

Work sample

Agentic Data Office

Work sample, anonymised —
governed MCP gateway and
controlled autonomy

Case summary, then deck

Problem

High-volume Data Office work was repetitive, inconsistent and hard to scale — while agent autonomy created new risks

Quality investigation, anomaly analysis and data-asset querying were repetitive, inconsistent and difficult to scale.

Agent autonomy created risks of exfiltration, irreversible actions, weak traceability and uncontrolled deployment.

The challenge: prove useful agent patterns without confusing technical feasibility with ROI, or allowing unsafe production changes.

Action

Lead R&D & Prototyping AI / advisor — the Data Office designed as a governed MCP gateway, with a six-week PoC under pass/fail criteria

Mapped processes and designed the Data Office as a governed MCP gateway across Dataiku, Starburst, BigQuery, dbt and Collibra.

Standardised agent and skill specifications: least-privilege boundaries, read-only defaults, cost/row ceilings, pre-validation, human-in-the-loop controls, journaling, rollback, assistant-to-autonomous autonomy tiers.

Defined a six-week PoC with pass/fail tests for MCP selection, governed writes and A2A delegation; demonstrated contested controls live, held a zero-leakage boundary, used steering governance to reject unsupported ROI claims.

Prioritised high-volume, reversible, evaluable pilots; deferred pipeline code generation until replay and reference-output testing existed; kept model deployment human-led.

Result

Reference framework delivered, all PoC criteria passed, three pilots prioritised — ROI measurement reserved for the pilots

Reference framework: skill/MCP catalogues, agent portfolios, dependency matrices, governance controls, red-team cases and a V0–V3 industrialisation roadmap.

PoC: selection across 15 natural-language questions met the 80% threshold with zero out-of-perimeter access and sourced answers; governed writes enforced human validation, cost/row ceilings, journaling and rollback; A2A delegation returned contracted results.

Pilots prioritised for analytics, quality control and catalogue/lineage.

ROI measurement reserved for subsequent pilots rather than invented from synthetic-data testing.

Work in Progress

Agentic Data Office

L'IA Agentique au service de la chaîne
de valeur de la data

R&D et Prototypage IA

Synthèse

Le Data Office peut devenir le **hub agentique de la data de l'entreprise**. Une feuille de route en **4 phases, sur 12 semaines**, pour l'amorcer.

L'enjeu

Une part importante de l'activité du DO (tâches chronophages, à jugement structurable, dispersées en silos) **peut être outillée par l'agentique**, au service de la chaîne de valeur de la donnée.

Faire du DO le hub agentique de la data :

- **gouverner** la façon dont tous les agents accèdent à la donnée (MCP gateway),
- **fournir** ses propres agents, réutilisables par les autres directions (A2A).

Construire la feuille de route en 4 phases : 1. Recensement (skills & MCP), 2. Portefeuille d'agents, 3. Analyse de valeur 4. Priorisation & planification

- **ancrer la feuille de route sur l'orga actuelle du DO**
- **co-construction** avec métiers sur **12 semaines**.

- Catalogues skills & MCP
- portefeuille d'agents
- proposition de valeur

● **feuille de route chiffrée (macro) séquencée en paliers V0→V3**

Projet pilote réutilisable pour d'autres directions du Groupe.

- **Cadrage uniquement** : on s'arrête à la feuille de route, avant l'implémentation.
- **Estimation dérisquée** : l'essentiel du travail est indépendant de la plateforme retenue, et beaucoup de briques agentiques existent déjà (Gemini, Dataiku, Collibra, dbt/BigQuery/Starburst).
- **Une seule décision structurante** à trancher en amont : la plateforme d'agents.

SOMMAIRE

01 Vision : l'agentique au service de la chaîne de valeur Data

02 Bâtir la feuille de route agentique

03 Phase 1 : Recensement des skills et MCP

04 Phase 2 : Définition du portefeuille d'agents

05 Phase 3 : Analyse de la valeur agentique

06 Phase 4 : Priorisation et planification

07 Next steps

08 Annexes

01

**Vision : l'agentique au
service de la chaîne de
valeur Data**

Pourquoi maintenant

Trois forces convergent : un besoin réel, une technologie mûre sur une stack déjà prête, et une fenêtre stratégique à saisir

Besoin réel

- Tâches chronophages nécessitant une méthode et un jugement structuré¹
- Expertise dispersée, tacite et peu capitalisée - reposant parfois sur des prestataires externes
- Time-to-data long, alors que la demande métier d'autonomie croît.
- Exigence de traçabilité et de contrôle (RGPD, ACPR) de plus en plus forte.

Faisabilité nouvelle

- Les agents savent désormais raisonner, planifier et utiliser des outils.
- MCP² rend les outils **existants** invocables par des agents.
- La stack data est déjà "Agent-ready" : dbt, BigQuery, Starburst, Tableau, Dataiku, Collibra.
- Le socle est déjà présent : Plateforme agentique Gemini ou Dataiku, gouvernée par Collibra.

Fenêtre stratégique

- Chaque direction peut déployer ses propres agents, mais sans cadre, l'accès à la donnée se fera en ordre dispersé.
- Se positionner **maintenant** comme le hub qui gouverne cet accès (v. le subir ensuite).
- Des premiers cas d'usage à fort impact et faible risque (lecture seule) sont possibles rapidement.

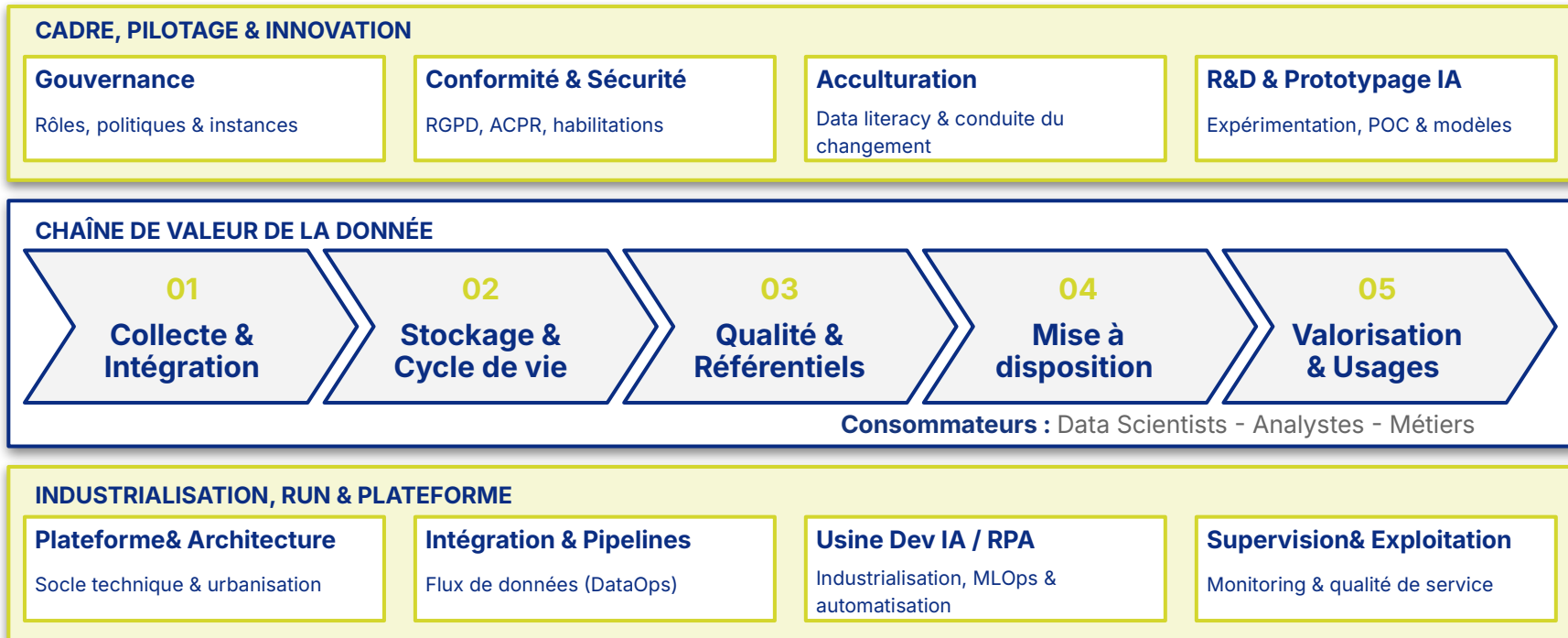
(1) investigation qualité, documentation, dev. pipelines, requêtes et rapports)

(2) MCP (*Model Context Protocol*) est un standard ouvert permettant d'invoquer des outils par des agents

1
2

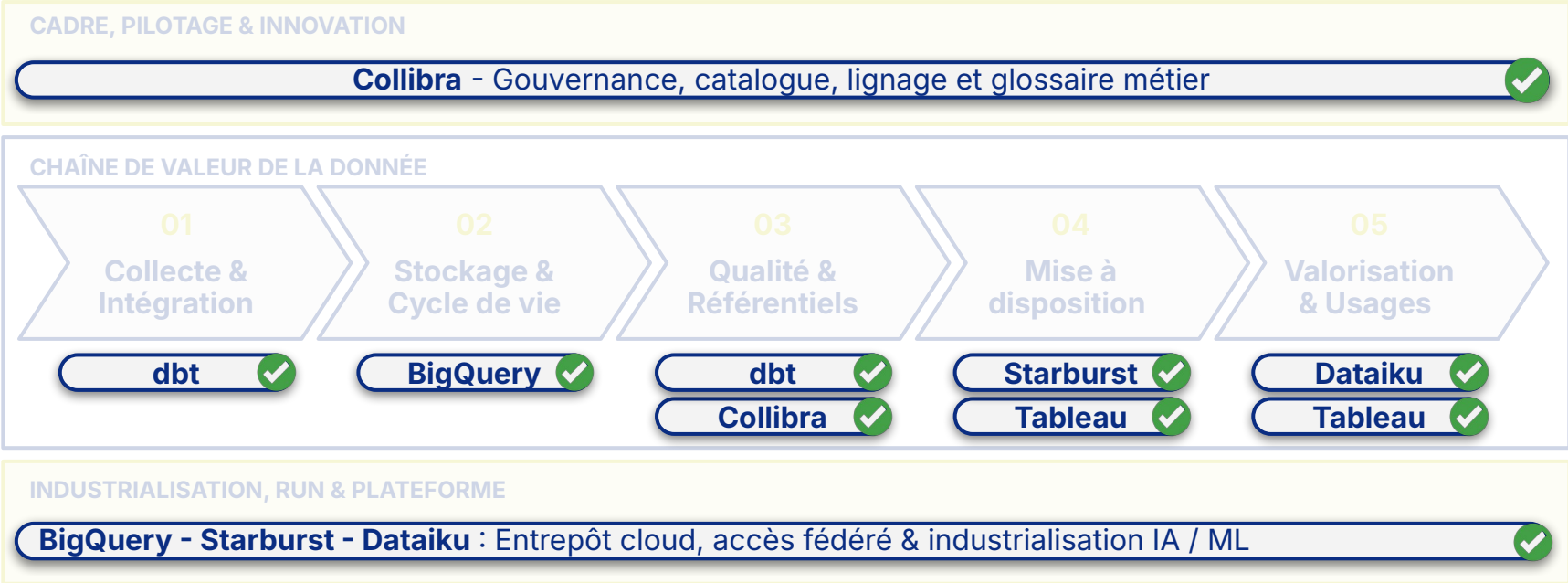
La chaîne de valeur de la donnée du Data Office

L'agentique permet de créer de la valeur à chaque maillon : de la collecte à la valorisation



1 Une stack data "agentique-ready" de bout-en-bout

La stack data est agentique-ready et outille toute la chaîne de valeur — chaque brique est mobilisable par les agents.



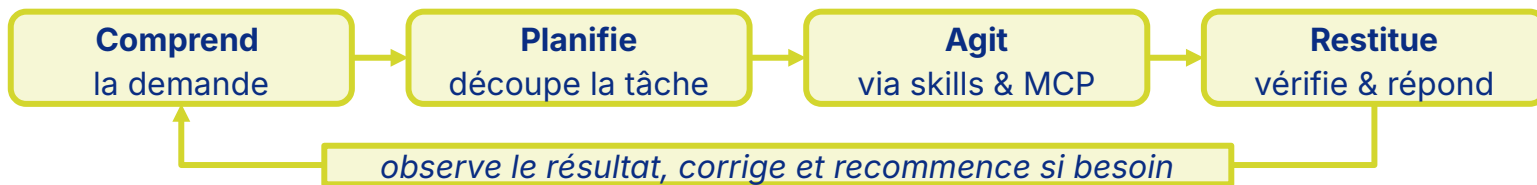
Lecture : chaque outil est positionné sous son maillon principal de la chaîne de valeur Data mais peut s'étendre en réalité sur les maillons voisins.

1.4 Qu'est-ce qu'un agent et que sait-il faire ?

Un agent comprend, planifie, agit et vérifie en boucle pour synthétiser, surveiller, investiguer, générer... au service des process du DO

Comment un agent procède

Les étapes d'exécutions d'un agent



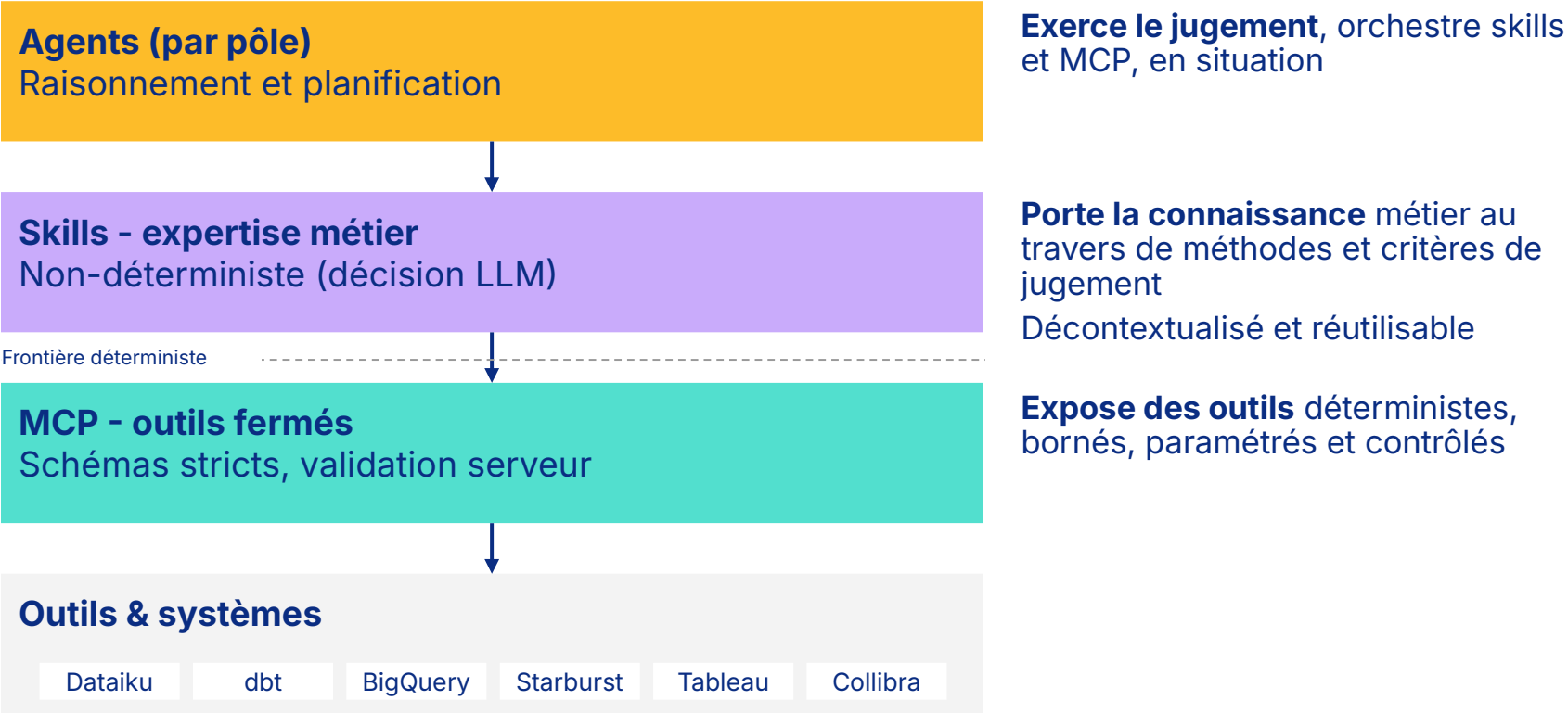
Ce qu'un agent sait faire

Les 8 catégories d'opportunités agentiques



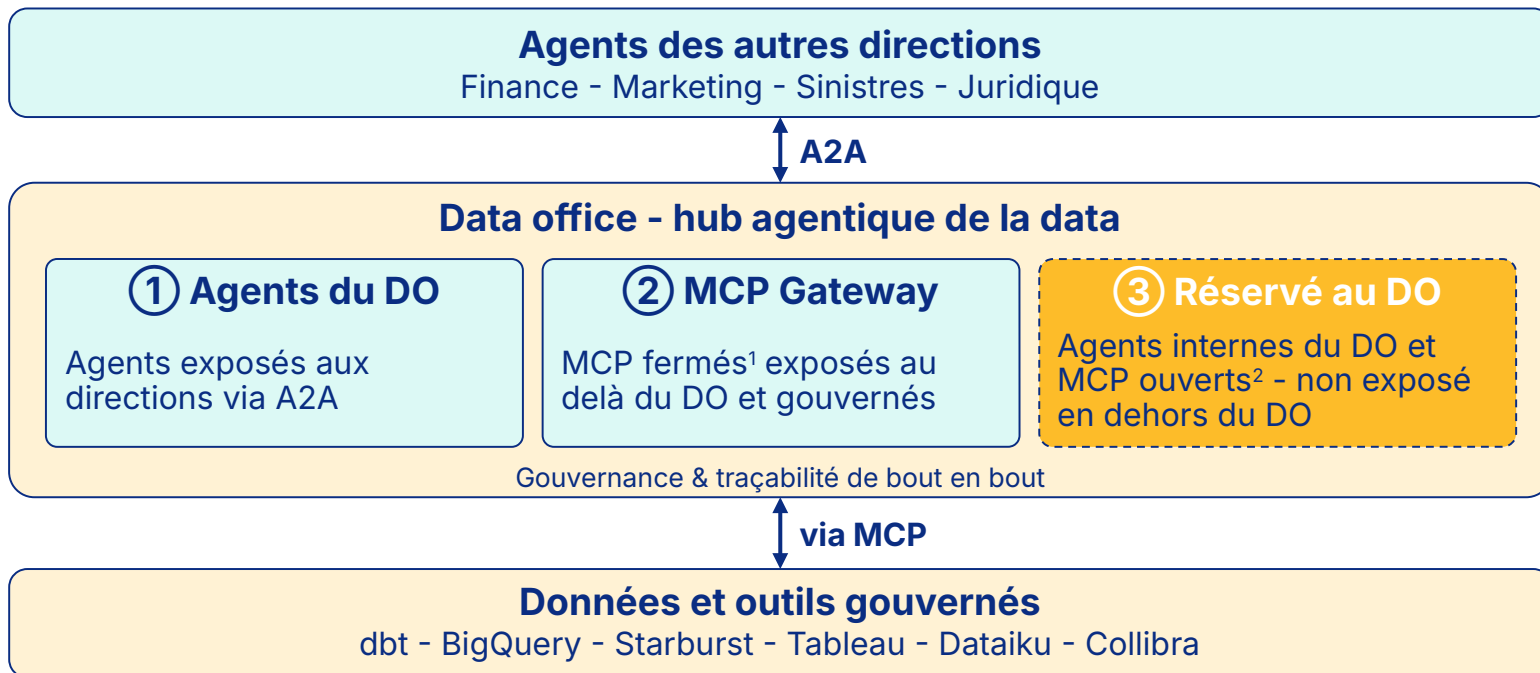
1 5 Trois briques : MCP expose, Skills portent, Agents exercent

Une frontière déterministe structure l'architecture



1.6 Vision cible : le DO, hub agentique de la data de l'entreprise

Deux facettes : gouverner l'accès agentique à la donnée (MCP gateway) et fournir ses propres agents aux autres directions (A2A)



(1) MCP n'exposant qu'une surface minimale et verrouillée (e.g. lecture seule, ou écriture simple, réversible, à champs validés). Faible latitude, risque minimal.

(2) MCP exposant une surface élargie : opérations métier à effet, écritures sensibles voire irréversibles. Latitude plus importante, risque opérationnel réel, expertise requise pour le concevoir et l'opérer.

02

Bâtir la feuille de route agentique

4 phases, ancrées sur l'organisation du DO, en 12 semaines

2.

Une démarche en quatre phases pour établir la feuille de route agentique

Chaque phase alimente la suivante : des briques aux agents, des agents à leur valeur, de la valeur à la trajectoire chiffrée



(1) Le filtre a 4 sorties : agent / automatisation / humain / différé

(2) gain métier, fréquence/volume, criticité & conformité, alignement stratégique

(3) évolution des rôles & du mode opératoire, conduite du changement

2.

Équipe cœur, pôles contributeurs, COPIL

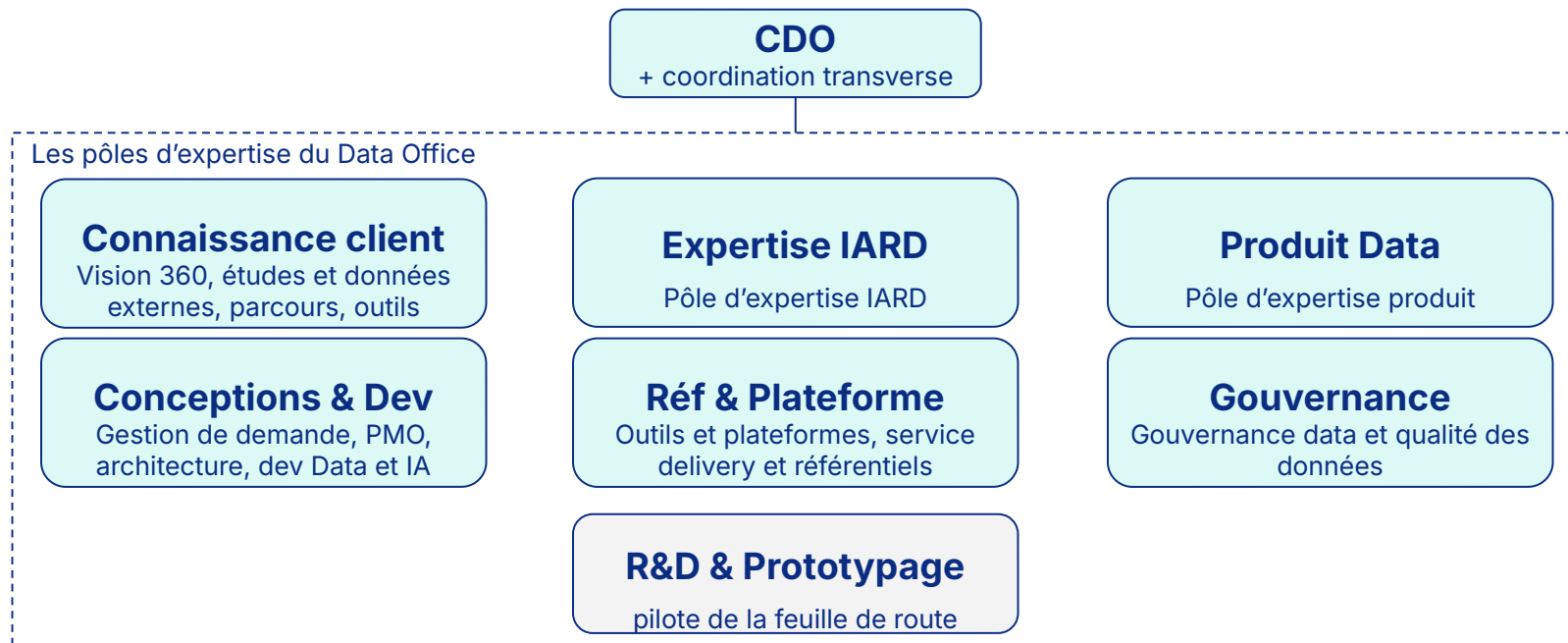
L'expertise vient des pôles, l'équipe cœur consolide

Équipe cœur	Équipe R&D & Prototypage IA pilote le cadrage, l'analyse, la synthèse, la consolidation et la production des livrables.
Contributeurs par pôle	Manager du pôle et 1-2 référents de son équipe, mobilisés en atelier DO agentique et aux points de validation .
Sponsor / COPIL	CDO et équipe de direction du Data Office - valident les jalons et arbitrent
Durée	12 semaines
Cadence	4 x séries de 2-3 thèmes traitant de thèmes métier DO conjoints (limiter le parallélisme), 1 ateliers DO Agentique par thème, Fonctionnement itératif (une passe large puis approfondissement).
Fonctionnement	Co-construction de la feuille de route avec les pôles du Data Office pour favoriser l'appropriation - l'expertise vient des pôles.
Livrables	Catalogues skills/MCP, fiches, portefeuille d'agents, matrices de dépendances, proposition de valeur, feuille de route Objectif de réutilisation ce qui est bâti par le DO pour généralisation autres directions le Groupe

3.

L'organisation du DO : là où réside l'expertise

Chaque pôle et chaque équipe porte des skills, des règles et du jugement - c'est la matière du recensement, pôle par pôle.



L'expertise vit dans chaque pôle et chaque équipe : la matière doit être collectée et analysée pour définir les skills, règles, jugement du DO agentique

Dix ateliers pour couvrir les pôles d'expertise

10 ateliers calés sur les pôles/équipes

#	Atelier	Pôle	Mission
1	Connaissance & parcours client	Connaissance Data Client	Construire la vue unifiée du client et optimiser les parcours multicanal
2	Product Mgmt Outils Data	Connaissance Data Client	Piloter le cycle de vie et l'usage des outils data mis à disposition des métiers
3	Expertise Data IARD	Expertise Data IARD	Apporter l'expertise data sur la tarification, le risque et la sinistralité des produits IARD
4	Produits Data	Produits Data	Concevoir et industrialiser les produits data exposés aux métiers (jeux de données, services)
5	Pilotage demande & projets	Conception et Développement Data & IA	Qualifier, prioriser et planifier les demandes data, et suivre les projets
6	Architectures et offres services data	Conception et Développement Data & IA	Définir les architectures de référence et les offres de services data
7	Développement Data	Conception et Développement Data & IA	Construire et maintenir les pipelines et traitements de données
8	Plateforme & delivery	Référentiels et Plateforme Data	Opérer la plateforme et livrer/exploiter les services data (fiabilité, coûts)
9	Référentiels	Référentiels et Plateforme Data	Gérer les référentiels et données de référence (client, tiers, produit)
10	Qualité & gouv. des données	Gouvernance Data	Définir et contrôler la qualité, la conformité et le lignage des données

3.

Déroulé standard d'un atelier métier DO

Capter processus, expertise et opportunités en une séance

Durée cible c. 3h, co-construction interactive

Participants : équipe cœur + manager entité / 1-2 référents.

Avant l'atelier : l'équipe cœur pré-remplit la cartographie pressentie des processus et quelques cas d'usage candidats

Agenda

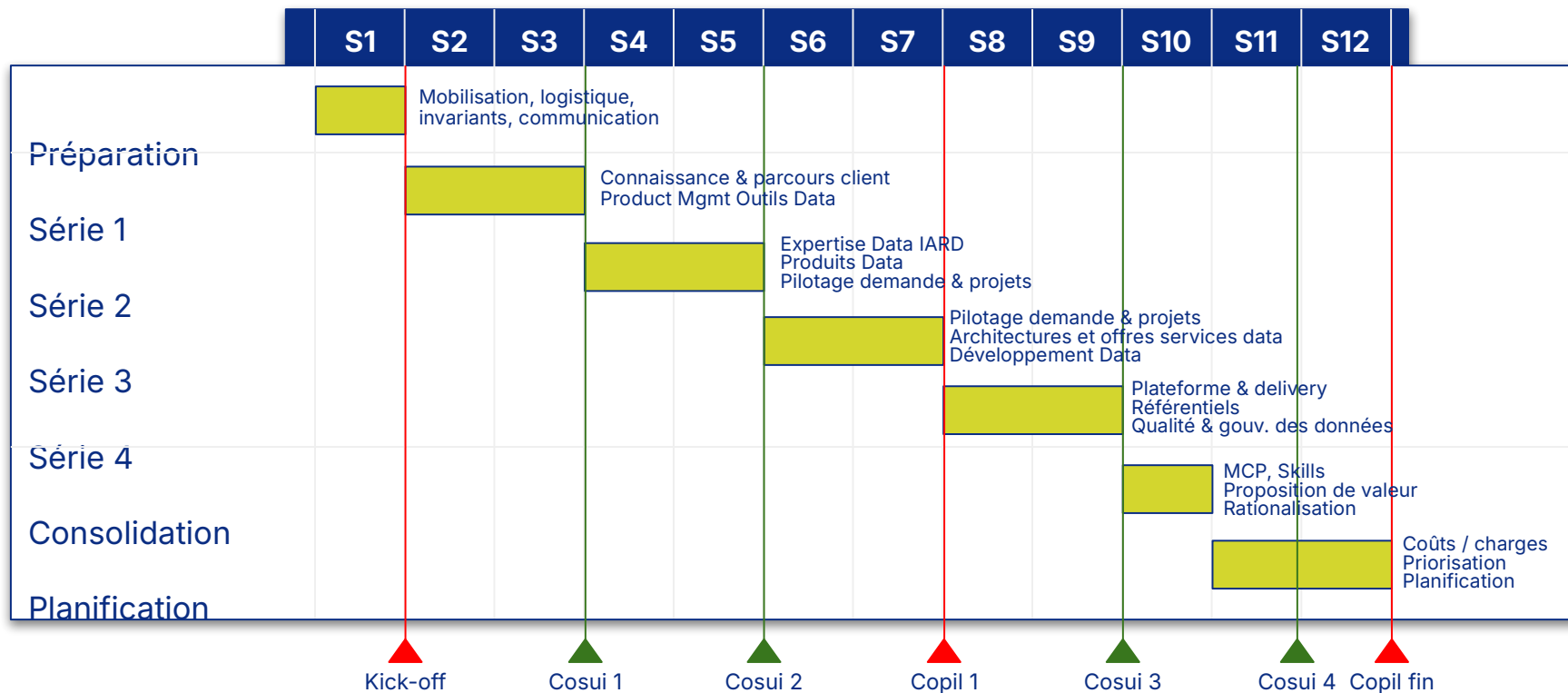
1. **Cadrage & objectifs** (~10 min) : contexte, concepts clés et terminologie agentique
2. **Validation des processus** (~30 min) : confirmer/compléter la liste des processus de l'équipe
3. **Capture d'expertise** (~50 min) : le cœur de l'atelier. Pour les processus clés, faire ressortir : règles métier, pièges, risques, jugement requis, points de contrôle, seuils d'escalade
4. **Identification des opportunités agentiques** (~45 min) : passer les processus au crible (synthèse, surveillance, investigation, triage, simulation, génération, self-service, orchestration). Pour chaque cas d'usage qui émerge : ce que ferait l'agent, les données/systèmes (→ MCP), le jugement (→ skill), l'autonomie pressentie, le point d'escalade.
5. **Qualification & priorisation à chaud** (~25 min) : trier rapidement les candidats (agent / automatisation / humain / différé), repérer les évidents et les « à creuser », noter la valeur perçue (sans chiffrage).
6. **Synthèse & suite** (~15 min) : récapituler décisions, actions, points à valider, calendrier de restitution.

Sorties de l'atelier : liste de processus validée, matière d'expertise par skill et identification des MCP sous-jacents, liste de cas d'usage candidats qualifiés à chaud.

Après l'atelier (équipe cœur) : formalisation - fiches skill, caractérisation des MCP, fiches cas d'usage - puis boucles de validation itératives avec l'équipe.

2.6 Calendrier de 12 semaines et 4 séries d'ateliers

Vagues de pôles + consolidation + feuille de route



Phase 1 : Recensement des skills et MCP

Approche - principes - livrables

3.

Approche

Entretien pôle → approfondissement N4 → pré-filtre (max 5 processus/thème)

1. Pour chaque Thème couvert, repérer les processus clés (activités métier récurrentes) au travers d'un entretien préalable avec chaque responsable de pôle / expert - ne retenir que l'essentiel et pas viser l'exhaustivité
2. Approfondissement sur process niveau 4 (enchaînement de tâches), et appliquer un préfiltre pour ne retenir que max 5 processus N4 prioritaires à analyser par thème - Pré-filtre d'entrée pour prioriser / guider les arbitrages :

Volume	Fréquence, échelle
Efficacité actuelle	Chronophage, source d'erreurs, de goulots ou de plaintes
Jugement structurable	Jugement répétitif et codifiable (discriminant agentique)
Multi-étapes / multi-sources	Enchaînement v. tâche unitaire
Faisabilité	Données / système accessibles, expertise formalisable

3. Qualifier chaque processus retenu pour en détailler les caractéristiques pour l'analyse agentique
 - Processus (formulé verbe + objet : « investiguer une anomalie qualité », « simuler un tarif »)
 - Déclencheur (ce qui le lance)
 - Finalité, livrable, KPI
 - Données & systèmes mobilisés ⇒ servira à révéler les **MCP** candidats
 - Décisions & jugements requis ⇒ servira à révéler le **skill** candidat
 - Fréquence / criticité → servira à prioriser

3.
2.

Principe : arbitrer skills v. MCP

Jugement = skill et opération outillée = MCP

Skill ou MCP ? Le critère du déterminisme permet de trancher

Skill : non-déterministe

méthode & critères de jugement
le LLM décide en situation

→ interpréter, arbitrer
ex. tarifier un risque IARD

Jugement = skill

MCP : déterministe

opération bornée & paramétrée
même entrée → même sortie

→ opération outillée
ex. lancer un job dbt

Opération outillée = MCP

3.

La fiche skill

Le template qui codifie l'expertise réutilisable

#	Champ	Consigne
1	Identité	Nom (slug domaine-objet), pôle propriétaire + initiales manager, version/date, statut (brouillon / validé / prod)
2	Objet	Ce que le skill permet à l'agent de faire
3	Déclencheurs	<i>invoquer si... / ne pas invoquer si...</i> (anti-périmètre, pour éviter les recouvrements entre skills)
4	Expertise encodée	concepts & définitions clés, règles métier, pièges connus
5	Méthodologie	étapes de raisonnement ordonnées
6	Données & classification	données manipulées + sensibilité / périmètre RGPD
7	MCP mobilisés	MCP + opérations utilisées (toujours déterministes)
8	Garde-fous & conformité	interdits explicites + contraintes réglementaires
9	Escalade humaine	Déclencheur → destinataire (rôle)
10	Critères de réussite (éval)	Comment juger que la réponse du skill est bonne
11	Limites & dépendances	limites connues, skills liés

La caractérisation MCP par outil

Chaque outil exposé en opérations bornées et contrôlées.

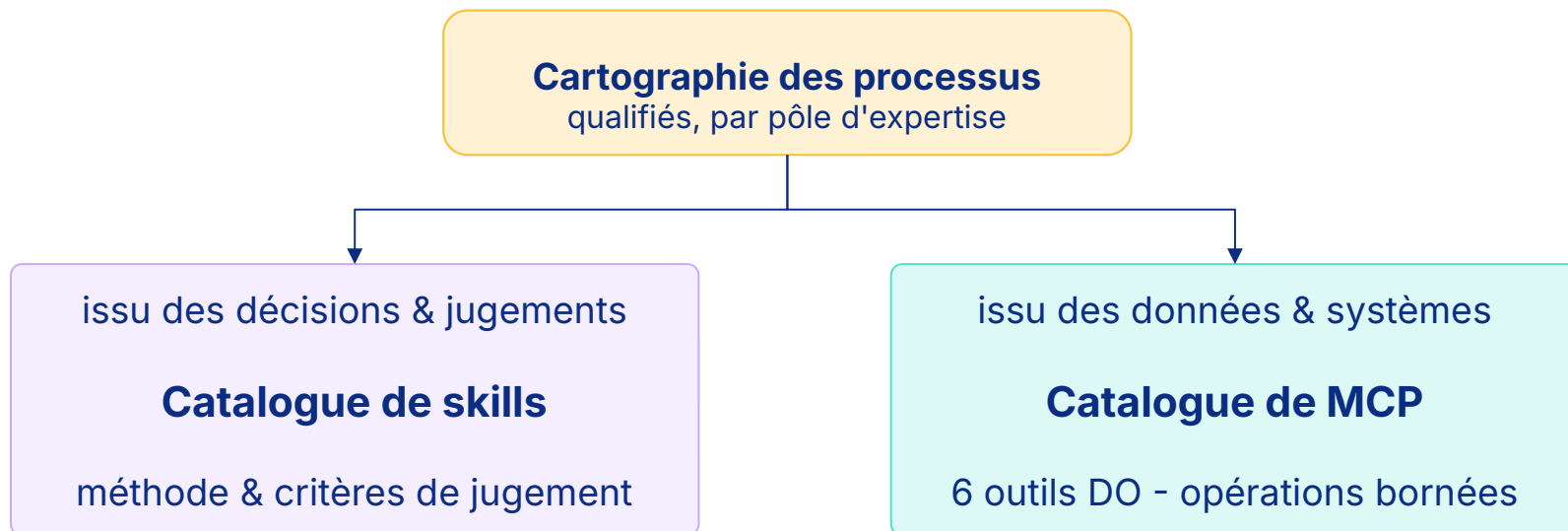
mcp-bigquery	mcp-dbt	mcp-dataiku	mcp-starburst	mcp-tableau	mcp-collibra
entrepôt analytique	Data transformation	ML / préparation	fédération multi-sources	Dataviz / BI	Data gouvernance
● Requêtes nommées et paramétrées (SQL figé + allow lists) ● Lecture seule ● Maîtrise du coût / plafonds ● MCP transversal à industrialiser	● Jobs prédéfinis uniquement ● run-time only ● Accès métadonnées du manifest ● Journalisation / reproductibilité ● Métriques d'exécution	● Modèles validés / déployés ● Exécution only (pas de nouveaux flows/recipes) ● Accès métadonnées (projet, flow...) ● Journalisation / reproductibilité ● Métriques d'exécution	● Requêtes féd. nommées et paramétrées (SQL figé + allow lists) ● Lecture seule (par policy) ● Fédération sans recopie des données ● Plafonds / limites requête ● Journalisation / reproductibilité	● Accès vues et classeurs existants ● Lecture / export only ● Filtres bornés (champs et valeurs allowlistés) ● Refresh extrait idempotent ● Exports plafonnés ● Journalisation / reproductibilité	● Lecture catalogue (assets, lignage, glossaire, règles & résultats DQ) ● Écritures via workflow humain¹ (propositions uniquement) ● Pivot de gouvernance transversal² ● Journalisation / reproductibilité

(1) seul MCP à casser le motif « lecture seule ». Il peut écrire, mais chaque écriture est gated par un workflow humain et ses écritures se bornent à des propositions devant être ensuite appliquées par un humain

(2) porte le contexte de conformité pour les autres MCP

3. Trois livrables : une cartographie, deux catalogues

La cartographie des processus révèle les briques ; on les range en deux catalogues : skills (jugement) et MCP (outils)

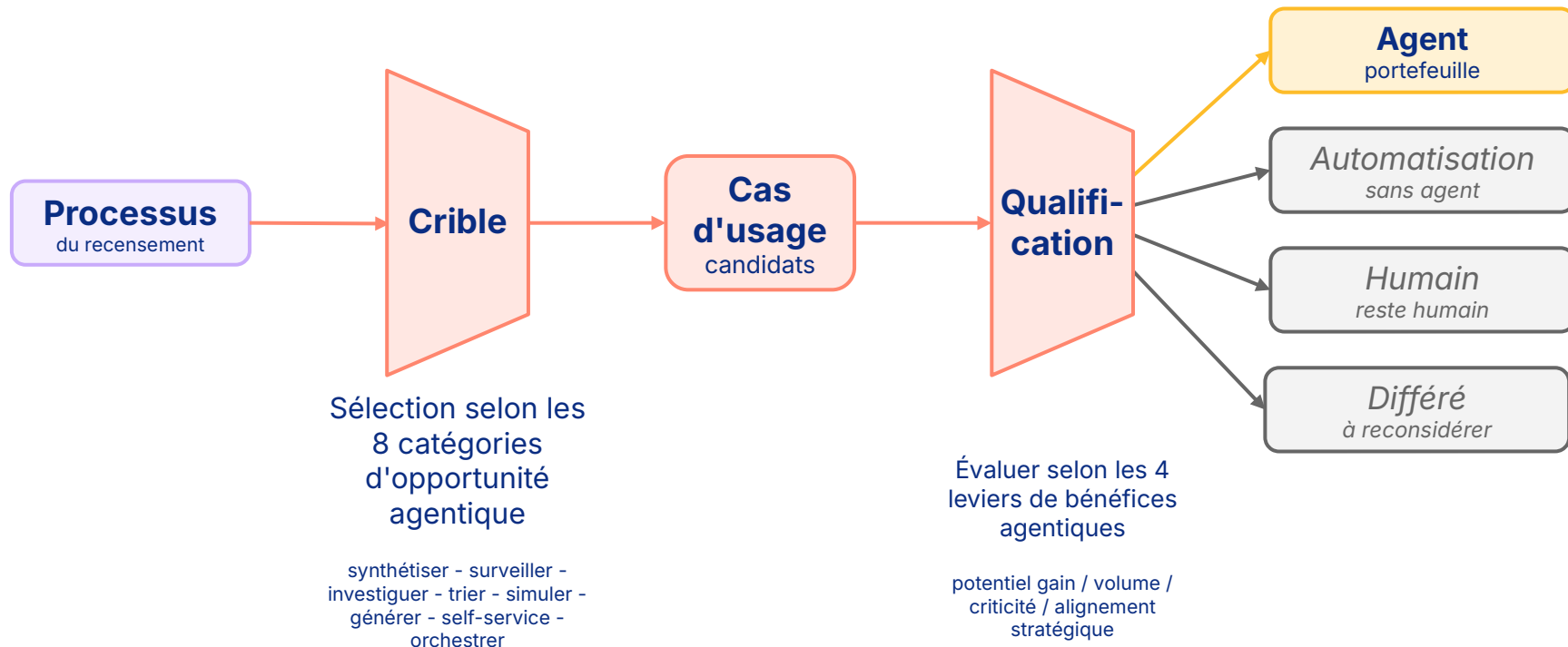


04

Phase 2 : Définition du portefeuille d'agents

4.1 Méthode : dériver puis qualifier

Huit catégories font émerger les cas d'usage ; quatre sorties les trient : seul "agent" rejoint le portefeuille



4.2 Illustration de cas d'usage agentiques Data

Capacités réutilisables construites sur la stack (via MCP) et leur valeur ajoutée

01 Self-service analytique & dataviz

Outils : Starburst · Tableau · BigQuery

Les métiers interrogent et visualisent les données en autonomie.

→ Mise à disposition

02 Catalogue & lignage automatisés

Outils : dbt · Collibra

Documentation, glossaire et lignage générés et tenus à jour.

→ Qualité & Référentiels

03 Contrôle qualité augmenté

Outils : dbt · BigQuery

Tests générés, anomalies et fraîcheur surveillées en continu.

→ Qualité · Supervision

04 Copilote pipelines & recipes

Outils : dbt · Dataiku

Transformations et recipes écrites et refactorées plus vite.

→ Intégration · Usine Dev

05 Conformité & gouvernance avant usage

Outils : Collibra

Certification, sensibilité RGPD et politiques vérifiées avant usage.

→ Conformité & Sécurité

06 Prototypage & mise en production IA

Outils : Dataiku

Du POC au modèle déployé plus vite, industrialisation maîtrisée.

→ R&D · Usine IA

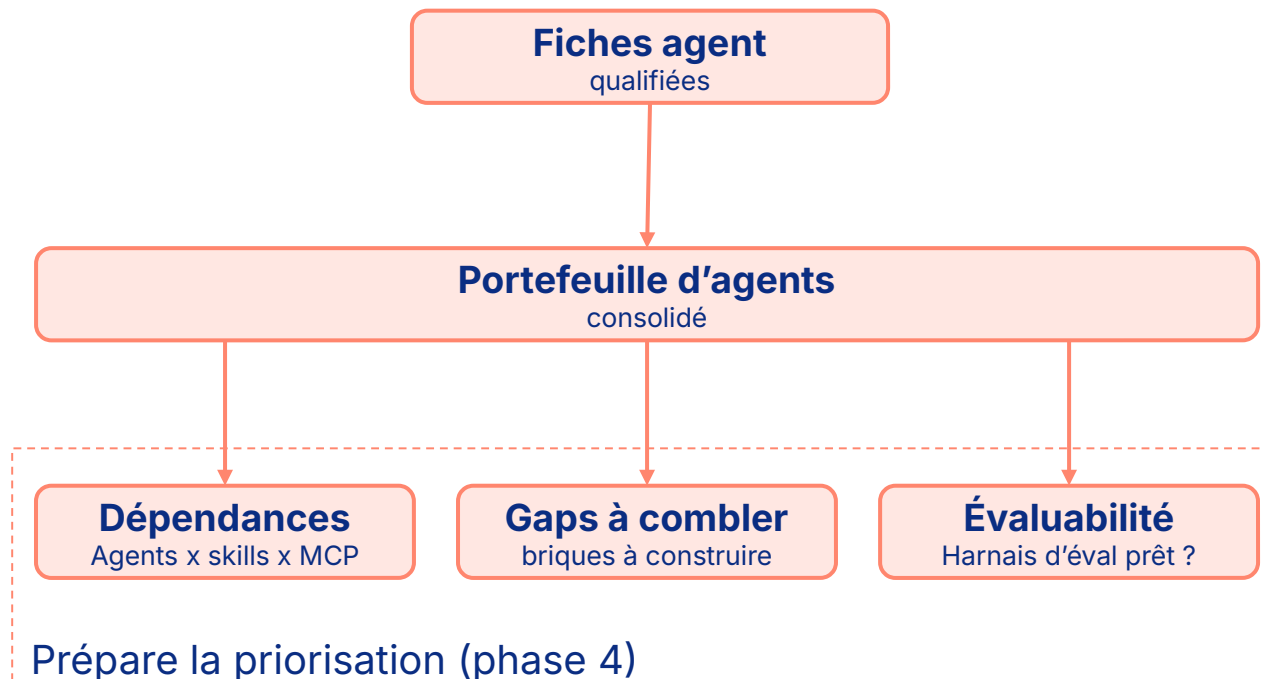
4.3 Livrable : la fiche agent

Compose skills + MCP + autonomie + escalade + harnais d'éval.

#	Champ	Consigne
1	Identité	nom, pôle propriétaire, version/date
2	Objectif & périmètre	objectif + processus couvert(s) + frontière de décision (ce qu'il fait / ne fait pas)
3	Skills mobilisés	principal + secondaires (renvoient aux fiches skill)
4	MCP & opérations	MCP et opérations autorisées, en <i>least privilege</i> (strict nécessaire)
5	Données & sensibilité	données manipulées + classification / enjeu de conformité
6	Niveau d'autonomie	sur l'échelle assistant → copilote → supervisé → autonome
7	Garde-fous	hérités des skills + propres à l'agent (interdits explicites)
8	Points d'escalade	déclencheur et destinataire (rôle)
9	Harnais d'éval	cas représentatifs + cas limites ; critères de réussite & métriques ; red-team (hors périmètre, exfiltration, refus d'escalade)
10	Dépendances & gaps	briques manquantes à construire (skills / MCP / données) ; agents ou processus liés
11	Déploiement & gouvernance	plateforme cible, ownership, versioning, monitoring, boucle d'amélioration

4.4 Livrable : le portefeuille consolidé

Consolidées, les fiches deviennent un portefeuille : dépendances, gaps et évaluabilité éclairent ce qu'on peut lancer en premier



05

Phase 3 : Analyse de valeur agentique

5.1 Bénéfices - Impacts - Transformation - Proposition de valeur

Lecture qualitative bénéfices x impacts, avant chiffrage

Bénéfices attendus	Impacts	Transformation induite	Proposition de valeur
● Temps : prise en charge des tâches répétitives à jugement structurable ● Qualité : moins d'erreurs, traitements homogènes ● Conformité & risque : traçabilité et points de contrôle systématiques ● Expérience : réponses plus rapides au métier, self-service accru	● Humain : rôles qui glissent de l'exécution vers la supervision ; montée en compétence ; adhésion ● Process : reconfiguration avec humain-dans-la-boucle, points de contrôle déplacés ● Organisation : ownership des agents, gouvernance, responsabilités ● Risque & conformité : nouveaux risques (autonomie, exfiltration) à encadrer	● Évolution vers un Data Office agentique supervisé ● Conduite du changement : accompagnement, montée en compétence, confiance progressive ● Le niveau d'autonomie comme curseur de l'ampleur de l'impact	● Lecture qualitative bénéfices x impacts par agent, qui prépare la priorisation ● Chiffrage et arbitrage coûts/bénéfices → feuille de route (activité 4)

5.
2.

Lecture bénéfices × impacts

Une matrice qui prépare la priorisation

06

Phase 4 : Priorisation et planification

6.1

Un chiffrage macro robuste à l'incertitude

Séparer l'indépendant de la plateforme (l'essentiel) de ce qui en dépend

Macro chiffrage : fourchettes / T-shirt sizing, hypothèses explicites, à raffiner une fois la solution retenue.

Fiabiliser malgré l'incertitude en séparant dans le chiffrage ce qui est **indépendant de la plateforme** (cas d'usage, skills, conception des MCP métier, analyse de valeur), soit l'essentiel du travail, de ce qui en **dépend** (runtime / orchestration des agents, intégration).

La majeure partie de la charge tient donc, quel que soit le choix final pour dérisquer l'estimation.

6.
2.

Croiser coûts/bénéfices et prioriser

Matrice de priorisation → allocation en vagues

6

Une feuille de route en 4 horizons de déploiement (V0→V3)

Socle → Quick wins → Extensions → Maturité



6.4 Quelle technologie pour l'agent ?

Quatre options d'orchestration possibles, à la lumière du SI existant

Gemini Enterprise Agent Platform (Google)

- + Gemini déjà dans toute l'entreprise — socle commun
- + Natif BigQuery & IAM — données au plus près
- + Gouvernance des tools (Cloud API Registry, MCP)
- + Serverless & scalable (Agent Engine)
- Souveraineté problématique
- Vendor lock-in
- Opacité budgétaire

AGENTS MÉTIERS

Dataiku Agent Hub / LLM Mesh

- + Déjà maîtrisé par le data office
- + Gouvernance & human-in-the-loop
- + Double rôle MCP (client + serveur)
- Cantonné au data office
- Pas un socle entreprise au delà DO

AGENTS DATA OFFICE

ILLUIN nAIxt Orchestration souveraine

- + Acteur français — souveraineté
- + Déjà présent dans le SI (solutions conversationnelles)
- + Low-code & industrialisation outillée
- + Agnostique au modèle
- Plateforme éditeur en plus
- Pas présente dans le SI

AGENTS APPLICATIFS

Framework tiers LangGraph, CrewAI...

- + Flexibilité maximale
- + Indépendance éditeurs
- Nouveau composant, pas de compétences
- Brique à opérer & sécuriser
- Gouvernance à reconstruire
- Redondant avec l'existant

À ÉVITER ICI

Solution possible (à évaluer)

Gemini Enterprise comme socle pour les métiers, Dataiku pour les agents du data office et nAIxt pour les agents applicatifs - modèle = choix séparé & réversible.

07

Next steps

Lancer la vague 1 et trancher les décisions structurantes

Prochaines étapes et décisions attendues

Lancer la vague 1 ; décisions COPIL (plateforme, sponsor, dispo experts)

Le Data Office devient le « MCP Gateway » de la data.

Nous ne sommes pas propriétaires de tous les agents.
Nous contrôlons la manière dont tous les agents peuvent appeler / créer des analyses à partir des données de la plateforme data.

Nous créons des agents spécialisés sur la data ou répondants à des besoins métier

3. Hypothèses d'estimation

A3. Hypothèses d'estimations (horizons de déploiement)

- Un prototype démontrable : 2 à 6 semaines ⇒ Un agent qui répond à des questions sociétaires en langage naturel, branché à une base via un serveur MCP existant (dbt, BigQuery), avec un LLM hébergé (Gemini) et 1-2 skills basiques. permet de supporter des démos, mais pas à déployer.
- Un pilote utilisable par quelques utilisateurs internes : 3 à 6 mois. Même agent que prototype, mais avec un catalogue de skills (5 à 10) réel, des garde-fous opérationnels (lecture seule par défaut, plafonds de coût, validation humaine sur les actions sensibles), une évaluation systématique (jeu de tests, mesures de qualité), une intégration aux outils existants (Collibra pour la gouvernance, journalisation), et un onboarding d'une dizaine d'utilisateurs internes Data Office. Horizon réaliste pour le premier cas d'usage de la liste en exemple (par exemple le self-service analytique).
- Un agent en production, sous gouvernance, ouvert aux métiers : 9 à 18 mois. ACPR-compatible, RGPD audité, conformité Collibra appliquée systématiquement, observabilité production-grade, gestion des incidents, formation des utilisateurs, processus de revue continue. La durée dépend du niveau d'exigence de conformité (v. complexité de l'agent)
- L'écriture et la sécurisation des skills. Chaque skill prend 1 à 3 semaines pour être robuste : définir le contrat typé, écrire les garde-fous, brancher l'observabilité, tester sur des cas réels, faire valider la couche de sécurité. Six skills = environ 3 mois.
- Les évaluations - mise en oeuvre de jeu de tests réutilisables pour tests de non régressions (changement de modèle, nouvelle skill, nouveau prompt) et qualification impact des évolutions (améliore ou dégrade l'agent). Construire un harness d'évals décent prend 4 à 8 semaines, et il faut le maintenir ensuite.
- L'intégration à la gouvernance existante. Brancher l'agent à Collibra pour qu'il vérifie sensibilité RGPD et habilitations avant chaque action, faire valider l'architecture par la sécurité et la conformité, obtenir les autorisations internes : est. 2 à 4 mois calendaires, dont l'essentiel est du temps d'attente et de revue, pas du développement.
- Vu stack (Gemini Enterprise déjà déployé, Dataiku au Data Office, Collibra pour la gouvernance, dbt/BigQuery/Starburst comme sources), beaucoup de briques structurelles existent déjà

4. PoC Starburst



Un PoC pour prouver les trois patterns du hub agentique

Trois démonstrations ciblées valident, sur la stack existante, les patterns qui fondent la vision cible — avant tout engagement d'industrialisation

Objectif du PoC : **démontrer la faisabilité technique des trois patterns structurants** sur Starburst × Dataiku, avec des données non sensibles.

Trois démonstrations :

- D1 sélection autonome sur **MCP fermés**
- D2 action gouvernée sur **MCP ouvert**
- D3 délégation inter-agents via **A2A**.

Ce que **le PoC n'est pas** : ni un choix de plateforme d'agents (décision structurante à part), ni un pilote métier, ni de la production.

Durée cible : 6 semaines, environnement isolé, périmètre volontairement minimal

D1, D2, D3 : trois patterns, trois preuves

Chaque démo prouve un pattern distinct : choisir (fermé), agir sous contrôle (ouvert), déléguer (A2A)

D1 — Sélection autonome sur MCP fermés (pattern « MCP gateway, diffusion large »)

- Un ensemble de Data Products Starburst (ex. sinistres IARD, contrats auto, client 360, référentiel géo) déclarés chacun comme **MCP fermé** : lecture seule, opérations bornées, schémas stricts.
- Question métier en langage naturel (ex. « montant moyen des sinistres auto par région en 2024 ? ») → l'agent Dataiku **découvre, compare et choisit** le bon Data Product à partir des seules métadonnées MCP, puis exécute et restitue.

Preuve apportée : la **découvrabilité** — un agent s'oriente seul dans un catalogue de MCP bien décrits.

D2 — Action gouvernée sur MCP ouvert (pattern « surface élargie, diffusion restreinte »)

- Un MCP Starburst **ouvert** : requête SQL élargie (cross-catalogue) + une écriture réelle (création d'une vue / matérialisation d'un agrégat).
- Garde-fous actifs et démontrés : pré-validation (EXPLAIN, plafonds lignes/coût), **validation humaine avant l'écriture** (human-in-the-loop), journalisation complète, rollback.

Preuve apportée : on peut **élargir la surface d'action sans perdre le contrôle** — le garde-fou se voit fonctionner.

D3 — Délégation inter-agents via A2A (pattern « agents exposés »)

- L'agent Dataiku **délègue une tâche de bout en bout** à un agent Starburst (ex. « prépare un extrait sinistres > 10 k€ et publie-le en vue ») via le protocole A2A (Agent Card, tâche, artefacts).
- L'agent Starburst planifie et exécute avec **ses propres outils** ; l'agent Dataiku ne voit que le contrat et le résultat.

Preuve apportée : l'**interopérabilité par contrat** — coopération sans couplage des internes.

Une architecture minimale sur la stack existante

Aucun composant exotique : Dataiku héberge les agents, Starburst expose données et actions — MCP et A2A
font le lien

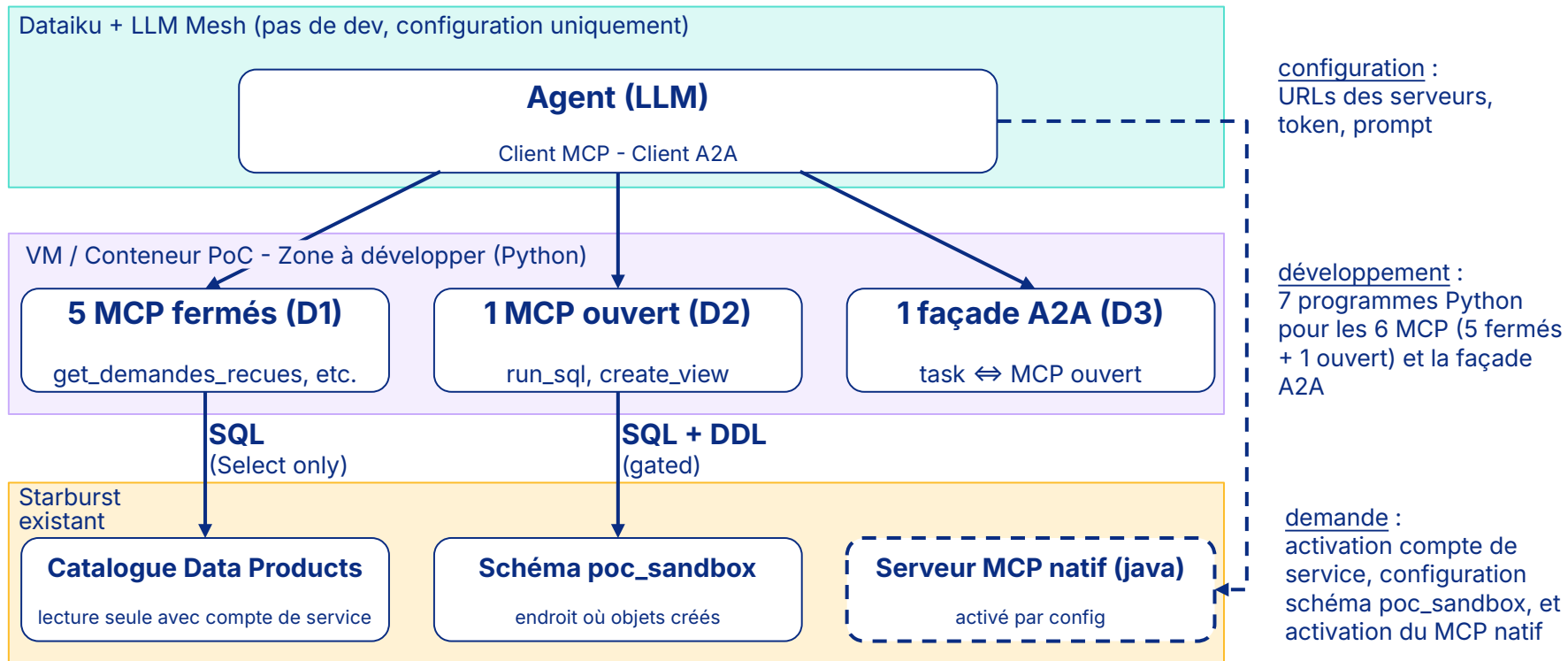
Hôte des agents	Dataiku (agent LLM + tool calling). Le choix de Dataiku ici = rapidité de mise en œuvre, sans préjuger de la plateforme cible (patterns portables par construction — standards ouverts).
Exposition des données/actions	Starburst — Data Products en MCP fermés (D1), endpoint MCP ouvert (D2), agent Starburst exposé A2A (D3).
Environnement	hors production, catalogue de test, données anonymisées ou synthétiques (conformité RGPD), comptes de service dédiés, RBAC propagé de bout en bout.
Traçabilité	journalisation systématique des appels MCP et des échanges A2A (qui, quoi, quand, avec quels paramètres).
Hypothèses à valider au démarrage	● disponibilité du MCP server Starburst et du support MCP côté Dataiku dans les versions/licences du Groupe ● existence d'un agent Starburst exposable A2A ● Disponibilité du LLM Mesh dans Dataiku

Critères mesurables fixés au démarrage du PoC

Le PoC est réussi si l'agent choisit juste, si aucun garde-fou n'est contourné, et si la délégation aboutit

D1	● jeu de 15 questions métier variées vérification de l'atteinte d'un taux de sélection du bon Data Product $\geq 80\%$ (faux négatifs $< 20\%$) ● 0 accès hors périmètre (faux positifs = 0%) ● réponse sourcée (Data Product cité dans les résultats)
D2	● 100 % des écritures passent par validation humaine ● toute requête au-delà des plafonds est refusée proprement ● chaque action tracée et réversible (rollback démontré)
D3	● tâche déléguée aboutie de bout en bout ● contrat d'échange (Agent Card + artefacts) documenté ● traçabilité inter-agents reconstituable a posteriori.
Transverse	● temps de mise en œuvre par pattern (indicateur d'industrialisabilité) ● limites rencontrées documentées.

Architecture générale du PoC



Un Serveur MCP est un programme autonome s'exécutant dans une VM

Petit programme
Python à développer
pour chaque MCP
(c. 100 lig. de code)
et à exécuter en VM

1. DÉCLARER le serveur
nom ← identifiant unique (ex. mcp-dp-demandes)
description ← ce qu'il sait faire, pour qui (description utilisée par l'agent pour choisir l'opération)
2. CONFIGURER l'accès au système exposé
connexion ← compte de service, DROITS MINIMAUX (SELECT-only si MCP fermé)
garde-fous ← listes de valeurs, plafonds (MAX_ROWS, timeout), deny-list de colonnes (PII)
3. DÉFINIR les outils
POUR CHAQUE intention métier : // Charge de développement des MCP
déclarer : nom, description, schéma des paramètres strictes // 1 intention = 1 outil
implémenter la fonction :
 - a. RE-VALIDER les paramètres // si hors schéma retourner une ERREUR propre
 - b. construire l'opération FIGÉE
template écrit par le dev + paramètres BINDÉS // le LLM ne compose JAMAIS l'opération
 - c. appliquer les garde-fous
plafonds, deny-list, masquage
 - d. exécuter sur le système
 - e. journaliser (qui, quoi, quand, params, résultat)
 - f. retourner le résultat structuré
4. DÉMARRER le transport : HTTP (serveur distant) + authentification

Fonctionnalités
fournies par le SDK
MCP - Pas de dev.

- BOUCLE :
- recevoir message JSON-RPC
 - ├ initialize → répondre version + capacités
 - ├ tools/list → répondre l'ANNUAIRE (généralisé depuis les déclarations du bloc 3)
 - └ tools/call → router vers la bonne fonction, renvoyer résultat ou erreur

Un serveur A2A est un programme autonome qui expose un agent

Définition publiée en
JSON dans
</well-known/agent-card.json>

1. DÉCLARER l'agent – l'Agent Card
 - nom, description ← ce que l'agent sait accomplir, équivalent de la description MCP
 - skills ← liste de capacités (ex. "publier une vue agrégée dans le sandbox, sous validation")
 - endpoint, auth ← où et comment le joindre

Petit programme
Python (c. 150 lignes) à
développer et
s'exécutant dans une
VM

2. CONFIGURER ce que l'agent utilise EN INTERNE
 - exécuteur ← LLM planificateur, OU logique scriptée
 - outils ← client MCP vers le MCP ouvert de D2 // l'agent A2A est un client MCP
 - stockage ← table des Tasks en cours (dict en mémoire au PoC)
3. DÉFINIR le traitement d'une tâche // ~80 % du travail
 - À RÉCEPTION d'un objectif (message/send) :
 - task ← créer Task(état = "submitted"), journaliser
 - état ← "working"
 - plan ← PLANIFICATEUR(objectif) // LLM ou script
 - POUR CHAQUE étape du plan :
 - SI étape = action sensible (écriture) :
 - appeler MCP create_view → "pending_approval"
 - état Task ← "input-required" // ← LE garde-fou
 - ATTENDRE l'approbation humaine // rien ne s'exécute
 - reprendre à l'approbation
 - SINON :
 - appeler l'outil MCP (run_sql, preview...)
 - journaliser (task-id → appel MCP) // corrélation
 - artefacts ← assembler (DDL, URI de la vue, stats, journal)
 - état ← "completed" (ou "failed" + motif)
4. DÉMARRER le transport
 - serveur HTTP : sert l'Agent Card + endpoints JSON-RPC : message/send, tasks/get + auth (token / OAuth)

Six semaines avec une équipe resserrée

Un binôme technique et sponsor DO

Équipe	● 1 tech lead data (Starburst / SQL / gouvernance) ● 1 ingénieur Dataiku-LLM (agents, MCP) ● sponsor/PO côté DO (arbitrages, accès) ● support admin Starburst et infra ● support éditeurs en appui ponctuel (Starburst, Dataiku)
Charges estimées	● 30-35 j/h au total
Planning (6 semaines)	● S0 prérequis & validation des hypothèses (accès, licences, environnement) ● S1-S2 socle + D1 ● S3-S4 D2 (garde-fous, human-in-the-loop) ● S5 D3 (A2A) ● S6 restitution & démos rejouables
Jalons	● revue de mi-parcours après D1 (go/no-go sur D2-D3) ● démo finale devant COPIL

Risques identifiés, replis prévus, suites préparées

Le principal risque est la maturité des briques éditeur

Maturité éditeur sur techno agentique (MCP server Starburst, MCP côté Dataiku, agent A2A)	● replis wrapper/façade — la preuve du <i>pattern</i> reste entière. ● A2A est un protocole récent : versions à figer en S0
Accès & habilitations	● dépendance aux équipes sécurité/infra pour l'environnement isolé, à engager dès démarrage.
Représentativité des données	● jeux synthétiques à préparer soigneusement pour que D1 (sélection) soit probante
Risque de sur-interprétation	● le PoC démontre des patterns, pas une architecture de production (perfs, HA, coûts non traités) ni une valeur métier (ROI, gains d'efficacité...) - Communiquer la finalité dès le début pour répondre et modérer les attentes
Suites si succès	● alimenter la feuille de route (V0) avec les patterns validés ● étendre à un MCP Collibra (gouvernance) ● instruire la décision plateforme d'agents avec des faits.