

Als het erop aankomt

Digitale autonomie als bestuurlijke
opdracht in een wereld van
afhankelijkheden



Inhoud

Executive Summary	3
Leven onder de zeespiegel	5
Wanneer afhankelijkheid zichtbaar wordt	7
Van IT-keuze naar bestuurlijke verantwoordelijkheid	9
Het ongemerkt verdwijnen van regie	12
Handelings-perspectief	14
Van impliciet gegroeid naar expliciet ontworpen	17
Als het erop aankomt, wat kost niets doen?	20
Tot slot: Hoe pakt u dit vandaag aan?	22
Over KPN	25

Executive Summary

Digitale autonomie als bestuurlijke verantwoordelijkheid

Digitale infrastructuur is geen ondersteunende functie meer. Zij vormt het fundament onder primaire processen, publieke dienstverlening en maatschappelijke continuïteit. Cloud, data en platformen bepalen vandaag direct de wendbaarheid, betrouwbaarheid en strategische positie van organisaties.

In een geglobaliseerde digitale keten is afhankelijkheid onvermijdelijk. Hyperscalers domineren de markt. SaaS-oplossingen stapelen zich op. Data beweegt over jurisdicties heen. Dit is geen moreel oordeel, maar een feitelijke realiteit. De bestuurlijke vraag is daarom niet of afhankelijkheid bestaat, maar of zij expliciet is ontworpen en beheersbaar is wanneer omstandigheden veranderen.

Zolang systemen functioneren, lijkt afhankelijkheid beheersbaar. De ware toets ligt echter in uitzonderlijke situaties: geopolitieke verschuivingen, aangescherpt toezicht, concentratierisico's, overnames, langdurige verstoringen. Op zulke momenten verschuift het gesprek van technologie naar verantwoordelijkheid. Dan wordt zichtbaar of keuzes expliciet zijn gewogen of organisch zijn gegroeid.

Digitale autonomie betekent niet onafhankelijkheid van de wereld. Het betekent het vermogen om binnen afhankelijkheid bestuurbaar te blijven. Dat vraagt om expliciete differentiatie: innovatie waar het kan, aanvullende governance waar dat nodig is en maximale autonomie waar afhankelijkheid niet uitlegbaar is. Het cloudcontinuüm biedt hiervoor een bestuurlijke keuzeruimte.





Investeren in digitale autonomie vraagt middelen. Het vergt inzicht in afhankelijkheden, herijking van cloudportfolio's, governance-versterking en contractuele borging van omkeerbaarheid. Deze kosten zijn planbaar en gefaseerd. De kosten van niets doen materialiseren daarentegen onder druk: herstellkosten, reputatieschade, compliance-risico's en gedwongen keuzes met beperkte onderhandelingsruimte.

Digitale autonomie is daarom geen IT-project, maar een governance vraagstuk. Het vraagt van bestuur en toezicht:

- het expliciet vaststellen van risicobereidheid en afhankelijkheidsprincipes;
- het ontwerpen van een samenhangend cloudportfolio binnen het continuüm;
- het borgen van autonomie in reguliere governance;
- en het bewust accepteren of mitigeren van resterende risico's.

Zoals Nederland onder de zeespiegel veilig is dankzij ontworpen bescherming, zo vraagt digitale infrastructuur om ontworpen afhankelijkheid. De kernvraag voor bestuurders luidt dan ook niet: gebruiken wij cloud?

Maar: kunnen wij aantonen dat wij de regie hebben, als het erop aankomt?

Leven onder de zeespiegel

Wie Nederland wil begrijpen, moet beginnen bij iets dat we zelden hardop zeggen: wij zijn een land dat in permanente onderhandeling leeft met de natuur. Wij leven niet ondanks kwetsbaarheid, maar dankzij het feit dat we haar serieus nemen. Onder de zeespiegel wonen is geen metafoor, het is een bestuurlijke realiteit. Je kunt het water niet wegstemmen. Je kunt het niet negeren. Je kunt hooguit besluiten hoe je ermee omgaat.

Wat ons land door de eeuwen heen sterk heeft gemaakt, is niet het bouwen van één grote dijk, maar het ontwikkelen van een bestuurscultuur waarin risico tastbaar wordt gemaakt. We rekenen scenario's door die we liever nooit meemaken. We investeren in bescherming die pas zichtbaar wordt als hij faalt. We organiseren verantwoordelijkheid zó dat niemand zich kan verschuilen achter "het is technisch" wanneer het misgaat. Waterveiligheid is geen project met een einddatum. Het is een doorlopende discipline van ontwerp, onderhoud, toetsing en herijking.

Digitale infrastructuur bevindt zich vandaag in precies diezelfde fase. Cloud, data, netwerken en platformen zijn niet langer ondersteunend; ze zijn dragend. Ze zijn de fundering waarop organisaties draaien: het betalingsverkeer, het patiëntendossier, de vergunningenketen, de logistieke planning, de klantinteractie, de productieaansturing, de fraudedetectie. Op papier kun je het "IT" noemen, maar in de praktijk is het de ruggengraat van de organisatie.



En net als water is het grensoverschrijdend. Het stroomt door ketens van leveranciers, jurisdicties, contracten, hardware, software-updates, menselijke toegang, supportprocessen en geopolitieke realiteiten. Dat maakt het krachtig, maar ook potentieel ontwrichtend. Niet omdat iemand 'fout' kiest, maar omdat complexiteit groeit terwijl overzicht verdampst.

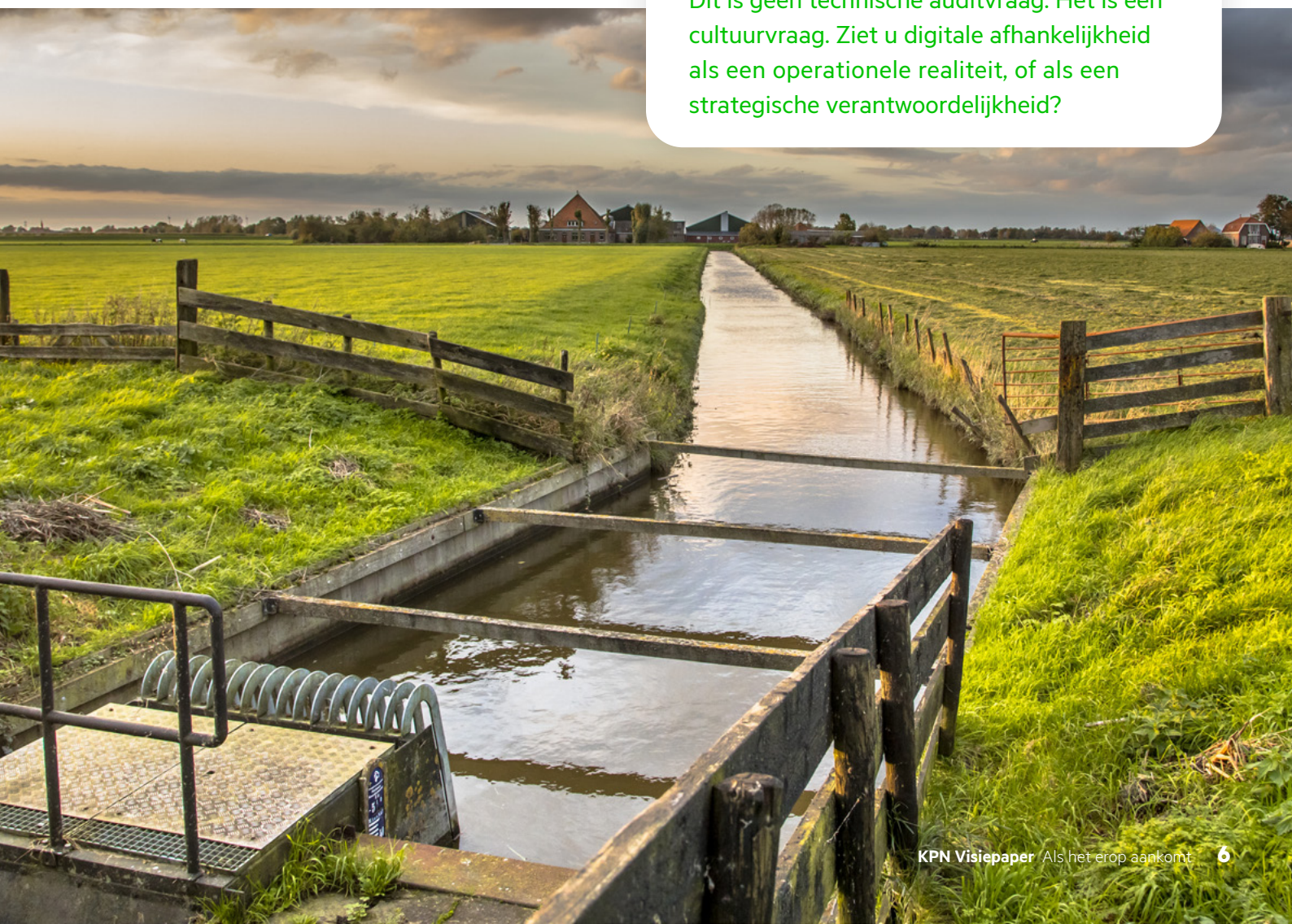
Daarom is de centrale vraag geen technologie-vraag. Het is een bestuursvraag, van dezelfde orde als waterveiligheid altijd is geweest: niet "hebben we water?", maar "hebben we het bestuurlijk in de hand?". Niet "gebruiken we cloud?", maar "is onze afhankelijkheid ontworpen, verantwoord en beheersbaar?". Wie onder de zeespiegel leeft, kan zich geen illusies permitteren. Wie op digitale infrastructuur draait, evenmin.

Bestuurlijke reflectie

Wat betekent "leven onder de zeespiegel" voor u?

Wanneer we de metafoor van waterveiligheid serieus nemen, dwingt dat tot zelfreflectie. In welke mate hebben wij digitale afhankelijkheid behandeld als een strategisch vraagstuk? Hebben wij scenario's doorgerekend die zich mogelijk nooit voordoen, maar waarvan de impact existentieel kan zijn? Of vertrouwen wij impliciet op de stabiliteit van leveranciers en markten? Waterveiligheid is in Nederland nooit afhankelijk geweest van goed vertrouwen alleen. Zij is gebaseerd op ontwerp, toetsing en periodieke versterking. De vraag is of onze digitale infrastructuur dezelfde mate van bestuurlijke aandacht krijgt als onze fysieke infrastructuur.

Dit is geen technische auditvraag. Het is een cultuurvraag. Ziet u digitale afhankelijkheid als een operationele realiteit, of als een strategische verantwoordelijkheid?



Wanneer afhankelijkheid zichtbaar wordt

Afhankelijkheid is zelden het onderwerp van gesprek op een rustige dag. Een dijk die zijn werk doet, is onzichtbaar.

Een rivier die binnen haar oevers blijft, levert geen headlines op. Dat is precies waarom afhankelijkheid gevaarlijk kan worden: niet omdat zij bestaat, maar omdat zij pas voelbaar wordt wanneer de omstandigheden kantelen.

Digitale afhankelijkheid werkt precies zo. Zolang systemen beschikbaar zijn, leveranciers leveren en contracten stilzwijgend doorlopen, voelt cloud als vanzelfsprekend. Het is efficiënt, flexibel, schaalbaar. Teams bewegen sneller. Innovatie komt dichterbij. De voordelen zijn concreet en dagelijks merkbaar.

Maar stel je een maandagochtend voor waarop iets wél schuift. Niet per se “een hack” of “een ramp”, maar een samenloop van omstandigheden die ineens bestuurlijk gewicht krijgt. Een toezichthouder vraagt door: onder welke jurisdictie valt dit kernproces? Wie kan erbij? Hoe toon je dat aan? Tegelijkertijd verandert er iets in de markt: een leverancier wordt overgenomen, een productlijn wordt aangepast, voorwaarden verschuiven. Ondertussen duiken er in het nieuws geopolitieke spanningen op die niets met jouw organisatie lijken te maken totdat je beseft dat jouw digitale keten daar wél mee verweven is.

In zo’n situatie verschuift het perspectief abrupt. Wat gisteren een operationele keuze leek, wordt vandaag een governancevraag.

Niet: “werkt het?”, maar: “kunnen we uitleggen waarom we het zo hebben ingericht?”

Niet: “hoe snel lossen we dit op?”, maar: “waarom hebben we zó weinig handelingsruimte?”

Dit is de essentie van de bestuurlijke toets die in jouw organisatie centraal staat: afhankelijkheid is geen probleem zolang zij binnen beheersbare kaders valt. Het probleem ontstaat wanneer de organisatie bij druk ontdekt dat die kaders nooit expliciet zijn ontworpen.

Waterveiligheid leert dat het echte oordeel niet valt bij normaal gebruik, maar bij uitzonderlijke omstandigheden. Digitale autonomie werkt identiek. Bestuurlijke rust ontstaat niet door te hopen dat het rustig blijft, maar door te ontwerpen voor het moment dat het niet rustig is.

Praktijkvoorbeeld: afhankelijkheid onder druk

Een denkbeeldige, maar herkenbare situatie

Een middelgrote publieke organisatie heeft de afgelopen jaren haar applicatielandschap grotendeels gemigreerd naar een internationale hyperscaler. De businesscase was overtuigend: schaalbaarheid, lagere CAPEX, toegang tot geavanceerde analytics. Er waren geen incidenten. Alles werkte.

Totdat een combinatie van nieuwe Europese regelgeving en geopolitieke spanning vragen oproept over datatoegang en jurisdictie. De toezichthouder vraagt: kunt u aantonen wie toegang heeft tot uw data, onder welke wettelijke regimes deze valt en hoe u handelt wanneer toegang wordt beperkt?

Technisch is het antwoord genuanceerd. Contractueel zijn er clausules. Operationeel is er vertrouwen. Maar bestuurlijk ontbreekt een expliciete afweging. De afhankelijkheid is gegroeid, maar nooit formeel gewogen.

Wat hier zichtbaar wordt, is niet falende technologie, maar het ontbreken van expliciet ontwerp.



Van IT-keuze naar bestuurlijke verantwoordelijkheid

Er was een tijd waarin cloud vooral werd besproken in termen van efficiëntie: minder datacenters, minder beheer, sneller innoveren. Dat gesprek paste bij een tijdperk waarin digitale systemen nog vooral ondersteunend waren. Het was logisch dat CIO's, IT-architecten en inkoopteams de beslissingen namen. Bestuurders keken naar businesscases, SLA's en kostenbesparingen en vertrouwden erop dat "IT het regelt".

Dat tijdperk ligt achter ons, maar veel organisaties gedragen zich nog alsof het nog bestaat.

Vandaag is digitale infrastructuur direct verbonden met continuïteit, maatschappelijke impact en vertrouwen. Als een zorginstelling niet kan plannen, is dat geen IT-issue maar zorgcontinuïteit. Als een gemeente niet kan uitkeren, is dat geen platformissue maar publieke dienstverlening. Als een bank niet kan verwerken, is dat geen storing maar financieel vertrouwen. De digitale laag is niet langer "een deel" van de organisatie. Het is de organisatie.

Daarom verandert ook de maatschappelijke verwachting. Wanneer het misgaat, wordt niet gevraagd welke architectuurkeuze ooit is gemaakt; men vraagt of het bestuur de regie had. Wanneer data onder druk komt te staan, vraagt men niet naar "de leverancier"; men vraagt of de organisatie haar verantwoordelijkheid heeft genomen. Wanneer toezicht aanscherpt, is "het is historisch gegroeid" geen acceptabel antwoord.

Zoals niemand waterveiligheid als een operationele keuze van een ingenieursafdeling beschouwt, zo kan cloud niet langer worden beschouwd als een gedelegeerd IT-dossier. Bestuur en toezicht hoeven geen technische details te beheersen, maar zij moeten wel kaders stellen: risicobereidheid, acceptabele afhankelijkheden, minimale eisen aan transparantie, auditability, exit en herstel.

Het echte verschil tussen een organisatie die 'cloud gebruikt' en een organisatie die 'digitale autonomie bestuurt' zit in één verschuiving: van impliciet naar expliciet. Niet iedere workload hoort in de boardroom, maar de principes die bepalen waar workloads wél en niet mogen landen, horen daar absoluut. Want dáárin ligt bestuurlijke verantwoordelijkheid.

Praktijk: wanneer externe invloeden de toegang beperken

Een internationaal opererende organisatie draaide haar kernsysteem volledig in een public cloud-omgeving van een buitenlandse leverancier. Jarenlang functioneerde dit probleemloos. De businesscase was overtuigend, de SLA's waren helder en de innovatiekracht groot.

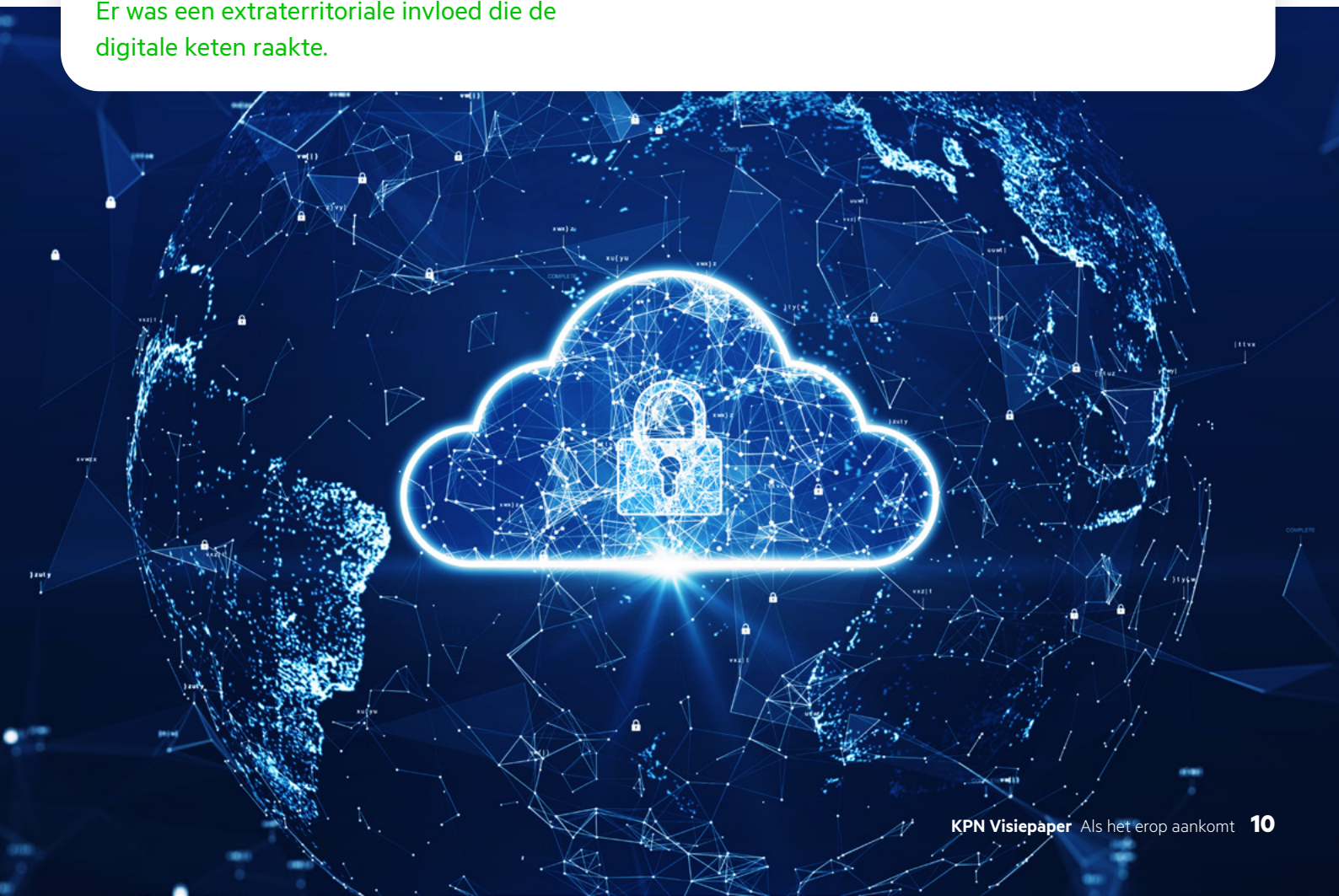
Totdat geopolitieke spanningen leidden tot aangescherpte export- en sanctieregels in het land waar de moederorganisatie van de IT-leverancier gevestigd was. Niet de organisatie zelf, maar de leverancier kwam onder druk te staan. Binnen enkele dagen werden bepaalde support- en beheertaken tijdelijk opgeschort in afwachting van juridische duiding. Toegang tot kritieke beheerfuncties werd beperkt.

Er was geen cyberaanval. Geen technisch falen.
Geen contractbreuk.
Er was een extraterritoriale invloed die de digitale keten raakte.

Wat zichtbaar werd, was niet een fout in technologie, maar een ontwerpkeuze die nooit bestuurlijk was gewogen. De organisatie had geen reëel uitgewerkt scenario voor het geval externe wetgeving directe impact zou hebben op toegang en support. Migratie bleek technisch mogelijk, maar operationeel complex en tijdrovend. In de tussentijd draaide de organisatie met beperkte handelingsruimte.

De les was helder: afhankelijkheid wordt niet alleen bepaald door techniek of contracten, maar ook door geopolitieke context. Digitale autonomie vraagt daarom niet alleen om SLA's, maar om expliciete afweging van jurisdictie, concentratierisico en omkeerbaarheid.

Het incident duurde weken.
Het bestuurlijke inzicht dat volgde, blijvend.



Extraterritoriale werking: wanneer buitenlandse wetgeving uw organisatie raakt

Digitale infrastructuur is grensoverschrijdend georganiseerd. Leveranciers opereren onder nationale wetgeving die ook buiten hun eigen landsgrenzen effect kan hebben. Dit noemen we extraterritoriale werking: wet- en regelgeving van één land kan invloed hebben op data, toegang of dienstverlening in een ander land.

Voor organisaties betekent dit dat afhankelijkheid niet alleen technisch of commercieel is, maar ook juridisch. Toegang tot data kan onder bepaalde omstandigheden worden gevorderd. Support of dienstverlening kan onder druk komen te staan door sancties of nationale veiligheidswetgeving.

De bestuurlijke vraag is daarom niet alleen waar data staat, maar onder welke rechtsmacht zij valt en of die afhankelijkheid expliciet is gewogen.

Digitale autonomie vraagt dat ook deze juridische dimensie onderdeel is van het ontwerp.



Het ongemerkt verdwijnen van regie



Verlies van regie is bijna nooit het gevolg van één grote fout. Het is een optelsom van kleine rationele keuzes die ieder voor zich verdedigbaar zijn. Een afdeling kiest een SaaS-oplossing omdat het de time-to-market halveert. Een project migreert naar een hyperscaler omdat data science daar sneller gaat. Een fusie brengt twee landschappen samen en de focus ligt op “het laten werken”, niet op het herontwerpen van governance. Inkoop verlengt contracten om escalaties te voorkomen. Teams lossen het praktisch op.

En zo ontstaat er langzaam iets wat je pas ziet als je uitzoomt: een landschap dat niemand integraal heeft ontworpen. Een digitale delta met zijtakken, sluizen, keringen en doorbraken maar zonder kaart.

Dit is het punt waarop de dijkenmetafoor werkelijk scherp wordt. Dijken die los van elkaar zijn gebouwd, kunnen jarenlang voldoende lijken. Totdat het water stijgt. Dan blijkt dat één zwakke schakel de hele keten ondermijnt. Niet omdat men nalatig was, maar omdat samenhang ontbrak.



In digitale infrastructuur zie je hetzelfde: cloudgebruik groeit sneller dan bestuurlijke kaders. SaaS stapelt zich op vaak buiten centraal zicht. Data verspreidt zich over platformen en regio's. Contractuele afhankelijkheden verharderen. Portability wordt een bijlage in plaats van een ontwerpprincipe. Ondertussen blijft de verantwoordelijkheid formeel bij het bestuur liggen, terwijl regie feitelijk diffuus wordt.

Het gevaar zit niet in cloud. Het gevaar zit in onbewuste cloud. In het feit dat je pas bij druk ontdekt hoe de keten echt in elkaar zit.

Daarom is digitale autonomie geen migratieprogramma, maar een regieprogramma. Het begint met de erkenning dat 'laten gebeuren' óók een keuze is. En dat uitstel zelden neutraal is: paden verharderen, afhankelijkheden verdiepen, en op het moment dat je móét bewegen is je bewegingsruimte kleiner en je rekening hoger.

Governance in de praktijk

Digitale autonomie wordt bestuurbaar wanneer zij wordt opgenomen in bestaande governance cycli. Dat betekent dat het geen parallel programma is, maar geïntegreerd wordt in strategische planning, risk reviews, portfolio-overleggen en auditcommissies.

Een volwassen aanpak kent vaste momenten van herijking. Net zoals waterkeringen periodiek worden getoetst, worden digitale afhankelijkheden periodiek beoordeeld op concentratie, jurisdictie, contractuele flexibiliteit en technologische lock-in. De vraag is niet of afhankelijkheid bestaat. De vraag is of zij expliciet in beeld is en periodiek wordt gewogen.

Wanneer autonomie onderdeel wordt van reguliere governance, verschuift zij van project naar principe.

Hoofdstuk 5

Handelings- perspectief

Autonomie betekent kunnen bewegen

Digitale autonomie krijgt pas betekenis wanneer zij zich vertaalt in handelingsperspectief. Niet in theorie, maar in de praktijk. Niet in een PowerPoint, maar in het vermogen om daadwerkelijk te bewegen wanneer omstandigheden veranderen.

Veel organisaties verwarren stabiliteit met controle. Zolang systemen functioneren en leveranciers leveren, lijkt alles beheersbaar. Maar controle wordt pas zichtbaar wanneer verandering noodzakelijk is. Wanneer regelgeving wijzigt. Wanneer geopolitieke spanningen invloed krijgen op digitale ketens. Wanneer strategische herpositionering vraagt om herinrichting van het IT-landschap. Of wanneer een leverancier zijn koers wijzigt en daarmee impliciet ook die van u.

Op dat moment blijkt of keuzes omkeerbaar zijn of dat zij ongemerkt onomkeerbaar zijn geworden.

Exit als ontwerpprincipe, niet als noodmaatregel

Een van de meest onderschatte dimensies van digitale autonomie is exit. Niet exit als dreiging, maar exit als ontwerpprincipe.

In veel contracten is exit een clause. In volwassen digitale architectuur is exit een uitgangspunt. Dat verschil is fundamenteel. Wanneer omkeerbaarheid pas wordt overwogen op het moment dat vertrek noodzakelijk is, is de afhankelijkheid al maximaal. Dataformaten zijn proprietary, integraties zijn diep verweven, kennis zit bij de leverancier, migratiepaden zijn complex en kostbaar.

Digitale autonomie vraagt daarom dat exit niet wordt behandeld als juridische voetnoot, maar als strategische randvoorwaarde. Dat betekent dat vooraf wordt nagedacht over vragen als:

- In welk formaat worden data opgeslagen en geëxporteerd?
- Hoe afhankelijk zijn wij van specifieke PaaS- of SaaS-functionaliteit?
- Wat is de feitelijke migratie-inspanning wanneer wij moeten verplaatsen?
- Hoeveel kennis en configuratie zit exclusief bij de leverancier?

Dit zijn geen technische details. Het zijn bestuurlijke vragen over bewegingsruimte.



Zoals een waterkering noodsluis bevat die zelden wordt gebruikt maar essentieel is voor vertrouwen in het systeem, zo moet een digitale architectuur het vermogen bevatten om gecontroleerd te kunnen verschuiven. Niet omdat men verwacht dat men continu migreert, maar omdat goed bestuur vraagt om de mogelijkheid daartoe.

Exit is geen migratiedrang. Exit is bestuurlijke zekerheid.

Vendor lock-in: wanneer afhankelijkheid structureel wordt

Vendor lock-in ontstaat zelden door één contract. Het ontstaat door een combinatie van technologische, organisatorische en financiële factoren. Een platform biedt unieke functionaliteit. Teams bouwen daarop voort. Integraties verdiepen zich. Specifieke tooling wordt leidend in processen. Opleidingen en kennis worden daarop afgestemd. Na verloop van tijd is de afhankelijkheid niet alleen technisch, maar ook organisatorisch verankerd.

Dit is niet per definitie verkeerd. Specialisatie kan waardevol zijn. Maar zonder expliciete afweging kan lock-in strategische flexibiliteit beperken.

Het risico van lock-in is niet dat overstappen onmogelijk is. Het risico is dat overstappen alleen nog mogelijk is tegen disproportionele kosten of onder grote tijdsdruk. Dan verandert afhankelijkheid van keuze in noodzaak.

Digitale autonomie vraagt daarom om een bewuste balans tussen benutten en begrenzen. Het benutten van innovatieve platformdiensten waar zij waarde toevoegen, en het begrenzen van structurele afhankelijkheid waar zij strategische wendbaarheid ondermijnt.

Dat betekent niet dat iedere organisatie multi-cloud moet opereren. Het betekent wel dat concentratie bewust wordt gewogen. Dat kritieke processen niet per definitie volledig afhankelijk zijn van één leverancier zonder scenarioanalyse. Dat contracten aandacht besteden aan dataportabiliteit en beëindigingsrechten. Dat kennis niet uitsluitend buiten de organisatie is belegd.

Autonomie betekent niet dat u nooit afhankelijk bent. Het betekent dat u weet hoe afhankelijk u bent en wat u kunt doen als dat moet veranderen.



Handelingsperspectief onder druk

Het moment waarop autonomie zijn waarde bewijst, is het moment waarop handelen noodzakelijk wordt. Een toezichthouder stelt nieuwe eisen. Een internationale leverancier komt onder politieke druk. Een strategische koerswijziging vraagt om herpositionering van kernsystemen.

Organisaties met vooraf ontworpen handelingsperspectief reageren anders dan organisaties die afhankelijkheid impliciet hebben laten groeien.

Zij hebben inzicht in welke workloads verplaatsbaar zijn. Zij weten welke afhankelijkheden contractueel en technisch begrensd zijn. Zij hebben migratiepaden doordacht, zelfs als die nooit volledig zijn uitgewerkt. Zij hebben governance ingericht die risico's periodiek herijkt.

Het verschil zit niet in snelheid alleen. Het verschil zit in rust.

Wanneer handelingsperspectief vooraf is ontworpen, ontstaat bestuurlijke rust zonder druk. Er is geen paniek, maar scenario's. Geen improvisatie, maar vooraf gewogen opties.

Zoals waterbeheer niet draait om het voorkomen van elke storm, maar om voorbereid zijn op stormen, zo draait digitale autonomie niet om het voorkomen van elke verstoring, maar om voorbereid zijn op verandering.

Van afhankelijkheid naar wendbaarheid

Digitale autonomie is daarmee geen defensieve strategie. Het is een vorm van strategische wendbaarheid. Organisaties die hun afhankelijkheden expliciet hebben ontworpen, kunnen innovatie blijven benutten zonder vast te zitten. Zij kunnen groeien zonder structurele kwetsbaarheid te vergroten. Zij kunnen kiezen, in plaats van gedwongen te worden.

Handelingsperspectief betekent dat digitale infrastructuur niet alleen functioneert, maar bestuurlijk stuurbaar blijft.

Niet om minder cloud. Niet om meer controle om de controle. Maar om het vermogen om te bewegen wanneer beweging noodzakelijk is.

Als het erop aankomt, wilt u niet ontdekken dat uw opties beperkt zijn. U wilt weten welke opties u heeft. En dat begint vandaag bij het ontwerpen van exit, omkeerbaarheid en bewuste afhankelijkheid.

Hoofdstuk 6

Van impliciet gegroeid naar expliciet ontworpen

De bestuurlijke keuzeruimte tussen innovatie en autonomie

Veel discussies over soevereiniteit stranden op een valse tegenstelling: alsof je óf volledig de hyperscalers omarmt óf alles terughaalet naar eigen infrastructuur. Dat klinkt daadkrachtig, maar het is zelden realistisch en bijna nooit bestuurlijk volwassen.

Nederland heeft nooit geprobeerd de zee weg te onderhandelen. Wij hebben geleerd dat water ruimte moet krijgen waar het kan en gekeerd moet worden waar het moet. Dat onderscheid (ruimte versus bescherming) heeft ons land niet alleen veilig gemaakt, maar ook welvarend. Het is precies die volwassenheid die het cloudcontinuüm bestuurlijk vertaalt.

Het cloudcontinuüm is, in de kern, geen technisch plaatje. Het is een kader om expliciete keuzes te maken over waar je afhankelijkheid accepteert en waar je haar begrenst. Aan de ene kant van het continuüm ligt public cloud: maximale innovatiekracht, snelheid, ecosysteemvoordeel. Daar zitten de diensten die teams in staat stellen om sneller te ontwikkelen, data slimmer te benutten en AI te versnellen. Voor veel organisaties is dit onmisbaar om concurrerend te blijven.



Maar innovatiekracht zonder bestuurlijke regie is als een rivier zonder kering: prachtig zolang hij rustig stroomt, ontwrichtend wanneer hij buiten zijn bedding treedt. Daarom hoort bij die linkerkant niet een “ja/nee”, maar een volwassen variant: supervised public cloud. Je benut de innovatie, maar je voegt governance toe: inzicht in dataflows, identiteitsbeheer, contractuele controle, monitoring, compliance-artefacten, en heldere spelregels voor wat er wél en niet thuishoort.

In het midden van het continuüm liggen sovereign platforms: omgevingen die cloudfunctionaliteit combineren met governance onder Nederlandse of Europese kaders. Dit midden is vaak waar bestuurders rust zoeken, niet omdat het alle risico's oplost, maar omdat het transparantie en herleidbaarheid vergroot. Het is de zone waar "wendbaarheid" en "uitlegbaarheid" elkaar kunnen ontmoeten. Niet als compromis, maar als bewuste ontwerpkeuze.

Aan de rechterkant van het continuüm liggen private en air-gapped omgevingen: maximale autonomie voor situaties waarin afhankelijkheid niet uitlegbaar is. Dit zijn geen standaard-oplossingen, net zoals een stormvloedkering geen standaardbrug is. Ze zijn bedoeld voor uitzonderlijke verantwoordelijkheden: vitale processen, nationale veiligheid, hoogkritische ketens. Juist door ze bewust en beperkt in te zetten, blijven ze geloofwaardig en bestuurbaar.

Het volwassen inzicht is dit: soevereiniteit is geen ideologie, maar differentiatie. Niet alles hoeft maximaal autonoom. Maar sommige onderdelen mógen dat ook niet níét zijn.

Bestuurders kunnen dit continuüm lezen als een "als-het-erop-aankomt-test". Waar kan de organisatie snelheid maximaliseren zonder de uitlegbaarheid te verliezen? Waar moet de organisatie transparantie en jurisdictie zwaarder laten wegen? En waar is maximale autonomie een randvoorwaarde, ongeacht kosten of complexiteit?

Zodra je deze vragen expliciet stelt, verandert cloud van een verzameling toolkeuzes in een bestuurlijk ontwerp. En precies daar ontstaat digitale autonomie.



Cloudcontinium Sovereign by design

Sovereign-by-Design doorbreekt dat patroon en maakt de verschuiving van:

Impliciet	Expliciet
Afhankelijkheden ontstaan vanzelf	Afhankelijkheden worden gekozen
Technologie stuurt besluitvorming	Ontwerp stuurt technologie
Verantwoordelijkheid is diffuus	Verantwoordelijkheid is herleidbaar
Soevereiniteit is abstract	Soevereiniteit is bespreekbaar

Van impliciet naar expliciet

Deze tabel vat samen waar het bij digitale autonomie écht om draait: niet technologie, maar hoe keuzes worden gemaakt.

Links ziet u het impliciete patroon. Afhankelijkheden ontstaan vanzelf, door snelheid en gemak. Technologie gaat sturen hoe besluiten worden genomen, terwijl de verantwoordelijkheid formeel bij bestuur en toezicht blijft liggen. Soevereiniteit wordt daarmee abstract en lastig bestuurbaar.

Rechts ziet u wat er gebeurt als autonomie door ontwerp wordt toegepast. Afhankelijkheden verdwijnen niet, maar worden bewust gekozen. Keuzes worden expliciet vastgelegd, verantwoordelijkheid wordt herleidbaar en soevereiniteit wordt bespreekbaar en uitlegbaar.

Dit is geen ideologische verschuiving en geen pleidooi voor meer of minder cloud. Het is een verschuiving in bestuurspraktijk: van impliciet naar expliciet. Pas dan ontstaat aantoonbare regie en precies dát is wat hierna centraal staat in de oproep tot actie.



Als het erop aankomt, wat kost niets doen?



Van abstract debat naar uitvoerbare regie

Elke boardroom die dit onderwerp serieus neemt, komt vroeg of laat bij dezelfde nuchtere vraag: wat kost dit en wat kost het als we niets doen?

De investering in regie is zichtbaar. Ze gaat over inventariseren, herontwerpen, hercontracteren, trainen, borgen. Over het soms tijdelijk parallel draaien van omgevingen om continuïteit te garanderen. Over het opbouwen van assurance: aantoonbaarheid richting audit, toezicht en maatschappij. Dit voelt als “kosten maken”, zeker wanneer er op dat moment geen incident is.

Maar waterveiligheid leert dat je dijken niet beoordeelt op hun rendement bij laagwater. Je beoordeelt ze op hun waarde bij hoogwater. De kosten van niets doen zijn zelden zichtbaar op de begroting, maar zij materialiseren onder druk: herstelkosten, productiviteitsverlies, reputatieschade, compliancefindings, boetes, en (het meest onderschat) gedwongen keuzes op ongunstige momenten. Dan betaal je niet alleen meer; je betaalt met minder tijd, minder alternatieven en minder onderhandelingsruimte.

De bestuurlijke vraag is daarom niet “doen we alles tegelijk?”

De vraag is: maken we risico expliciet en beheersbaar, of accepteren we dat we later betalen onder slechtere omstandigheden?

Hoe maak je dit bestuurbaar? Door digitale autonomie te behandelen zoals je waterveiligheid behandelt: als governanceprogramma, niet als IT-project. Dat betekent dat bestuur en toezicht kaders stellen en eigenaarschap organiseren. Dat betekent dat je principes definieert (waar is afhankelijkheid acceptabel, onder welke voorwaarden, met welke minimale eisen aan transparantie en exit?). Dat betekent dat je een meerjarig programma mandateert met duidelijke scope, meetpunten en herijkingsmomenten. Dat betekent dat je een target cloudportfolio per domein vastlegt binnen het continuüm, niet als vendor-keuze, maar als risicokeuze. En dat betekent dat je resterende risico's niet laat "zweven", maar expliciet accepteert of begrenst met tijdslijnen.

KPN brengt dit vraagstuk terug naar drie samenhangende stappen: inzicht, ontwerp, borging.

Eerst maken we afhankelijkheden zichtbaar op een manier die bestuurders begrijpen: wat is kritiek, waar zit concentratie, onder welke jurisdicties valt de keten, welke SaaS is kernproceskritisch, waar ontbreekt governance, wat is de feitelijke omkeerbaarheid? Niet als technische lijst, maar als bestuurlijke spiegel. Daarna ontwerpen we samen de positionering binnen het continuüm: waar benut je innovatie onder supervised governance, waar kies je voor sovereign platforms, waar is maximale autonomie noodzakelijk? En vervolgens borgen we dit in governance en assurance: contractueel, operationeel en auditbaar, zodat een bestuurder niet alleen gelooft dat het klopt, maar het ook kan aantonen wanneer er vragen komen.

KPN's geloofwaardigheid in dit domein komt niet uit theorie, maar uit praktijk: werken in omgevingen waar uitval geen optie is, waar continuïteit en betrouwbaarheid ontworpen moeten zijn voor "het meest kritische scenario". Die discipline van ontwerpdenken, risico-denken en keten-denken vertalen we naar organisaties die hun digitale dijken willen versterken zonder innovatie te verliezen.

Het doel is niet een wereld zonder afhankelijkheid. Het doel is een wereld waarin afhankelijkheid niet ongemerkt groeit, maar bewust wordt gekozen. Waar innovatiekracht blijft, maar bestuurlijke uitlegbaarheid meegroeit. Waar de organisatie handelingsperspectief heeft, ook wanneer omstandigheden kantelen.

Want uiteindelijk is dat de toets waar dit hele verhaal om draait. Niet op rustige dagen. Niet wanneer alles werkt. Maar wanneer het erop aankomt.



Tot slot: Hoe pakt u dit vandaag aan?

Digitale autonomie is geen toekomstvisie die kan wachten tot een volgende strategieronde. Zij is een bestuurlijke realiteit die vandaag begint. Niet met een grote migratie. Niet met een ideologisch statement. Maar met het expliciet maken van wat nu impliciet is.

Voor veel organisaties is het grootste risico niet dat zij “de verkeerde cloud” gebruiken. Het grootste risico is dat zij niet exact weten hoe hun afhankelijkheid is opgebouwd, hoe geconcentreerd zij is en hoe zij zich gedraagt onder druk. Afhankelijkheid groeit zelden via één grote beslissing. Zij groeit via pragmatische projectkeuzes, verlengde contracten, fusies, optimalisaties en innovaties. Dat maakt haar begrijpelijk, maar ook bestuurlijk diffuus.

**De vraag is dus niet: moeten wij iets veranderen?
De vraag is: weten wij precies wat wij vandaag verdedigen?**

Daarom begint digitale autonomie bij vier samenhangende bewegingen.

1. Maak afhankelijkheid expliciet

Digitale autonomie begint niet bij migreren, maar bij inzicht. Zolang afhankelijkheid impliciet blijft, kan zij niet worden gewogen. Bestuurders moeten kunnen beantwoorden welke processen werkelijk kritiek zijn voor continuïteit, waar deze draaien, onder welke juridische kaders zij vallen en hoe geconcentreerd de afhankelijkheid in leveranciers is.

Dit vraagt geen technische diepgang op bestuursniveau, maar wel bestuurlijke transparantie. Wie heeft toegang tot kernprocessen? Wat gebeurt er bij uitval of geopolitieke verschuiving? Hoe snel kunnen wij handelen wanneer omstandigheden veranderen?

Wanneer afhankelijkheid zichtbaar wordt gemaakt, verschuift het gesprek van aannames naar feiten. Van vertrouwen naar ontwerp. Pas dan ontstaat de ruimte om bewust te kiezen.

2. Bepaal waar afhankelijkheid acceptabel is en waar niet

Volledige onafhankelijkheid is in een geglobaliseerde economie niet realistisch. De kracht van moderne cloud ligt juist in internationale schaal, innovatiekracht en ecosystemen. De bestuurlijke volwassenheid zit daarom niet in het afwijzen van afhankelijkheid, maar in het differentiëren ervan.

Het cloudcontinuüm biedt hier een bestuurlijke keuzeruimte. Sommige workloads mogen maximaal profiteren van internationale innovatie, mits governance op orde is. Andere processen vragen om aanvullende controle binnen nationale of Europese kaders. Weer andere processen zijn zo fundamenteel dat externe afhankelijkheid daar beperkt moet blijven.

Deze differentiatie vraagt expliciete besluitvorming. Niet ieder systeem verdient dezelfde mate van autonomie. Maar sommige systemen mogen dat ook niet níét krijgen.

Zodra deze afwegingen zijn vastgelegd, verandert cloud van een verzameling leveranciers in een ontworpen landschap.

3. Borg autonomie in governance, niet in een project

Digitale autonomie kan niet worden gerealiseerd via een tijdelijk programma dat na twee jaar wordt afgerond. Zij wordt duurzaam wanneer zij onderdeel wordt van reguliere governance.

Dat betekent dat cloudkeuzes worden getoetst aan vastgestelde principes. Dat investeringsbesluiten worden gewogen tegen risicobereidheid. Dat contracten expliciete aandacht besteden aan transparantie, auditability en omkeerbaarheid. Dat risicoacceptatie geen stilzwijgend gevolg is, maar een bewust genomen besluit.

Waterveiligheid is in Nederland sterk omdat zij periodiek wordt herzien. Digitale autonomie vraagt dezelfde ritmiek. Niet als reactie op incidenten, maar als terugkerend bestuursmoment.

Wanneer autonomie verankerd raakt in governance, verschuift zij van initiatief naar principe.

4. Investeer in regie voordat u onder druk moet handelen

Elke bestuurlijke beslissing kent een financiële dimensie. Investeren in autonomie vraagt middelen: inzicht, herontwerp, hercontractering, soms herpositionering van workloads. Deze kosten zijn zichtbaar en planbaar.

De kosten van niets doen zijn minder zichtbaar, maar potentieel groter. Zij materialiseren onder druk: bij incidenten, bij toezicht, bij geopolitieke verschuivingen. Dan worden keuzes gedwongen, migraties versneld en onderhandelingen gevoerd vanuit zwakte.

Het verschil zit niet alleen in euro's. Het verschil zit in bestuurlijke ruimte.

**Investeren in regie
betekent kiezen in rust.
Niets doen betekent
handelen onder druk.**

Digitale autonomie is daarmee geen kostenpost, maar een vorm van risicomanagement op strategisch niveau.

Slotreflectie: 'Als het erop aankomt'

Dit document pleit niet voor minder cloud. Het pleit niet voor isolatie. Het pleit niet voor wantrouwen jegens internationale technologie. Het pleit voor volwassen bestuur.

Nederland is veilig omdat het water serieus neemt, niet omdat het water afwezig is. Digitale autonomie vraagt precies diezelfde houding. Het erkennen van afhankelijkheid als realiteit, en het weigeren haar aan het toeval over te laten.

Wanneer omstandigheden stabiel zijn, lijkt alles beheersbaar. Maar de ware toets ligt in het moment dat omstandigheden verschuiven. Wanneer toezicht vragen stelt. Wanneer markten veranderen. Wanneer geopolitiek invloed krijgt op digitale ketens. Wanneer continuïteit onder druk staat.

Op dat moment wordt zichtbaar of afhankelijkheid een toevallige uitkomst was of een bewust ontworpen keuze.

Als het erop aankomt, wilt u niet ontdekken hoe uw digitale landschap werkelijk in elkaar zit. U wilt het al weten.

**En dat is de kern
van digitale autonomie:
niet onafhankelijk
van de wereld,
maar bestuurbaar
binnen haar grenzen.**



Over KPN

KPN als strategische partner

Digitale autonomie raakt iedere bestuurder anders. Niet omdat de technologie verschilt, maar omdat de verantwoordelijkheid verschilt. Wat voor een CIO een architectuurvraag is, is voor een CFO een risicovraag. Wat voor een CEO een strategische afweging is, is voor een toezichthouder een vraag naar uitlegbaarheid.

KPN ondersteunt organisaties vanuit dat bestuurlijke perspectief.

Voor de CEO: strategische continuïteit en reputatie

Als CEO bent u verantwoordelijk voor de lange termijn. Digitale infrastructuur bepaalt vandaag uw wendbaarheid, uw concurrentiekracht en het vertrouwen van klanten of burgers. Wanneer digitale ketens onder druk komen te staan, raakt dat direct uw reputatie en strategische positie.

KPN helpt u om digitale afhankelijkheden niet als operationeel detail te behandelen, maar als onderdeel van uw strategische risicoprofiel. Wij ontwerpen hybride IT-landschappen waarin innovatie mogelijk blijft, zonder dat bestuurlijke controle verdwijnt. Zo blijft uw organisatie toekomstgericht én robuust.

Voor de CFO: risico, investeringszekerheid en voorspelbaarheid

Als CFO kijkt u naar kosten, maar vooral naar risico en voorspelbaarheid. Concentratie in leveranciers, contractuele lock-in en onvoorziene migraties kunnen financiële impact hebben op het moment dat u die het minst kunt gebruiken.

KPN ondersteunt bij het expliciet maken van afhankelijkheden en het beheersbaar ontwerpen van cloudportfolio's. Wij helpen om exit- en portabilityafspraken niet als bijlage te behandelen, maar als onderdeel van investeringszekerheid. Zo verschuift IT van potentiële financiële onzekerheid naar bestuurbare asset.

Voor de CIO: samenhang en beheersbaarheid in een hybride landschap

Als CIO opereert u in de complexiteit van legacy, cloud, SaaS en nieuwe digitale initiatieven. U moet innoveren én stabiliteit waarborgen. U moet snelheid faciliteren zonder compliance te verliezen.

KPN treedt op als system integrator die het volledige landschap overziet van security tot cloud, van netwerk tot werkplek. Wij zorgen dat technologische componenten naadloos samenwerken binnen duidelijke governancekaders.



Dit betekent dat per workload bewuste keuzes worden gemaakt over datalocatie, regie en afhankelijkheid, zodat innovatie geen nieuwe kwetsbaarheid creëert.

Voor de CRO, CISO en compliance-verantwoordelijken: beheersbaarheid en uitlegbaarheid

Voor risk- en compliance-functies is digitale infrastructuur geen innovatievraagstuk, maar een beheersvraagstuk. Onder welke jurisdicties valt data? Wie heeft toegang? Wat gebeurt er bij verstoringen of geopolitieke veranderingen?

KPN helpt organisaties hun digitale keten inzichtelijk, auditbaar en herleidbaar te maken. Wij integreren cybersecurity, identity, monitoring en governance als structurele bouwstenen van het landschap. Niet als losse maatregelen, maar als samenhangend ontwerp dat standhoudt onder toezicht.

Voor toezichthouders en commissarissen: expliciete regie

Voor toezichthouders gaat het uiteindelijk om één vraag: kan het bestuur aantonen dat digitale afhankelijkheden expliciet zijn gewogen en beheersbaar zijn ingericht?

KPN ondersteunt bij het vertalen van technische realiteit naar bestuurlijke uitlegbaarheid. Door differentiatie binnen het cloudcontinuüm en expliciete vastlegging van afhankelijkheden ontstaat een digitaal landschap dat niet alleen functioneert, maar ook verantwoord kan worden.

Voor Nederland: Sectoroverstijgend en vanuit één principe

Of u nu actief bent in publieke dienstverlening, zorg, financiële sector, industrie of vitale infrastructuur: digitale infrastructuur vormt het fundament van uw primaire processen. Wanneer die onder druk komt te staan, raakt dat direct uw maatschappelijke of economische opdracht.

KPN is zelf onderdeel van de Nederlandse kritieke infrastructuur. Betrouwbaarheid en beschikbaarheid zijn voor ons geen abstracte waarden, maar dagelijkse praktijk. Vanuit die ervaring ontwerpen wij IT-oplossingen die innovatie mogelijk maken, terwijl bestuurlijke controle behouden blijft.

Wij verbinden niet alleen systemen, maar ook verantwoordelijkheden. Wij leveren niet alleen technologie, maar bestuurbare autonomie.

Zo ondersteunen wij bestuurders in wat uiteindelijk hun kernverantwoordelijkheid is: continuïteit, vertrouwen en toekomstbestendigheid.

Voor een beter werkend Nederland, daar doen we het voor.

Daarom KPN

Vertrouw op het netwerk van Nederland. Wij zijn verantwoordelijk voor dé vitale communicatiediensten. En daar profiteren al onze klanten van mee.

Wij geloven in partnerschap.

We nemen je mee in nieuwe technologische ontwikkelingen. Laten zien wat het je oplevert. Niet eenmalig, maar blijvend.

Veiligheid staat bij ons voorop.

We beschermen onze netwerken 24/7 en bieden je een scala aan securitydiensten. Je rekent op strikte beveiliging.

Maak een afspraak

Ga naar www.kpn.com/SI of neem contact op met je accountmanager van KPN voor een afspraak.



Over KPN

KPN is de natuurlijke partner voor digitale autonomie

Verbinding

Wij kennen Nederland en Nederland kent ons. Veel organisaties en consumenten van Nederland zijn al klant van KPN en vertrouwen op onze dienstverlening.

Dienstverlening

Met ons brede zakelijk portfolio op het gebied van Cloud, Werkplek, Connectiviteit, Data, Security en SIAM kunnen we een aanzienlijk deel van de soevereine klantbehoefte invullen.

Nederland

Als Nederlands bedrijf (incl. beschermwal overheid) met lokale datacenters, duizenden POP's en een eigen internet exchange bieden we als enige een volledige end-to-end soevereine infrastructuur. Als lokaal (NIS2) bedrijf begrijpen we de wet- en regelgeving.

Digitalisering

We helpen vele gerenommeerde Nederlandse organisaties met het digitaliseren van hun missiekritische bedrijfsvoering. Wij weten hoe schaalbaarheid georganiseerd moet worden.

Kennis en innovatie

Wij willen van betekenis zijn. Dit doen we met > 1000 experts in verschillende samenwerkingsvormen afhankelijk van de situatie bij onze klant.

Duurzaam

Wij zetten alles op alles om iedereen te verbinden met een duurzame toekomst. Onze duurzaamheid en social return resultaten behoren tot de beste ter wereld.