Digitale Soevereiniteit

Een QA Consulting Framework

Bestuurders in de publieke sector staan voor een belangrijke opgave: grip herwinnen op de digitale infrastructuur waarop onze samenleving draait. Niet door zich af te sluiten van innovatie, maar door bewust te kiezen voor autonomie. Het Soevereiniteitskader biedt daarvoor een concrete en meerlagige benadering.

Iris Haaijer

iris@qaconsulting.nl

Waarom dit nu een bestuurlijk vraagstuk is

De combinatie van geopolitieke spanningen, een verslechterende relatie tussen de EU en de VS en een concentratie van kritieke overheidssystemen bij een handvol buitenlandse leveranciers maakt de publieke sector zichtbaar kwetsbaar. Digitale soevereiniteit is geen theoretisch vraagstuk meer. Het is een acute bestuurlijke noodzaak geworden.

Geopolitieke Spanningen

Verslechterende EU-VS relaties verhogen de risico's van afhankelijkheid van buitenlandse technologiepartijen.

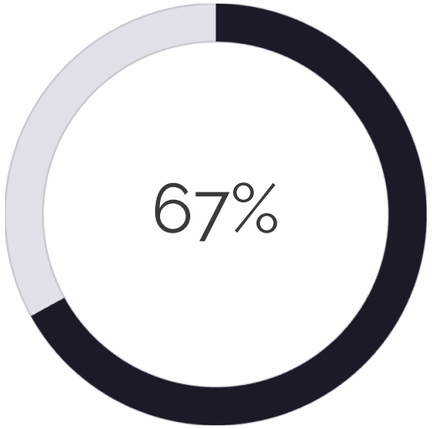
Leveranciersconcentratie

Kritieke overheidssystemen zijn geconcentreerd bij een handvol buitenlandse aanbieders.

Bestuurlijke Urgentie

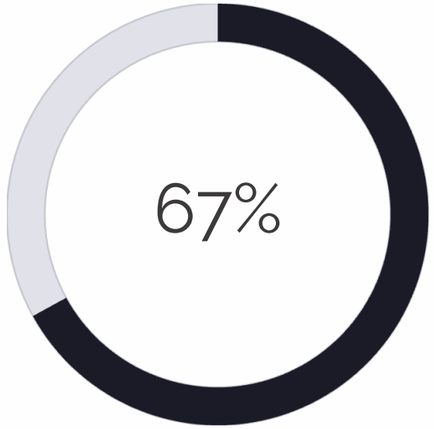
Wat eerder een IT-vraag was, is nu een strategisch bestuursthema dat raakt aan nationale weerbaarheid.

De Feiten: Een Ontnuchterend Beeld



Marktconcentratie

Van de materiële public clouddiensten bij het Rijk wordt ingekocht bij drie grote Amerikaanse bedrijven: Amazon, Microsoft en Google.



Zonder risicoafweging

Van de diensten die onder de primaire taak van organisaties vallen, heeft voorafgaand geen risicoafweging plaatsgevonden.

Drie fundamentele principes onder druk

Digitale Soevereiniteit
Wie heeft controle over onze data?

Continuïteit van Dienstverlening
Kunnen we blijven functioneren bij verstoring?

Gegevensbescherming
Zijn gegevens van burgers voldoende beschermd?

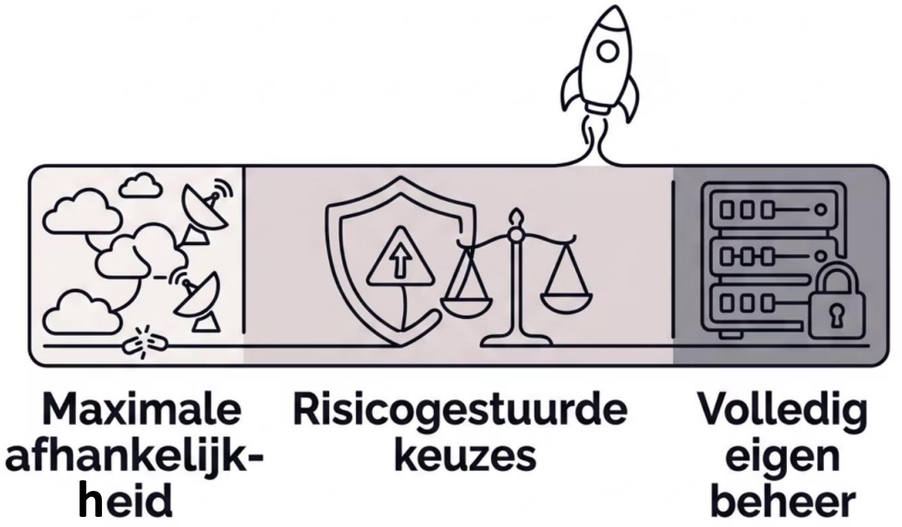
⚠ De Amerikaanse CLOUD Act geeft Amerikaanse autoriteiten vergaande bevoegdheden om toegang te krijgen tot data van Europese burgers — ook wanneer die data fysiek in Europa is opgeslagen.

> "Het gaat er niet om alles zelf doen, maar dat we zélf kunnen kiezen en controle houden." — Staatssecretaris Van Marum, december 2025

Wat betekent Digitale Soevereiniteit?

Digitale soevereiniteit is het vermogen om autonoom te kunnen beslissen en handelen over de essentiële digitale aspecten van onze economie, maatschappij en democratie. Het gaat om het bewust inrichten en gebruiken van digitale systemen en de daarmee gegenereerde en opgeslagen data, inclusief de gerelateerde werkprocessen.

Het is nadrukkelijk **geen streven naar volledige digitale onafhankelijkheid**. Dat is in de moderne, onderling verbonden technologiewereld niet haalbaar en ook niet wenselijk. Maar binnen mondiale afhankelijkheden zijn keuzes mogelijk die publieke waarden als privacy, veiligheid en democratie beschermen.



In de praktijk wordt digitale soevereiniteit vaak teruggebracht tot de vraag: *'Waar staat mijn data?'* Dat is een te beperkte weergave van de kwestie.

Soevereiniteit is geen binaire keuze, maar een spectrum. Binnen dit spectrum moeten bewuste, risicogestuurde keuzes gemaakt worden, afhankelijk van het doel, het risicoprofiel en de sectorspecifieke vereisten.

Het Soevereiniteitsframework: Vijf versterkende pijlers

Het soevereiniteitsframework benadert soevereiniteit niet als één maatregel, maar als een samenspel van vijf versterkende pijlers. Elke pijler richt zich op een specifieke dimensie van controle. Samen vormen ze een duurzame basis voor een strategie voor digitale autonomie.

Juridische Waarborgen

Wettelijke en contractuele basis voor soevereiniteit

Technische Waarborgen

Technische inrichting voor daadwerkelijke controle

Organisatorische Waarborgen

Borging in dagelijkse besturing en besluitvorming

Continuïteit & Exit

Publieke taak uitvoeren ook onder druk

Cyberweerbaarheid

Verbinding met bredere digitale weerbaarheid

Pijler 1: Juridische Waarborgen

De eerste pijler legt de wettelijke en contractuele basis voor soevereiniteit: voldoen aan EU-wet- en regelgeving (zoals DORA, NIS2, GDPR), en actieve bescherming tegen de extraterritoriale werking van buitenlandse wetten zoals de CLOUD Act.

Contractuele verankering

Data-eigendom, auditrechten en ketentransparantie voor alle leveranciers vastleggen in contracten.

Data-locatie & Jurisdictie

Clausules over data-locatie, jurisdictie en beperkingen op doorgifte buiten de EU opnemen.

Exit & Escrow

Standaard exitbepalingen en escrowregelingen bij kritieke en vitale diensten verplicht stellen.

Soevereine Aanbesteding

Aanbestedingen bewust toetsen aan soevereiniteitsprincipes, inclusief eisen rond EU-jurisdictie en open standaarden.

Het rapport *Van Kwetsbaar naar Weerbaar* (2025) en de Algemene Rekenkamer pleiten beide voor het verplicht stellen van modelclausules voor data-eigendom, escrow, step-in rechten en migratie afspraken in alle contracten rond vitale diensten. **Juridische zekerheid is geen sluitpost, maar de eerste verdedigingslinie.**

Pijler 2: Technische Waarborgen

De tweede pijler richt zich op de technische inrichting van de digitale omgeving. Hier gaat het om maatregelen die organisaties in staat stellen om daadwerkelijk controle uit te oefenen, onafhankelijk van het gedrag van leveranciers.

Encryptie & Sleutelbeheer

Data versleuteld met eigen sleutels is voor leveranciers onleesbaar, zelfs bij een juridisch verzoek.

Netwerk-isolatie

Strikte scheiding tussen gevoelige en minder gevoelige systemen vermindert het aanvalsoppervlak.

Infrastructure-as-Code

Configureerbare en reproduceerbare infrastructuur die niet afhankelijk is van één specifiek platform.

Open Standaarden

Architectuur en open dataformaten die portabiliteit en interoperabiliteit garanderen.

Nieuwe systemen moeten worden ontworpen op basis van **resilience by design** en cloudagnostische principes: een heldere scheiding tussen data, applicaties en infrastructuur. De portabiliteitstoets hoort een standaard onderdeel te zijn van elk architectuurbesluit.

Pijler 3: Organisatorische Waarborgen

De derde pijler borgt soevereiniteit niet alleen in beleidsdocumenten, maar ook in de dagelijkse besturing en besluitvorming van de organisatie. Technische en juridische maatregelen falen immers als mensen en processen niet meebewegen.

Nederlandse Integratiepartner

Een intermediair die de kennis en regie bij de eigen organisatie houdt, in plaats van die volledig bij de leverancier te laten.

Segregation of Duties

Functiescheiding tussen beheer, inkoop, juridisch en audit om ongewenste machtsconcentraties te voorkomen.

Duidelijke Rolverdeling

Expliciete eigenaarschappen voor soevereiniteitsvraagstukken bij bestuurders, CIO/CDO, CISO en lijnmanagers.

Security & Privacy Board

Een overlegorgaan dat de soevereiniteitsagenda op strategisch niveau bewaakt en de balans zoekt tussen innovatie en controle.

Digitale soevereiniteit vraagt expliciete bestuurlijke keuzes: wat wil je in eigen hand houden, waar accepteer je afhankelijkheid, en onder welke voorwaarden? Sleutelrollen in inkoop, juridisch, architectuur, security en business moeten vendor lock-in en jurisdictierisico's herkennen en mitigeren.

Pijler 4: Continuïteit & Exit

De vierde pijler waarborgt dat de organisatie ook onder druk — bij een verstoring, een leveranciersfaillissement, geopolitieke escalatie of een cyberaanval — haar publieke taak kan blijven uitvoeren.

Escrowregelingen

Voor kritieke applicaties en data, zodat broncode en gegevens altijd toegankelijk blijven.

Europees IP-eigendom

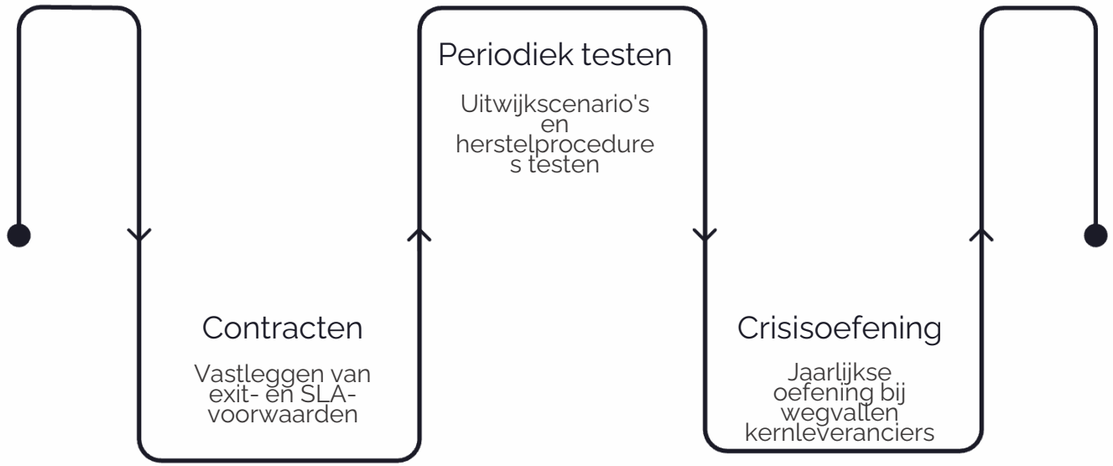
Bescherming bij een mogelijke overname van een leverancier door een niet-Europese partij.

Exit-bepalingen

Het recht om te migreren, inclusief actieve ondersteuning van de leverancier bij de overdracht.

Knowledge Transfer

Als contractuele verplichting, zodat kritieke kennis niet volledig bij externe partijen blijft berusten.



⚠ Continuïteitsmaatregelen moeten periodiek worden getest door uitwijkscenario's en herstelprocedures daadwerkelijk uit te voeren.

Pijler 5: Cyberweerbaarheid

De vijfde pijler verbindt digitale soevereiniteit met bredere digitale weerbaarheid. Soevereiniteit zonder adequate verdediging is kwetsbaar; cyberweerbaarheid zonder soevereiniteitsdenken is onvolledig.

1

Defense-in-depth

Gelaagde verdediging waarbij het falen van één beveiligingsmaatregel niet direct leidt tot een totale compromittering.

2

Compliance BIO2, NIS2 & GDPR

Het naleven van de geldende kaders als minimum, niet als maximum.

3

Dreigingsbescherming

Specifieke bescherming tegen ransomware, DDoS en insider threats die overheidsorganisaties disproportioneel hard treffen.

4

Incidentprotocol

Duidelijke procedures voor detectie, respons en herstel, inclusief communicatie richting burgers en partners.

Overheidsorganisaties doen er goed aan de Europese kaders NIS2 en DORA niet als externe verplichting te zien, maar als **codificatie van wat robuust bestuur moet vereisen**. De NIS2-richtlijn breidt verplichtingen voor cybersecurity substantieel uit naar alle organisaties die essentieel zijn voor het functioneren van de samenleving.

Governance als bindend element

Het soevereiniteitsframework staat of valt met alle vijf pijlers. Soevereiniteit is geen IT-dossier dat de CIO kan afhandelen — het is een **bestuursvraagstuk**. Governance op drie niveaus is daarvoor essentieel.

Strategisch

Twee keer per jaar — het bestuur bespreekt soevereiniteitsambities, stelt kaders vast en monitort KPI's: percentage systemen onder EU-jurisdictie, portabiliteitsgraad en gemiddelde hersteltijd bij uitval.

Tactisch

Maandelijks — de CIO/CDO, CISO en inkoopfunctie bewaken actief de naleving van het vastgestelde beleid en signaleren afwijkingen.

Operationeel

Dagelijks/wekelijks — teams voeren concrete maatregelen uit: van encryptieconfiguratie tot contractbeheer en leveranciersmonitoring.

Visie Digitale Autonomie (december 2025)

De Nederlandse overheid erkent de governance-noodzaak. Instrumenten: aanscherpen van cloudbeleid, bundelen van IT-inkoop, stimuleren van open standaarden en investeren in digitaal vakmanschap.

Agenda DOSA

De Agenda Digitale Open Strategische Autonomie biedt het bredere beleidskader:

> *"Open waar het kan, beschermend waar dat moet."*

Van analyse naar actie

Digitale soevereiniteit is geen eindpunt, maar een richting. Het soevereiniteitsframework helpt bestuurders om te bepalen welke kant hun organisatie op moet, en stap voor stap te operationaliseren. Een effectieve aanpak begint met een classificatie van het IT-landschap: welke processen en data zijn werkelijk kritiek en vitaal?

Op basis van die classificatie kunnen de vijf pijlers worden ingezet als checklist en als afwegingskader. De vragen die op bestuurlijk niveau leidend zijn:

Per pijler wordt voor elk van de vier besturingselementen (Management & Organisatie, Mens & Cultuur, Processen & Procedures en Tools & Technologie) vastgesteld of de randvoorwaarden daadwerkelijk zijn ingericht. Zo ontstaat een vertaling van de huidige staat en een gerichte agenda voor verandering. **Echte soevereiniteit ontstaat in zekerheid, ongeacht de onderliggende technologie.**

1 Juridisch

Kiezen wij bewust voor een juridisch verdedigbare mate van afhankelijkheid, of laten we een afhankelijkheidspositie feitelijk door leveranciers en buitenlandse wetgeving opleggen?

2 Technisch

Is onze digitale architectuur zo ontworpen dat we binnen een redelijke termijn en tegen aanvaardbare kosten kunnen migreren als geopolitiek, wetgeving of leveranciersbeleid daar aanleiding toe geven?

3 Organisatorisch

Is soevereiniteit expliciet belegd in bestuurlijke portefeuilles, KPI's en besluitvormingskaders, en hebben sleutelrollen de benodigde kennis?

4 Continuïteit

Kunnen wij, als morgen een grote cloudleverancier uitvalt of politiek wordt afgeschakeld, onze kerndienstverlening zichtbaar en verantwoord voortzetten?

5 Cyberweerbaarheid

Hebben wij als bestuur voldoende inzicht en invloed om aannemelijk te maken dat onze digitale weerbaarheid op minimaal NIS2-niveau is, en durven we daarop persoonlijk aangesproken te worden?