedrijfsimpact Canvas is opgenomen in bijlage 2 (slides praktische instrumenten).

7.5 Stakeholder power grid

Relevante stakeholders worden geïnventariseerd en geclassificeerd, inclusief hun belangen, verantwoordelijkheden en invloed.

Te gebruiken bij inrichting van governance en in (informeel) stakeholder management.

Een sjabloon en een voorbeeld voor een Stakeholder Power Grid zijn opgenomen in bijlage 2 (slides praktische instrumenten).



Figuur 2 - Stakeholder Power Grid

7.6 Dreigingsactoren

Het boek *Computer Security Handbook* van Seymour Bosworth & Michel Kabay bevat een voorbeeld van een classificatie van dreigingsactoren. Nadenken over wie exact de dreigingsactoren zijn, en wat hun beweegredenen zijn (of kunnen zijn) kan nuttig zijn bij eigen aanpassingen/aanvullingen in het eerdergenoemde overzicht van potentiële dreigingen.

De motivatietypen zijn opgenomen in bijlage 1 (werkblad praktische instrumenten), op het tabblad dreigingsactoren. Dit is uitbreidbaar met eigen of andere indelingen – er zijn bijvoorbeeld ook modellen die commercieel gewin en terrorisme (destructieve ideologie) als aanvullende motivatietypen benoemen.

7.7 Architectuur heatmap

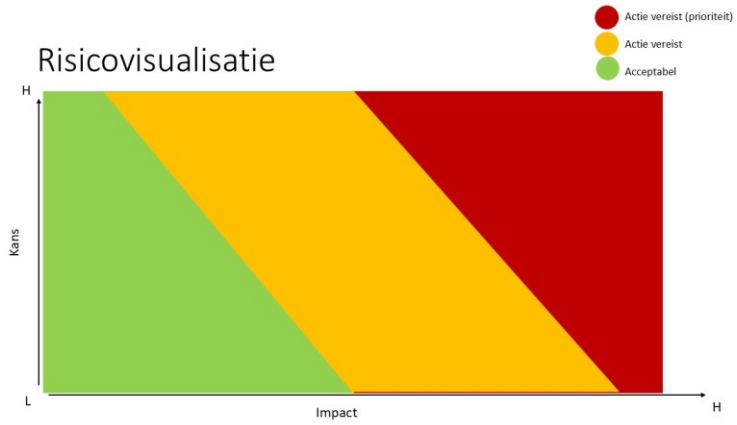
Als je een architectuurplaat hebt die breed herkend wordt, kun je die als heatmap gebruiken voor digitale soevereiniteit: plot de risico's (bijvoorbeeld met kleuren) of prioriteiten (met nummering) op deze plaat, en gebruik de plaat in de afstemming met/overtuiging van stakeholders.

Als basisplaten kunnen wellicht dienen: referentie-architectuur, capability model, bedrijfsfunctiemodel, proceslandschap, systeemlandschap.

7.8 Risicomatrix

Een risicomatrix lijkt een beetje op het bedrijfsimpact canvas, maar wordt veel gedetailleerder uitgewerkt. Deze stel je op door eerst alle relevante risico's te identificeren en vervolgens per risico twee dingen te bepalen: **de kans** dat het optreedt en **de impact** ervan op de organisatie. Deze lijst met risico's kun je als lijst managen. Daarnaast kun je hem ook visualiseren door elk risico te plotten in een diagram, of de aantallen risico's op te nemen in een matrix, meestal met kans op de verticale as en impact op de horizontale as.

Hoge kans én hoge impact risico's vragen directe actie, terwijl lage kans en lage impact risico's kunnen worden gemonitord. Op basis van deze ordening kun je besluiten welke risico's je accepteert en welke je zult moeten mitigeren. Door de eerder bepaalde risicotolerantie te vertalen naar concreet **wel** of **niet** te accepteren risicoscores, kun je concretiseren wat je wel accepteert (linksonder de diagonaal horend bij de gekozen risicotolerantie) en wat niet (rechtsboven de diagonaal).



Figuur 3 - Risico evaluatie matrix

7.9 Self-assessment ('radar')

Een self-assessment is een passend evaluatie-instrument om te beoordelen in hoeverre risicobeheersmaatregelen effectief zijn in de bestaande situatie, versus in hoeverre dat in de doelsituatie gewenst is.

Een voorbeeld van een self-assessment vragenlijst is opgenomen in bijlage 1 (werkblad praktische instrumenten), op het tabblad Self-assessment. Deze lijst dient beschouwd te worden als een eerste aanzet, die aansluit bij de risicocategorieën van het Cloud Sovereignty Framework van de EU, maar waarbij het DANW-model breder wordt toegepast dan alleen cloud.

In de praktijk kan een (methodische) uitbreiding met andere vragen noodzakelijk blijken. Het model zelf is opgezet met standaardfunctionaliteiten, dus door de digitaalkundige architect eenvoudig aanpasbaar.

7.10 Potentiële maatregelen

De waarde van een analyse van digitale soevereiniteit blijkt pas echt wanneer de uitkomsten worden vertaald naar concrete architectuurkeuzes en maatregelen. Zonder deze vertaalslag blijft het onderwerp hangen op het niveau van bewustwording en risicobeschrijving.

7.10.1 Maatregelcategorieën

Voor iedere organisatie zijn het vertrekpunt, de risico's en doelstellingen anders, daarom bevat deze whitepaper geen uitputtende lijst van maatregelen. Wel is in bijlage 1 (werkblad praktische instrumenten), tabblad maatregelen, een overzicht opgenomen met daarin:

- Mogelijke maatregelcategorieën
- Voorbeelden
- De verwachte effectiviteit van de maatregelen
- De soevereiniteitsdoelen waaraan ze kunnen bijdragen

Waar externe partijen betrokken zijn, is bij de maatregelen steeds verondersteld dat ze gevestigd zullen zijn in de eigen, relevante jurisdictie (Nederland, de EU, of de niet-EU landen die wel tot de EER behoren). Is dat niet het geval, dan dient de effectiviteit van maatregelen zelf beoordeeld te worden.

7.10.2 Maatregeleffectiviteit

Risicomethodieken hanteren normaliter een volgende maatregeltypering:

- Vermijden (ISO 27005: “Avoid”): voortzetting van de bestaande situatie wordt niet geaccepteerd, er wordt een nieuwe situatie gecreëerd;
- Verminderen (ISO 27005: “Modify”): voortzetting van de bestaande situatie wordt geaccepteerd met aanvullende maatregelen die het risico verkleinen;
- Verzekeren (ISO 27005: “Share”): voortzetting van de bestaande situatie wordt geaccepteerd waarbij de negatieve effecten worden verlegd naar buiten de eigen organisatie;
- Accepteren (ISO 27005: “Retain”): voortzetting van de bestaande situatie wordt geaccepteerd.

In bijlage 1 (werkblad praktische instrumenten), tabblad Maatregeleffectiviteit, is met bovenstaande maatregeltypering aangegeven hoe eventuele maatregelen bijdragen aan risicobeheersing. Het gaat hier om een inschatting van de werkgroep. “Accepteren” komt niet in het schema voor, aangezien we ervan uitgaan dat verbetering van de soevereiniteit het doel is.

Op het tabblad Maatregeleffectiviteit (kort) is een wat compacter overzicht opgenomen, waarbij we een geaggregeerde inschatting van het effectiviteitsniveau van een maatregelcategorie geven, per soevereiniteitsdoel.

8 Governance, rollen en verantwoordelijkheden

Digitale soevereiniteitsvraagstukken gaan typisch niet alleen over risicobeheersing en te nemen maatregelen binnen bestaande architectuur. Ze zijn bij uitstek een bestuurlijke en beleidsmatige verantwoordelijkheid, die in overeenstemming met de juiste governance genomen moet worden. Daarbij is ook bewustwording nodig: digitale soevereiniteit wordt vaak pas als vraagstuk herkend wanneer afhankelijkheden al diep in processen en technologie zijn verankerd.

Uit de voorgaande hoofdstukken is duidelijk, dat digitale soevereiniteit een vast onderdeel moet zijn van risk management en reguliere architectuurgovernance. De besluiten en richtlijnen die daaruit voortvloeien dienen ook hun plaats te krijgen in opvolgende processen, bijvoorbeeld in sourcing en portfoliobeslissingen. Als dat goed gebeurt, zijn geen afzonderlijke governance gremia of bestuurlijke besluitvormingsprocessen nodig. Dat vereist dan wel, dat het onderwerp vroegtijdig en integraal wordt meegenomen in ontwerp en besluitvorming. Daarnaast dient digitale soevereiniteit een beoordelingsaspect te zijn in de periodieke herijking van risico's, risicobereidheid en de fit/gap met de doelarchitectuur.

Goede governance op digitale soevereiniteit vereist, dat afhankelijkheden van leveranciers, platformen, data, ketenpartners en jurisdictie (wetgeving en overheden) zichtbaar, bespreekbaar en toetsbaar worden gemaakt. Dat voorkomt dat keuzes impliciet of ad hoc ontstaan en zorgt dat ze bewust en navolgbaar worden afgewogen. Want net als andere risicogebieden vraagt digitale soevereiniteit om periodieke toetsing, omdat er altijd sprake is van veranderende situaties – zowel intern als extern. Afhankelijkheden, risico’s en marktomstandigheden veranderen in de tijd. Wat vandaag acceptabel is, kan morgen onwenselijk blijken door geopolitieke ontwikkelingen, marktconcentratie, wijzigende regelgeving of technologische lock-in.

De volgende stakeholders spelen daarin een rol:

- De enterprise architect speelt een centrale rol in het verbinden van strategische doelstellingen, risicokaders en architectuurkeuzes.
- De security-architect en CISO dragen bij aan de beoordeling van dreigingen, beheersmaatregelen en restrisico’s.
- Business owners en proceseigenaren zijn nodig om classificaties en impact te bepalen.
- Privacy, juridische functies en inkoop stellen randvoorwaarden op het gebied van gegevensbescherming, contractering en leveranciersrelaties.
- Het bestuur en management zijn uiteindelijk verantwoordelijk voor expliciete acceptatie van restrisico’s en voor het maken van afgewogen keuzes wanneer belangen botsen.

9 Conclusies en aanbevelingen

Digitale soevereiniteit is geen modeterm en ook geen geïsoleerd beleidsconcept. Het is een fundamenteel vraagstuk over regie, afhankelijkheid en bestuurbaarheid in een steeds complexer digitaal landschap.

Deze whitepaper laat zien dat digitale soevereiniteit het best benaderd kan worden als een contextafhankelijk architectuurvraagstuk. Voor architecten betekent dit dat zij bij ontwerp en besluitvorming expliciet aandacht moeten besteden aan de mate waarin organisaties controle behouden over hun kritieke processen, data, technologie en ketenrelaties. Niet alles hoeft maximaal autonoom te worden ingericht, maar afhankelijkheden moeten wel expliciet worden gemaakt, beoordeeld en bestuurlijk gewogen. Een gestructureerde aanpak, ondersteund door een expliciet model voor risicotolerantie voor digitale soevereiniteit en praktische analysetools, helpt om die afweging transparanter en consistenter te maken.

De belangrijkste aanbeveling is om digitale soevereiniteit structureel te verankeren in architectuur, governance en risicosturing. Organisaties die daarin slagen, vergroten hun vermogen om bedrijfsdoelstellingen en autonomie in balans te brengen en om onderbouwde keuzes te maken in een complex en veranderlijk digitaal ecosysteem. Organisaties die dit nalaten, lopen het risico dat cruciale afhankelijkheden pas zichtbaar worden op het moment dat deze problematisch zijn geworden.

10 Gebruikte bronnen en inspiratiebronnen

Nr	Omschrijving
1	European Commission, Directorate-General for Digital Services. *Cloud Sovereignty Framework, Version 1.2.1 – October 2025*. European Commission, 2025.
2	European Commission - *European Interoperability Framework – Implementation Strategy COM 134 final,* 2017.
3	European Commission - *Open Source Software Strategy 2020–2023* , 2020.
4	European Commission, Joint Research Centre. *Open but Not Powerless: Towards a Common Understanding of EU Digital Sovereignty*. European Commission, 2025.
5	European Parliament Research Service - *Digital sovereignty for Europe*, 2020.
6	ENISA - *EUCS – Cloud Services Scheme* (draft candidate scheme), 2020.
7	European Union - *Regulation (EU) 2016/679* (General Data Protection Regulation), 2016.
8	European Union - *Directive (EU) 2022/2555* NIS2 Directive, 2022.
9	European Union - *Regulation (EU) 2022/2554* Digital Operational Resilience Act, DORA, 2022.
10	European Union - *Regulation (EU) 2024/1689* (Artificial Intelligence Act), 2024.
11	ISO - *ISO 31000:2018 – Risk management* — Guidelines, 2018
12	ISO/IEC. *ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. ISO, 2022.
13	The Open Group. *The TOGAF® Standard, 10th Edition*. The Open Group, 2022.
14	Bosworth, S., Kabay, M. E., & Whyne, E. (Eds.). *Computer Security Handbook* (6th ed.). Wiley.
15	The SABSA Institute – *SABSA® Executive Summary; business-driven, risk and opportunity focused security architecture methodology.*

11 Begrippenlijst

Afhankelijkheid

De situatie waarin een organisatie voor het realiseren, beheren of continueren van een digitale capability, dienst of waardestroom mede is aangewezen op een externe partij, technologie, ketenpartner, jurisdictie of voorziening.

Architectuurbesluit

Een besluit over de inrichting van processen, informatievoorziening, applicaties, technologie of governance dat structurele invloed heeft op beheersbaarheid, continuïteit, vervangbaarheid en digitale soevereiniteit.

Bedrijfskritische waardestroom

Een waardestroom, proces of dienstverlening waarvan verstoring onaanvaardbare gevolgen heeft voor de primaire taakuitvoering, publieke waarden, wettelijke verplichtingen, veiligheid, continuïteit of reputatie van de organisatie.

Cloud-soevereiniteit

De mate waarin cloudvoorzieningen kunnen worden ingezet zonder ongewenste juridische, operationele, technische of geopolitieke afhankelijkheden, en met behoud van aantoonbare regie over data, toegang, continuïteit en vervangbaarheid.

Contextanalyse

De gestructureerde analyse van externe en interne factoren die relevant zijn voor een soevereiniteitsvraagstuk, zoals stakeholders, ketenrelaties, jurisdicties, marktomstandigheden, wet- en regelgeving, maatschappelijke factoren en technologische ontwikkelingen.

Cybersoevereiniteit

Beschermen en controleren van de virtuele ruimte van computernetwerken binnen (lands)grenzen inclusief (cyber) security maatregelen en internet governance.

Datasoevereiniteit

De mate waarin een organisatie zeggenschap en feitelijke regie houdt over haar data, inclusief opslag, verwerking, toegang, gebruik, overdraagbaarheid en verwijdering.

Digitale autonomie

Het vermogen van een organisatie om in het digitale domein zelfstandig keuzes te maken en zelf uitvoering ter hand te nemen om afhankelijkheden te verminderen wat betreft inrichting, gebruik, wijziging en vervanging van digitale middelen en om controle te houden over de verwerking, opslag en toegang tot de eigen data.

Digitale soevereiniteit

Het vermogen van een organisatie om juridische, bestuurlijke en operationele regie te behouden over haar digitale middelen, data, processen en afhankelijkheden, zodanig dat zij haar strategische, maatschappelijke of operationele doelstellingen kan blijven realiseren binnen aanvaardbare grenzen van risico en afhankelijkheid. Het gaat daarbij niet om volledige onafhankelijkheid, maar om

aantoonbare beheersing van kritieke afhankelijkheden en het vermogen om verantwoorde keuzes te maken.

Digitale soevereiniteitsrisico

Het risico dat een organisatie door afhankelijkheden, technische keuzes, leveranciersmacht, geopolitieke ontwikkelingen, ongunstige jurisdictie, gebrek aan vervangbaarheid of verlies van zeggenschap haar doelstellingen niet meer binnen aanvaardbare grenzen kan realiseren.

Governance

Governance is de handeling of de wijze van besturen, de gedragscode en het toezicht op organisaties. In het geval van een onderneming of een non-profitorganisatie wordt governance gerelateerd aan consistent management, samenhangend beleid, processen en beslissingsrechten voor een bepaalde bevoegdheid.

In de context van digitale soevereiniteit is de betekenis van governance: het samenstel van sturing, besluitvorming, verantwoordelijkheden en toetsing waarmee een organisatie digitale afhankelijkheden en keuzes rond soevereiniteit expliciet, aantoonbaar beheerst en periodiek herijkt.

Interoperabiliteit

Het vermogen van systemen, diensten en organisaties om op basis van open of breed toepasbare afspraken gegevens en functionaliteit uit te wisselen en samen te werken zonder onnodige afhankelijkheid van één leverancier of gesloten ecosysteem.

Juridische afhankelijkheid

De afhankelijkheid die ontstaat doordat dienstverlening, data of operationele controle mede onderworpen is aan wet- en regelgeving, rechtspraak of overheidsingrijpen buiten de gewenste of veronderstelde jurisdictie.

Kritieke afhankelijkheid

Een afhankelijkheid waarvan verstoring, wijziging of beëindiging leidt tot onaanvaardbare impact op bedrijfskritische processen, continuïteit, bestuurlijke controle, compliance, veiligheid of maatschappelijke taakuitvoering.

Lock-in

De situatie waarin een organisatie feitelijk niet of slechts tegen disproportionele kosten, tijd, risico of complexiteit kan overstappen naar een alternatief. Lock-in kan technisch, contractueel, operationeel, financieel, organisatorisch of juridisch van aard zijn.

Mitigerende maatregel

Een architectonische, technische, contractuele, organisatorische of bestuurlijke maatregel die de kans op of impact van een soevereiniteitsrisico verlaagt, of de afhankelijkheid beter beheersbaar maakt.

Open standaard

Een publiek beschikbare, breed toepasbare en niet onnodig beperkende afspraak voor gegevensuitwisseling, protocollen, interfaces of modellen, die interoperabiliteit, overdraagbaarheid en vervangbaarheid ondersteunt.

Regie

Het vermogen van een organisatie om richting te geven aan digitale keuzes, voorwaarden te stellen, risico's af te wegen, maatregelen af te dwingen en zo aantoonbaar controle te houden over afhankelijkheden en uitkomsten.

Restrisico

Het risico dat overblijft nadat bestaande of aanvullende maatregelen zijn getroffen. Restrisico's vragen expliciete acceptatie, aanvullende mitigatie of bestuurlijke escalatie wanneer zij buiten de vastgestelde risicobereidheid vallen.

(Soevereiniteits-) Risicotolerantie

Ook te omschrijven als risicohouding voor soevereiniteit.

De expliciet vastgestelde mate van risico en afhankelijkheid die een organisatie, voor een bepaalde context of waardestroom, bereid is te accepteren. Dit vormt het toetsingskader voor architectuurbesluiten, uitzonderingen en prioritering van maatregelen.

Sourcing

De wijze waarop een organisatie digitale capabilities, diensten of middelen verwerft, organiseert en aanstuurt, bijvoorbeeld via eigen uitvoering, uitbesteding, gezamenlijke inkoop, cloudafname of platformgebruik. Sourcing keuzes hebben direct effect op afhankelijkheid en soevereiniteit.

Technologische autonomie

De bredere mate waarin een organisatie of samenleving zelfstandig kan beschikken over essentiële digitale capaciteiten, kennis, middelen en alternatieven.

Toetsbaarheid

De mate waarin keuzes over digitale afhankelijkheden, architectuur en maatregelen expliciet, navolgbaar, herhaalbaar en controleerbaar zijn voor architectuurgovernance, management, audit en toezicht.

Vervangbaarheid

De mate waarin een organisatie in staat is een leverancier, platform, dienst of technologie gecontroleerd te verlaten, inclusief de praktische uitvoerbaarheid daarvan in termen van data-export, migratie, overdracht van kennis, configuraties, contracten en beheer. Vervangbaarheid is een voorwaarde om lock-in te beperken.

Waardestroom

De samenhangende reeks activiteiten, voorzieningen, data en actoren waarmee een organisatie waarde levert aan een interne of externe afnemer.

Opmerking: In deze whitepaper is de waardestroom een logische scope-eenheid voor analyse van kritiekheid, afhankelijkheden en risicotolerantie.

12 Bijbehorende hulpmiddelen

Bij deze whitepaper horen de volgende hulpmiddelen:

- Werkblad praktische instrumenten
- Slides praktische instrumenten
- Context Model Canvas
- Bedrijfsimpact Canvas
- Risicotolerantiemodel
- Self-assessment/radar