



M1151 · LECTURE ACADÉMIQUE

Initiation au management de la data

De la collecte à la décision : rendre les données fiables, gouvernées et utiles



Data Management
DATA MANAGEMENT

SÉANCE 3 / 3 **Gouvernance, sécurité et valorisation des données**

ENSEIGNANT

Pr. Youness BOUTYOUR

youness.boutyour@um5.ac.ma

PUBLIC CIBLE

Génie de la data

1ère année

INSTITUTION

Université Mohammed V de Rabat

Ecole Nationale Supérieure d'Informatique et d'Analyse des
Systèmes

Plan de la séance

SÉANCE 3 / 3 – GOUVERNANCE, SÉCURITÉ ET VALORISATION DES DONNÉES

01 Fondements et mise en œuvre de la gouvernance des données

02 Sécurité juridique et technique des données

03 Évaluation de la performance et valorisation des données

04 Synthèse

Objectifs pédagogiques

OBJECTIFS PÉDAGOGIQUES

3 OBJECTIFS

- 01 Mettre en place une bonne gouvernance des données
- 02 Sécuriser juridiquement et techniquement les données
- 03 Évaluer les résultats d'une bonne gouvernance des données

CHAPITRE

Gouvernance, sécurité et valorisation des données

01

Fondements et mise en œuvre de la gouvernance des données

Volumétrie et production contemporaine des données

En 2021, les données étaient déjà produites à une échelle difficile à imaginer.

- **Environ 300 milliards** de mails envoyés et reçus dans le monde chaque jour.
- **Environ 40 milliards** d'enregistrements exposés selon une estimation de 2021.
- **Environ 500 millions** de tweets publiés chaque jour.
- **Environ 167 millions de vidéos** regardées par minute sur TikTok.

Ordres de grandeur historiques de 2021 — ces chiffres sont des estimations ; voir les références [1] à [3] et [9] sur la slide finale.

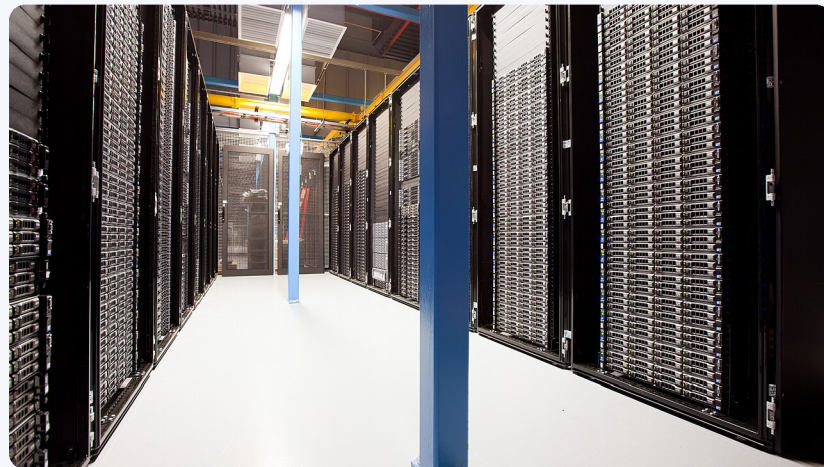


Figure 1. Salle de serveurs : une infrastructure adaptée à la croissance des volumes de données. * Réf. [4].

Genèse historique des données

- **Antiquité grecque** — À Délos, des stèles gravées attestent déjà la comptabilité du sanctuaire.
- **Second Empire** — Napoléon III organise un réseau météorologique télégraphique pour collecter des observations. *Réf. [5].*
- **Avant le numérique** — Carnets d'adresses et de numéros : des bases de données gérées sans ordinateur.



Figure 2. Une trace ancienne de la production et de la conservation des données. *
Réf. [4].

IDÉE CLÉ

Le numérique n'a pas inventé les données.
Il a surtout démultiplié leur volume, leur circulation et notre capacité à les transformer.

Données et activités organisationnelles

Dans une organisation, les données accompagnent presque chaque activité.

- Ressources humaines
- Clients et prospects
- Prestataires et partenaires
- Comptabilité et activité historique
- Événements et usages

Les principales sources de données

DOMAINE	EXEMPLES DE DONNÉES
Ressources humaines	dossiers, contrats, compétences
Clients et prospects	identité, contacts, interactions
Finance et activité	transactions, budgets, résultats
Partenaires et prestataires	contrats, coordonnées, services

Idée clé : une organisation produit et utilise des données à chaque étape de son activité. La gouvernance devient nécessaire dès qu'il faut les comprendre, les protéger, les partager ou décider à partir d'elles.

Management et gouvernance des données : distinction conceptuelle

MANAGEMENT DES DONNÉES

Faire fonctionner les données au quotidien :

- les organiser et les classer ;
- les mettre à jour et les exploiter.

GOUVERNANCE DES DONNÉES

Cadre de règles, de rôles, de processus et de décisions qui encadre la gestion des données :

- définir une direction et des règles ;
- partager les responsabilités et les objectifs.

- **À retenir** : le management rend la donnée exploitable ; la gouvernance la pilote au service d'une stratégie.
- **Le véritable risque** : être submergé par les données, sans les comprendre ni les maîtriser.
- **Exemple** : le management dédoublonne une fiche client ; la gouvernance décide qui peut la modifier et selon quelles règles.

Organisation en silos : limites de la fragmentation

Définition — silo de données : environnement isolé, difficilement accessible aux autres systèmes.

- Un service conserve ses données et travaille de son côté.
- La **DSI** — Direction des systèmes d'information — peut être réduite à un rôle de support technique.

SERVICE ISOLÉ	EXEMPLE DE DONNÉES
Ressources humaines	dossiers du personnel
DSI	systèmes et accès
Communication	contenus et campagnes
Finances	budgets et transactions

Conséquences : peu de circulation entre services, doublons et vision

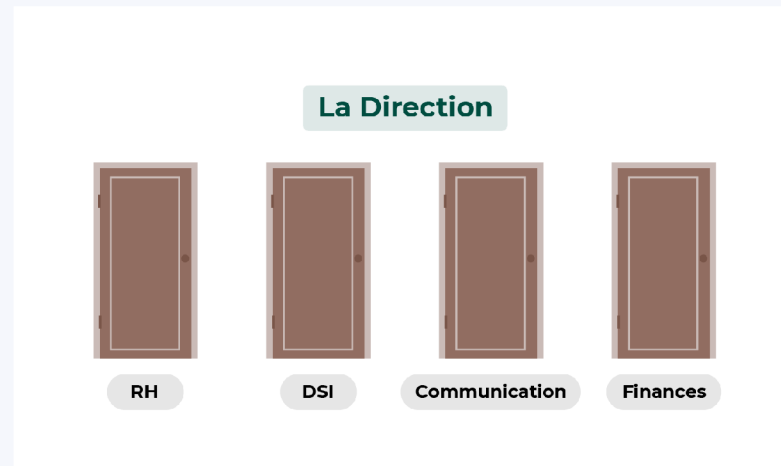


Figure 4. Dans une organisation en silos, les services restent isolés les uns des autres. * Réf. [6].

Master Data Management : centralisation des données de référence

MDM — Master Data Management : discipline et outillage qui gèrent, synchronisent et fiabilisent les données de référence.

- Il répond aux données dispersées entre plusieurs systèmes.
- Il réduit les données incomplètes, obsolètes ou incohérentes.



Gouvernance des données : pilotage stratégique

DG — Data Governance (gouvernance des données) :

cadre de décision et de pilotage de l'ensemble des données de l'organisation.

Dans ce cours, nous utilisons **DG** pour désigner la gouvernance globale. La **MDG** (Master Data Governance) désigne plus spécifiquement la gouvernance des données maîtres.

- La donnée est inscrite au cœur du projet de l'entreprise.
- Elle est pilotée par une stratégie commune, au-delà de l'outillage.
- Des règles et des responsabilités partagées.
- Une qualité, une sécurité et une interopérabilité suivies.
- Une donnée pilotée pour créer de la valeur et soutenir les décisions.

Exemple de décision : qui est responsable de la qualité d'une fiche client ? Qui valide sa modification ? Qui suit les

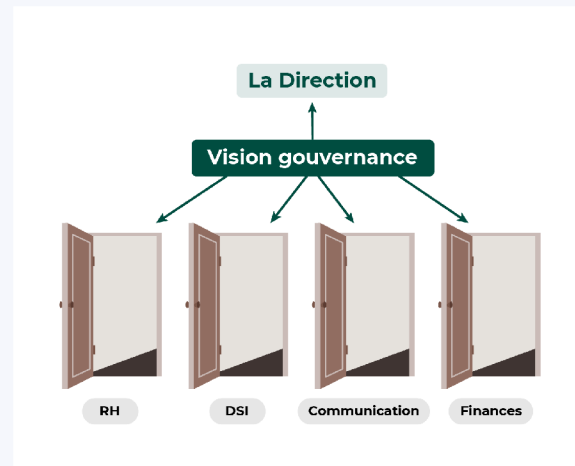


Figure 5. La vision de gouvernance relie la direction et les différents départements. * Réf. [6].

VISION GOUVERNANCE

Les départements ouvrent leurs portes.
La donnée devient un actif commun au service de la stratégie.

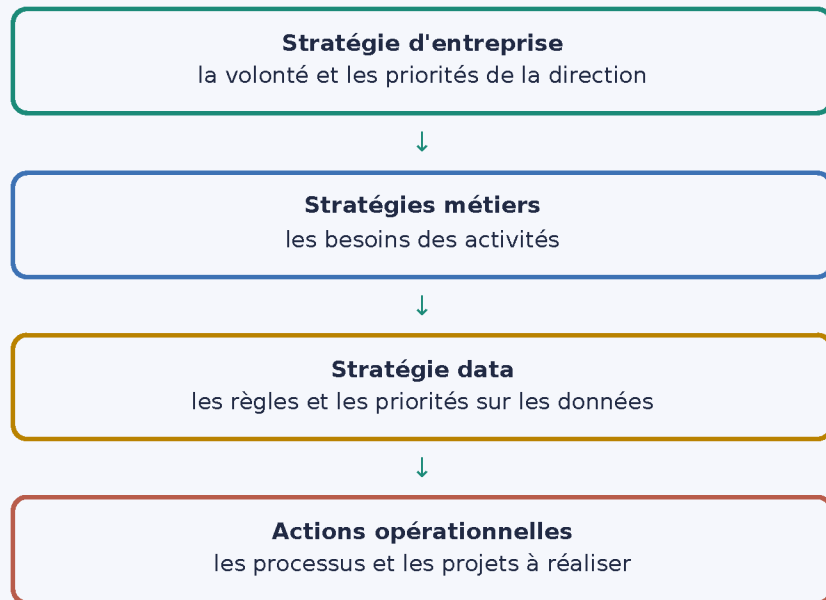
Trois niveaux de maîtrise des données

NIVEAU	PÉRIMÈTRE	QUESTION PRINCIPALE	EXEMPLE
Management des données	Toutes les données	Comment les organiser et les exploiter ?	mettre à jour, classer, analyser
MDM	Données maîtres	Comment fiabiliser les entités clés ?	dédoublonner les fiches clients
DG	Toutes les données	Qui décide et selon quelles règles ?	définir les accès et les responsabilités

À retenir : le MDM est une pratique de gestion ciblée sur les données maîtres ; la DG fixe le cadre stratégique et les règles applicables à l'ensemble des données.

En pratique : le MDM fiabilise la fiche client ; la DG désigne le responsable, fixe les règles et organise le suivi.

Alignement stratégique de l'entreprise et de la donnée



Définition — alignement stratégique : cohérence entre les objectifs de l'entreprise, les stratégies métiers et les actions opérationnelles.

- Les processus sont uniformisés.
- La stratégie data sert les stratégies métiers.
- Les stratégies métiers servent la stratégie d'entreprise.

Vision de gouvernance : traduction concrète de l'alignement stratégique dans la gestion des données.

Question de mise en pratique : quelle priorité de l'entreprise doit être traduite en règle, processus ou projet data ?

Vision intégrée de la gouvernance des données

La gouvernance ne concerne pas uniquement la DSI.

Elle relie les dimensions humaines, organisationnelles et techniques de l'entreprise.

- culture et éthique ;
- rôles et responsabilités ;
- politiques, méthodes et processus ;
- compétences, services et information.

Idée clé : une démarche globale rend les décisions compréhensibles et applicables par tous.

Test rapide : si une règle data ne précise ni son responsable, ni son processus d'application, ni son indicateur de suivi, elle reste difficilement gouvernable.

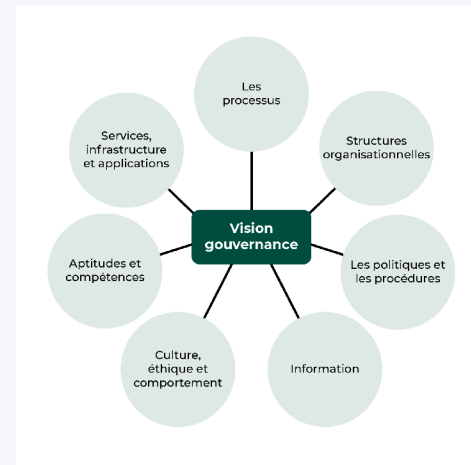


Figure 6. La vision de gouvernance articule structures, politiques, information, culture, compétences, services et processus. * Réf. [6].

Objectifs de la gouvernance des données

- **Définir et communiquer** les stratégies, politiques, normes, architectures et procédures.
- **Suivre la conformité** aux réglementations et aux règles internes.
- **Augmenter la confiance** des équipes dans les données.
- **Encourager et superviser** les projets et services de gestion des données.
- **Résoudre les problèmes** liés aux données plus facilement.
- **Comprendre et promouvoir la valeur** des données.

À retenir : la gouvernance transforme une intention stratégique en règles, pratiques et résultats mesurables.

Synthèse

- **Les données sont partout** : il faut en prendre conscience, sans s'en inquiéter.
- **Le numérique a changé l'échelle** : il a multiplié le volume, la circulation et la vitesse d'exploitation des données.
- **Le risque des silos** : des données isolées circulent peu, se dupliquent et donnent une vision incomplète.
- **La progression est simple** : gérer les données, mieux les maîtriser, puis les piloter au service d'une stratégie globale.
- **MDM et DG sont différents** : le MDM gère et fiabilise les données maîtres ; la DG définit la stratégie, les règles et les responsabilités pour l'ensemble des données.
- **La gouvernance est alignée** : la stratégie data traduit la stratégie d'entreprise et ses objectifs en actions concrètes.
- **La finalité** : améliorer la qualité et la confiance dans les données pour soutenir les décisions et créer de la valeur.

Message clé : la gouvernance des données transforme une masse de données en ressource maîtrisée et utile à la décision.

CHAPITRE

Gouvernance, sécurité et valorisation des données

02

Cartographier et maîtriser le cycle de vie des données

Cycle de vie des données

Définition — cycle de vie de la donnée : étapes successives par lesquelles une donnée entre dans l'entreprise, y est utilisée, puis est archivée ou supprimée.

- 01 **Entrée :** la donnée naît ou est acquise.
- 02 **Vie :** elle est consultée, modifiée, analysée, partagée ou corrigée.
- 03 **Fin de vie :** elle est archivée, anonymisée ou supprimée.

Idée clé : avant de gouverner une donnée, il faut savoir quand et comment elle entre dans votre périmètre.

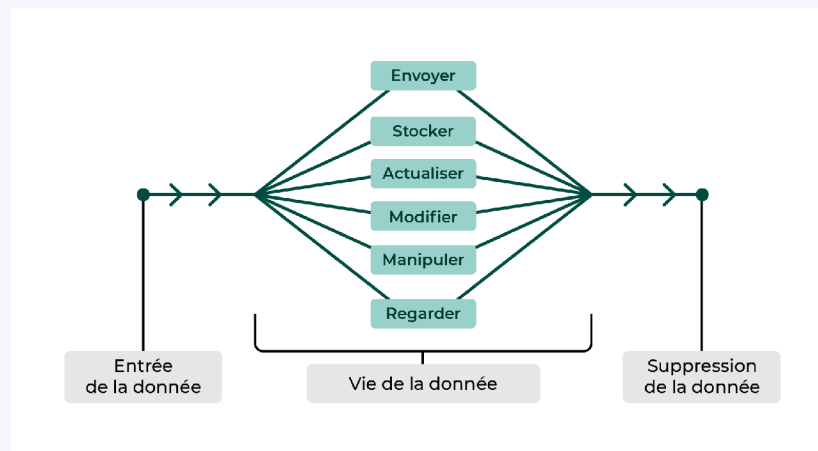


Figure 7. Cycle de vie de la donnée : entrée, usages et suppression. * Réf. [6].

Provenance et flux d'entrée des données

La **provenance** désigne l'origine d'une donnée, son producteur et le chemin par lequel elle arrive dans l'entreprise.

Pourquoi est-ce critique ? Si vous oubliez une porte d'entrée, vous risquez d'oublier toutes les données qui passent par cette porte.

- identifier la source ;
- documenter le contexte de collecte ;
- conserver les conditions d'accès et d'utilisation.



Figure 8. Exemples de portes d'entrée des données.

Référencement et inventaire des données

Définition — répertoire de données : liste structurée des données détenues par l'entreprise, de leur source, de leur usage et des règles qui leur sont applicables.

Répertorier consiste à transformer les sources identifiées en une **cartographie globale**.

- nommer les données et leur propriétaire ;
- décrire leur source, leur format et leur usage ;
- associer les règles de sécurité, d'accès et de conservation.

Typologie des données selon l'accès et l'identifiabilité

- **Données à caractère personnel** — informations permettant d'identifier directement ou indirectement une personne. *Ex. : nom, e-mail, adresse IP, comportements.*
- **Données publiques** — données accessibles à un large public ou diffusées selon un régime d'ouverture. *Accessibles ne signifie pas toujours réutilisables.*
- **Données privées** — données protégées ou limitées par des droits spécifiques. *Ex. : droit d'auteur, secret des affaires.*

Nuance et vigilance : « publique » ou « privée » décrit surtout l'accès et le régime de diffusion ; « personnelle » décrit la possibilité d'identifier une personne. Ces catégories peuvent donc se recouper. Avant tout usage ou partage, vérifiez les règles applicables.

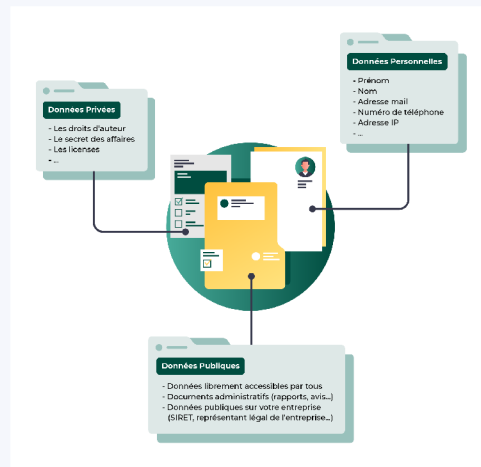


Figure 9. Cartographie des données personnelles, publiques et privées. * Réf. [6].

Hiérarchisation des données selon leur valeur et leur risque

Hiérarchiser, c'est classer les données selon leur intérêt pour l'entreprise et selon les usages qu'elle en fait.

- **Données transactionnelles ou d'activité :** informations produites par les opérations — commandes, quantités, résultats ou événements.
- **Données maîtres :** entités métier principales et relativement stables — client, produit, fournisseur.
- **Données de référence :** valeurs contrôlées qui qualifient les données — pays, statut, catégorie ou canal.
- **Métadonnées :** informations qui décrivent les données — format, origine, date, propriétaire ou niveau de qualité.

Dimension transversale : les métadonnées documentent chacune des autres catégories ; elles ne constituent pas un niveau hiérarchique strict. Les données maîtres et de référence sont complémentaires,

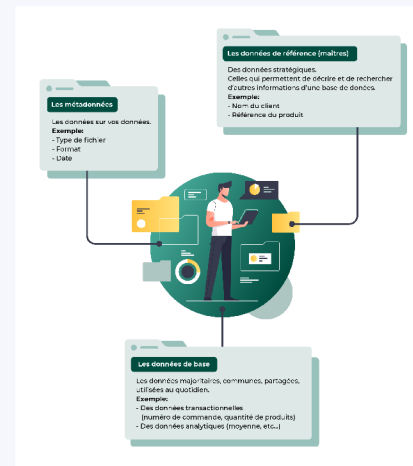


Figure 10. Données transactionnelles, données de référence et métadonnées. * Réf. [6].

Dictionnaire de données et langage commun

Définition — dictionnaire de données : nomenclature qui définit les données, leurs catégories et leurs caractéristiques.

- même vocabulaire pour tous les métiers ;
- formats et définitions harmonisés ;
- meilleure interopérabilité entre les systèmes.

Si la donnée est le contenu, la métadonnée est le contexte.

Donnée	Définition	Format
Client	Personne acheteuse	Identifiant
Date commande	Date de transaction	AAAA-MM-JJ
Montant	Valeur totale	Décimal

Figure 11. Exemple simplifié de dictionnaire de données.

Fin de vie et suppression des données

Une donnée ne doit pas être conservée indéfiniment « au cas où ». Sa durée de vie doit être justifiée par un usage, une obligation ou une valeur documentée.



Figure 12. De la base active à la suppression. * Réf. [6].

Le tri est une action de gouvernance :

il réduit les risques, les coûts et l'accumulation de données inutiles.

Anonymisation et préservation de l'utilité des données

Définition — anonymisation : rendre définitivement impossible l'identification d'une personne, directement ou indirectement, en tenant compte des risques d'individualisation, de corrélation et d'inférence.

- supprimer les identifiants inutiles ;
- réduire le niveau de précision ;
- conserver uniquement la valeur analytique nécessaire.

À distinguer de la pseudonymisation : une donnée pseudonymisée peut encore être rattachée à une personne avec des informations supplémentaires. L'anonymisation doit être vérifiée au regard des moyens raisonnablement accessibles.

Avant

« David Dupond, 34 ans, a vu Batman le 28 avril 2022 au Grand Rex. »



Après anonymisation

« Une personne de 30 à 35 ans a vu Batman en avril 2022 à Paris. »

Illustration simplifiée :

l'analyse statistique reste possible, mais l'anonymisation réelle doit être démontrée au regard des risques.

Synthèse

Cartographie et cycle de vie des données

- **Identifier** : repérer les portes d'entrée et documenter la provenance.
- **Répertoirer** : construire une cartographie des données et des règles applicables.
- **Hiérarchiser** : distinguer données transactionnelles ou d'activité, données maîtres, données de référence et métadonnées transversales.
- **Conserver avec mesure** : définir les phases actives et d'archivage.
- **Supprimer ou anonymiser** : mettre fin aux données qui n'ont plus de finalité.

Message clé : une cartographie utile relie chaque donnée à une source, une catégorie, un responsable, un usage et une durée de vie.

Étape suivante : traduire cette connaissance en plan d'action de gouvernance.

CHAPITRE

Gouvernance, sécurité et valorisation des données

03

Formaliser la stratégie en plan d'action de gouvernance

Cadrage du plan de gouvernance

Avant de planifier les actions, il faut préciser :

- 01 **La finalité** — quel objectif de l'entreprise le plan doit-il servir ?
- 02 **Le périmètre** — quelles données, activités et entités sont concernées ?
- 03 **Les priorités** — quels risques et quels cas d'usage traiter en premier ?
- 04 **Les contraintes** — quelles obligations, ressources, compétences et échéances ?

Le cadrage doit produire un socle partagé :

- un **sponsor** et des parties prenantes identifiés ;
- des **objectifs mesurables** et un périmètre explicite ;
- une première analyse des **risques, dépendances et moyens** ;
- des critères de **priorisation** connus de tous.

Point de passage : le cadrage relie la stratégie d'entreprise au plan d'action ; il évite de lancer des projets data sans finalité ni responsable.

Postures organisationnelles de gouvernance

La stratégie dépend du niveau de maturité, du risque accepté et des objectifs de l'entreprise.

POSTURE DÉFENSIVE

Prioriser les audits et la conformité.

Réduire les risques avant toute valorisation.

Avancer lorsque les garanties sont établies.

POSTURE OFFENSIVE

Mener sécurisation et valorisation en parallèle.

Accepter davantage d'incertitude.

Disposer d'une maturité data suffisante.

Principe de décision : la stratégie pertinente se situe souvent entre ces deux postures ; elle doit être proportionnée au contexte de l'entreprise.

Pilotage itératif de la gouvernance

Méthode agile : approche itérative qui accepte les changements, produit des versions fonctionnelles et utilise les retours des utilisateurs pour progresser.

- **Projet :** résultat et étapes largement définis à l'avance.
- **Produit data :** objectif global connu, mais trajectoire ajustée par les apprentissages.
- Commencer par une version minimale fonctionnelle, recueillir les retours et améliorer progressivement la gouvernance.

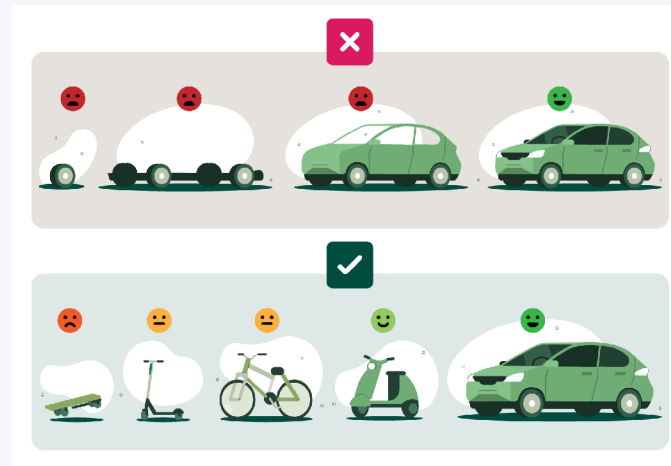


Figure 13. Une stratégie fonctionnelle s'améliore par étapes successives. * Réf. [6].

Référentiel DAMA-DMBOK et domaines de gouvernance



Figure 14. La roue DAMA regroupe les domaines du management des données. * Réf. [6].

DAMA : *Data Management Association.*

DMBOK : *Data Management Body of Knowledge*, référentiel des domaines du management des données.

La roue met en relation :

- gouvernance des données ;
- architecture et modélisation ;
- stockage, intégration et sécurité ;
- documents, contenus et données maîtres ;
- métadonnées et qualité ;
- entreposage et analyse.

Représentation pédagogique inspirée du DAMA-DMBOK

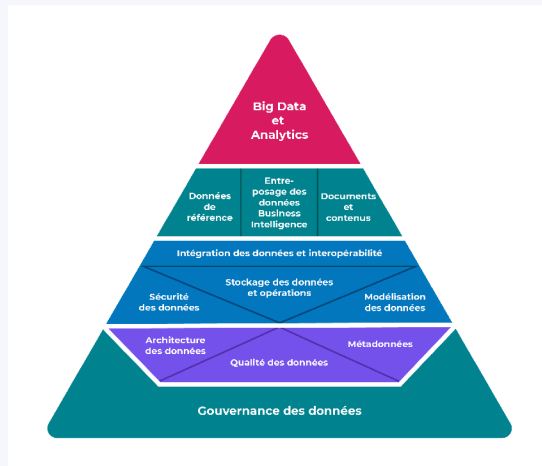


Figure 15. Représentation inspirée du DMBOK ; elle ne constitue pas une échelle officielle de maturité. * Réf. [6].

- 01 **Gouvernance des données** — définir les règles, les responsabilités et les décisions.
- 02 **Récupérer, identifier et sécuriser** — connaître les données et réduire les risques immédiats.
- 03 **Stocker, gérer et améliorer la qualité** — structurer les données et l'architecture du système d'information.
- 04 **Analyser et créer de la valeur** — produire des statistiques, des résultats et des décisions.

À retenir : le DMBOK est un référentiel de domaines ; cette pyramide sert uniquement à organiser la discussion pédagogique. Les domaines sont interdépendants, et non disposés selon une maturité universelle.

Critères de sélection des outils de gouvernance

- **Glossaire et dictionnaire** — classer les données, harmoniser les définitions et partager une nomenclature.
- **Gestion du cycle de vie** — tracer les données, journaliser les modifications et gérer les métadonnées.
- **Gestion de la gouvernance** — gérer les rôles, les droits d'accès, les actions et les indicateurs.
- **Processus métiers** — documenter les procédures, les tâches et les tableaux de bord.

Critère de choix : le bon outil correspond au contexte, aux compétences, aux risques et aux objectifs.



Figure 16. Exemples d'outils de gestion et de gouvernance des données. * Réf. [6].

Collibra, Alteryx, Talend, Informatica, OvalEdge et autres solutions.

Formalisation des procédures de gouvernance

Charte de gouvernance : document partagé qui décrit les règles, les rôles, les processus et les décisions attendues pour l'utilisation des données.

- standardiser les pratiques ;
- rendre les décisions compréhensibles ;
- faciliter l'application des règles au quotidien.

La charte répond aux questions concrètes :

- Où stocker une donnée : serveur local ou cloud ?
- Puis-je utiliser cette donnée personnelle ?
- Quel niveau de sécurité appliquer ?
- Quelle action réaliser dans mon processus métier ?

Une règle devient opérationnelle lorsqu'elle associe un responsable, une action et une preuve.

Acteurs et instances de la gouvernance des données

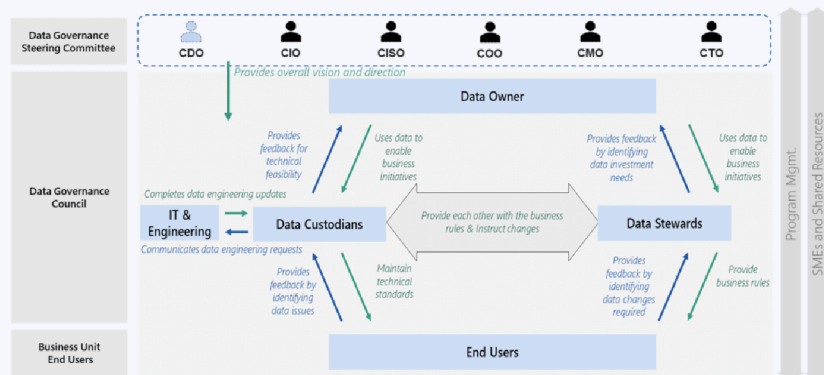


Figure 17. Modèle de collaboration entre les principaux acteurs de la gouvernance des données. * Réf. [7].

Principe — La gouvernance est collective : les acteurs décident, définissent les règles, les mettent en œuvre et signalent les écarts.

Dans le schéma : CDO = Chief Data Officer ; CIO = Chief Information Officer ; CISO = Chief Information Security Officer ; COO = Chief Operating Officer ; CMO = Chief Marketing Officer ; CTO = Chief Technology Officer.

Lire l'image de haut en bas :

- **Comité directeur** : donne l'orientation, arbitre les priorités et soutient la stratégie data.
- **Data Owner** : porte la responsabilité métier d'un domaine : usages autorisés, qualité attendue et décisions d'accès.
- **Data Stewards** : traduisent les règles en pratiques métier, suivent la qualité et remontent les besoins d'évolution.

Répartition des responsabilités de gouvernance

Les quatre questions à poser pour chaque acteur : qui décide, qui porte la responsabilité, qui exécute et qui contrôle ?

ACTEUR	DÉCIDE	RESPONSABLE	EXÉCUTE	CONTRÔLE
Comité directeur	orientations	arbitrage stratégique	—	résultats et priorités
Data Owner	usages et accès	qualité du domaine	valide les demandes métier	indicateurs et risques
Data Steward	—	définitions et règles métier	applique et documente	qualité et écarts
Data Custodian	—	contrôles techniques	administre et sécurise	journaux et alertes
IT, utilisateurs et experts	besoins et usages	fonctionnement opérationnel	développe, utilise et signale	anomalies et utilité

Sigles du comité directeur : CDO (*Chief Data Officer*), CIO (*Chief Information Officer*), CISO (*Chief Information Security Officer*), COO (*Chief Operating Officer*), CMO (*Chief Marketing Officer*) et CTO (*Chief Technology Officer*).

Élaboration du plan de gouvernance

Définition — **plan de gouvernance** : traduction de la stratégie de l'entreprise en actions coordonnées, attribuées et mesurables.

Le chemin de construction :

- 01 **Aligner** — relier la vision de l'entreprise aux priorités data.
- 02 **Cadrer** — fixer des objectifs mesurables et un périmètre.
- 03 **Prioriser** — arbitrer selon la valeur, le risque et l'effort.
- 04 **Planifier** — définir actions, moyens, échéances et indicateurs.
- 05 **Responsabiliser** — préciser qui décide, réalise et contrôle.

Une feuille de route relie :

- les objectifs de l'entreprise ;
- les actions prioritaires ;
- les responsabilités et les ressources ;
- les échéances et les indicateurs de suivi.

Principe : chaque étape doit produire une décision documentée et vérifiable.

Fiche action : traçabilité de la décision

Chaque action doit être suffisamment précise pour être réalisée, suivie et contrôlée.

CHAMP	QUESTION À RENSEIGNER
Objectif	Quel résultat est attendu ?
Périmètre	Quelles données sont concernées ?
Action	Quelle méthode et quelles étapes ?
Responsable	Qui décide et qui réalise ?
Échéance	Quelles ressources et dépendances ?
Indicateur	Quelle preuve et quel suivi ?

Validation et suivi des actions de gouvernance

Exemple d'action : réduire les doublons clients de 20 % en trois mois → dédoublonnage du CRM, **Data Owner** identifié, taux de doublons suivi chaque semaine.

Test de cohérence : chaque action répond-elle à un objectif, possède-t-elle un responsable et produit-elle une preuve mesurable ?

Livrable : une feuille de route partagée — objectifs → actions → responsabilités → échéances → indicateurs → points de décision.

Synthèse

Plan d'action de gouvernance

- **Appliquer l'alignement stratégique** : partir de la vision d'entreprise pour arriver au plan de gouvernance.
- **Se familiariser avec de nouvelles méthodes** : méthodes agiles, DMBOK et roue DAMA correspondent mieux au contexte numérique.
- **S'appuyer sur des outils adaptés** : ils facilitent le travail collectif, car la gouvernance des données n'est pas une mission solitaire.
- **Documenter le travail collectif** : mettre en place des procédures communes dans une charte de gouvernance.

Message clé : un plan de gouvernance transforme une ambition stratégique en décisions coordonnées et vérifiables.

CHAPITRE

Gouvernance, sécurité et valorisation des données

04

Sécurité juridique et technique des données

Proportionnalité des mesures de sécurité au niveau de risque

Principe de proportionnalité : le niveau de sécurité doit être adapté à la sensibilité des données, aux menaces et aux conséquences possibles d'un incident.

- Une sécurité trop faible expose l'entreprise à des pertes, des sanctions et une atteinte à sa réputation.
- Une sécurité excessive peut ralentir l'innovation et compliquer inutilement les usages.
- La politique de sécurité traduit donc un **choix de gouvernance** : quel niveau de risque l'entreprise accepte-t-elle ?

SITUATION	RÉPONSE ATTENDUE
Risque sous-estimé	renforcer les mesures
Risque correctement évalué	protéger de façon proportionnée
Risque surestimé	simplifier sans perdre la maîtrise

Idée clé : faire assez pour réduire le risque, mais pas plus que nécessaire.

Culture organisationnelle du risque

La culture du risque désigne la manière dont une organisation identifie, discute, accepte et traite les risques dans ses décisions.

- **Risque métier** : des données inexactes entraînent une mauvaise décision ou une mauvaise action.
- **Risque financier** : une erreur, une fraude ou une non-conformité peut provoquer des coûts et des sanctions.
- **Risque juridique** : un traitement de données peut contrevenir au RGPD ou à une autre obligation.
- **Risque d'image** : une fuite ou une indisponibilité peut altérer la confiance des clients et partenaires.

Question de gouvernance : quels risques l'entreprise accepte-t-elle, lesquels doit-elle réduire et qui décide ?

Sensibilité et criticité des données

La **sensibilité** dépend notamment de la nature des données, de leur contexte, des personnes concernées et des conséquences d'une divulgation, d'une modification ou d'une perte.

- secret des affaires et données stratégiques internes ;
- données personnelles à risque élevé ;
- données nécessaires à la continuité d'une activité critique.

Catégories particulières de données personnelles

- origine raciale ou ethnique ;
- opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale ;
- données génétiques ou biométriques ;
- données de santé, vie sexuelle ou orientation sexuelle.

Leur traitement est en principe interdit, sauf exceptions prévues par le RGPD. Une protection renforcée est donc nécessaire.

Graduation des mesures de sécurité

Grille pédagogique : les niveaux doivent être précisés selon le contexte et le référentiel de l'organisation.

BESOIN DE SÉCURITÉ	EXEMPLES DE DONNÉES	MESURES À COMBINER
Élémentaire	données peu sensibles et peu exposées	sauvegardes, mises à jour, comptes individuels
Modéré	données internes ou personnelles courantes	habilitations, journalisation, sensibilisation
Important	données stratégiques ou traitements à risque	chiffrement, cloisonnement, audits ciblés
Élevé	données critiques ou forte menace	analyse de risque approfondie, tests, supervision et plan de continuité

À retenir : la mesure pertinente n'est pas la plus lourde ; c'est celle qui réduit efficacement le risque identifié.

Méthode EBIOS Risk Manager pour l'analyse du risque numérique



Figure 18. Méthode EBIOS Risk Manager. * Réf. [9].

EBIOS Risk Manager est une méthode d'appréciation et de traitement du risque numérique publiée par l'ANSSI.

- 01 cadrer l'étude et le socle de sécurité ;
- 02 identifier les sources de risque ;
- 03 construire les scénarios stratégiques ;
- 04 construire les scénarios opérationnels ;
- 05 définir le traitement et le suivi du risque.

Finalité : relier les enjeux métier, les menaces et les mesures de sécurité dans une décision partagée.

De l'analyse du risque à la décision de sécurité

Une analyse de risque ne consiste pas seulement à produire une liste de menaces. Elle doit conduire à des décisions.

- **Identifier** les biens, les missions, les menaces et les événements redoutés ;
- **Évaluer** la vraisemblance et les impacts possibles ;
- **Choisir** les mesures techniques, organisationnelles et physiques ;
- **Accepter ou réduire** le risque résiduel, avec une responsabilité clairement attribuée ;
- **Suivre** l'évolution des risques et l'efficacité des mesures.

Homologation de sécurité : décision formelle, lorsqu'elle est requise, par laquelle l'autorité responsable accepte un niveau de risque résiduel pour un système donné.

Analyse d'impact relative à la protection des données (AIPD)

AIPD — Analyse d'impact relative à la protection des données : étude requise lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes.

- Elle concerne le traitement, pas uniquement l'outil informatique.
- Elle associe enjeux juridiques, organisationnels et techniques.
- Elle doit être réévaluée si le traitement ou le niveau de risque évolue.

Les trois volets à documenter

- 01 **Décrire** le traitement : finalités, données, personnes, durées et acteurs.
- 02 **Vérifier** la nécessité, la proportionnalité et le respect des droits.
- 03 **Traiter** les risques de sécurité et leurs impacts sur la vie privée.

Livrable : des mesures techniques et organisationnelles justifiées par les risques constatés.

Audit de la sécurité des systèmes d'information

AUDIT INTERNE

réalisé par l'organisation ;

mesure la maîtrise réelle et les écarts ;

aide à piloter l'amélioration ;

AUDIT EXTERNE

réalisé par un prestataire indépendant ;

apporte un regard extérieur et vérifie un périmètre défini ;

peut contribuer à démontrer la conformité.

Un audit doit permettre de :

- établir un état des lieux objectif ;
- vérifier l'adéquation des systèmes aux besoins métier ;
- identifier les vulnérabilités et les risques de disponibilité ;
- prioriser les actions correctives.

Attention : un audit décrit un état à un moment donné ; il doit être complété par un suivi régulier.

Tests d'intrusion et limites de l'évaluation de sécurité

Test d'intrusion (*Pen Test*) : évaluation autorisée qui cherche à identifier et, si nécessaire, à exploiter des vulnérabilités dans un périmètre défini.

- Il simule les actions possibles d'un attaquant.
- Il peut être réalisé depuis l'extérieur ou depuis l'intérieur du système.
- Le niveau d'information fourni à l'auditeur peut varier : boîte noire, grise ou blanche.
- Il doit être planifié, autorisé et encadré pour éviter les interruptions de service.

Limite : un test d'intrusion n'est pas exhaustif. Il complète les audits d'architecture, de configuration, de code et d'organisation.

Mesures techniques de sécurité de l'information

Sécurité de l'information : préserver la confidentialité, l'intégrité et la disponibilité des informations.

PROPRIÉTÉ	QUESTION À POSER
Confidentialité	Qui peut accéder à l'information ?
Intégrité	Comment détecter une modification non autorisée ?
Disponibilité	Comment maintenir ou rétablir l'accès ?

Exemples de mesures

- authentification robuste et gestion des comptes ;
- mises à jour, durcissement et sauvegardes ;
- chiffrement adapté aux données et aux échanges ;
- journalisation, supervision et détection ;
- tests réguliers et plan de reprise.

ISO/IEC 27001 définit les exigences d'un système de management de la sécurité de l'information fondé sur la gestion des risques. Réf. [11].

Mesures organisationnelles et physiques de sécurité

Mesures organisationnelles

- procédures et règles communes ;
- sensibilisation et formation ;
- séparation des responsabilités ;
- revues périodiques des droits ;
- gestion des incidents et des prestataires.

Cloisonnement et habilitations

- limiter l'accès aux seules données nécessaires à la mission ;
- séparer les environnements, les services et les niveaux de privilège ;
- protéger aussi les supports physiques : dossiers RH, armoires, bureaux et locaux ;
- réduire l'impact d'une compromission en évitant l'accès généralisé.

Principe du moindre privilège : chaque personne dispose uniquement des droits nécessaires à son activité.

Politique de sécurité des systèmes d'information (PSSI)

PSSI — Politique de sécurité des systèmes d'information : document de référence qui décrit les règles, responsabilités, mesures et procédures destinées à maintenir le niveau de sécurité attendu.

- préciser les données et systèmes concernés ;
- définir les rôles, les responsabilités et les habilitations ;
- formaliser les mesures techniques, organisationnelles et physiques ;
- prévoir la gestion des incidents, des sauvegardes et de la continuité ;
- organiser les contrôles, les audits et la mise à jour de la politique.

Une PSSI utile est vivante : elle est connue, appliquée, contrôlée et révisée lorsque les risques ou les systèmes évoluent.

Synthèse

Sécurité juridique et technique des données

- **Évaluer le risque** : partir de la sensibilité des données, des menaces et des impacts.
- **Proportionner les mesures** : protéger suffisamment sans créer de contraintes inutiles.
- **Analyser** : utiliser l'analyse de risque, EBIOS Risk Manager et, si nécessaire, une AIPD.
- **Vérifier** : compléter la politique par des audits et des tests encadrés.
- **Protéger** : combiner mesures techniques, organisationnelles et physiques.
- **Formaliser** : inscrire les règles, responsabilités et contrôles dans une PSSI.

Message clé : la sécurité est une décision de gouvernance fondée sur un risque évalué, traité et suivi.

Culture de sécurité et responsabilisation des collaborateurs

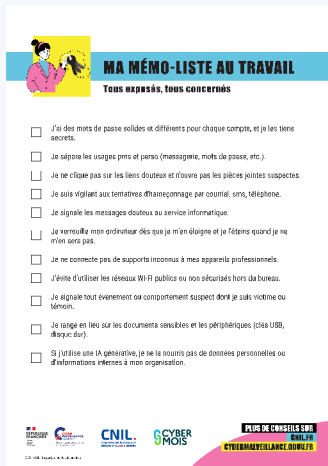


Figure 19. Mémo des cyber-réflexes au travail. * Réf. [10].

La sécurité est l'affaire de tous : chaque personne qui consulte, modifie, transporte ou partage une donnée contribue à la sécurité du système d'information.

- La direction fixe le niveau de risque acceptable et donne les moyens d'agir.
- La DSI et les équipes sécurité déploient les protections et accompagnent les utilisateurs.
- Chaque collaborateur applique les règles, reste vigilant et signale les événements suspects.

Objectif : faire de la sécurité une pratique quotidienne, et non une consigne ponctuelle.

Typologie des violations de données

Une violation de données est un incident qui compromet la confidentialité, l'intégrité ou la disponibilité des données.

TYPE D'INCIDENT	CE QUI SE PASSE	EXEMPLE DE SITUATION
Vol	Un accès non autorisé permet d'emporter des données.	Un ordinateur contenant des fichiers stratégiques est dérobé.
Fuite	Des données sont divulguées à des personnes non autorisées.	Un fichier de données personnelles est publié sur Internet.
Modification	Des données sont altérées sans autorisation.	Un compte utilisateur est modifié par un intrus.
Destruction	Des données sont supprimées ou rendues indisponibles.	Un fichier client est effacé sans sauvegarde exploitable.

Réflexe : qualifier l'incident selon la triade **confidentialité — intégrité — disponibilité** avant de choisir les mesures à prendre.

Réponse organisationnelle aux incidents de sécurité

La première réponse suit quatre actions :

- 01 **Détecter et contenir** : repérer la faille et limiter sa propagation.
- 02 **Qualifier** : identifier les données touchées, les personnes concernées et les conséquences possibles.
- 03 **Corriger** : supprimer la cause de l'incident et restaurer un fonctionnement sûr.
- 04 **Prévenir la récurrence** : renforcer les mesures et documenter le retour d'expérience.

Si des données personnelles sont concernées :

NIVEAU DE RISQUE	ACTION MINIMALE
Aucun risque	documenter l'incident dans le registre interne
Risque pour les personnes	documenter et notifier la CNIL dans les meilleurs délais, au plus tard sous 72 h
Risque élevé	notifier la CNIL et informer les personnes concernées rapidement

Le délai de 72 heures concerne les violations susceptibles d'engendrer un risque pour les droits et libertés. * Réf. [10].

Construction d'une culture interne de sécurité

La culture de sécurité désigne l'ensemble des connaissances, habitudes et comportements qui permettent de réduire les risques au quotidien.

- 01 **Observer les pratiques réelles** : faire décrire les habitudes de travail, y compris les pratiques informelles.
- 02 **Faire comprendre les menaces** : relier chaque règle à un risque concret pour l'entreprise et les personnes.
- 03 **Former et entraîner** : proposer des formats réguliers, courts et adaptés aux métiers.
- 04 **Mesurer et améliorer** : suivre les signalements, les exercices et les incidents sans culpabiliser les collaborateurs.

Une sensibilisation efficace cherche d'abord à améliorer les pratiques ; elle ne transforme pas l'erreur en faute individuelle.

Identification des pratiques à risque

Pratiques à rechercher lors des audits et des entretiens :

- copier des données professionnelles sur un espace personnel ;
- partager un document sans vérifier ses droits d'accès ;
- utiliser un outil non validé par l'entreprise ;
- conserver des données plus longtemps que nécessaire ;
- laisser un poste ou un support amovible sans surveillance.

Méthode d'entretien

- 01 Demander à la personne de décrire une journée de travail ordinaire.
- 02 Repérer les écarts entre la procédure et la pratique.
- 03 Évaluer le risque associé à chaque écart.
- 04 Co-construire une solution réaliste et vérifiable.

Principe pédagogique : parler des situations et des processus plutôt que rechercher un responsable à sanctionner.

Principales menaces de cybersécurité

MENACE	DÉFINITION COURTE	RÉFLEXE ATTENDU
Rançongiciel	logiciel malveillant qui chiffre les données et demande une rançon.	isoler le poste, alerter et ne pas improviser une restauration.
DDoS	attaque qui surcharge un service pour le rendre indisponible.	activer le dispositif de continuité et l'escalade prévue.
Hameçonnage (<i>phishing</i>)	message trompeur destiné à obtenir des informations ou provoquer une action.	vérifier l'expéditeur, le lien et le contexte avant d'agir.
Risque humain	perte, erreur ou divulgation liée à une pratique de travail.	protéger les supports et signaler rapidement toute anomalie.

À retenir : la vigilance humaine complète les protections techniques ; elle ne les remplace pas.

Accessibilité des bonnes pratiques de sécurité

Les règles doivent être simples, visibles et répétées :

- expliquer les données sensibles et les comportements attendus ;
- diffuser une charte, des fiches réflexes et un canal de signalement ;
- organiser des formations courtes et régulières ;
- utiliser des exercices ou simulations encadrés ;
- adapter les messages aux métiers et aux niveaux de responsabilité.

Un dispositif de sensibilisation doit répondre à trois questions :

- 01 Que dois-je protéger ?
- 02 Que dois-je faire dans une situation à risque ?
- 03 Qui dois-je prévenir et dans quel délai ?

L'ANSSI recommande des actions régulières, adaptées aux publics et portant notamment sur les informations sensibles, les règles de sécurité et le signalement des événements suspects. * Réf. [9].

Sécurisation des mots de passe et des accès

Un **mot de passe robuste** est long, difficile à deviner, unique pour un service et protégé contre la réutilisation.

- privilégier une phrase de passe ou un mot de passe généré par un gestionnaire ;
- utiliser un secret différent pour chaque service ;
- activer l'authentification multifacteur lorsqu'elle est disponible ;
- ne jamais communiquer un mot de passe ni le noter à la vue de tous ;
- changer immédiatement un mot de passe soupçonné d'être compromis.

Test rapide : parmi `1234abcd` , `Thomas04091989` et une phrase de passe aléatoire, le dernier choix est généralement le plus robuste — à condition de ne pas le réutiliser.

Protection des postes, des mises à jour et des usages

Sur le poste de travail

- verrouiller automatiquement la session après une courte période d'inactivité ;
- installer les mises à jour depuis les sources officielles ;
- limiter les supports amovibles et analyser les téléchargements ;
- sauvegarder les données selon les règles de l'entreprise.

Entre vie privée et vie professionnelle

- séparer les comptes, équipements et espaces de stockage ;
- ne pas utiliser un outil personnel pour traiter des données professionnelles ;
- informer les collaborateurs des règles d'utilisation et de contrôle ;
- prévoir une procédure claire en cas de perte, d'erreur ou de suspicion.

La sécurité doit protéger l'activité sans organiser une surveillance disproportionnée des salariés.

Synthèse

Sensibiliser l'entreprise aux mesures de sécurité

- **Partager la responsabilité** : la sécurité concerne la direction, les équipes techniques et chaque utilisateur.
- **Reconnaître les incidents** : vol, fuite, modification et destruction appellent une réaction structurée.
- **Réagir sans attendre** : contenir, qualifier, corriger et prévenir la récurrence.
- **Former régulièrement** : partir des pratiques réelles et des menaces rencontrées par les métiers.
- **Simplifier les réflexes** : mots de passe robustes, verrouillage, mises à jour, vigilance et signalement.

Message clé : une culture de sécurité transforme les règles écrites en comportements observables et réduit les risques avant qu'ils ne deviennent des incidents.

Droit contraignant et conformité juridique des traitements



Figure 20. Le cadre européen de protection des données. *
Réf. [12].

Le droit « dur » désigne les règles juridiquement contraignantes : lois, règlements, décrets et obligations sectorielles.

- Une politique interne ne peut pas remplacer une obligation légale.
- La conformité concerne les données, les traitements, les acteurs, les outils et les transferts.
- Le responsable doit pouvoir démontrer les mesures prises et les décisions documentées.

Méthode : identifier le texte applicable, vérifier son périmètre, documenter la conformité et organiser une veille.

État des lieux de la conformité

La conformité (*compliance*) est la capacité d'une organisation à respecter les règles qui s'appliquent à ses activités et à en apporter la preuve.

- Cartographier les traitements de données personnelles et les données sensibles.
- Identifier les responsables, sous-traitants, co-responsables et destinataires.
- Vérifier les finalités, les bases légales, les durées de conservation et les transferts.
- Contrôler les mesures de sécurité et les modalités d'exercice des droits.
- Classer les écarts selon leur gravité, leur urgence et leur impact.

Attention : le DPD (*Délégué à la protection des données*, ou **DPO** en anglais) accompagne et pilote la conformité lorsqu'il est désigné ; il ne porte pas seul la responsabilité juridique de l'organisation.

Rôles du DPD/DPO et des responsables de traitement

DPD / DPO — Délégué à la protection des données

- conseille l'organisation et les équipes ;
- sensibilise les collaborateurs ;
- contrôle la conformité et suit les actions correctives ;
- coopère avec l'autorité de contrôle ;
- tient un rôle indépendant dans l'exercice de ses missions.

À ne pas confondre

- Le **responsable du traitement** détermine les finalités et les moyens.
- Le **sous-traitant** traite les données pour le compte du responsable.
- La **CNIL** ou la **CNDP** contrôle la protection des données selon le pays concerné.

Le DPO est obligatoire dans certains cas prévus par le RGPD ; sa désignation n'est pas automatiquement exigée pour toute organisation. * Réf. [12].

Registre des activités de traitement

Le registre des activités de traitement est un document de pilotage qui décrit les traitements réalisés par l'organisation et les mesures qui les encadrent.

ÉLÉMENT À DOCUMENTER	QUESTION DE CONTRÔLE
Finalité	Pourquoi ces données sont-elles collectées ?
Données et personnes	Quelles catégories de données et de personnes sont concernées ?
Acteurs et destinataires	Qui traite, consulte ou reçoit les données ?
Base légale	Quel fondement autorise le traitement ?
Conservation	Combien de temps les données sont-elles gardées ?
Sécurité et transferts	Quelles protections et quels transferts sont prévus ?

Résultat attendu : une vision vérifiable des traitements, des responsabilités et des risques résiduels.

Audit de conformité : démarche en quatre étapes

- 01 **Segmenter l'organisation** : RH, finance, marketing, juridique, DSI, opérations...
- 02 **Interroger les relais métier** : données traitées, outils utilisés, accès, durées et destinataires.
- 03 **Formaliser les constats** : comptes rendus, zones d'ombre, écarts entre les procédures et les pratiques.
- 04 **Prioriser et agir** : registre, calendrier de mise en conformité, responsables et preuves attendues.

Bonne pratique : utiliser des entretiens courts et un questionnaire commun afin de comparer les traitements entre services.

Cadres juridiques européens applicables aux données

TEXTE	RÔLE PRINCIPAL
RGPD — règlement (UE) 2016/679	protection des personnes et encadrement des traitements de données personnelles.
Directive ePrivacy 2002/58/CE	confidentialité des communications électroniques et règles liées aux cookies, via les législations nationales.

TEXTE	RÔLE PRINCIPAL
Data Governance Act — règlement (UE) 2022/868	faciliter le partage et la réutilisation de certaines données dans un cadre de confiance.
Digital Services Act — règlement (UE) 2022/2065	responsabiliser les intermédiaires et plateformes en ligne.

Distinction essentielle : le RGPD protège les personnes et leurs données personnelles ; les autres textes répondent à des enjeux complémentaires. * Réf. [12].

Principes fondamentaux du RGPD

- **Licéité, loyauté et transparence** : informer et traiter sur une base juridique valable.
- **Finalité** : collecter pour des objectifs déterminés, explicites et légitimes.
- **Minimisation** : ne traiter que les données nécessaires.
- **Exactitude** : maintenir les données correctes et à jour.
- **Limitation de conservation** : supprimer ou anonymiser lorsque la conservation n'est plus justifiée.
- **Intégrité et confidentialité** : protéger les données par des mesures appropriées.
- **Responsabilité démontrée** : conserver les preuves des choix, contrôles et actions correctives.

Les personnes disposent notamment de droits d'information, d'accès, de rectification, d'effacement, de limitation, d'opposition et, selon les cas, de portabilité.

Cadre marocain de protection des données personnelles

Loi n° 09-08

La loi marocaine n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel constitue le cadre général national.

- Elle définit les données personnelles, les traitements et les données sensibles.
- Elle impose des principes de finalité, proportionnalité, qualité, conservation et sécurité.
- Elle garantit des droits aux personnes concernées.

CNDP — Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel

- contrôle et accompagne la conformité ;
- reçoit les déclarations et demandes d'autorisation ;
- intervient notamment pour les données sensibles, les interconnexions et certains transferts à l'étranger.

Le décret n° 2-09-165 précise l'application de la loi n° 09-08. * Réf. [13].

Comparaison des obligations européennes et marocaines

SUJET	UNION EUROPÉENNE	MAROC
Texte central	RGPD — règlement (UE) 2016/679	Loi n° 09-08 et décret n° 2-09-165
Autorité	Autorité nationale de contrôle, par exemple la CNIL en France	CNDP
Pilotage	responsable du traitement, sous-traitant et DPO dans certains cas	responsable du traitement, sous-traitant et représentant lorsque prévu
Formalités	registre et obligations de conformité ; formalités variables selon les traitements	déclaration ou autorisation auprès de la CNDP selon le traitement
Transferts	encadrés par le RGPD et les garanties appropriées	demande de transfert à l'étranger selon les règles de la CNDP

À retenir : la loi n° 09-08 est l'équivalent fonctionnel marocain du cadre général de protection des données personnelles, mais les procédures et les obligations ne sont pas identiques au RGPD. * Réf. [13].

Articulation entre conformité, secteur et territoire

Avant de traiter une donnée, posez quatre questions :

- 01 **Quelle donnée ?** personnelle, sensible, publique, stratégique ou sectorielle ?
- 02 **Quelle finalité ?** paie, santé, prospection, service public, sécurité, recherche...
- 03 **Quel territoire ?** Maroc, Union européenne, autre pays ou transfert international ?
- 04 **Quel texte complémentaire ?** droit du travail, santé, finance, télécommunications, archivage, cybersécurité...

Le RGPD ou la loi n° 09-08 donnent le cadre général ; un texte sectoriel peut ajouter des obligations spécifiques.

Synthèse

Respecter le droit applicable aux données

- **Commencer par un audit** : cartographier les traitements, les acteurs, les finalités et les écarts.
- **Documenter** : tenir le registre et conserver les preuves de conformité.
- **Responsabiliser** : clarifier le rôle du DPO, du responsable du traitement et du sous-traitant.
- **Appliquer le bon texte** : distinguer RGPD, ePrivacy, DGA, DSA et règles sectorielles.
- **Adapter au pays** : au Maroc, appliquer la loi n° 09-08 sous le contrôle de la CNDP.
- **Assurer une veille** : les textes, décisions et recommandations évoluent.

Message clé : la conformité n'est pas une formalité finale ; c'est une démarche continue de décision, de preuve et d'amélioration.

Droit souple et gouvernance des données

Le droit « souple » regroupe des recommandations, référentiels, lignes directrices, chartes et normes qui ne sont pas toujours juridiquement contraignants, mais qui orientent les pratiques et facilitent la conformité.

- Il aide à interpréter et appliquer les obligations.
- Il fournit des méthodes et des preuves de bonne pratique.
- Il permet d'adapter la règle au contexte métier et au niveau de risque.

Droit dur / droit souple

DROIT DUR	DROIT SOUPLE
impose une obligation ;	recommande une méthode ;
prévoit parfois une sanction ;	aide à démontrer une démarche sérieuse ;
fixe un cadre minimal ;	précise comment atteindre ce cadre.

Principe : le droit souple ne permet pas d'écarter une obligation légale ; il aide à la mettre en œuvre.

Protection des données dès la conception (Privacy by design)

Privacy by design signifie « protection des données dès la conception » : les exigences de vie privée et de sécurité sont prises en compte dès le cadrage d'un produit ou d'un service.

- associer le DPO, les métiers, les architectes et les développeurs dès le début ;
- limiter les données collectées aux besoins réels du projet ;
- choisir une architecture et des paramètres par défaut protecteurs ;
- prévoir les droits, la conservation, la sécurité et les preuves dans les spécifications ;
- réaliser une AIPD lorsque le traitement est susceptible d'engendrer un risque élevé.

Bénéfice : corriger une décision de conception en amont coûte généralement moins cher que corriger un système déjà déployé. * Réf. [10].

Accountability et démonstration de la conformité

Accountability signifie que l'organisation doit respecter les principes de protection des données et être capable de démontrer ce respect.

- identifier les risques et les choix effectués ;
- formaliser les règles, responsabilités et procédures ;
- conserver les preuves de contrôle et de décision ;
- réévaluer les mesures lorsque le traitement évolue.

Documents utiles

- registre des activités de traitement ;
- politique de confidentialité ;
- contrats et instructions aux sous-traitants ;
- analyse d'impact relative à la protection des données ;
- procédures d'exercice des droits et de gestion des violations.

L'accountability transforme la conformité en système de pilotage documenté. * Réf. [10].

Droit et conception des produits data

Le raisonnement juridique intervient avant la décision technique, afin d'éclairer les options plutôt que de valider un projet terminé.

- 01 Décrire la finalité et les données réellement nécessaires.
- 02 Comparer plusieurs architectures et scénarios d'usage.
- 03 Évaluer les obligations, les risques et les coûts associés.
- 04 Choisir une solution proportionnée et documenter le raisonnement.

Exemple : pour une application de santé en phase de prototype, ne pas collecter de données de santé tant qu'elles ne sont pas nécessaires peut éviter un traitement prématuré et réduire les contraintes d'hébergement et de sécurité.

Co-construction juridique et métier

Le DPO accompagne le produit

- il propose des alternatives conformes ;
- il aide à arbitrer entre valeur, risque et effort ;
- il traduit les exigences juridiques en critères compréhensibles ;
- il vérifie que les décisions prises restent documentées.

Questions à poser en atelier

- Cette donnée est-elle indispensable à la finalité ?
- Peut-on obtenir le même résultat avec moins de données ?
- Qui doit y accéder et pendant combien de temps ?
- Quelle mesure protège les personnes et l'activité ?
- Quelle preuve conserver pour expliquer le choix ?

La conformité devient ainsi un critère de conception, au même titre que la sécurité, le coût ou l'expérience utilisateur.

Clarification des idées reçues sur le RGPD

IDÉE REÇUE	RÉALITÉ À RETENIR
« Le RGPD empêche de traiter des données. »	Il encadre les traitements et impose de respecter des principes, des droits et une base légale.
« Il faut toujours demander le consentement. »	Le consentement est l'une des six bases légales ; le contrat, l'obligation légale, la mission d'intérêt public, l'intérêt vital et l'intérêt légitime peuvent aussi s'appliquer selon le cas.
« La conformité est une validation finale. »	Elle se construit dès la conception, puis se vérifie et se met à jour pendant tout le cycle de vie.
« Une fois le traitement déclaré, tout est réglé. »	L'organisation doit continuer à informer, sécuriser, documenter et respecter les droits.

La base légale doit être choisie avant le traitement et adaptée à sa finalité ; le consentement ne prévaut pas automatiquement sur les autres bases. * Réf. [10].

Durée de conservation et justification du choix

La **durée de conservation** doit correspondre à la finalité du traitement et aux obligations applicables.

- vérifier s'il existe une durée légale ou sectorielle ;
- distinguer base active, archivage intermédiaire et suppression ;
- limiter la conservation lorsque la finalité est atteinte ;
- anonymiser lorsque la conservation statistique est nécessaire ;
- documenter le raisonnement et prévoir une revue périodique.

SITUATION	DÉCISION À DOCUMENTER
durée imposée par un texte	appliquer la durée et sa justification ;
aucune durée imposée	définir une durée proportionnée à la finalité et au risque ;
besoin historique ou statistique	anonymiser ou archiver selon les conditions applicables.

Il n'existe pas une durée universelle valable pour toutes les données : le choix doit être cohérent, proportionné et révisable.

Synthèse

Utiliser le droit souple comme outil de gouvernance

- **Comprendre la complémentarité** : le droit dur fixe les obligations ; le droit souple aide à les appliquer.
- **Concevoir en amont** : intégrer la protection de la vie privée et la sécurité dès le projet.
- **Démontrer** : appliquer l'accountability par des règles, des preuves et des contrôles.
- **Co-construire** : faire travailler ensemble DPO, métiers, équipes techniques et direction.
- **Éviter les automatismes** : choisir la base légale, l'architecture et la durée de conservation au cas par cas.

Message clé : le droit devient un levier de décision lorsqu'il est mobilisé assez tôt pour orienter le produit, réduire le risque et créer de la confiance.

CHAPITRE

Gouvernance, sécurité et valorisation des données

05

Évaluation de la performance et valorisation des données

Objectifs, indicateurs et tableaux de bord de performance



Illustration pédagogique. Un tableau de bord rend les résultats visibles et discutables.

Évaluer une gouvernance des données consiste à vérifier si les actions engagées produisent les effets attendus pour l'organisation.

- partir des objectifs définis dans le plan de gouvernance ;
- traduire ces objectifs en résultats observables ;
- choisir des indicateurs fiables et utiles à la décision ;
- suivre les résultats à une fréquence adaptée ;
- interpréter les écarts avant d'engager une action corrective.

Question directrice : les mesures de gouvernance améliorent-elles réellement la qualité, la maîtrise et la valeur des données ?

Traduction des objectifs stratégiques en cibles mesurables

Un objectif général doit être reformulé pour devenir **spécifique, mesurable, daté et interprétable**.

FORMULATION GÉNÉRALE	CIBLE MESURABLE
Réduire les coûts d'un service	réduire les coûts de 10 % d'ici la fin du semestre
Augmenter le nombre de clients	augmenter le nombre de clients de 20 % sur l'exercice
Accélérer une activité	réduire le délai de traitement de deux semaines à une semaine
Améliorer la qualité du service	atteindre un taux de satisfaction de 90 % selon une méthode définie

Principe : un indicateur n'a de sens que par rapport à une cible, une période et une méthode de calcul explicites.

Distinguer mise en œuvre et efficacité

Indicateurs de mise en œuvre

Ils vérifient que les actions prévues ont effectivement été réalisées.

- référentiel déployé ;
- règles documentées ;
- collaborateurs formés ;
- contrôles activés ;
- responsables désignés.

Indicateurs d'efficacité

Ils vérifient que les actions produisent les résultats attendus.

- baisse du taux de doublons ;
- réduction du délai de traitement ;
- amélioration de la qualité ;
- diminution des incidents ;
- augmentation de la satisfaction des utilisateurs.

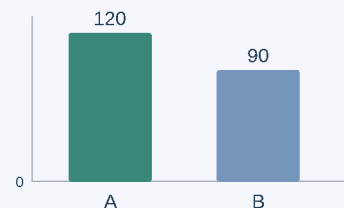
Attention : une action peut être complètement déployée sans atteindre son objectif d'efficacité.

Structurer les indicateurs clés de performance

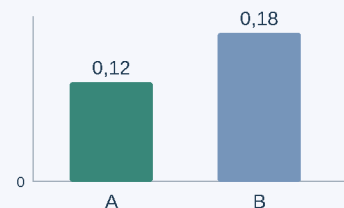
KPI signifie *Key Performance Indicator*, ou **indicateur clé de performance**. Il s'agit d'une mesure définie avant l'action afin d'en suivre l'avancement et les effets.

- **Productivité** : ressources mobilisées et opérations réalisées dans un délai donné.
- **Qualité** : conformité, exactitude, complétude et respect des règles.
- **Capacité** : volumes traités, stockés, supprimés ou rendus accessibles.
- **Stratégie** : contribution des actions aux objectifs de l'organisation.

Énergie sur la journée (kWh)



Énergie / surface (kWh/m²)



Lecture critique : un indicateur global peut conduire à une conclusion différente d'un indicateur rapporté à une unité pertinente.

Concevoir un tableau de bord utile à la décision

Un tableau de bord ne juxtapose pas des chiffres : il organise des informations nécessaires à une décision.

- afficher la définition, la source, l'unité et la cible de chaque indicateur ;
- préciser le responsable de la collecte et de l'interprétation ;
- distinguer les tendances, les seuils d'alerte et les écarts à la cible ;
- relier chaque écart à une action ou à un point de décision ;
- limiter le nombre d'indicateurs aux mesures réellement utiles.

Fiche minimale d'un KPI : nom, définition, formule, source, fréquence, responsable, cible, seuil d'alerte et décision associée.

Adapter la fréquence de suivi à l'horizon de l'objectif

HORIZON DE L'OBJECTIF	FRÉQUENCE POSSIBLE
incident ou activité critique	suivi continu ou quotidien
action opérationnelle	suivi hebdomadaire ou mensuel
amélioration de qualité	suivi mensuel ou trimestriel
objectif stratégique	revue trimestrielle ou semestrielle

- mesurer trop tôt un objectif de long terme peut produire une fausse alerte ;
- mesurer trop tard une activité critique retarde la réaction ;
- la fréquence doit être révisée si le contexte, le risque ou le processus change ;
- le tableau de bord doit rendre visibles les évolutions, pas seulement une valeur isolée.

Règle de méthode : la fréquence de suivi doit être cohérente avec la vitesse de variation du phénomène observé.

Interpréter les résultats dans leur contexte

Un écart entre une cible et un résultat ne signifie pas automatiquement que la gouvernance a échoué.

- conjoncture économique et évolution de la demande ;
- crise internationale ou événement exceptionnel ;
- évolution réglementaire ou sectorielle ;
- transformation de l'organisation, des outils ou des processus ;
- modification de la qualité ou de la disponibilité des données sources.

Démarche d'analyse : observer l'écart, rechercher les facteurs internes et externes, puis décider s'il faut corriger l'action, la cible, la mesure ou le calendrier.

Synthèse

Évaluer la performance d'une gouvernance des données

- **Partir des objectifs** : transformer les orientations stratégiques en cibles mesurables.
- **Distinguer les résultats** : séparer mise en œuvre des actions et efficacité obtenue.
- **Choisir les bons KPI** : mesurer la productivité, la qualité, la capacité et la contribution stratégique.
- **Organiser le suivi** : documenter les indicateurs dans un tableau de bord et adapter la fréquence.
- **Interpréter avec prudence** : tenir compte des facteurs externes avant de modifier un plan d'action.

Message clé : une mesure n'est utile que si elle éclaire une décision et permet d'améliorer la gouvernance.

Amélioration de la qualité des données : dimensions et confiance collective



Figure 21. La qualité des données comme condition de confiance. * Réf. [6].

La qualité des données désigne leur aptitude à répondre aux usages et aux objectifs de l'organisation, selon des critères explicites et vérifiables.

- elle se définit par rapport à une finalité et à un contexte ;
- elle concerne toute la chaîne de vie des données ;
- elle constitue un objectif central de la gouvernance ;
- elle conditionne la fiabilité des analyses et des décisions.

Question directrice : quelles propriétés une donnée doit-elle posséder pour être utilisable, fiable et utile ?

Dimensions de la qualité des données : actualité et maîtrise

- **Actualité** : la donnée est suffisamment fraîche et mise à jour pour l'usage prévu.
- **Sécurité** : elle est protégée par des mesures adaptées à sa sensibilité et à son risque.
- **Conformité** : sa collecte, son utilisation et sa conservation respectent les règles applicables.
- **Traçabilité** : son origine, ses transformations, ses accès et ses usages peuvent être reconstitués.

Règle de gouvernance

- 01 définir la propriété attendue ;
- 02 préciser le seuil acceptable ;
- 03 identifier la source et le responsable ;
- 04 contrôler régulièrement la propriété.

Une règle de qualité utile est formulée de manière observable : elle permet de constater un écart et de décider d'une action corrective.

Dimensions de la qualité des données : intégrité et utilité

- **Intégrité** : la donnée est fiable et n'a pas été altérée de manière non autorisée.
- **Disponibilité** : elle est classée, accessible et disponible au moment du besoin.
- **Cohérence** : elle repose sur une définition, un référentiel et une nomenclature communs.
- **Complétude et précision** : elle contient les informations nécessaires avec le niveau d'exactitude attendu.

Une qualité dépendante de l'usage

La même donnée peut être suffisamment précise pour un tableau de bord exploratoire et insuffisante pour une décision réglementaire.

- expliciter le niveau de précision requis ;
- distinguer donnée manquante et donnée non applicable ;
- définir les règles de contrôle par domaine métier ;
- documenter les exceptions acceptées.

Définir les règles de qualité selon la stratégie de l'organisation

Les critères de qualité ne sont pas uniquement techniques : ils traduisent les priorités, les risques et les engagements de l'organisation.

- **Référentiel commun** : une même donnée doit conserver la même signification dans les différents systèmes.
- **Responsabilité** : chaque règle doit être associée à un responsable de la qualité et à un processus de correction.
- **Priorisation** : les contrôles portent d'abord sur les données critiques pour l'activité, les personnes ou la conformité.
- **Traçabilité** : les définitions, seuils, contrôles et corrections doivent être documentés.
- **Sobriété numérique** : l'usage de la donnée doit aussi tenir compte de la consommation de stockage, de calcul et d'énergie.

Une donnée peut donc être « de qualité » pour une organisation si elle respecte ses critères métier, juridiques, techniques et environnementaux.

Relier qualité des données et confiance collective

Données de faible qualité

- décisions fondées sur des informations inexacts ou obsolètes ;
- temps consacré à rechercher, corriger et retraiter les données ;
- baisse de productivité et augmentation des coûts ;
- risques pour la réputation, la conformité et les revenus.

Données de qualité

- décisions plus rapides et mieux justifiées ;
- coopération facilitée entre les métiers ;
- anticipation des situations et réduction des risques ;
- identification d'opportunités et création de valeur.

Confiance collective : chaque équipe peut utiliser les mêmes données avec une compréhension partagée de leur sens, de leur qualité et de leurs limites.

Organiser l'amélioration continue de la qualité

- 01 **Définir** les dimensions et les règles de qualité pour chaque domaine.
- 02 **Mesurer** les écarts avec des indicateurs documentés.
- 03 **Diagnostiquer** les causes : source, saisie, transformation, référentiel ou processus.
- 04 **Corriger** les données et, si nécessaire, le processus qui produit l'erreur.
- 05 **Prévenir** la réapparition par des contrôles, une formation et une responsabilisation adaptées.

La qualité ne se résume pas à nettoyer ponctuellement une base : elle se construit dans les processus et se maintient dans la durée.

Synthèse

Améliorer la qualité des données

- **Définir les critères** : actualité, sécurité, conformité, traçabilité, intégrité, disponibilité, cohérence, complétude et précision.
- **Contextualiser la qualité** : les exigences dépendent de la finalité, du métier et du risque.
- **Responsabiliser** : associer chaque règle à une source, un responsable, un seuil et une action corrective.
- **Créer la confiance** : des données fiables réduisent les coûts, les erreurs et les décisions risquées.
- **Améliorer en continu** : mesurer les écarts, traiter les causes et prévenir leur réapparition.

Message clé : la qualité des données n'est pas une propriété acquise une fois pour toutes ; c'est un résultat collectif de la gouvernance.

Création de valeur par la gouvernance des données

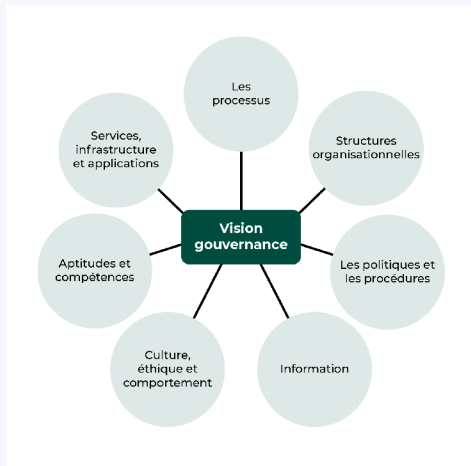


Illustration. La gouvernance relie la stratégie, l'organisation et les usages des données.

La valeur des données ne se limite pas à leur vente : elle correspond à leur contribution aux décisions, aux performances et à la maîtrise des risques.

- réduire les pertes et les coûts liés aux données mal maîtrisées ;
- renforcer la confiance dans les outils et les informations ;
- améliorer la productivité des équipes ;
- anticiper les problèmes et les opportunités ;
- orienter les actions vers les objectifs de l'organisation.

Question directrice : comment transformer une donnée gouvernée en bénéfice observable pour l'organisation ?

Distinguer valeur préservée et valeur créée

Valeur préservée

La gouvernance évite des pertes qui seraient difficiles à voir directement dans les comptes.

- temps perdu à rechercher ou corriger les données ;
- décisions erronées dues à une information de faible qualité ;
- coûts de réparation après un incident de sécurité ;
- risques de non-conformité et d'atteinte à la réputation.

Valeur créée

La gouvernance permet de produire de nouveaux bénéfices à partir de données fiables et accessibles.

- confiance des équipes dans les données ;
- gains de productivité et réduction des délais ;
- anticipation des situations et des besoins ;
- nouvelles opportunités et amélioration du service.

Les deux dimensions sont liées : prévenir une perte libère des ressources pour créer davantage de valeur.

Transformer les données en indicateurs de valeur

Une donnée devient utile à la décision lorsqu'elle est contextualisée, comparée et reliée à un objectif.

- 01 **Donnée** : une mesure, un événement ou une observation.
- 02 **Indicateur** : une donnée calculée selon une définition et une méthode explicites.
- 03 **Interprétation** : une comparaison avec une cible, une période ou une référence.
- 04 **Décision** : une action décidée à partir de l'information interprétée.
- 05 **Valeur** : un gain, un risque évité ou une capacité d'anticipation observable.

Exemple : le taux d'ouverture d'une newsletter devient une information de valeur lorsqu'il permet d'ajuster le contenu, le jour d'envoi ou la segmentation.

Inscrire la gouvernance dans une boucle d'amélioration

- 01 définir un objectif et une action ;
- 02 mesurer les résultats ;
- 03 analyser les écarts et les effets inattendus ;
- 04 réorienter l'action ou en lancer une nouvelle ;
- 05 vérifier à nouveau la valeur obtenue.

Une gouvernance n'est jamais figée

- une méthode peut produire moins d'effets que prévu ;
- une action peut révéler un nouveau problème ;
- un résultat peut ouvrir une nouvelle opportunité ;
- le plan doit évoluer avec les usages et le contexte.

Principe d'apprentissage : une action imparfaite devient utile si elle produit une information permettant d'améliorer la suivante.

Exploiter la sérendipité dans l'analyse des données

La sérendipité désigne la découverte d'un résultat inattendu alors que l'on cherchait autre chose.

- une analyse peut faire apparaître une corrélation non anticipée ;
- un indicateur peut révéler une cause différente de celle supposée ;
- un usage secondaire peut devenir un nouveau cas d'usage ;
- ces découvertes doivent être vérifiées avant de guider une décision.

La sérendipité n'est pas l'absence de méthode : elle suppose des données accessibles, une qualité suffisante et une capacité à examiner les résultats inattendus.

Anticiper les évolutions par l'analyse prédictive

L'analyse prédictive exploite des données historiques pour identifier des tendances, des profils ou des événements susceptibles de se produire.

- projeter une évolution à partir de séries temporelles ;
- repérer des comportements ou des situations récurrentes ;
- comparer plusieurs scénarios ;
- réduire l'incertitude avant une décision.

Exemple : planifier une newsletter

- observer l'évolution du taux d'ouverture pendant six mois ;
- identifier une performance supérieure le mardi ;
- tester cette hypothèse sur une période définie ;
- ajuster le calendrier si l'effet est confirmé.

Plus les données sont fiables, contextualisées et représentatives, plus l'anticipation peut être pertinente — sans devenir une certitude.

Encadrer le profilage et les usages prédictifs

Les analyses prédictives peuvent conduire à établir des profils ou à prendre des décisions concernant des personnes : elles doivent donc être encadrées.

- définir clairement la finalité et les données utilisées ;
- vérifier la qualité, la représentativité et les biais possibles ;
- informer les personnes lorsque le traitement l'exige ;
- distinguer anonymisation et pseudonymisation ;
- évaluer les risques pour les droits et libertés ;
- prévoir une intervention humaine lorsque la décision automatisée peut produire des effets importants.

Règle de prudence : une prédiction est un résultat probabiliste à discuter, pas une vérité automatique ni une justification suffisante à elle seule.

Synthèse

Créer de la valeur par une gouvernance des données

- **Préserver la valeur** : réduire les coûts, les erreurs, les incidents et les risques de non-conformité.
- **Créer de la valeur** : améliorer la productivité, la confiance, l'anticipation et les services.
- **Transformer** : relier données, indicateurs, interprétation et décision.
- **Apprendre** : utiliser les écarts et les découvertes inattendues pour réorienter les actions.
- **Anticiper avec prudence** : exploiter l'analyse prédictive tout en encadrant le profilage et les biais.

Message clé : la valeur des données apparaît lorsque la gouvernance permet de mieux décider, d'apprendre plus vite et d'agir avec moins de risques.

Communication et valorisation des résultats de la gouvernance

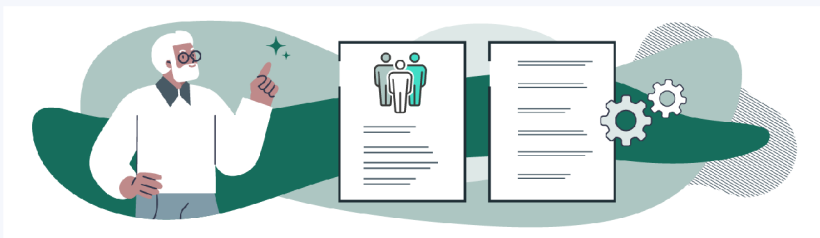


Figure 22. Communiquer pour rendre la valeur des données visible. * Réf. [6].

La communication des résultats permet de rendre les effets de la gouvernance compréhensibles, discutables et utiles à l'action.

- interpréter les résultats avec les personnes qui utilisent les données ;
- expliquer les raisons, la méthode et les limites des actions menées ;
- valoriser les progrès sans masquer les difficultés ;
- maintenir l'engagement des équipes dans la durée.

Question directrice : comment transformer un résultat mesuré en compréhension partagée et en mobilisation collective ?

Interpréter collectivement les résultats

La comitologie désigne l'organisation de décisions et de discussions au sein de comités réunissant plusieurs parties prenantes.

- les équipes métier apportent la connaissance du terrain et des usages ;
- les équipes techniques expliquent les sources, les traitements et les limites ;
- la gouvernance met les résultats en relation avec les objectifs et les risques ;
- la direction arbitre les priorités et les moyens lorsque cela est nécessaire.

Principe : la personne qui produit un indicateur n'est pas nécessairement celle qui peut le mieux en interpréter les causes ou les conséquences.

Organiser la communication interne

Objectifs

- expliquer pourquoi le plan de gouvernance a été lancé ;
- montrer les effets obtenus et les écarts persistants ;
- solliciter les retours des utilisateurs ;
- renforcer l'appropriation des règles et des outils.

Formats mobilisables

- ateliers thématiques et revues de résultats ;
- questions adressées aux référents métier ;
- présentations structurées et tableaux de bord ;
- espace partagé, lettre interne ou réunion d'équipe ;
- temps ouvert de discussion et de retour d'expérience.

La communication interne ne sert pas seulement à informer : elle permet aussi de corriger l'analyse et d'améliorer le plan d'action.

Concevoir des restitutions claires et responsables

Sur la forme

- sélectionner les indicateurs utiles au public visé ;
- privilégier les graphiques, schémas et comparaisons lisibles ;
- présenter une information à la fois et expliciter les unités ;
- rendre visibles la cible, l'écart et la tendance.

Sur le fond

- rappeler le problème et l'objectif poursuivi ;
- décrire la méthode et les sources utilisées ;
- distinguer faits, interprétations et hypothèses ;
- présenter les limites sans mettre en difficulté les personnes ;
- conclure par les décisions et les prochaines actions.

Valoriser les résultats auprès des parties prenantes

Communication externe

- publier des résultats vérifiables et compréhensibles ;
- montrer les bénéfices pour les clients, partenaires et usagers ;
- partager les progrès en matière de qualité, de sécurité ou de conformité ;
- adapter le niveau de détail aux publics concernés.

Exemples de résultats valorisables

- amélioration du taux d'ouverture d'une campagne ;
- réduction des doublons ou des données erronées ;
- diminution des incidents et des risques ;
- amélioration de la conformité ;
- meilleure protection des données des clients.

Communiquer sur la valeur suppose de respecter la confidentialité, de vérifier les chiffres et de ne pas exagérer les conclusions.

Formaliser un plan de communication des résultats

Un plan de communication complète le plan de gouvernance et précise les conditions de diffusion des résultats.

- 01 **Quoi ?** message, résultat, méthode et niveau de preuve.
- 02 **À qui ?** direction, métiers, équipes techniques, clients, partenaires ou public.
- 03 **Où ?** réunion, atelier, tableau de bord, intranet, newsletter, événement ou réseau professionnel.
- 04 **Comment ?** format, vocabulaire, visualisation et niveau de détail.
- 05 **Quand ?** calendrier, fréquence, moment de décision et suivi.

Fiche minimale : public cible, objectif de communication, message clé, canal, responsable, calendrier, indicateur de portée et modalité de retour.

Synthèse

Communiquer pour valoriser la gouvernance des données

- **Interpréter ensemble** : associer les métiers, les équipes techniques et la gouvernance.
- **Informier régulièrement** : rappeler les objectifs, la méthode, les résultats et les limites.
- **Soigner les restitutions** : rendre les données lisibles, utiles et honnêtes.
- **Valoriser les progrès** : montrer les bénéfices obtenus pour l'organisation et ses parties prenantes.
- **Planifier la communication** : répondre à quoi, à qui, où, comment et quand communiquer.

Message clé : une action de gouvernance produit davantage de valeur lorsqu'elle est comprise, discutée et rendue visible.

06

Consolider les acquis de la séance

Synthèse globale de la séance

De la donnée dispersée à la valeur maîtrisée

ÉTAPE	QUESTION DIRECTRICE	RÉSULTAT ATTENDU
Gouverner	Qui décide, selon quelles règles et avec quels objectifs ?	Une stratégie et un plan d'action partagés
Sécuriser	Quels risques devons-nous réduire et quelles obligations respecter ?	Des mesures proportionnées, documentées et appliquées
Évaluer	Comment savons-nous que la gouvernance produit des effets ?	Des indicateurs, des preuves et des décisions d'amélioration

Idee centrale : la gouvernance des données n'est ni un simple outil ni une action ponctuelle. C'est un système de pilotage qui relie stratégie, responsabilités, qualité, sécurité et création de valeur.

Synthèse globale — démarche à retenir

Une boucle de pilotage

- 01 **Cartographier** les données, leurs sources, leurs usages et leur cycle de vie.
- 02 **Prioriser** les données selon leur valeur, leur sensibilité, leur qualité et leur risque.
- 03 **Responsabiliser** les acteurs : décideurs, responsables, exécutants et contrôleurs.
- 04 **Formaliser** les règles, les procédures, les mesures de sécurité et les preuves de conformité.

Des résultats à rendre visibles

- 01 **Mesurer** la qualité, la conformité, la sécurité, l'usage et la valeur créée.
- 02 **Interpréter** les résultats avec les métiers et les équipes techniques.
- 03 **Communiquer** les progrès, les limites et les décisions à prendre.
- 04 **Améliorer** en continu le plan de gouvernance.

À retenir : une donnée utile est une donnée définie, fiable, accessible, protégée et utilisée dans un cadre clair.

Références

- 01 20 Minutes — estimation des données exposées en 2021.
- 02 WordStream — estimation du volume de tweets.
- 03 YoomWeb — estimation d’usage de TikTok.
- 04 Wikimedia Commons — salle de serveurs (CC BY-SA 3.0) et compte financier de l’Érechthéion (CC BY 4.0).
- 05 NOAA Climate.gov — stations météorologiques télégraphiques de 1849.
- 06 OpenClassrooms — illustrations des figures 4 à 7, 9 à 10, 12 à 16 et 21 à 22.
- 07 Metis Strategy — modèle de collaboration des acteurs de la gouvernance.
- 08 Visual Capitalist — ordres de grandeur historiques et estimations de 2021.
- 09 ANSSI — EBIOS Risk Manager, sensibilisation et bonnes pratiques de sécurité.
- 10 CNIL — AIPD, violations, anonymisation, accountability, bases légales et privacy by design.
- 11 ISO — exigences de l’ISO/IEC 27001 pour les systèmes de management de la sécurité de l’information.
- 12 Union européenne — EUR-Lex — RGPD, ePrivacy, Data Governance Act et Digital Services Act.
- 13 CNDP Maroc — loi n° 09-08, décret d’application et obligations nationales.