



Radar klantgerichtheid en digitale transformatie

Overheidssector

Brussels Gewest

Cel monitoring – pijler DT - Paradigm

Februari 2025

INLEIDING	3
Intro	3
Een woordje uitleg bij de Radar	3
Een woordje uitleg bij de Radar	3
RADAR PARADIGM V4	5
Antwoorden op de enquête	5
Radar Kwadrant Klantgerichtheid	5
Radar Kwadrant Digitale overheid	7
Kwadrant Zoom AI	11
Kwadrant security Smals	13
INTERNE OPVOLGING PARADIGM	15
OPVOLGING op gewestelijk niveau	16
METHODOLOGIE	17
OVER	18

INLEIDING

Intro

Als digitale orchestrator van het Gewest heeft Paradigm **innovatie** centraal geplaatst in zijn waarden.

Innovatie betekent waakzaamheid, omdat innovatie verband houdt met een specifieke context, maatschappelijke, technologische en organisatorische uitdagingen.

Het concept van de Radar biedt een overzicht van de trends en een prioritering ervan. Door de Radar regelmatig bij te werken, kunnen we de evolutie van deze prioriteiten en de daaruit voortvloeiende acties volgen.

Deze twee Radars voor *klantgerichtheid* en *digitale transformatie overheidssector* zijn een momentopname van de kennis en van de context. Het is een instrument dat past binnen een gestructureerde monitoring en daarmee een interessante tool is om innovatieactiviteiten te starten terwijl we in lijn blijven met de eigen uitdagingen, de context en de opdracht van Paradigm. (*Ordonnantie Paradigm: 4^o het staat in voor **het observeren**, implementeren, integreren, beheren, begeleiden, beveiligen en adviseren over netwerken en informatiesystemen, digitale, telematica-, cartografie en telecommunicatieprojecten en bevoegdheden met betrekking tot digitale en informatie- en communicatietechnologieën binnen het Brusselse digitale ecosysteem.*)

In deze editie richten we ons op het gebied van AI en op het gebied van beveiliging, waarbij we een kijkje nemen bij de Radar van Smals (www.smals.be) op dit specifieke gebied.

Dit is de vierde editie van de Radar. Sinds de eerste editie zijn de prioriteiten duidelijk verschoven en zijn er nieuwe trends vastgesteld.

Een woordje uitleg bij de Radar

De Radar voor digitale transformatie en klantgerichtheid is onderverdeeld in vier prioriteitszones, met de meest bruikbare trends in het midden. De trends worden gerangschikt volgens hun relevantie en potentiële impact op de digitale transformatieactiviteiten van de spelers in de overheidssector van het Brussels Gewest.

De Radar voor digitale transformatie en klantgerichtheid is een nuttig instrument voor de gewestelijke bestuursorganen in het Brussels Gewest die willen innoveren en op de hoogte willen blijven van de nieuwste trends in digitale transformatie.

In zijn eerste zones kan de Radar helpen om een gestructureerde monitoring te ontwikkelen en innovatieactiviteiten te lanceren, terwijl het in fase blijft met de specifieke uitdagingen, context en digitale transformatie-opdracht van Paradigm en van de instellingen van het Brussels Gewest in het algemeen.

Het woord "Radar" is afkomstig uit de militaire luchtvaart, waar het door middel van een scansysteem objecten en vliegtuigen in het luchtruim kan detecteren.

De typische weergave voor luchtverkeersleiders is deze scan, die naderende punten onderscheidt. Op basis van deze afbeelding kan de luchtverkeersleider acties ondernemen en prioriteiten stellen.

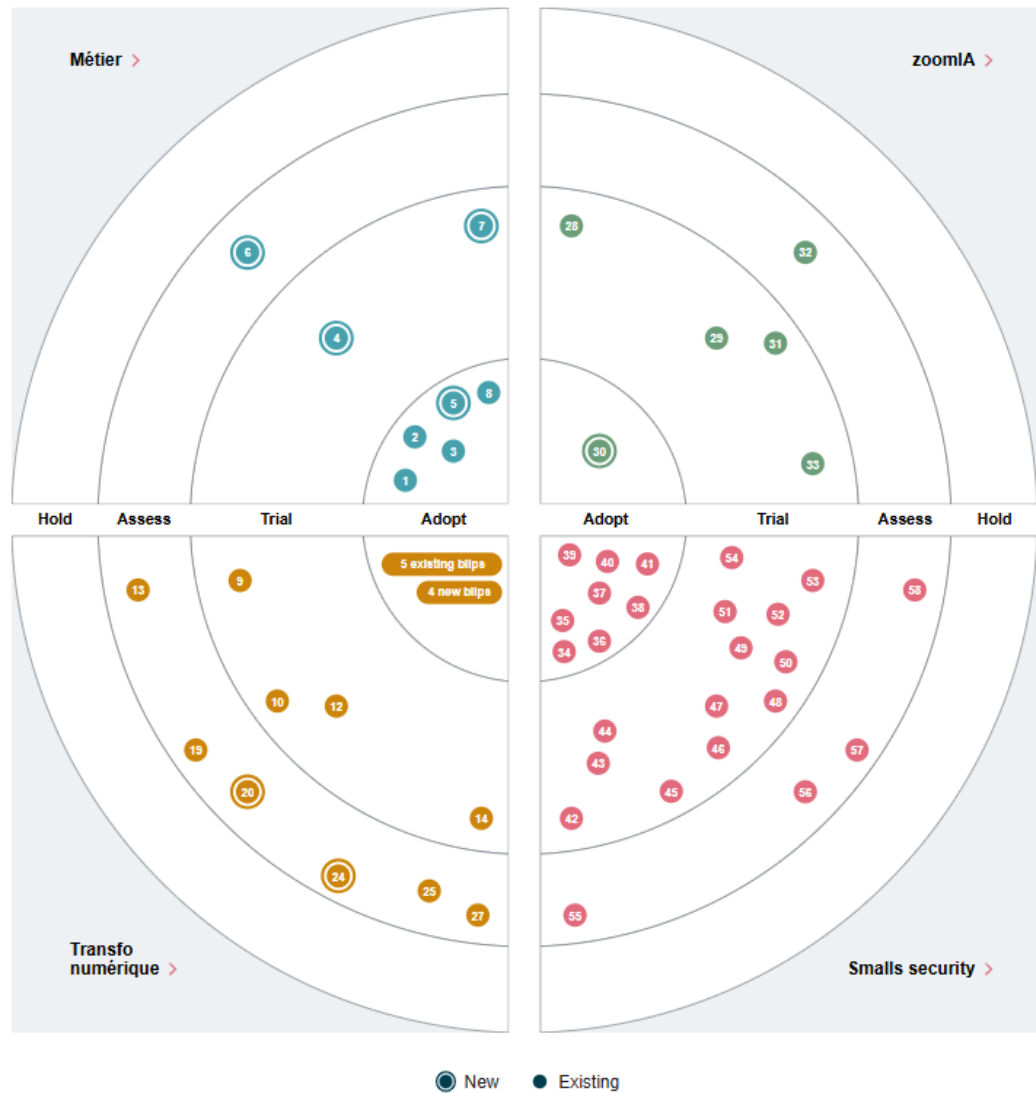
De term "radar" is overgenomen in de context van een scan; dit keer gaat het om opkomende trends die meer of minder impact zullen hebben in de nabije toekomst.

Elementen van een trendradar zijn:

- Een trend en een korte definitie
- Deze trend geprioriteerd op 4 gradaties van relevantie, waarbij wat zich in het midden bevindt het belangrijkste is

De radar moet worden gelezen aan de hand van 4 cirkels van relevantie:

- (adopt) Actie - actie ondernemen
- (trial) Studie - verdiepen, voorbereiden
- (assess) Monitoring – in de gaten houden
- (hold) Pauze - buiten beschouwing laten voor de geanalyseerde periode



Beeld: 4 trendradars. Het thema in een dubbele cirkel is van categorie veranderd/nieuw toegevoegd t.o.v. vorig jaar.

RADAR PARADIGM V4

Antwoorden op de enquête

De deelnemers benadrukten het belang van bepaalde vakgebonden principes voor het **ontwerp** van een applicatie: **duurzame IT, gebruikerservaring**, vereenvoudiging en mutualisering. Wat op zich vanzelfsprekend zou moeten zijn.

Andere bekommernissen zijn nauw verbonden met het juiste gebruik van IT en van middelen: de juiste integratie van **AI en het gebruik ervan** (prompting,...), ondersteuning van de komst van zogenaamde '**low code**'-applicaties die weinig technische ervaring vergen,... Vervolgens is er het **regelgevingskader**, dat moet worden beoordeeld en aangepast.

De meest opvallende trend is de echte vraag naar actie op het gebied van risicobeheer in verband met **cyberbeveiligings**verschijnselen, een domein dat duidelijk wordt gezien als een reële bedreiging voor de continuïteit van overheidsdiensten.

Radar Kwadrant Klantgerichtheid

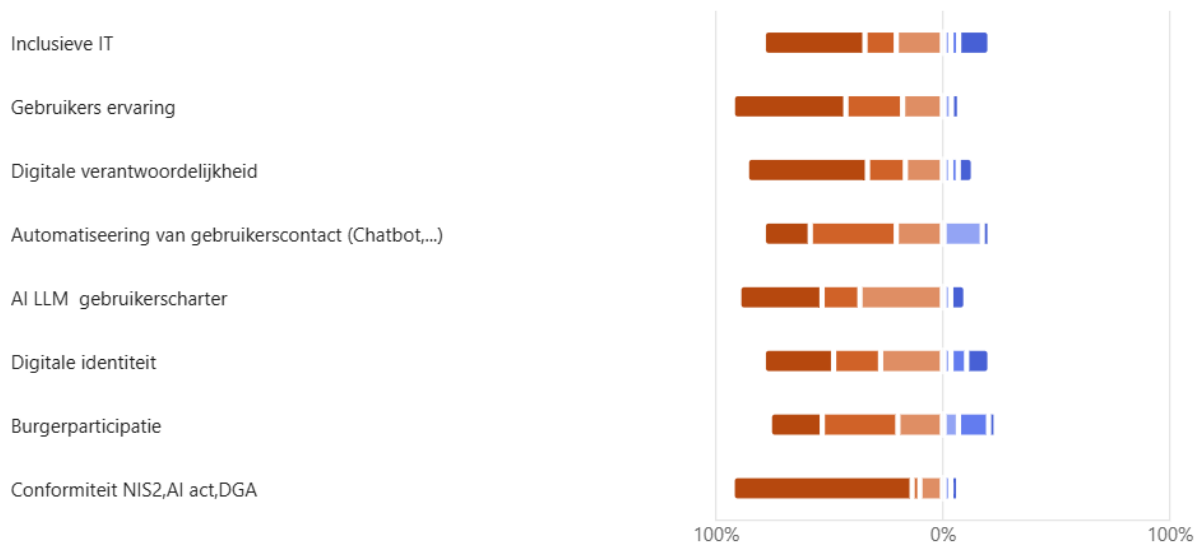
Het is interessant om de door de klanten geuite prioriteiten te bundelen met de trends in zakelijke toepassingen die verband houden met burgers/bedrijven en hun relevantie.

- 1 (adopt) Actie - actie ondernemen
- 2 (trial) Studie - verdiepen, voorbereiden
- 3 (assess) Monitoring - in de gaten houden
- 4 (hold) Pauze - buiten beschouwing laten voor de geanalyseerde periode
- 5 buiten perimeter
- 6 geen mening

■ 1 ■ 2 ■ 3 ■ 4 ■ 5 ■ 6

(resultaten van de enquête)

● 1 ● 2 ● 3 ● 4 ● 5 ● 6



In het kwadrant Action/Adopt vinden we duidelijk het **trio van conformiteit met de wetgeving NIS2/DGA/AI-verordening, duurzame IT en gebruikerservaring** terug.

Uitleg bij de gebruikte termen in de Radar klantgerichtheid:

Adopt	Inclusieve IT	Digitale inclusie, of e-inclusie, is een proces dat tot doel heeft digitale toegankelijkheid te bieden aan elk individu, met name op het gebied van telefonie en internet, en hen digitale vaardigheden bij te brengen. Deze vaardigheden zullen hen in staat stellen om deze middelen te gebruiken als hefboom voor hun sociale en economische integratie.
Adopt	Gebruikers-ervaring	De klantbeleving is de manier waarop klanten de merkervaring waarnemen op basis van hun interacties ermee. Het is de algehele perceptie die iemand heeft van de organisatie. Dit omvat het volledige traject van elke klantinteractie, van wat ze als eerste zien op advertentiemateriaal tot wat ze denken na een gesprek met het klantondersteuningsteam na aankoop. Hoe positiever de interacties, des te beter de mogelijke ervaring.
Adopt	Duurzame IT	Informatietechnologie heeft een dubbele impact op de huidige ecologische crisis. Ze kan de ecologische voetafdruk van bestaande processen verminderen, maar ze heeft een aanzienlijke ecologische voetafdruk (carbon footprint) gedurende haar hele levenscyclus (van mijnbouw tot elektronisch afval). De overheid zou het eerste moeten maximaliseren en het tweede minimaliseren.
Adopt	AI – LLM use policy	Implementering van een intern beleid op de werkplek voor toegang tot goedgekeurde AI-tools om een veilige omgeving te bieden en de productiviteit te verhogen.
Adopt	Conformiteit aan wetgeving (NIS2, DGA,...)	NIS2, de “GDPR-verordening voor cyberbeveiliging” omvat een hele reeks regels rond het beveiligen van informatie;

		de DGA of Data Governance Act heeft het over regels rond het delen van gegevens.
Trial	Automatisering gebruikers-contact (chatbot)	Automatisering van klantenondersteuning omvat alles wat gericht is op het verminderen of elimineren van de noodzaak van menselijke betrokkenheid bij het oplossen van klantverzoeken. Dit kan bijvoorbeeld automatische beantwoording van e-mails of zelfs van telefoonoproepen omvatten. Het omvat ook ondersteuning voor callcentermedewerkers door suggesties voor antwoorden te bieden, via interne chatbots of zelfs een eigen virtuele assistent.
Trial	Burger-participatie	Het gebruik van informatietechnologieën om de betrokkenheid en zelforganisatie van burgers te bevorderen met als doel maatschappelijke meerwaarde te creëren. De burger kan één of meerdere rollen vervullen, zoals gegevensleverancier.
Assess	Digitale identiteit	De portemonnees voor digitale identiteit (DIW) maken het delen van identiteitsgegevens en allerlei soorten attesten mogelijk tussen een onbeperkt aantal organisaties en toepassingsgebieden. Dankzij de Europese DIW kunnen burgers hun identiteit aantonen en de informatie van hun DIW delen, terwijl ze controle houden over hun gegevens.

Een ander zicht:

Adopt

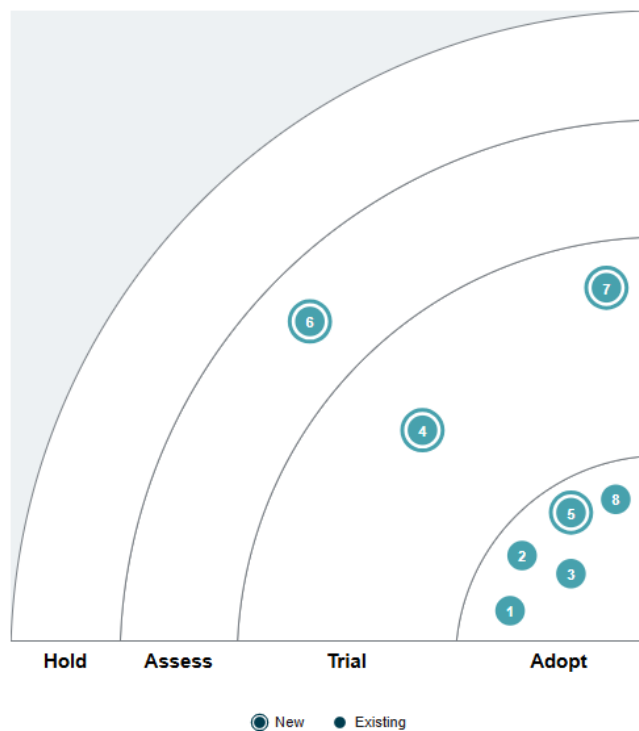
- 1. IT inclusif ▼
- 2. Expérience utilisateur ▼
- 3. Numérique responsable ▼
- 5. IA – LLM use policy ▼
- 8. Conformité aux réglementations (NIS2,DGA,...) ▼

Trial

- 4. Automatisation contact utilisateur (chatbot) ▼
- 7. Participation citoyenne ▼

Assess

- 6. Pièces d'identité digitalisées ▼



Radar Kwadrant Digitale overheid

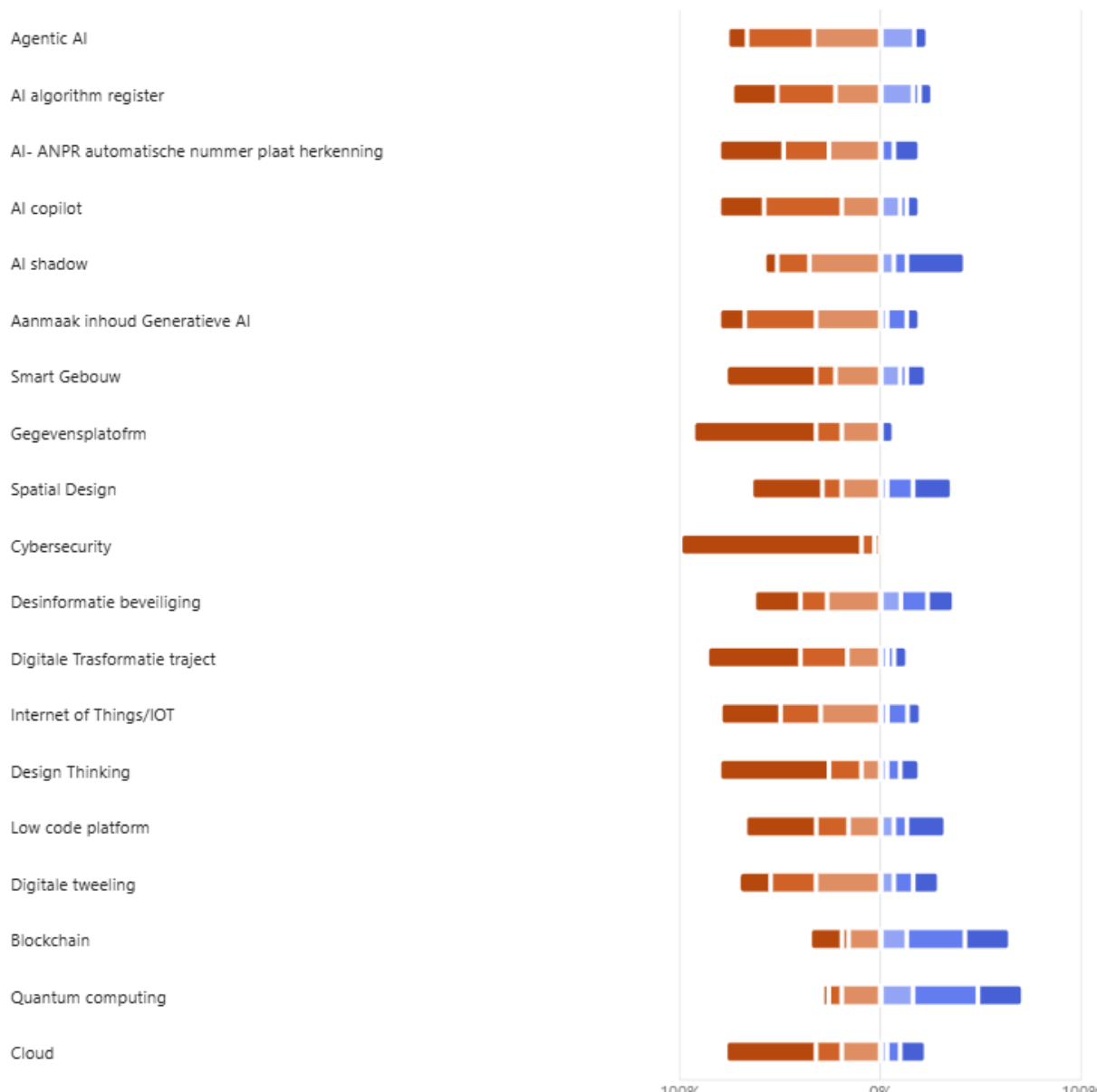
De term digitale overheid verwijst naar trends die een impact hebben op overheidsdiensten. Deze trends hebben vaak een digitale component, gezien de versnelling van technologische trends, maar ook een methodologische component die nodig is in een transformatieproces (zoals design thinking).

- 1 (adopt) Actie - actie ondernemen
- 2 (trial) Studie - verdiepen, voorbereiden
- 3 (assess) Monitoring – in de gaten houden
- 4 (hold) Pauze - buiten beschouwing laten voor de geanalyseerde periode
- 5 buiten perimeter
- 6 geen mening

(samenvatting enquête)

In het kwadrant Action/Adopt vinden we duidelijk het **trio cyberbeveiliging** (de echte nummer 1), gevolgd door **gegevensplatform** en **gebruik van tools in Design Thinking**.

(Radar digitale transformatie overheidssector)



Uitleg bij de gebruikte termen in de Radar digitale overheid:

Adopt	IA-ANPR en andere intelligente technologieën	ANPR (automatic number plate recognition) is een systeem dat via videobeelden nummerplaten kan herkennen, en zo bijvoorbeeld automatisch een parkeerslagboom zal openen in een ondergrondse parkeergarage.
Adopt	Smart Building, GML	Een “smart building”, of slim gebouw integreert een laag digitale tools met vele voordelen, variërend van het optimaliseren van energiebronnen tot het comfort van medewerkers. Voor bedrijven gaat dit gepaard met het verlagen van de operationele kosten terwijl ze hun teams de best mogelijke werkomstandigheden bieden.
Adopt	Gegevensplatform	Een gegevensplatform is een allesomvattende oplossing voor het importeren, verwerken, analyseren en presenteren van gegevens die worden gegenereerd door systemen, processen en infrastructuren van moderne digitale bedrijven.
Adopt	Spatial design	Spatial design verbetert de fysieke wereld digitaal met technologieën zoals augmented reality en virtual reality.
Adopt	Cybersecurity	Cybersecurity bestaat uit technologieën, processen en praktijken die zijn ontworpen om netwerken, computers, applicaties en gegevens te beschermen tegen aanvalle

		schade of ongeautoriseerde toegang. De verdediging tegen krachtige en georganiseerde aanvallers wint aan belang. Ransomware vormt een zorgwekkende trend.
Adopt	Sensorenplatform en Internet of Things (IoT)	Met het Internet of Things (IoT) verbinden vele (elektromechanische) objecten, samen met talrijke sensoren en adapters, zich met het Internet en genereren ze een overvloed aan gegevens. Dit kan een impact hebben op bestaande bedrijven en tegelijkertijd nieuwe mogelijkheden bieden.
Adopt	Aanpak Design thinking	Gebruikt om de ontwikkeling van software, producten en diensten te verbeteren. Empathie voor gebruikers en het verzamelen van informatie over hun behoeften en motivaties zijn cruciaal. Gebruikt voor digitale innovatie waarbij de nadruk wordt gelegd op mensen. Nauw verbonden met mensgericht ontwerpen en aanvaarding van (overheids)applicaties.
Adopt	Low code platform	Software platform waarbij een computerprogramma kan worden aangemaakt zonder grondige kennis van een codeertaal.
Adopt	Cloud	Cloud computing betreft gegevensopslag en verwerking op externe servers op het internet, in plaats van op de eigen computer/server.
Trial	AI: AI agent	Agentische AI-systemen plannen en ondernemen autonoom acties om door de gebruiker gedefinieerde doelen te bereiken. Agentische AI biedt de belofte van een virtuele werkkraft die menselijk werk kan ontlasten en aanvullen.
Trial	AI: Algoritmeregister	Een publieke oplisting van AI-algoritmen die door de overheid worden gebruikt met uitleg over de werking ervan, dit om transparantie te bevorderen.
Trial	Copilot	Activering van Microsoft Copilot in de klassieke bureautica-applicaties
Trial	AI: Creëren van inhoud via generatieve AI	Generatieve of conversatieve AI - waarvan de meest bekende chatGPT - is een computersysteem waarbij een AI getrainde robot of Agent een gesprek kan aangaan met een eindgebruiker op een tamelijk natuurlijk wijze.
Assess	Shadow AI	Of schaduw AI: het gaat om het gebruik van generatieve AI binnen een organisatie voor werkdoeleinden zoals het opmaken van artikelen of het schrijven van code en dit buiten de governance van de IT-afdeling om; dit kan een impact hebben op kritieke bedrijfsinformatie zoals het lekken van gevoelige gegevens, het creëren van niet-conforme softwarecode, enz.
Assess	Desinformatie	Desinformatiebeveiliging is een opkomende categorie van technologie die systematisch vertrouwen onderscheidt en tot doel heeft methodologische systemen te bieden voor het waarborgen van integriteit, het beoordelen van authenticiteit, voorkomen van identiteitsfraude en het volgen van de verspreiding van schadelijke informatie.
Assess	Traject digitale transformatie	Door gebruik te maken van de nieuwste technologieën (zoals het Internet of Things (IoT), data-analyse, machine learning...) kunnen operationele modellen worden veranderd / omgevormd en kunnen nieuwe robuuste digitale modellen worden gecreëerd.
Assess	Digitale tweeling	Een digitale tweeling is een dynamische virtuele kopie van een object, proces, systeem, netwerk, omgeving, of zelfs een persoon, die zich identiek gedraagt aan de tegenhanger in de echte wereld. Een digitale tweeling wordt gebruikt om mogelijke prestatieresultaten en problemen te voorspellen die de tegenhanger in de echte wereld zou kunnen ondervinden. (voorbeeld voor simulatie/voorspelling ramp)
Assess	Blockchain	De blockchain maakt gedecentraliseerde verificatie van de regels en onschendbare opslag mogelijk. Dit kan de afhankelijkheid van de centrale partijen verminderen. De blockchain wordt gepresenteerd als een technologie die de transparantie kan vergroten en frictie kan verminderen, bijvoorbeeld in transformatieprocessen en supply chain management.
Assess	Quantum computing	Gebruik van geavanceerde modellen van kwantummechanica in de computerwetenschappen, dat gevaren kan meebrengen rond IT-systemen op het gebied van beveiliging en cryptografie.

Trial

9. IA: Agent IA	▼
10. IA: Registre d'algorithme	▼
12. Copilot	▼
14. IA: Création de contenu par IA générative	▼

Adopt

11. IA-ANPR et autre technologies intelligente	▼
17. Informatique spatiale	▼
21. Plateforme de senseurs et Internet des objets	▼
23. Plateforme low code	▼
15. Smart Building, GML	▼
16. Plateforme de données	▼
18. Cybersécurité	▼
22. Approche de gestion en design thinking	▼
26. Cloud	▼

Assess

13. Shadow AI	▼
19. Désinformation	▼
20. Parcours Transformation digitale	▼
24. Jumeau numérique	▼
25. Blockchain	▼
27. Quantum computing	▼



Kwadrant Zoom AI

Gezien de populariteit en het belang van AI genereert deze specifieke focus op AI-trends een enorme vraag naar 'trial' of studies.

Het kwadrant Zoom AI laat ons de prioriteiten met betrekking tot AI zien.

- 1 (adopt) Actie - actie ondernemen
- 2 (trial) Studie - verdiepen, voorbereiden
- 3 (assess) Monitoring – in de gaten houden

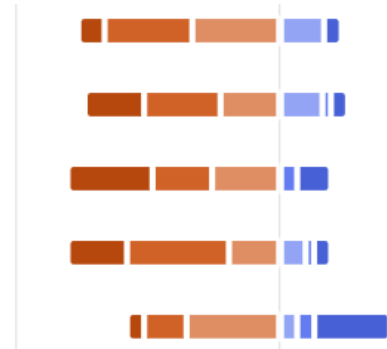
Agentic AI

AI algorithm register

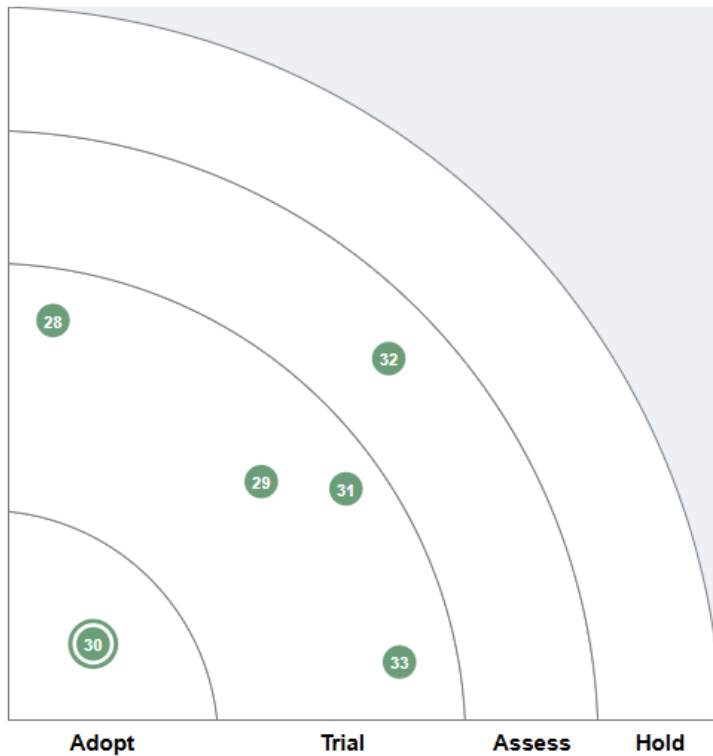
AI- ANPR automatische nummer plaat herkenning

AI copilot

AI shadow



Adopt	AI-ANPR en andere intelligente technologieën	ANPR (automatic number plate recognition) is een systeem dat via videobeelden nummerplaten kan herkennen, en zo bijvoorbeeld automatisch een parkeerslagboom zal openen in een ondergrondse parkeergarage.
Trial	AI: AI agent	Agentische AI-systemen plannen en ondernemen autonoom acties om door de gebruiker gedefinieerde doelen te bereiken. Agentische AI biedt de belofte van een virtuele werkracht die menselijk werk kan ontlasten en aanvullen.
Trial	AI: Algoritmeregister	Een publieke oplijsting van AI-algoritmen die door de overheid worden gebruikt met uitleg over de werking ervan, dit om transparantie te bevorderen.
Trial	Copilot	Activering van Microsoft Copilot in de klassieke bureautica-applicaties
Trial	AI: Creëren van inhoud via generatieve AI	Generatieve of conversatieve AI - waarvan de meest bekende chatGPT - is een computersysteem waarbij een AI getrainde robot of Agent een gesprek kan aangaan met een eindgebruiker op een tamelijk natuurlijk wijze.
Assess	Shadow AI	Of schaduw AI: het gaat om het gebruik van generatieve AI binnen een organisatie voor werkdoeleinden zoals het opmaken van artikelen of het schrijven van code en dit buiten de governance van de IT-afdeling om; dit kan een impact hebben op kritieke bedrijfsinformatie zoals het lekken van gevoelige gegevens, het creëren van niet-conforme softwarecode, enz.



Trial

- 28. IA : Agent IA
- 29. IA : Registre d'algorithme
- 31. Copilot
- 33. IA : Création de contenu par IA générative

Adopt

- 30. IA-ANPR et autre technologies intelligente

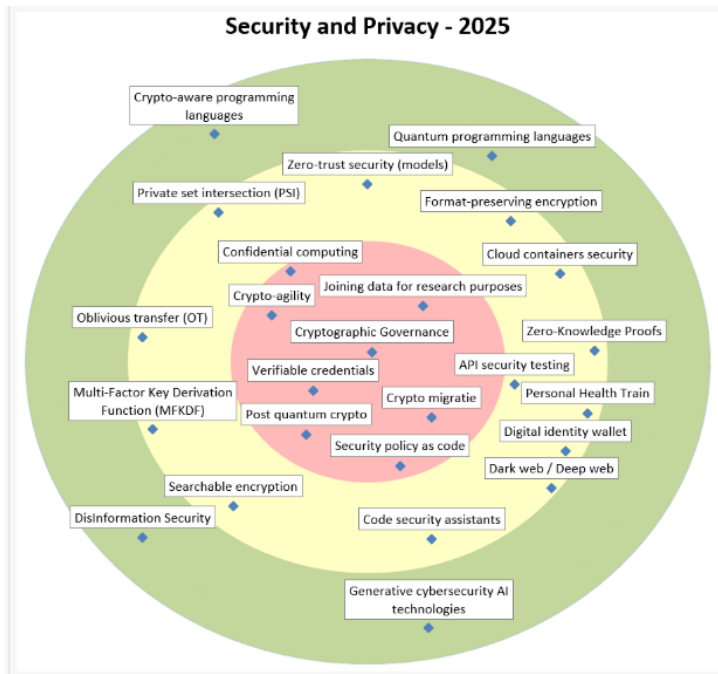
Assess

- 32. Shadow AI

Kwadrant security Smals

Vervolgens voegen we, buiten de enquête, een analyse toe van Smals research m.b.t. het thema (cyber)security.

De legende is hier licht anders, omdat het kwadrant anders gebruikt wordt. Het wordt gebruikt om het werk van de cel research van Smals te prioriteren, dus het deel Adopt staat centraal in de onderzoeksagenda van 2025.



Adopt	Security policy as code	Voor een organisatie of een gewest is het noodzakelijk om concrete aanbevelingen te hebben voor het gebruik van cryptografie. Het formuleren van deze aanbevelingen in de vorm van code vergroot de kennis, automatisering en veiligheid.
Adopt	Crypto migration	Tijdens het volgende decennium zouden kwantumcomputers die relevant zijn voor cryptografie een bedreiging kunnen vormen voor de huidige generatie public key cryptografie. Een voorbereiding op de migratie, die traag en tijdrovend zal zijn, is noodzakelijk.
Adopt	Verifiable credentials	Digitale inloggegevens die de W3C-standaard volgen en de informatie kunnen weergeven die gevonden wordt in traditionele fysieke inloggegevens. Deze inloggegevens zijn een van de aanbevolen standaarden voor de portemonnee voor digitale identiteit van de Europese Unie.
Adopt	Post quantum crypto	Cryptografische algoritmen waarvan wordt aangenomen dat ze veilig zijn tegen een aanval door een kwantumcomputer. De meest relevante zijn de NIST-standaardisatieprocedure en netwerkgebaseerde cryptografie.
Adopt	Confidential computing	Confidential computing (CC) stelt een entiteit in staat om berekeningen op gegevens uit te voeren zonder toegang te hebben tot de gegevens zelf en kan samenwerking tussen wantrouwende organisaties vergemakkelijken. CC kan op gecentraliseerde wijze worden gedaan met homomorfe versleuteling of een vertrouwde uitvoeringsomgeving (Trusted Execution Environment - TEE) of op gedecentraliseerde wijze met beveiligde multiparty-berekening.
Adopt	Crypto-agility	Bij het ontwerpen van cryptografische protocollen is cryptografische behendigheid of crypto-behendigheid het vermogen om te schakelen tussen meerdere cryptografische primitieven. Het vergemakkelijkt de migratie van oude cryptografische protocollen naar nieuwe, zoals van moderne openbare sleutelcryptografie naar post-kwantum cryptografie.

Adopt	Joining data for research purposes	Om hun onderzoek uit te voeren, hebben vorsers vaak toegang nodig tot niet-geaggregeerde gegevens die verspreid zijn over verschillende organisaties. Er bestaan verschillende mogelijkheden om dit te doen op een manier die de privacy respecteert.
Trial	Zero Trust security (models)	Het belangrijkste concept achter Zero Trust is “nooit vertrouwen, altijd verifiëren”, wat betekent dat apparaten standaard niet vertrouwd mogen worden, ook al zijn ze verbonden met een bedrijfsnetwerk zoals het bedrijfs-LAN en zelfs wanneer ze vooraf geverifieerd werden. Ook bekend als 'perimeterloze beveiliging'.
Trial	Format-preserving encryption	Formaatbehoudende encryptie (FPE) beschermt gegevens in rust en in gebruik, en wanneer ze toegankelijk zijn via applicaties, met behoud van de oorspronkelijke lengte en formaat van de gegevens. FPE kan daarom worden gebruikt om gegevens te beschermen op het ogenblik van opname, van opslag in een database of van toegang via datapijplijnen, zonder de bestaande applicaties significant te wijzigen.
Trial	Cloud containers security	Cloud containers security verwijst naar de implementatie van beveiligingsprocessen, tests en controles voor containergebaseerde architecturen in cloudcomputing-omgevingen. Containerbeheertools zoals Kubernetes bieden capaciteiten voor het inzetten, schalen en bewaken van de containerinfrastructuur en kunnen het potentiële aanvalsoppervlak vergroten.
Trial	API security testing	API's vormen een belangrijk aanvalsoppervlak voor webapplicaties. API-beveiligingstests zijn gespecialiseerde beveiligingstests die kwetsbaarheden in API's identificeren. API-beveiligingstests omvatten ook geautomatiseerde API-detectie om te helpen een API-inventaris bij te houden.
Trial	Digital Identity Wallet	De portemonnees voor digitale identiteit (DIW) maken het delen van identiteitsgegevens en allerlei soorten attesten mogelijk tussen een willekeurig aantal organisaties en use cases. Dankzij de Europese DIW zouden burgers hun identiteit moeten kunnen aantonen en de informatie van hun DIW delen, terwijl ze controle houden over hun gegevens.
Trial	Code security assistants	Code security assistants maken gebruik van de capaciteiten van generatieve AI-modellen en statische analyse om ontwikkelaars te helpen kwetsbaarheden in de beveiliging van een bepaalde codebasis te identificeren, analyseren en beperken. Ze kunnen helpen kwetsbaarheden vroegtijdig te identificeren door op te treden als geautomatiseerde code reviewers. Ze zouden ook kunnen helpen bij het automatiseren van bepaalde aspecten van beveiligingscontroles die anders wellicht handmatige inspanning vereisen. Ze kunnen ook bijstaan bij het genereren van code met de beste beveiligingspraktijken.
Trial	Multi-Factor Key Derivation Function (MFKDF)	Er bestaan wachtwoordgebaseerde sleutelafleidingsfuncties om een cryptografische sleutel af te leiden uit een wachtwoord.
Trial	Searchable encryption	Doorzoekbare symmetrische versleuteling (SSE) is een vorm van versleuteling waarmee men efficiënt kan zoeken in een verzameling versleutelde documenten of bestanden zonder deze te kunnen ontsleutelen.
Trial	Oblivious transfer (OT)	Een onbewust overdrachtsprotocol (OT) is een type protocol waarbij een afzender een van mogelijk vele stukjes informatie naar een ontvanger verzendt, maar niet weet welke informatie (als die er al is) is overgedragen.
Trial	Private set intersection (PSI)	Bij Private Set Intersectie kunnen twee partijen die sets bezitten versleutelde versies van die sets vergelijken om de intersectie te berekenen. In dit scenario onthult geen van beide partijen iets aan de andere partij, behalve de elementen van de intersectie.
Trial	Personal Health Train	De Personal Health Train (PHT) heeft als doel om gedistribueerde gezondheidsgegevens met elkaar te verbinden en waarde te creëren door het gebruik van bestaande gezondheidsgegevens voor burgers, de zorgsector en het wetenschappelijk onderzoek te vergroten.
Trial	Zero-Knowledge Proofs	In de cryptografie is een zero-knowledge-proof een protocol waarmee de ene partij (de bewijsvoerder) aan een andere partij (de vericator) kan bewijzen dat een bepaalde bewering waar is, terwijl er wordt vermeden dat aan de vericator informatie wordt doorgegeven die verder gaat dan slechts het feit dat de bewering waar is.

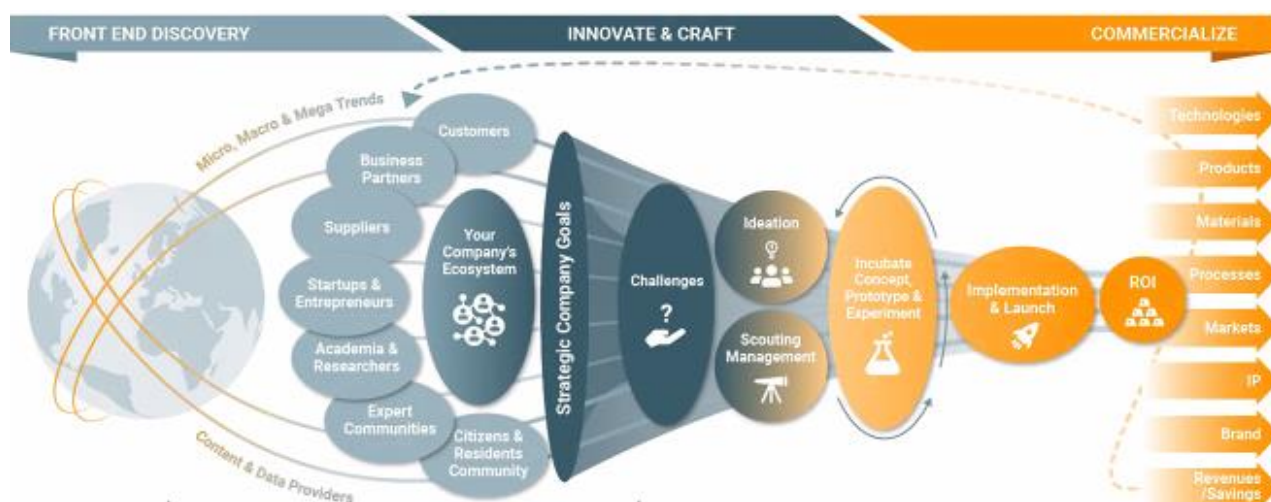
Trial	Dark web / Deep web	Het Deep Web omvat internetcontent die niet geïndexeerd is door zoekmachines, terwijl het Dark Web een onderdeel is dat toegankelijk is via speciale browsers en vaak wordt geassocieerd met anonimiteit en criminele activiteiten. Inzicht hierin is belangrijk voor cybersecurity, wetshandhaving en toegang tot niet-geïndexeerde informatie.
Assess	Quantum programming languages	Naarmate kwantumcomputers krachtiger worden, wordt het steeds relevanter om kwantumalgoritmen te kunnen schrijven. Dit is gebaseerd op andere principes dan klassieke talen en vereist daarom een nieuwe set vaardigheden.
Assess	Generative cybersecurity AI technologies	Generatieve AI-technologieën in cybersecurity zijn niet-traditionele methoden voor het verbeteren van analysemethoden in systeem- en applicatiebeveiligingstechnologie (bv. het analyseren van gebruikersgedrag, het verbeteren van de detectie van potentiële aanvallen vanuit systeemlogs).
Assess	DisInformation Security	Desinformatie ondermijnt het vertrouwen, manipuleert de publieke opinie en bedreigt de maatschappelijke stabiliteit en veiligheid. Beveiliging tegen desinformatie richt zich op het opsporen en bestrijden van de opzettelijke verspreiding van valse informatie, met behulp van een verscheidenheid aan technologieën.
Assess	Crypto-aware programming languages	Bij het ontwikkelen van beveiligde, krachtige cryptografische software wordt de programmeur geconfronteerd met een breed gamma aan problemen. In tegenstelling tot klassieke programmeertalen bieden cryptografisch-bewuste programmeertalen de programmeur ondersteuning hiervoor.

INTERNE OPVOLGING PARADIGM

De Radar voor digitale transformatie overheidssector en klantgerichtheid is een monitoringtool om trends en prioriteiten op het gebied van digitale transformatie te volgen.

Het stelt gebruikers in staat opkomende trends te **visualiseren** en deze te prioriteren op basis van hun belang. De Radar voor digitale transformatie is een momentopname die regelmatig kan worden bijgewerkt om de evolutie van de prioriteiten en de daaruit voortvloeiende acties te volgen.

Deze trends- en prioriteitenradar is de vierde editie (editie Q1 2025).



Illustratie van het innovatietraject: (bron Qmarkets innovation) – De Radar bevindt zich aan de linkerkant, in het "front-end discovery" gedeelte, waar trends worden geanalyseerd. Vervolgens is het de bedoeling om innovatieprojecten op te zetten in het "innovate and craft"-gedeelte, ideeën te

genereren, scouting te beheren (zoeken naar bestaande start up applicaties), een lab te creëren om benaderingen in een experimentele omgeving te testen (sandbox), om daarna over te gaan naar een meer algemene aanpak voor lancering en gebruik.

OPVOLGING op gewestelijk niveau

De Radar en de visualisatie ervan kunnen worden gebruikt om bepaalde trends te prioriteren en initiatieven in innovatie te structureren.

Het ADOPT-kwadrant bestaat uit thema's die op het niveau van de gewestelijke governance moeten worden aangepakt. Het kan gebeuren dat in het ADOPT-kwadrant thema's worden gevonden die nog niet zijn aangesneden, terwijl dat volgens de monitoring wel het geval zou moeten zijn. Een thema als cybersecurity kan dan worden opgehelderd tijdens de **Ontmoetingen rond Digitale Technologie** en er kan een actieplan en structuur worden opgezet in de **governance en de architectuur + het Bureau voor digitale aankopen**.

Het TRIAL- of STUDY-kwadrant vertegenwoordigt belangrijke trends die de komende 2-3 jaar al dan niet de ADOPT-fase bereiken. Deze trends kunnen verkend worden tijdens een editie van de Ontmoetingen rond Digitale Technologie en kunnen worden opgenomen in een portfolio van innovatieprojecten (innovation portfolio), voor gefinancierde projecten (verkennende trajecten/POC) die worden beheerd in een gewestelijk lab zoals het C_lab; ondersteund door innovatieve overheidsopdrachten (BDA) voor validatie/experimenten.

Het ASSESS, MONITORING-kwadrant stelt entiteiten in staat om trends te verkennen via actieve monitoring en deze te delen (bv. samenvattingen van bezoeken aan beurzen / lezingen / studies / kennisbibliotheek).

Het HOLD-kwadrant vertegenwoordigt trends die niet worden gemonitord/opgevolgd.

Hoe werkt dit en waar past het binnen de waardecreatiecyclus van Paradigm?

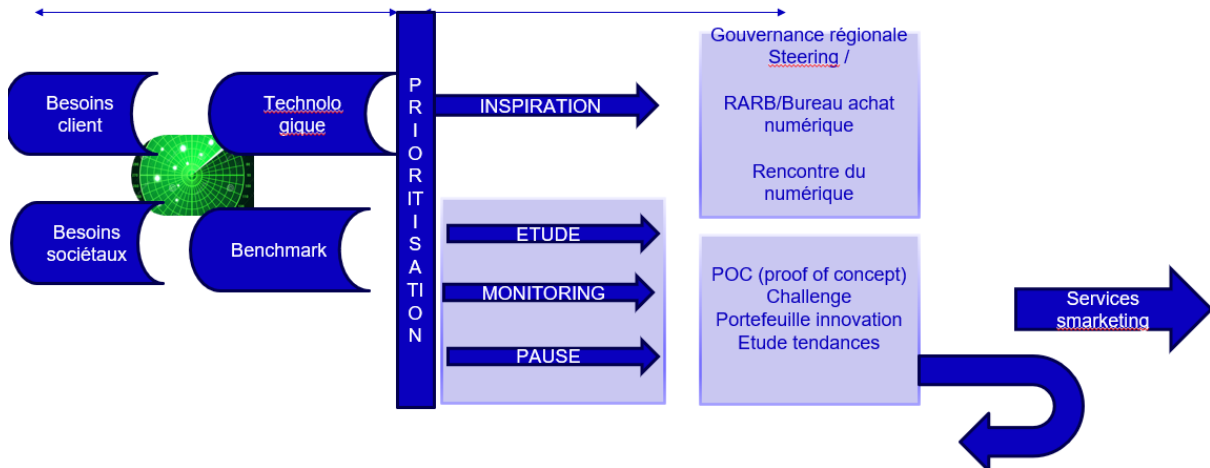
De Trends Radar is een van de aspecten die gestructureerde monitoring bij Paradigm mogelijk maakt.

Deze monitoring bestaat uit externe informatie zoals rapporten en technologische trends, evenals zwakkere signalen die intern opborrelen vanuit overheidsinstanties, klanten en maatschappelijke behoeften. Er wordt ook gekeken naar vergelijkbare steden en hun behoeften/projecten die werden uitgerold.

Op basis van deze monitoringtrends en de prioritering ervan zal de radar de volgende stappen beïnvloeden:

1. Filtering van de Radar en afstemming op de opdracht en het strategische plan van Paradigm.
2. Tagging voor concrete acties die moeten worden uitgerold in de innovatieportfolio beheerd door de pijler Digitale Transformatie DT.
 - Uitrol van acties die een scherpere monitoring vereisen (deelname aan conferenties, lezingen, enz.).
 - Uitrol van proof of concept/verkennende trajecten (met als tool de omkadering en de facilitering van C_lab sandbox, de betrokkenheid van de actoren van het ecosysteem, bestaande partnerschappen, integratie in een Europees onderzoeksproject, enz.).
 - Uitrol van tests van diensten op transversale wijze met een testklant.

- o Deze acties worden gekenmerkt door een duidelijke beperking in de tijd en een belangrijke evaluatie ("lessons learned") na elk experiment omdat het proof of concept, bijvoorbeeld, eindigt met een vrij snelle evaluatie.
3. Raming van de impact van bepaalde trends op de gewestelijke architectuur.
 4. Creatie van diensten en integratie in de Smarketing-roadmap, in lijn met de trends en de vraag van klanten.
 5. Een nieuwe editie naar aanleiding van de Radar en een herstart van de prioritering en monitoring.



METHODOLOGIE

De Radar werd als volgt opgezet:

- Interne en externe enquête (gewestelijke governance) Paradigm november 2024
 - Document met bedrijfs-/IT-trends (Gartner en anderen)

Figure 1: Gartner Top Technology Trends in Government for 2024

Realize risk	Reimagine value	Evolve operations
<ul style="list-style-type: none"> • Adaptive security 	<ul style="list-style-type: none"> • Digital identity ecosystems • AI for decision intelligence 	<ul style="list-style-type: none"> • Digital platform agility • Programmatic data management

- Uitwisseling met het Digital Transformation team
- Met dank aan Smals research voor de methodologische uitwisselingen <https://www.smalsresearch.be/> en de editie 2025: Research Radar 2025 | Smals Research

Enquête met	antwoorden
• Een deelnemer van een regionale Brussels administratie buiten Paradigm	5
• Een deelnemer van Paradigm	19
• Een deelnemer van Iristeam - IT cells	7
• Een deelnemer van gemeente/OCMW	0

- Inspiratie uit andere meer technologische radars Thoughtworks <https://www.thoughtworks.com/radar> en Devoteam <https://techradar.devoteam.com/>

[en Zalando https://opensource.zalando.com/tech-radar/](https://opensource.zalando.com/tech-radar/)
<https://techradar.devoteam.com/>,

- [Stad Amsterdam Tech Radar https://www.amsterdam.nl/innovatie/digitalisering-technologie/tech-radar/](https://www.amsterdam.nl/innovatie/digitalisering-technologie/tech-radar/)
- Gartner 2024 Top Technology and Business Trends in Government
- Gartner 2025 Top Tech trends [2025-top-tech-trends-ebook.pdf](#)
- Techtrends report go.infotech.com/it-tech-trends-2025-report
- Tech watch interoperable Europe <https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/document/public-sector-tech-watch-adoption-ai-blockchain-and-other-emerging-technologies-within-european>
- Focus AI <https://www.fastcompany.com/91254053/25-experts-predict-how-ai-will-change-business-and-life-in-2025>
- Livre blanc "Tendances Technologiques 2025" - SFEIR <https://drive.google.com/file/d/1aziGjjU7ZkDEflgXxdOp16S4jd6BLZQd/view>
- Belgian Digital Economy 2024 <https://economie.fgov.be/nl/publicaties/belgian-digital-economy-0>

OVER

Voor alle opmerkingen, voorstellen tot verbetering of om deel te nemen aan de volgende editie voorzien voor de maand juni 2025:

tdelestre@paradigm.brussels (lead innovation Paradigm - Tanguy De Lestré - 0486384618)

De Radar is een monitoringtool die Paradigm aanbiedt in het kader van zijn innovatiewaarde, van zijn opdracht vastgelegd in de Ordonnantie Paradigm, en wordt ondersteund door verkennende activiteiten (experimenteertraject en faciliterende dienst).